mPulse mobile

ORIGINAL

PROPOSAL PREPARED BY:

mPulse Mobile, Inc.

PROPOSAL PREPARED FOR:

Nebraska Department of Health and Human Services – RFP 6111 Z1

NEBRASKA

Good Life. Great Mission.

DEPT. OF HEALTH AND HUMAN SERVICES

Prepared by

mPulse Mobile
Jeremy Watson
Sr. Director, Healthcare Solutions
Jeremy.Watson@mpulsemobile.co

mpulsemobile.com

July 31, 2019

REQUEST FOR PROPOSAL FOR CONTRACTUAL SERVICES FORM

Request for Proposal Number: 6111 Z1

BIDDER MUST COMPLETE THE FOLLOWING

By signing this Request for Proposal for Contractual Services form, the bidder guarantees compliance with the procedures stated in this Request for Proposal, and agrees to the terms and conditions unless otherwise indicated in writing and certifies that bidder maintains a drug free work place.

Per Nebraska's Transparency in Government Procurement Act, Neb. Rev Stat § 73-603 DAS is required to collect statistical information regarding the number of contracts awarded to Nebraska Contractors. This information is for statistical purposes only and will not be considered for contract award purposes.

_____ NEBRASKA CONTRACTOR AFFIDAVIT: Bidder hereby attests that bidder is a Nebraska Contractor. "Nebraska Contractor" shall mean any bidder who has maintained a bona fide place of business and at least one employee within this state for at least the six (6) months immediately preceding the posting date of this RFP.

______I hereby certify that I am a Resident disabled veteran or business located in a designated enterprise zone in accordance with Neb. Rev. Stat. § 73-107 and wish to have preference, if applicable, considered in the award of this contract.

_____ I hereby certify that I am a blind person licensed by the Commission for the Blind & Visually Impaired in accordance with Neb. Rev. Stat. §71-8611 and wish to have preference considered in the award of this contract.

FORM MUST BE SIGNED USING AN INDELIBLE METHOD (NOT ELECTRONICALLY)

FIRM:	**mPulse Mobile, Inc.**
COMPLETE ADDRESS:	**16530 Ventura Blvd., Suite 500** **Encino, CA 91436**
TELEPHONE NUMBER:	**888-678-5735 ext. 700**
DATE:	**07/30/2019**
SIGNATURE:	
TYPED NAME & TITLE OF SIGNER:	**Brian Chudleigh, CFO**

Form A
Bidder Contact Sheet
Request for Proposal Number 6111 Z1

Form A should be completed and submitted with each response to this RFP. This is intended to provide the State with information on the bidder's name and address, and the specific person(s) who are responsible for preparation of the bidder's response.

Preparation of Response Contact Information	
Bidder Name:	**mPulse Mobile, Inc.**
Bidder Address:	**16530 Ventura Blvd., Suite 500** **Encino, CA 91436**
Contact Person & Title:	**Jeremy Watson, Sr. Director, Healthcare Solutions**
E-mail Address:	**jeremy.watson@mpulsemobile.com**
Telephone Number (Office):	**888-678-5735 ext. 768**
Telephone Number (Cellular):	**502-777-2051**
Fax Number:	**888-678-5735**

Each bidder should also designate a specific contact person who will be responsible for responding to the State if any clarifications of the bidder's response should become necessary. This will also be the person who the State contacts to set up a presentation/demonstration, if required.

Communication with the State Contact Information	
Bidder Name:	**mPulse Mobile, Inc.**
Bidder Address:	**16530 Ventura Blvd., Suite 500** **Encino, CA 91436**
Contact Person & Title:	**Jeremy Watson, Sr. Director, Healthcare Solutions**
E-mail Address:	**jeremy.watson@mpulsemobile.com**
Telephone Number (Office):	**888-678-5735 ext. 768**
Telephone Number (Cellular):	**502-777-2051**
Fax Number:	**888-678-5735**

MPULSE MOBILE CORPORATE OVERVIEW

A. BIDDER IDENTIFICATION AND INFORMATION

The bidder should provide the full company or corporate name, address of the company's headquarters, entity organization (corporation, partnership, proprietorship), state in which the bidder is incorporated or otherwise organized to do business, year in which the bidder first organized to do business and whether the name and form of organization has changed since first organized.

Full Company Name: mPulse Mobile, Inc.
Headquarters Address: 16530 Ventura Blvd., Suite 500 Encino, CA 91436
Entity Organization: Corporation
State of Incorporation: California
Year First Organized to do Business: 2014
Name or organization changes since doing business: 0

B. FINANCIAL STATEMENTS

The bidder should provide financial statements applicable to the firm. If publicly held, the bidder should provide a copy of the corporation's most recent audited financial reports and statements, and the name, address, and telephone number of the fiscally responsible representative of the bidder's financial or banking organization.

If the bidder is not a publicly held corporation, either the reports and statements required of a publicly held corporation, or a description of the organization, including size, longevity, client base, areas of specialization and expertise, and any other pertinent information, should be submitted in such a manner that proposal evaluators may reasonably formulate a determination about the stability and financial strength of the organization. Additionally, a non-publicly held firm should provide a banking reference.

The bidder must disclose any and all judgments, pending or expected litigation, or other real or potential financial reversals, which might materially affect the viability or stability of the organization, or state that no such condition is known to exist.

The State may elect to use a third party to conduct credit checks as part of the corporate overview evaluation.

mPulse Mobile is a privately held corporation founded in 2014 with annual recurring revenue exceeding $10 million. The company size is 75 – 100 employees. Several marquee customers include Kaiser Permanente, Humana, Cook County Illinois (County Care), John Hopkins / Priority Partners, and Providence Health Services. mPulse's specialization is providing a mobile health engagement platform used to improve health outcomes for our customers.

Bank Reference – Attachment A

State Certificate of Good Standing – Attachment B

C. CHANGE OF OWNERSHIP

If any change in ownership or control of the company is anticipated during the twelve (12) months following the proposal due date, the bidder should describe the circumstances of such change and indicate when the change will likely occur. Any change of ownership to an awarded vendor(s) will require notification to the State.

No anticipated change in ownership

D. OFFICE LOCATION

The bidder's office location responsible for performance pursuant to an award of a contract with the State of Nebraska should be identified.

Office Location: 16530 Ventura Blvd., Suite 500 Encino, CA 91436

E. RELATIONSHIPS WITH THE STATE

The bidder should describe any dealings with the State over the previous ten (10) years. If the organization, its predecessor, or any Party named in the bidder's proposal response has contracted with the State, the bidder should identify the contract number(s) and/or any other information available to identify such contract(s). If no such contracts exist, so declare.

No such contract exists.

F. BIDDER'S EMPLOYEE RELATIONS TO STATE

If any Party named in the bidder's proposal response is or was an employee of the State within the past twelve (12) months, identify the individual(s) by name, State agency with whom employed, job title or position held with the State, and separation date. If no such relationship exists or has existed, so declare.

No such relationship exists or has existed.

If any employee of any agency of the State of Nebraska is employed by the bidder or is a subcontractor to the bidder, as of the due date for proposal submission, identify all such persons by name, position held with the bidder, and position held with the State (including job title and agency). Describe the responsibilities of such persons within the proposing organization. If, after review of this information by the State, it is determined that a conflict of interest exists or may exist, the bidder may be disqualified from further consideration in this proposal. If no such relationship exists, so declare.

No such relationship exists.

G. CONTRACT PERFORMANCE

If the bidder or any proposed subcontractor has had a contract terminated for default during the past five (5) years, all such instances must be described as required below. Termination for default is defined as a notice to stop performance delivery due to the bidder's non-performance or poor performance, and the issue was either not litigated due to inaction on the part of the bidder or litigated and such litigation determined the bidder to be in default.

It is mandatory that the bidder submit full details of all termination for default experienced during the past five (5) years, including the other Party's name, address, and telephone number. The response to this section must present the bidder's position on the matter. The State will evaluate the facts and will score the bidder's proposal accordingly. If no such termination for default has been experienced by the bidder in the past five (5) years, so declare.

If at any time during the past five (5) years, the bidder has had a contract terminated for convenience, non-performance, non-allocation of funds, or any other reason, describe fully all circumstances surrounding such termination, including the name and address of the other contracting Party.

No such termination for default has been experienced by mPulse Mobile, Inc. in the past five (5) years.

H. SUMMARY OF BIDDER'S CORPORATE EXPERIENCE

The bidder should provide a summary matrix listing the bidder's previous projects similar to this RFP in size, scope, and complexity. The State will use no more than three (3) narrative project descriptions submitted by the bidder during its evaluation of the proposal.

The bidder should address the following:

Provide narrative descriptions to highlight the similarities between the bidder's experience and this RFP. These descriptions should include:

- The time period of the project;
- The scheduled and actual completion dates;
- The Contractor's responsibilities;
- For reference purposes, a customer name (including the name of a contact person, a current telephone number, a facsimile number, and e-mail address); and,
- Each project description should identify whether the work was performed as the prime Contractor or as a subcontractor. If a bidder performed as the prime Contractor, the description should provide the originally scheduled completion date and budget, as well as the actual (or currently planned) completion date and actual (or currently planned) budget.

Contractor and subcontractor(s) experience should be listed separately. Narrative descriptions submitted for Subcontractors should be specifically identified as subcontractor projects.

If the work was performed as a subcontractor, the narrative description should identify the same information as requested for the Contractors above. In addition, subcontractors should identify what share of contract costs, project responsibilities, and time period were performed as a subcontractor.

All examples of Corporate Experience are outlined on the attachments C – E and all engagements were directly managed by mPulse Mobile.

Attachment C – Case Study – Kaiser Permanente – JMIR Peer Reviewed Study to improve Medication Refill Rates
Attachment D – Case Study – Kaiser Permanente – Mobile Engagement for Improving Diabetes Self-Management
Attachment E – Case Study – Home State Health – Improving HEDIS Measures of a Medicaid population

Additional contact information for these customers and others can be provided for further reference checks.

I. SUMMARY OF BIDDER'S PROPOSED PERSONNEL/MANAGEMENT APPROACH

The bidder should present a detailed description of its proposed approach to the management of the project.

The bidder should identify the specific professionals who will work on the State's project if their company is awarded the contract resulting from this RFP. The names and titles of the team proposed for assignment to the State project should be identified in full, with a description of the team leadership, interface and support functions, and reporting relationships. The primary work assigned to each person should also be identified.

The bidder should provide resumes for all personnel proposed by the bidder to work on the project. The State will consider the resumes as a key indicator of the bidder's understanding of the skill mixes required to carry out the requirements of the RFP in addition to assessing the experience of specific individuals.

Resumes should not be longer than three (3) pages. Resumes should include, at a minimum, academic background and degrees, professional certifications, understanding of the process, and at least three (3) references (name, address, and telephone number) who can attest to the competence and skill level of the individual. Any changes in proposed personnel shall only be implemented after written approval from the State.

The bidder will assign a project manager and shall provide sufficient staffing from project kickoff through the end of the contract, including all optional renewal periods. The project manager will be responsible for the management, oversight, and coordination of project including timely resolutions to project issues. The project manager will participate in weekly meetings with DHHS and prepare status reports

Sales Director will manage the initial relationship between Client and mPulse Mobile. Strategic Account Director will facilitate the overarching goal to ensure Nebraska's initiatives are handled and implemented appropriately. On a day to day basis, Nebraska's contacts will interact with mPulse Mobile's assigned Account Manager and Project Manager/ Customer Success Lead. If necessary, the Behavioral Data Scientist Lead can be involved in the process of scoping and implementation of the strategic initiatives using Artificial Intelligence.

Sales Director -- Jeremy Watson
Strategic Account Director – Melissa Palladino [Resume Provided]
Account Manager – Meenah Atayee. [Resume Provided]
Project Manager / Customer Success Lead – Lidia Maruska [Resume Provided]
Optional: Behavior Data Scientist Lead – Rena Prayaga

J. SUBCONTRACTORS

If the bidder intends to subcontract any part of its performance hereunder, the bidder should provide:

- name, address, and telephone number of the subcontractor(s);
- specific tasks for each subcontractor(s);
- percentage of performance hours intended for each subcontract; and
- total percentage of subcontractor(s) performance hours.

No intention to use subcontractors for the work performed in this Proposal

MPULSE MOBILE TECHNICAL APPROACH

A. UNDERSTANDING OF THE PROJECT REQUIREMENTS

Provide a narrative that illustrates the bidder's understanding of the State's requirements and project schedule. Include a summary description of how the proposed solution will address the purpose and requirements and include a project planning approach.

The mPulse Mobile solution has been developed to help healthcare organizations and agencies engage and activate their clients and members through tailored SMS mobile communications.

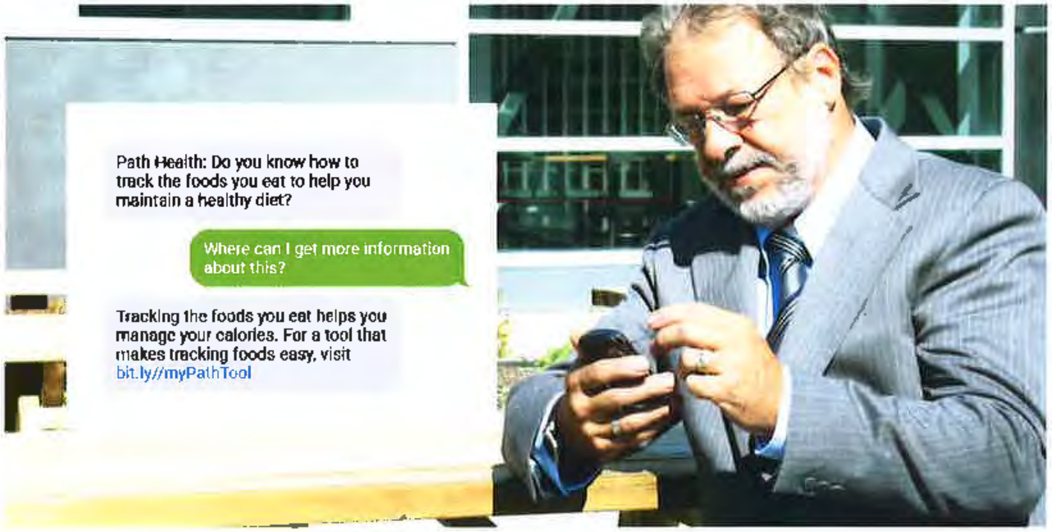
When healthcare consumers are not engaged, they struggle to effectively manage the complexity of healthcare. Clients miss getting the care that they need, and health systems incur unnecessary costs.

Engaged patients cost less to treat. Public agencies must invest in patient engagement strategies to be successful in the value-based care environment. Cost efficiency is crucial, so organizations need a scalable communication solution that can address a wide-range of patient engagement challenges across the care continuum. The solution must be easy for patients to adopt and use, otherwise it will have little impact on outcomes.

Low awareness of services prevents patients from getting important care that they need. mPulse Mobile will partner with DHHS to help educate patients about available economic programs and care services and drive them to take action on their health.

Hi Jane. Path Urgent Care is your nearest Urgent Care clinic. The current wait time is 35 minutes. It is located at 1345 Ventura Ave. Encino, CA 91346. For alternate options reply MORE.

Chronic conditions require intensive treatment. mPulse Mobile helps to engage members on how they can better manage their condition and provide notifications and reminders, so members take action to meet care milestones.

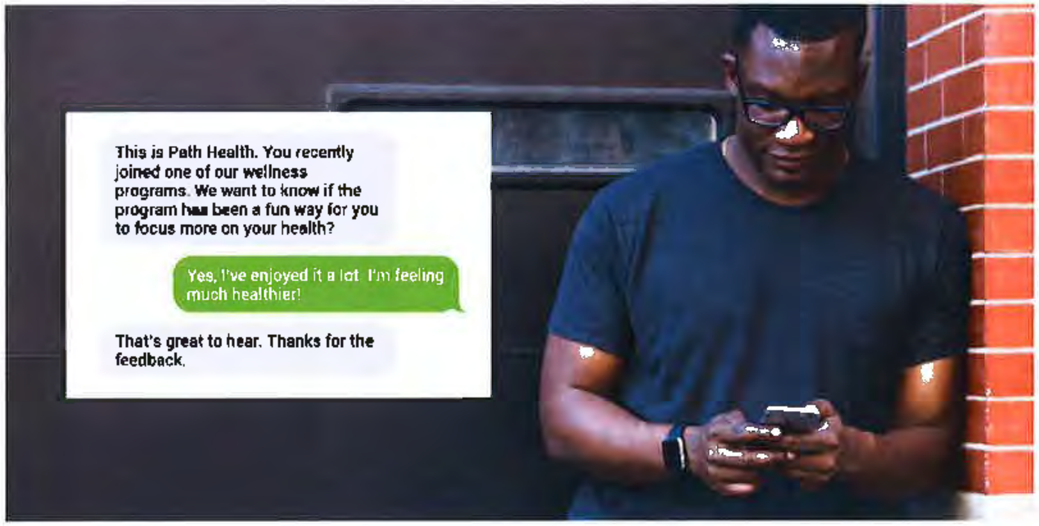


Path Health: Do you know how to track the foods you eat to help you maintain a healthy diet?

Where can I get more information about this?

Tracking the foods you eat helps you manage your calories. For a tool that makes tracking foods easy, visit bit.ly//myPathTool

Surveys provide important insights about consumers' experiences with health services, but they can be costly and inefficient to administer. Leverage mobile channels to efficiently reach consumers and deliver surveys with high response rates and quick response times.

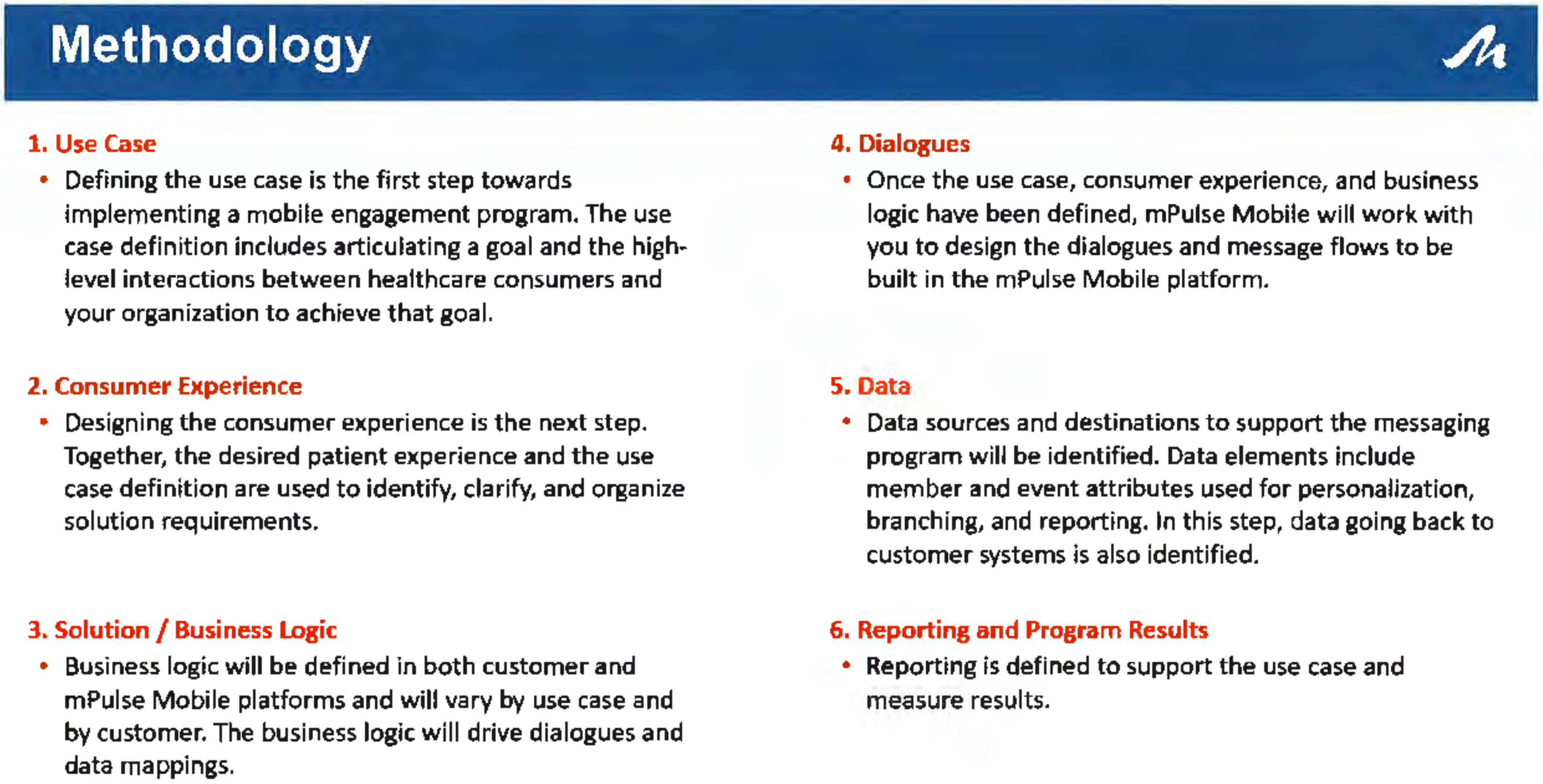


This is Path Health. You recently joined one of our wellness programs. We want to know if the program has been a fun way for you to focus more on your health?

Yes, I've enjoyed it a lot. I'm feeling much healthier!

That's great to hear. Thanks for the feedback.

mPulse Mobile follows a proven methodology to successfully address these challenges. The mPulse Mobile project planning approach maps this methodology to DHHS people, process and technology so that mobile communication strategies can be implemented efficiently, effectively and in a timely manner.



Methodology

1. Use Case

- Defining the use case is the first step towards implementing a mobile engagement program. The use case definition includes articulating a goal and the high-level interactions between healthcare consumers and your organization to achieve that goal.

2. Consumer Experience

- Designing the consumer experience is the next step. Together, the desired patient experience and the use case definition are used to identify, clarify, and organize solution requirements.

3. Solution / Business Logic

- Business logic will be defined in both customer and mPulse Mobile platforms and will vary by use case and by customer. The business logic will drive dialogues and data mappings.

4. Dialogues

- Once the use case, consumer experience, and business logic have been defined, mPulse Mobile will work with you to design the dialogues and message flows to be built in the mPulse Mobile platform.

5. Data

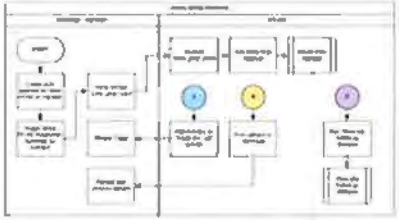
- Data sources and destinations to support the messaging program will be identified. Data elements include member and event attributes used for personalization, branching, and reporting. In this step, data going back to customer systems is also identified.

6. Reporting and Program Results

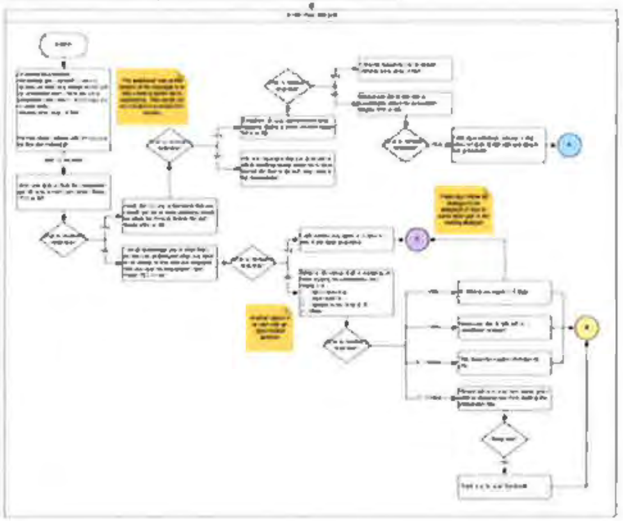
- Reporting is defined to support the use case and measure results.

Mobile communications and dialogues are developed that map and interface with DHHS workflows and member journeys.

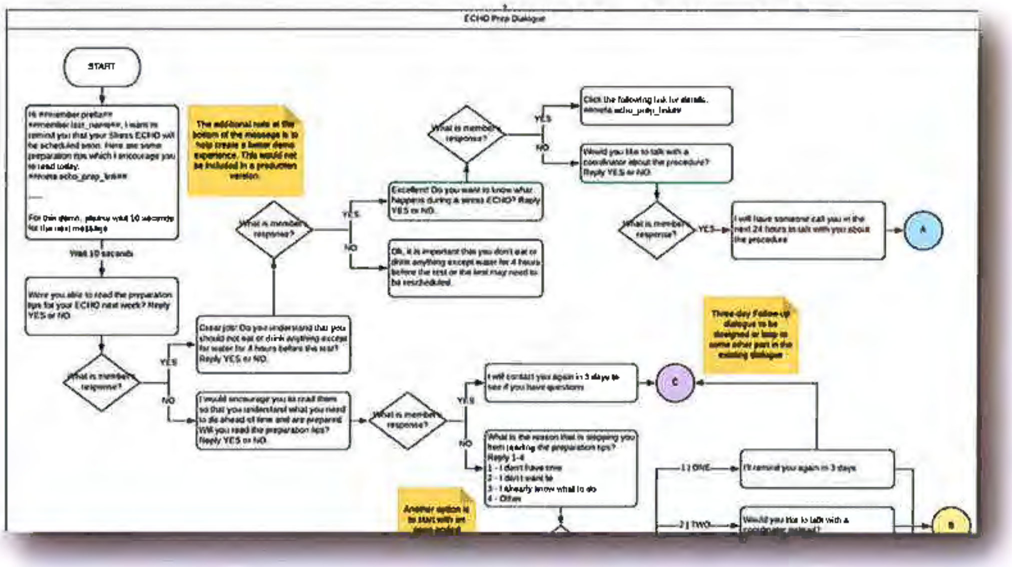
Customer Workflow



mPulse Dialogue



The healthcare consumer experience is diagramed so that all stakeholders associated with DHHS programs are able to collaborate on and approve mobile communication programs.



Hi ##member.prefname ##member.last_name##, I want to remind you that your Stress ECHO will be scheduled soon. Here are some preparation tips which I encourage you to read today.
##meta.echo_prep_link##

—

For this demo, please wait 10 seconds for the next message

The additional note at the bottom of the message is to help create a better demo experience. This would not be included in a production version.

Were you able to read the preparation tips for your ECHO next week? Reply YES or NO

Great job! Do you understand that you should not eat or drink anything except for water for 4 hours before the test? Reply YES or NO

I would encourage you to read them so that you understand what you need to do ahead of time and are prepared. Will you read the preparation tips? Reply YES or NO

Excellent! Do you want to know what happens during a stress ECHO? Reply YES or NO

Ok, it is important that you don't eat or drink anything except water for 4 hours before the test or the test may need to be rescheduled.

Click the following link for details. ##meta.echo_prep_link##

Would you like to talk with a coordinator about the procedure? Reply YES or NO

I will have someone call you in the next 24 hours to talk with you about the procedure

Three-day follow-up dialogue to be designed or loop to some other part in the existing dialogue

I will contact you again in 3 days to see if you have questions

What is the reason that is stopping you from reading the preparation tips? Reply 1-4
1 - I don't have time
2 - I don't want to
3 - I already know what to do
4 - Other

I'll remind you again in 3 days

Would you like to talk with a coordinator instead?

Another option is to start with an open ended

Reporting and analysis is supported through the mPulse Mobile Insights Dashboard and operational reporting tools. All aspects of mobile engagement can be measured to ensure program impact and results.

Operational

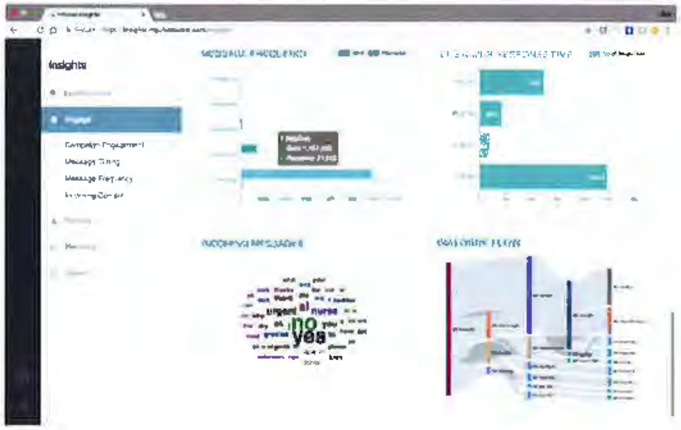
- Sent/received
- Member counts

Engagement

- Link Clicks
- Response Time
- Dialogue Status
- Rules Triggered

Analytics

- Program Results
- Behavior Change



Please see the Attachment K Solution Design related to project implementation.

FUNCTIONAL BUSINESS AND TECHNICAL REQUIREMENTS TRACEABILITY MATRIX

Bidders must complete Attachment 1 for the proposed solution and include it with their bid. Detailed responses to the technical and functional requirements of the proposed solution must be provided in the response matrices.

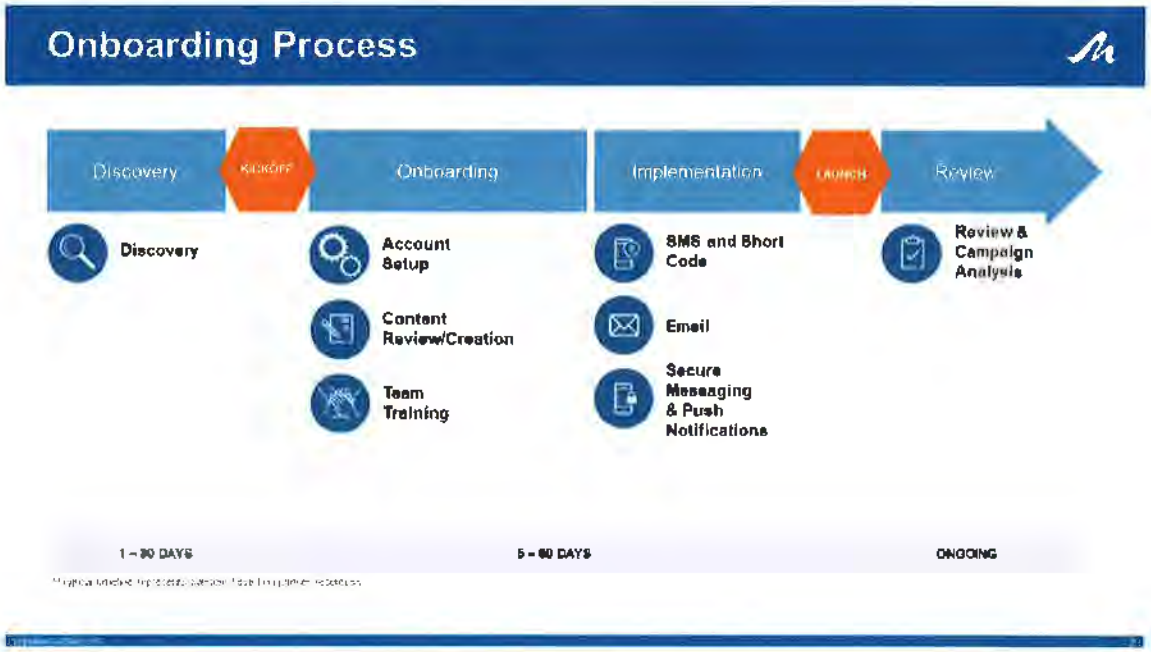
Please see Attachment 1 Functional Business/Technical Requirements Traceability Matrix

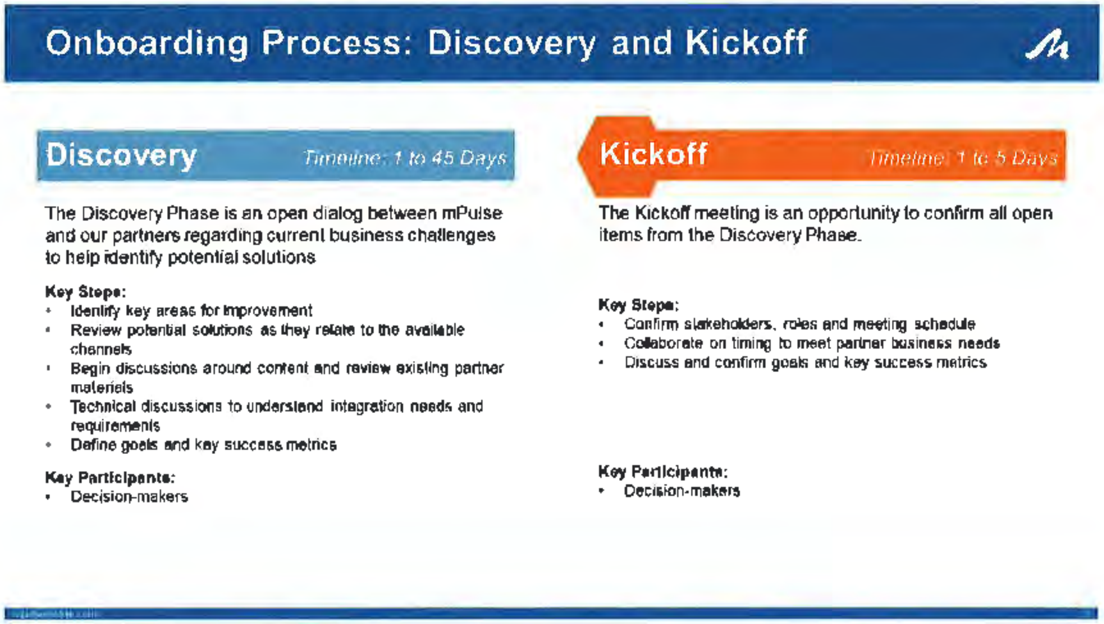
DRAFT PROJECT WORK PLAN

Provide a draft work plan identifying tasks, resources/staffing needed, deliverables, dependencies, timelines, and milestones.

Both onboarding and post-implementation timelines and project tasks are critical to program success. mPulse mobile incorporates a phased approach based on our proven methodology that maps to DHHS practices. Phases include Discovery, Onboarding, Implementation and Review. Post-implementation reviews ensure that programs are performing as expected and provide an opportunity for adjusting or enhancing dialogues and campaigns.

See Attachment K Solution Design and Attachment I Project Plan / Timeline task break down related to project implementation and Solution Design Template


Onboarding Process



Onboarding Process: Discovery and Kickoff

Discovery

Timeline: 1 to 45 Days

The Discovery Phase is an open dialog between mPulse and our partners regarding current business challenges to help identify potential solutions

Key Steps:
- Identify key areas for improvement
- Review potential solutions as they relate to the available channels
- Begin discussions around content and review existing partner materials
- Technical discussions to understand integration needs and requirements
- Define goals and key success metrics

Key Participants:
- Decision-makers

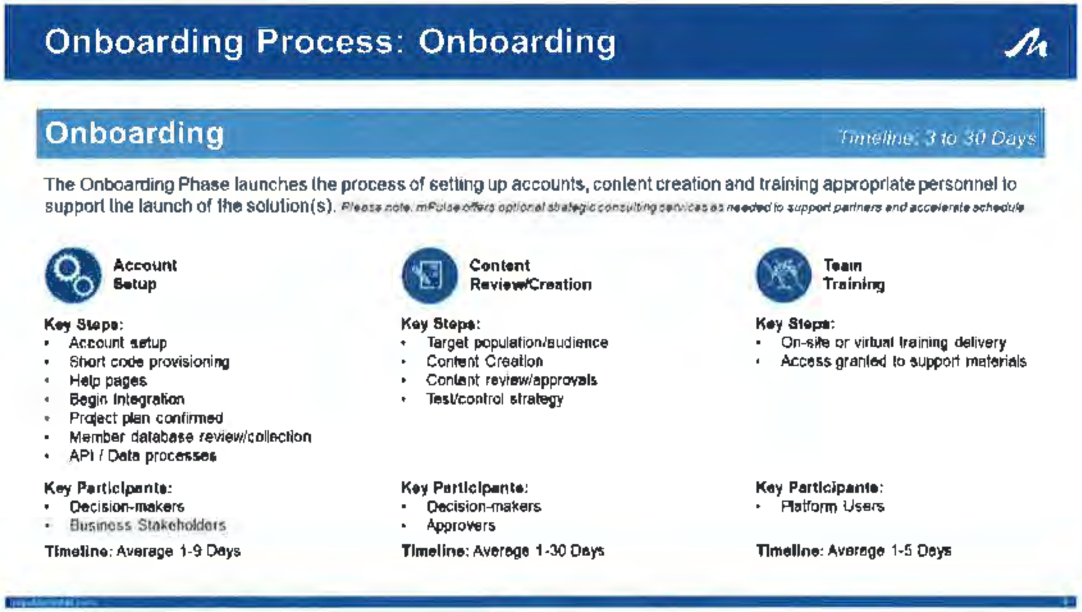
Kickoff

Timeline: 1 to 5 Days

The Kickoff meeting is an opportunity to confirm all open items from the Discovery Phase.

Key Steps:
- Confirm stakeholders, roles and meeting schedule
- Collaborate on timing to meet partner business needs
- Discuss and confirm goals and key success metrics

Key Participants:
- Decision-makers



Onboarding Process: Onboarding

Onboarding

Timeline: 3 to 30 Days

The Onboarding Phase launches the process of setting up accounts, content creation and training appropriate personnel to support the launch of the solution(s). *Please note: mPulse offers optional strategic consulting services as needed to support partners and accelerate schedule*

Account Setup

Key Steps:
- Account setup
- Short code provisioning
- Help pages
- Begin Integration
- Project plan confirmed
- Member database review/collection
- API / Data processes

Key Participants:
- Decision-makers
- Business Stakeholders

Timeline: Average 1-9 Days

Content Review/Creation

Key Steps:
- Target population/audience
- Content Creation
- Content review/approvals
- Test/control strategy

Key Participants:
- Decision-makers
- Approvers

Timeline: Average 1-30 Days

Team Training

Key Steps:
- On-site or virtual training delivery
- Access granted to support materials

Key Participants:
- Platform Users

Timeline: Average 1-5 Days

Onboarding Process: Launch & Review

Launch *Timeline: 1 to 5 Days*

Once implementation and QA are complete, we will launch the campaign(s) on the go-live date determined with our partner.

Key Steps:

- Launch initial campaign(s)
- High-level review of initial results sent to business partners (Based on initial results, content changes may be applicable)
- A/B testing
- Continued database building of targeted members

Key Participants:

- Decision-makers

Review *Timeline: Ongoing*

After campaign launch, mPulse will coordinate a meeting with our partner to conduct a thorough review and discuss next steps to help optimize campaign(s)

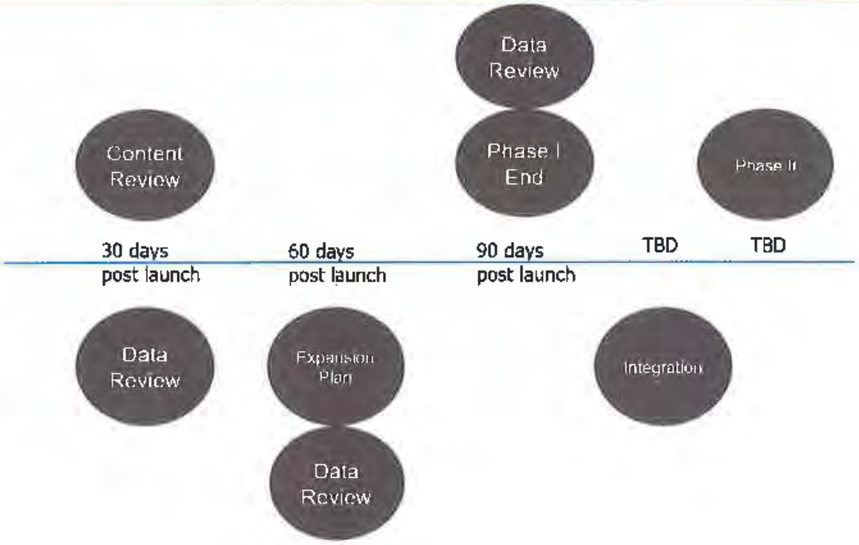
Key Steps:

- In-depth review of initial campaign results
- Confirm results of A/B testing
- Continued database building
- Project milestone review
- Confirm ongoing campaign path and set recurring meeting schedules and reporting schedules

Key Participants:

- Decision-makers

Post Launch - Key Milestones



Content Review

Data Review

30 days post launch

Expansion Plan

Data Review

60 days post launch

Data Review

Phase I End

90 days post launch

TBD

Integration

TBD

Phase II

PAGES LEFT OUT BY BIDDER

Capability Layers

Communicate

Overview

mPulse Mobile's Communicate layer includes an enterprise-class cloud-based Communication Platform that delivers one-way messages, notifications and compliance related response handling over SMS, email, push notifications, mobile web, and interactive voice response (IVR) channels.

The Communicate layer establishes the highest levels of messaging performance, governance and data management that are required by enterprise healthcare organizations.

The Communicate layer is where member information is stored and managed allowing for robust preference management guided by consumer attributes. A suite of message trigger options can be configured to support a wide range of use cases (e.g., time, date, recurrence, and consumer profile changes).

Standard Messaging Programs

Coordinated 1-way messages are the basic form of messaging program. These messages are coordinated based off a range of message triggers (e.g., date, time, event, location, and age).

SMS Content: Message Length and Foreign Language Support

mPulse Mobile supports multibyte character encoding for SMS, which means characters for all international languages are supported. In addition, we support a character limit of up to 1000 characters (dependent on device) by leveraging message concatenation available in most mobile devices.

Channel and Language Preferences

Channel and language preferences are stored and managed at the individual consumer level.

Communicate Dashboard

The Communicate Dashboard provides message delivery metrics that reveal how well the consumer population has been reached (e.g., total messages delivered, bounce rates, click-through rates, etc.)

Engage

Overview

The Engage layer includes all functionality of the Communicate Layer.

The Engage layer transforms the consumer touchpoint from one-way push messaging to two-way automated and manual dialogues, creating a more engaging experience for consumers. mPulse Mobile's Engagement Engine automates dialogues based on the consumer's message responses and external data inputs. Automated interactions use rule-based branching logic that allows consumers to navigate through the program based on their message responses.

Engagement Console

The mPulse Mobile Engagement Console (EC) is a web-based application that enables one-on-one communication and member data management. It can be used to initiate manual message-based interactions with consumers as well as supplementing automated dialogues by surfacing inbound messages (mobile originated [MO] messages) for health organization staff to triage and respond to, and it can also be used to manually add members and trigger dialogues.

Sentiment Assessment

Consumer sentiment is a powerful measure of messaging program acceptance. The analysis classifies each consumer response across a five-point scale from "Highly Negative" to "Highly Positive".

Results can be viewed at the consumer, segment, or population level. Sentiment Assessment provides clear guidance about the consumer preference of different programs or specific content within programs.

Natural Response Handling (NRH)

Real-time interpretation of consumer text responses enables more sophisticated dialogues and solution-specific conversational agent capabilities.

Engage Dashboard

The Engage Dashboard highlights engagement measures that reveal how engaged the consumer population is (e.g., response rates, response topics, consumer sentiment).

Professional Services

Development

Content Development

mPulse Mobile works with clients' content development services and combines their requirements with its experience in mobile messaging to drive program outcomes and consumer focused healthcare messaging. Program content is developed with consideration to reading and health literacy. Additionally, mPulse Mobile provides guidance on all messaging content required from a regulatory compliance standpoint.

Dialogue Development

mPulse Mobile dialogue development services can be used to edit existing program dialogues or build entirely new dialogues for specific customer defined challenges.

The service includes development of the branching logic, content development for all messages included in the dialogues, and set-up of dialogues in mPulse Mobile's Engagement Engine.

Translation Services

mPulse Mobile supports multiple languages and will arrange Translation Services to ensure content is communicated effectively. Additional fees will apply.

Custom Development

mPulse Mobile offers custom integration and service expansion capabilities. Additional fees will apply based on project scope.

Consulting

Behavioral Data Science

mPulse Mobile's experienced Behavioral Data Science team is a core component of its solution offering. The team provides detailed research, analysis, and recommendations to optimize behavior change on a range of health engagement challenges in a specific population.

Adoption of core behavioral science principals has been identified as an area of opportunity to improve how people make decisions and act on them.

Preference Management and Mobile Messaging Strategy

mPulse Mobile provides consulting services to help develop a preference management and mobile messaging strategy across an enterprise organization.

On-Boarding

Client Kick-off

mPulse Mobile will schedule an initial kick-off meeting to review the contract and requirements discussed during the sales process, introduce post-sales resources (e.g., Account Management, Client Success, Behavioral Data Science), and begin developing a project plan.

Account Setup

mPulse Mobile will grant access to a fully configured and functioning account in mPulse Mobile's HITRUST certified Platform. The Platform is available 24 hours a day, 7 days a week, 365 days a year.

Account Management

mPulse Mobile will assign a dedicated Account Manager for the term of this contract. mPulse Mobile's Account Managers provide expertise in mobile health engagement that ensures the messaging program achieves optimal results.

Short Code Provisioning

A short code is a 5 or 6-digit number used as an address to send and receive SMS messages.
mPulse Mobile will coordinate the application, provisioning, and testing process for purchased Dedicated Short Code (or alternative number type) from the Common Short Code Administration registrar and will utilize this Short Code for SMS messaging programs for the duration of the contract and any contract renewals.

Phone Number Assessment

mPulse Mobile will conduct an initial one-time phone number assessment to determine what phone numbers can receive SMS text messages.

Program Development

Use Case Review

mPulse Mobile will provide best practices to the designing and implementing of use cases specific to each customer's needs.

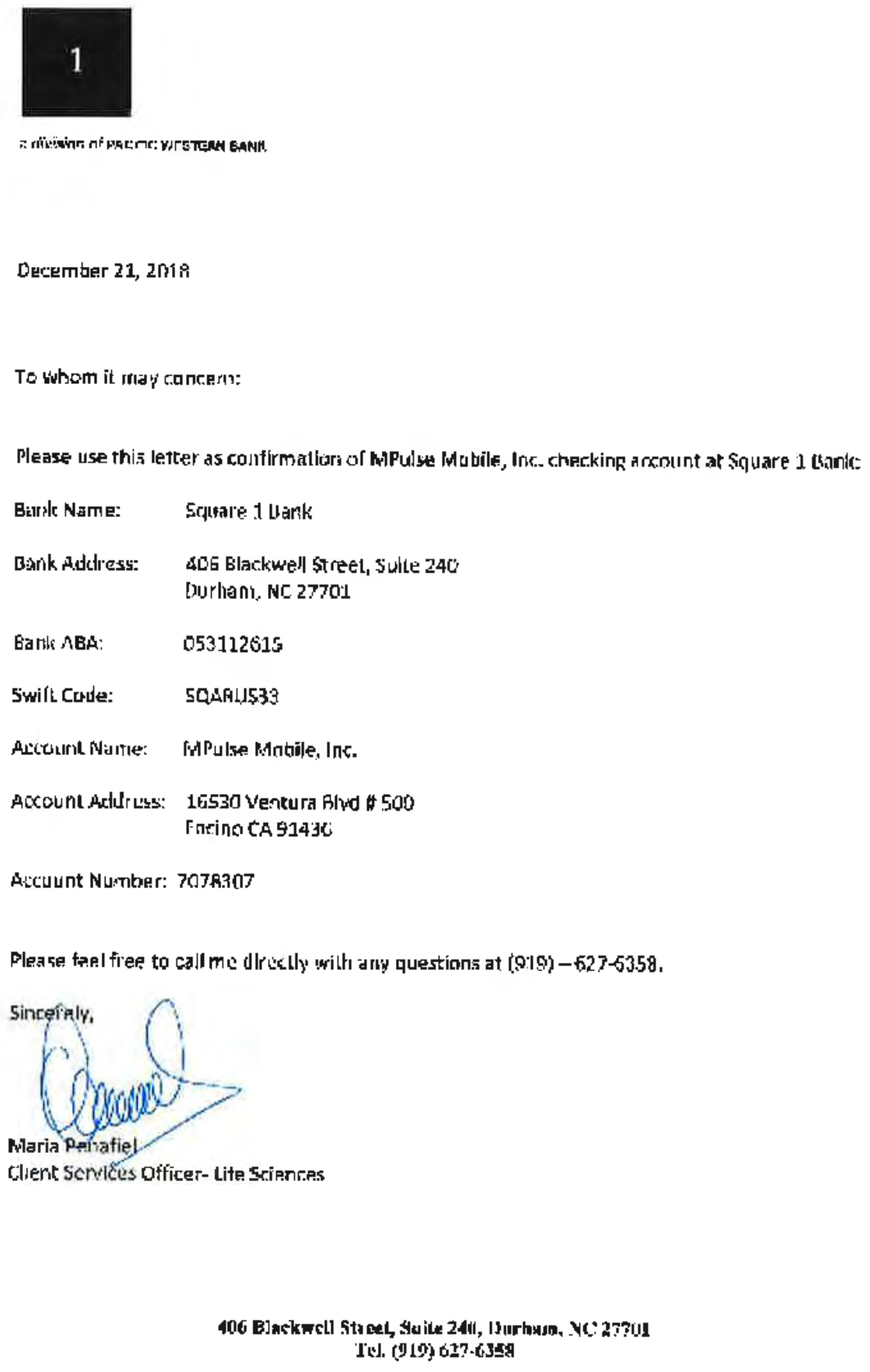
Identify Data Requirements

To accommodate customer needs, mPulse Mobile supports several data transfer methods: RESTful APIs, callbacks, automated SFTP, and manual input tools.

Content Development and Review

Each customer has a different content review and approval process. Your Account Management team will work with you to develop content to support your program and help support navigating your internal approval process.

Attachment A - Bank Reference



1

a division of PACIFIC WESTERN BANK

December 21, 2018

To whom it may concern:

Please use this letter as confirmation of MPulse Mobile, Inc. checking account at Square 1 Bank:

Bank Name:	Square 1 Bank
Bank Address:	406 Blackwell Street, Suite 240 Durham, NC 27701
Bank ABA:	053112615
Swift Code:	SQARUS33
Account Name:	MPulse Mobile, Inc.
Account Address:	16530 Ventura Blvd # 500 Encino CA 91436
Account Number:	7078307

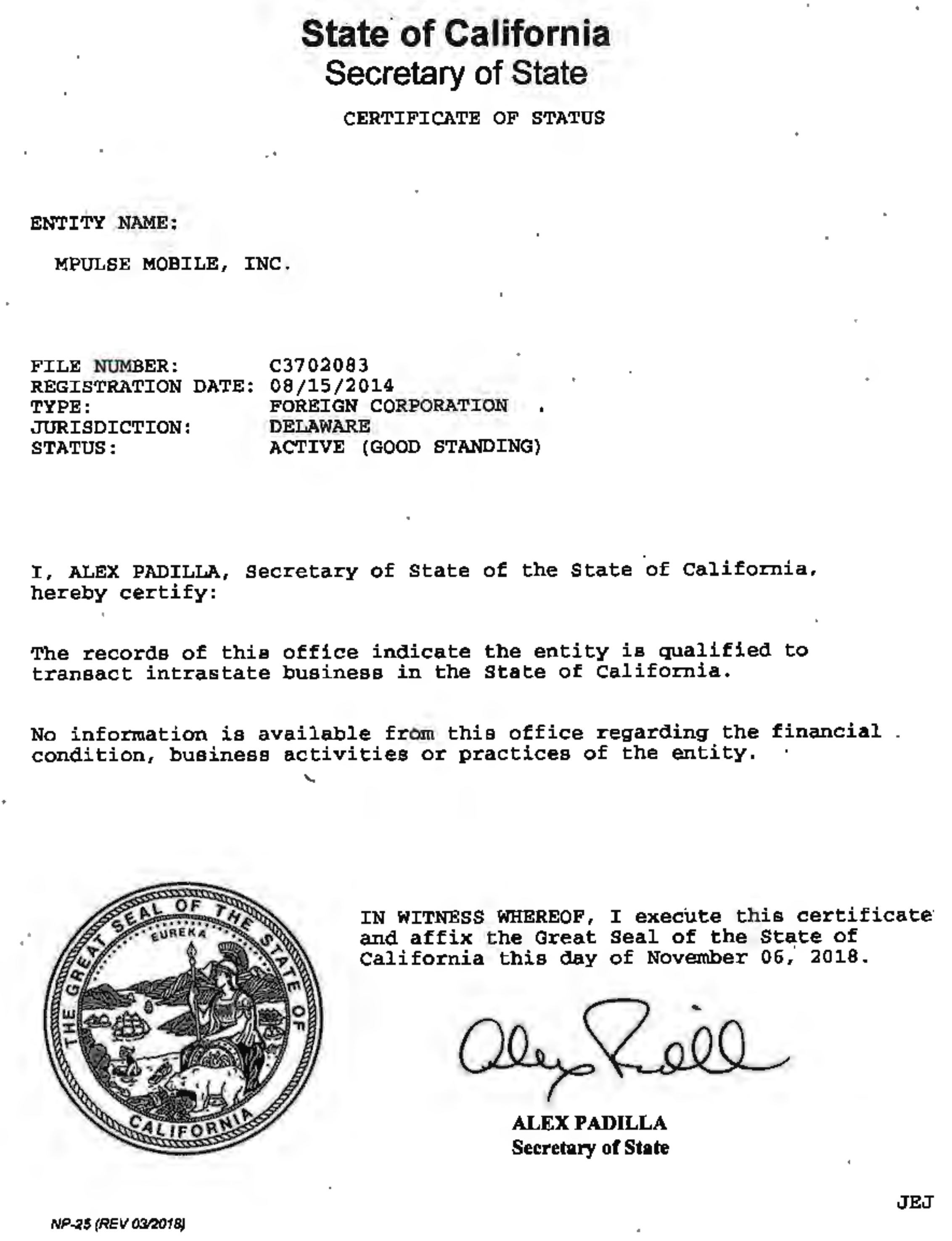
Please feel free to call me directly with any questions at (919) – 627-6358.

Sincerely,

Maria Peñafiel
Client Services Officer- Life Sciences

406 Blackwell Street, Suite 240, Durham, NC 27701
Tel. (919) 627-6358

Attachment B – California State Certificate of Good Standing



State of California
Secretary of State

CERTIFICATE OF STATUS

ENTITY NAME:

MPULSE MOBILE, INC.

FILE NUMBER:	C3702083
REGISTRATION DATE:	08/15/2014
TYPE:	FOREIGN CORPORATION
JURISDICTION:	DELAWARE
STATUS:	ACTIVE (GOOD STANDING)

I, ALEX PADILLA, Secretary of State of the State of California, hereby certify:

The records of this office indicate the entity is qualified to transact intrastate business in the State of California.

No information is available from this office regarding the financial condition, business activities or practices of the entity.

THE GREAT SEAL OF THE STATE OF CALIFORNIA EUREKA

IN WITNESS WHEREOF, I execute this certificate and affix the Great Seal of the State of California this day of November 06, 2018.

ALEX PADILLA
Secretary of State

JEJ

NP-25 (REV 03/2018)

Attachment C – Case Study – Kaiser Permanente – JMIR Peer Reviewed Study

Medicare Chronic Condition Medication Refill

KAISER PERMANENTE.

Kaiser Permanente is the largest integrated managed care organization in the US, with over 11 million health plan members

Goal

- Increase Rx refill rate for Medicare plan members with chronic conditions, who are non-adherent with their prescription refills:
- Increase refill rate %
- Generate operational efficiencies
- Impact Star Ratings

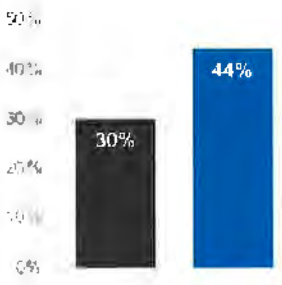
Execution

- mPulse Mobile's dialogue-based Rx Refill Solution allowed consumers to confirm their refill directly through the text channel
- Over 12,000 patients received Rx Refill workflows
- Solution required identify verification before confirming refill, achieved using interactive text functionality
- Automated text dialogues uncovered barriers to adherence
- KP Pharmacy staff used mPulse's Engagement Console to deliver text support for the refill process

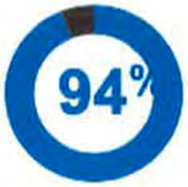
Data

Statistically significant increase in chronic condition medication adherence rates

3-MONTH Rx REFILL RATES



PATIENT SATISFACTION



The study was published with Kaiser and mPulse mobile as joint authors in the Journal of Internet Medical Research https://mhealth.jmir.org/2018/1/e30/

Results

- In a 3-month study the mPulse group had a 44% refill rate vs 30% in the Comparison group
- 96% of survey respondents (1250 patients) said they found the mPulse solution easy to use
- Anecdotal reporting indicated the back-office processing became 2x more efficient using the MEC compared to phone follow-up
- 92% neutral to very positive sentiment
- 1.6% program opt-out rate

Attachment D – Case Study – Kaiser Permanente – Mobile Engagement for Improving Diabetes Self-Management

Diabetes Self-Management Behavior Change

KAISER PERMANENTE.

Kaiser Permanente Orange County has 49,000 diabetics. 23,000 are controlled diabetics with A1c <7, 24% of whom will have their levels rise above 7 by their next HbA1c check.

Goal

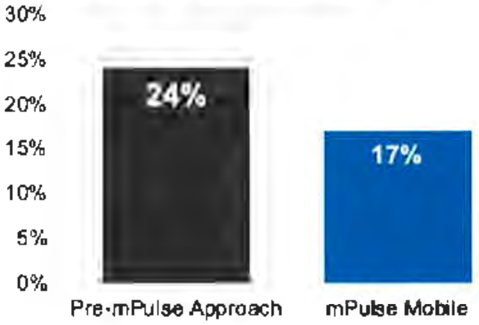
- Improve diabetes self-management to help patients with controlled diabetes stay in control
- Assess the effectiveness of Conversational AI solutions to drive behavior change for diabetes self-management

Execution

- Kaiser implemented mPulse's Conversational AI Diabetes Self-Management solution to drive healthy behavior change
- The solution used mPulse's Activation Intelligence product to deliver automated tailored dialogues to controlled diabetic members over a period of 6 months following their A1c test result
- Members received their A1c results directly in the text channel after an identity verification process

Data

% OF IN-CONTROL DIABETIC PATIENTS FALLING OUT OF A1C CONTROL



Results

- An assumed opt-in was used to engage 22,650 patients and 11,238 (49.6%) elected to receive their A1c results directly in the text channel.
- >276,000 dialogues were delivered, an average of 21 tailored conversations per member focused on behavior change
- 78% of patients requested to be messaged 2 or more times per week, with a 23.2% overall response rate for the program
- Reduction in controlled diabetics falling out of control from 24% to 17%
- Conversational AI solutions required minimal staff involvement and freed up key care resources

Attachment E – Case Study – Home State Health – Improving HEDIS Measures of a Medicaid population

Medicaid HEDIS Measure Improvement

home state health

Home State Health is a Medicaid plan in Missouri with 240,000 members, 85% of whom are under the age of 18

Goal

- Orchestrate delivery of tailored conversations to engage members and activate them to complete key health tasks
- Drive increased completion of key health checks and preventive screenings
- Improve utilization of health services

Execution

- mPulse orchestrated automated text message conversations with members across 40 topics to help improve key HEDIS measures
- 19,208 members received the messages, with topics prioritized by a dynamic profile of each member's engagement rate, communication preferences, previous responses and plan data
- 81 unique dialogue types were sent to members to ensure maximum engagement
- Over 444,700 automated conversations were completed during a 1-year period of ongoing engagement

Data and Results

	Well Child[1] 0–11	Adolescent Well Care 12–19	Dental Visit 2–20	Lead Screening < 2	Breast Cancer Screening Women 50–74	Cervical Cancer Screening Women 21–64
Overall Visit %	• 68.4%	• 44.7%	• 58.1%	• 57.3%	• 29.8%	• 26.9%
Text Group Visit %	• 82%	• 54.5%	• 66.9%	• 66.8%	• 42.4%[2]	• 38.4%
Difference	• +13.6pp	• +9.8pp	• +8.8pp	• +9.5pp	• +12.6pp	• +11.5pp

[1] The Well Child (0-11) might apply to several HEDIS measures.

[2] Sample size is very small for breast cancer screenings and results may not be generatable for this measure.

[3] The "Overall Visits" metric includes the text group and applies to the entire qualified age group in the MCO's member population. We did not break out a separate "no text" group but results would be even stronger if this was the case since the text group outcomes had a lift effect on overall visits

Attachment F – Resume – Melissa Palladino

Melissa Palladino

Rockport, MA – 10966 – 978.546.9192 – mbpalladino@gmail.com
https://www.linkedin.com/in/melissa-palladino-431b4413/

Strategic Account Director

Strategic Planning – Customer Satisfaction - Project Management

Full Project Lifecyle Development

Marketing & Sales Growth

Cross-Functional Collaboration

Content Development

Product Management

Customer Satisfaction

Healthcare

Strategic Partnership Building

Vendor Relationships

Dedicated and highly analytical product-oriented director with extensive experience guiding new projects from conception and design to final launch while prioritizing revenue.

Broad knowledge of the full project development lifecycle, and a proven ability to collaborate with cross-functional teams to meet project deadlines.

Repeated success leveraging strong communication skills to build consensus among stakeholders, customers, and industry leaders.

Strong knowledge of the healthcare field, and a dedication to engaging in continued professional development.

Skilled leader; readily able to collaborate across organizational levels and teams to drive growth and innovation.

CAREER ACCOMPLISHMENTS

- Planned, cultivated, and launched the highest grossing product partnership at Heatlhx.
- Secured the largest contracts in Eliza Corporations history; several 3-year contracts ranging from $3.5M to $6M, designing solutions for health plans that serve Medicare, Medicaid, Commercial, and Exchange populations.
- Optimized operating budgets by strategically negotiating environmental cleanup contracts with the Florida Department of Environmental Protection.
- Strategically repositioned an entire real estate company during the recession by quickly overhauling a multi-tenant business property and driving occupancy from 45% to 95%.

PROFESSIONAL EXPERIENCE

mPulse Mobile—Los Angeles, CA **11/18-present**

Strategic Account Director

Dedicated professional managing a team of Account Executives and a $3 m national book of business in the health care space.

- Entrusted with client satisfaction and achievement of strategic business goals
- Drive account revenue growth by meeting client needs and introducing additional platform capabilities
- Manage career growth and satisfaction of Account Executive team

Notable clients: Kaiser Permanente, Humana, Highmark, Cambia, Providence, United Concordia Dental, McKesson

Healthx—Indianapolis, IN 4/2017-9/2018

Health Plan Market Director, 5/18-9/18

Served as subject matter expert communicating all federal and local healthcare regulations and laws. Analyzed current processes and procedures and integrated process improvement plans to maintain regulatory compliance. Collaborated with executives to execute strategic planning, explore potential strategic partnerships, and lead new initiatives. Prepared newsletters, blog posts, and social media content to communicate strategic initiatives to the community. Compiled and presented content on regulations, trending issues, healthcare innovation and partner initiatives.

- Entrusted with presenting member engagement and healthcare innovation presentations at national health care conferences.
- Coordinated two bi-annual Advisory committees, connecting chief executives and leaders to execute strategic planning.

Product Strategy Director, 4/17-5/18

Coordinated complete support for new products from design to development to final product implementation. Guided strategic planning, defining scope, timeline, and goals. Mentored sales teams to drive revenue for new product lines. Executed market analysis to cultivate innovative marketing strategies. Represented the product team at events, promoting services and products to industry leaders to accelerate growth.

- Drove revenue by $6M in ARR in the first year of the launching the Healhx Mobile Engagement Suite.

Eliza Corporation—Danvers, MA 4/2009-4/2017

Director of Solution Design, Health Engagement Design Group

Liaised with sales teams, clients, engineering teams, and product development teams to plan and launch multi-year and multi-million-dollar projects. Managed the full project development lifecycle, composing proposals, conducting research, guiding product teams, defining marketing techniques, and training team members. Integrated process improvements, documenting solutions and benefits. Leveraged a comprehensive understanding of the healthcare industry to drive innovation and brand activation.

- Managed a team of Solution Designers, guiding in best practices, assigning focused strategic initiatives, and mentoring professional and personal growth.
- Supported a wide range of sales efforts and customer relations in the health care space, including health plans, PBMs, pharmaceuticals, and durable medical equipment.
- Crafted configurable solutions resulting in multi-year contracts of up to $7.5 million.

Team Lead, Health Engagement Design Group, 9/12-6/14

Planned and delivered multi-channel health care campaigns. Leveraged interactive voice response technology, SMS, and email campaigns to reach new audiences. Liaised with vendors to develop new digital engagement techniques, including testing and coding email campaigns. Collected and analyzed large datasets to update and improve health care engagement strategies. Coordinated maintenance of the asset library.

- Oversaw content strategy and creation of new solution line targeted at Medicare members with a goal toward lifting Part C and D Star measures.

Content Designer, Health Engagement Design Group, 4/09-9/12

Provided exemplary customer service, gathering requirements, managing expectations, and liaising with team members to meet client goals. Coordinated with sales and marketing teams to cultivate a brand style guide and align marketing campaigns accordingly. Expertly composed content for varying audiences to promote interactive campaigns and engage health plan members.

- Leveraged Agile methodology to productively collaborate with vendors.
- Spearheaded an email platform integration project, collaborating with engineers to integrate the new program and troubleshoot the transition.

CAROLSTAN PROPERTIES—Orlando, FL 6/2010-Present

President

Orchestrated remote operations of a $10M dollar, real estate holding company. Served high-level customers like Verizon and Dunbar Armored Cars. Coordinated capital improvement projects, integrating environmental compliance efforts, including FDEP-mandated clean up. Improved tenant satisfaction by executing semi-annual site visits. Cultivated strategic business relationships with partners in wealth management, banking, security, and environmental engineering.

- Successfully negotiated a contentious building repair issue, resulting in a major national company taking responsibility for 85% of the cost.

ADDITIONAL EXPERIENCE

- **KARATE INSTRUCTOR,** AUTHENTIC KARATE TRAINING CENTER, Develop curriculum and teach classes for adult karate students.
- **PROFESSIONAL CHEF,** Planned, cooked, and presented gourmet meals for large events, restaurants, private clients, and intimate dinners. Collaborated with a variety of vendors and clients to bring their ideas to life.
- **OWNER & OPERATION,** GLOUCESTER GUIDED TOURS, Managed operations of themed walking tours in historical locations.

TECHNICAL PROFICIENCIES

Operating Systems:	Windows OS, Apple OS, Android OS
Software:	Jira, Confluence, Salesforce, SharePoint, Google Docs, Google Analytics, Exact Target, Microsoft Office Suite, Visio, Facebook Page Administration
Methodologies:	Agile, Scrum

EDUCATION AND CERTIFICATIONS

Maine College of Art, Portland, ME
Bachelor of Fine Art in Sculpture

Colby College, Waterville, ME
Bachelor of Arts in Psychology

Proficient in French, English, and Spanish

Attachment G – Resume – Meenah Atayee

MEENAH ATAYEE

1725 East Avenida De Las Flores, Thousand Oaks, CA 805-732-3074

PROFESSIONAL EXPERIENCE

mPulse Mobile, Encino, CA **National Account Executive**

meenahatayee@gmail.com

April 2018 - Present

● Manage portfolio of strategic enterprise healthcare and IDN accounts, encompassing ~1.5 million end users, serving as the strategic and primary contact for clients.

○ Notable Clients: Livongo (SF, CA), Kaiser Permanente National Marketing (Oakland, CA), KP Digital Notifications (Oakland, CA) and multiple KP regional business units (national).

- ● Responsible for leading overall design, implementation and deployment of omni-channel services for digital outreach, including: clinical SMS texting (appointment reminders, pre-surgery care, virtual video visits), custom member web portals (member benefit access) and email campaigns.
- ● Primary trainer for end users of mPulse Platform, leading on-site and remote training webinars for clients.
- ● Collaborate with Product and Client Success on API integrations and other specifications for program use cases, leading internal QC and client UAT, collaborating with product and engineering team to identify and resolve any issues prior to production launch.
- ● Analyze campaign and program outcomes post launch, developing and providing ongoing analytical insights to clients with actionable recommendations to increase engagement and drive desired behavior change (i.e improve HEDIS score measures, improve office visit no-show rates).
- ● Conduct quarterly on site client meetings with c-level and executive management to discuss strategic growth and assess retrospective use cases & program results.

Deep 6 AI, Pasadena, CA March 2017 - March 2018 **Director, Customer Success**

- ● Reported to the CEO with direct ownership of overseeing the implementation and strategic management of all accounts, leading the post sales process and maintaining ongoing client relationship, sustaining high user adoption and product engagement.
  - ○ Successfully launched pilot program across Cedars-Sinai Medical Center, resulting in a three-year enterprise-wide partnership for clinical trial recruitment.
  - ○ Launched first global client in Australia with three regional pilot sites.
- ● Responsible for leading weekly internal and external project management calls with clients,

vendors and internal teams. Conducted bi-weekly meetings with product, engineering and leadership to deliver user feedback and prioritize future features, conducting quality assurance on upcoming releases, escalating urgent bug fixes to engineering and ensuring minimal risks of new deployments.

- • Defined processes for remote and on-premise software implementation and customer support, optimizing cross department communication and troubleshooting.

Jiff (Castlight Health), Oakland, CA June 2016 - November 2016 **Customer Success Manager**

- • Served as primary point of contact/project manager for client, working with clients on-site and remotely from point of sale through lifetime of client, leading program scoping, product development, marketing and implementation/training of Jiff mobile and web application post initial launch.
- • Managed portfolio of six enterprise accounts across various industries including Fortune 500 clients, building and maintaining relationships with clients and their vendors through weekly calls, webinars and on-site visits to ensure successful deployment and integration of product.

• Responsible for measuring and tracking platform adoption and engagement post launch, working with clients to hit target KPIs, presenting reports to C-level executives and key stakeholders.

Augmedix, San Francisco, CA December 2013 - May 2016 **Senior Clinical Operations Special Projects Manager**

- • Responsible for managing and serving as Program Manager for global training operations at partner and vendor sites across India and Bangladesh, designing, implementing and maintaining operational training processes and curriculum for OUS clinical documentation specialists.
  - ○ Served as the function manager for first production facility in Dhaka, Bangladesh, collaborating with consultant group Ernst and Young for the recruitment and training of management and production staff.
  - ○ Six week trip to India in June 2015 oversee and evaluate training operations at sites in Bangalore and Chennai, performing workflow and compliance audits, organizing and leading on site workshops on best practices for training.
- • Responsible for owning all project plans, leading bi-weekly webinars and meetings with stakeholders, reviewing project milestones and flagging all potential project roadblocks, working with team to resolve any issues.
- • Developed operational metrics dashboard to map vendor staff performance against corporate goals and customer-driven KPIs. Provided visibility and insight into training quality, production headcounts and workforce utilization trends for strategic decision-making.

Lead, Training Management & Logistics September 2014 - March 2015

- • Created and implemented internal company-wide training protocols and policies including

HIPAA compliance and product training.

- • Designed and implemented ICD-10 training for all clinical documentation specialists
- • Revamped the EMR core training program for all incoming field employees as part of onboarding.

Implementation/Account Manager December 2013 - March 2015

- • Functioned as part of a 20-member startup team to manage the implementation of Augmedix platform of remote scribing through integration of Google Glass, servicing numerous independent and large healthcare systems including Dignity Medical Foundation, DaVita Healthcare (Albuquerque), and OC Podiatry.

- • Initiated baseline data gathering and workflow analysis at all sites, and closely coordinated with executive management and client representatives to integrate product with the client EHR, ensuring customized solution aligned with the design and operation of each clinical practice.

EDUCATION

California Lutheran University, Thousand Oaks, CA May 2012 Bachelors of Science in Biological Science

ADDITIONAL SKILLS

- • Highly Proficient in Salesforce CRM, Google Docs, Zendesk, Tableau, MS Excel, Google Analytics
- • Proficient in Business Process Improvement, Strategic Planning
- • Strong IT Project Management skills with proficiency in project management software (MS

Project, Smartsheets, Asana, and JIRA/Confluence)

- • Well versed in medical terminology and multiple EHR platforms including Epic, AllScripts,

Practice Fusion

Attachment H – Resume – Lidia Maruska

LIDIA MARUSKA

• LOS ANGELES, CA • LIDIAMARUSKA18@GMAIL.COM • (619)458-7718 • LINKED IN •

QUALIFICATIONS

Strong oral, written and interpersonal communication skills

Comfortable in prioritizing tasks at hand in a fast-paced organization

Passionate about making a difference in patient engagement in health/wellness

CLIA & HIPAA Compliant, with experience in EMR systems for patient demographic information

Over ten years of experience in customer service and working with and educating patients & clients

Knowledge of: *Microsoft Office, QuickBooks, SPSS, SalesForce, SQL, JIRA, Smartsheet, API integrations*

RELATED EXPERIENCE

mPulse Mobile, Encino, CA *June 2017 – Present*
Product Delivery Analyst → Client Success Manager – Team Lead

- Gather critical technical requirements for implementation of healthcare communication with patient members, ensuring success of product releases for clients
- Manage implementations by working with Product, Analytics and Account Management teams to ensure all solutions are rolled out effectively and efficiently (SmartSheet)
- Demonstrates knowledge of information technologies by communication through customer service, troubleshooting issues & gather essential details for ticketing system (JIRA)
- Identify and diagnose issues reported with client facing platforms & text messaging workflows by looking to the logs & database (SQL)
- Initiate, track and resolve analytics requests & support inquires
- Coordinate training & on boarding of new employees of the Client Success Team
- Provide leadership to a team of 8 Client Success Analysts & Client Success Managers through the implementation process: from the Plan/Design to the Support phase
- Recruit, evaluate and train Client Success employees & contribute to performance evaluations for CS team
- Facilitate collaborative meetings across various departments: Product, Analytics, Behavioral Science
- Build and maintain vital relationships with internal teams and external clients

LCMS Solutions, La Jolla, CA *March 2015 – March 2017*
Laboratory Support Analyst → Operations Coordinator

- Supporting clinical diagnostic laboratory operations: Customer Service, Sales, Financa, HR & Compliance
- Understanding of accounts payable & accounts receivable
- Compiling invoices into QuickBooks and daily reconciliation of multiple bank accounts
- Running monthly quires of physician representative accounts
- Collection of medical billing information for insurance, Medicare and Worker's Compensation
- Aiding Sales Manager in traveling to clients to teach collection protocol & updating of SalesForce accounts
- Creating and distributing marketing material to physician's offices and clinics
- Organization of specimen materials to be shipped out for collection
- Assisting HR with educating and enrolling employees on benefit plans
- Monitoring of employee timesheets and processing of bi-weekly payroll

Freeman Yoga, Fullerton, CA *April 2014 – May 2015*
Front Desk Receptionist

Be.group – Kirkwood Assisted Living, Orange, CA *August 2013 – December 2013*
Activities Coordinator Intern

Customer Service *2008 – 2015*
Nekter Juice Bar, Brea, CA *2014 – 2015*
CHOMPS Sushi Bar and Grill, Fullerton, CA *2012*

Pacific Coast Lemonade, Del Mar, CA	*2011-2013*
Closet Rapture, Del Mar, CA	*2010*

EDUCATION

California State University, Fullerton

Bachelor's Degree in Health Science	August 2011 – August 2015
Health Promotion and Disease Prevention	GPA – 3.5

Dean's List award

Selected Coursework

Integrative Health, Nutrition and Disease, Epidemiology, Measurements and Statistics of Health, Research Methods, Stress Management, Complementary Medicine and Alternative Healing Therapies, Anatomy and Physiology, Determinants of Health Behavior, Survey Chemistry Lab, Worksite Health Promotion, Health Promotion in Aging Populations

Attachment I – Project Plan / Timeline

COMMUNICATE USE CASE PLAN

Task Name	Duration
Design & Planning	10d
Planning	10d
Define use case objectives	3d
Gather requirements	3d
Confirm data transfer (CSV upload?)	1d
Create detailed scope, requirements, and project plan	2d
Review & approve project plan and Solution Document	1d
Design	10d
Message Content	10d
Create, design & document: Campaign message, 3 automatic responses, and triggers.	6d
Review & request changes	1d
Implement changes & return for approval	2d
Approve content & design	1d
Technical Solution	6d
Design technical solution (automation - events and audience updates)	2d
Update Solution Document	1d
Approve Solution Document	1d
Build	17d
Account setup	9d
Provision shortcode	1d
Create client platform account	1d
Create user accounts	1d
Client training	1d
Campaign content & testing	4d
Build campaign & set content	2d
Test triggers & message content	1d
Approval & sign off	1d
Execute	10d
Deliver	6d
Go-live planning with Client	2d
Go-live with test group (100 members)	1d
Confirm test group success	1d
Go-live with all members	1d
Monitor	5d
Closing - Review project	2d

ENGAGE USE CASE PLAN

Task	Duration
Planning and Design	**16d**
Planning - Project	**16d**
Discuss message goals, channels, content and content approval process along with any need for mPulse content creation help	1d
Confirm data file structure/headers and frequency/location of drop	1d
Discuss Report Requirements	1d
Create detailed scope and requirements and project timeline	4d
Review and approve project timeline and Solution Document	2d
Design - Message Content and Dialogues	**10d**
Design and document dialogue workflows, content, rules, ARs, preset messages, and events (template - Dialogues and message content)	5d
Review and request changes	1d
Implement Changes	1d
Approve dialogues and message content	1d
Design - Technical Solution	**4d**
Design - Technical Solution	3d
Document solution to include message placeholders (add Solution template)	1d
Review and Approve Solution Document	1d
Build	**23d**
Setup account	**14d**
Receive short code	1d
Provision and setup account	4d
Build - Message Dialogues and Content	**9d**
Build dialogues and content	5d
Test dialogues and content (mPulse QA)	3d
Test dialogues and content (mPulse with Client UAT)	1d
UAT - end to end testing of Automated File Pick-up and messaging	**4d**
API Integration	
Review high-level data flow - client's expectation of API integration	
Turn on APIs	1d
Turn on Callbacks	1d
Create API access key	1d
Test APIs	5d
Integrate APIs with systems (includes testing), if needed from Client	
Integration Testing, if needed by Client	
Execute	**16d**
Deliver	**6d**
Go Live Planning with Client	2d
Go-live with test group (less than 100 users)	1d
Confirm test group success	2d
Go-live with full group (all users)	1d

Monitoring - Reports and Review	5d
Post Implementation / Review	5d
Closing - Review of Project	**1d**

Attachment K – Solution Design

NEBRASKA

DEPT. OF HEALTH AND HUMAN SERVICES

Solution Design

Table of Contents

1 Background Information 19
1.1 DHHS .... Error! Bookmark not defined.
1.2 Business Goals 19
1.3 December 2017 Press Release .... Error! Bookmark not defined.
2 Solution Methodology 21
2.1 Use Case 21
2.2 Member Experience 21
2.3 Business Logic 21
2.4 Dialogs 21
2.5 Data 21
2.6 API 21
3 Solution Overview 22
3.1 mPulse Engagement Console 23
3.1.1 User Access 23
3.2 Messaging Limitations 23
3.2.1 Common Limitations 23
3.2.2 CSV Limitations 23
3.3 Data Integration: Batch (CSV) Integration 23
3.3.1 CSV File Format and Fields 23
3.3.2 SFTP / File Transfer Details 23
3.3.3 mPulse File Processing 23
3.3.4 mPulse Return File 23
3.4 API Integration 23
3.4.1 Assumptions 23
3.4.2 mPulse API Overview 23
3.4.3 API flow for Use Case 1 23
3.4.4 Event Upload API to For Use Case 1 24
3.5 Reporting 27
4 Project Management 27
4.1 Project Tracking Milestones 27
4.2 Project Timeline 27
4.3 Project Teams 28
4.3.1 DHHS Team 28
4.3.2 mPulse Team 28
4.4 Training 28

1 Background Information

1.1 Nebraska DHHS

1.2 Business Goals

2 Project Environment

[redacted]**PROJECT ENVIRONMENT**

The State is soliciting bids for a solution to meet the needs of the Nebraska DHHS. DHHS divisions that will initially use texting comprise of Children and Family Services (CFS), Public Health (PH), and Medicaid and Long Term Care (MLTC). In the future, other DHHS divisions and/or programs may utilize the texting solution.

1. The initial programs include the following and may include several sub-programs:

   a. **CFS – Economic Assistance:** Economic Assistance programs include Supplemental Nutrition Assistance Program (SNAP), Employment First, Aid to Dependent Children, Refugee Resettlement, Energy Assistance, Child Care Subsidy, Aged, Blind, and Disabled as well as Social Services for Aged and Disabled.

   b. **CFS – Protection and Safety:** Child Welfare and Adult Protective and Safety services include prevention activities and coordination, child and adult protective services, foster care and independent living, adoption, domestic violence, safety and treatment services, and educational initiatives.

   c. **CFS – Child Support Enforcement (CSE):** Child Support Enforcement is a family-first program intended to ensure families' self-sufficiency. The program goals are to ensure that children have the financial and medical support of both their parents; to foster responsible behavior towards children; and to emphasize that children need both parents involved in their lives.

   d. **PH - Women, Infants, and Children (WIC):** WIC provides healthy foods, nutrition, and breastfeeding education and support, and referrals to community services for eligible pregnant breastfeeding and postpartum women and infants and children up to age 5. Provides breastfeeding peer counseling services to pregnant and postpartum women.

   e. **PH – Newborn Screening (NNSP)** - The Nebraska Newborn Screening Program includes bloodspot screening for inherited and congenital infant and childhood onset diseases.

   f. **PH - Early Hearing Detection and Intervention Program (EHDI)** - Program for newborn hearing screening.

   g. **PH – Metabolic Food Program** – Program provides reimbursement for purchase of foods for Nebraska residents who have been diagnosed with a metabolic disease and require pharmaceutically manufactured metabolic foods for dietary treatment or to prevent significant illness or disability related to the metabolic disease.

   h. **Medicaid and Long Term Care:** The Division of Medicaid and Long-Term Care (MLTC) oversees the Nebraska Medicaid program, home and community services for the elderly and persons with disabilities, and the State Unit on Aging.

2. Initial usage for text messaging is planned for various client events/transactions including but not limited to: interview reminders, verification and review/recertification due reminders, renewals, notifications when correspondence is available on the client's account, daily appointment

reminders, daily missed appointment notifications, monthly messages to pre-identified participants such as certification end dates and food benefits pick-up, ad hoc messaging, emergency alerts or closed clinic messages sent within sixty 60 minutes of generation of the ad hoc messages.

Annual usage figures provided are estimates and are not to be construed as either a minimum or maximum text quantity. Contractor must not impose minimum text quantity requirements. The estimated number of text messages per month for the first year is expected to be approximately 105,000 for Economic Assistance, 45,000 for Protection and Safety, 54,000 for Child Support, 25,000 for WIC, 4,000 for other Public Health programs, 50,000 for Medicaid. This accounts for an estimated DHHS monthly total of 283,000 texts for the month and 3,400,000 texts per year.

3. Initial State backend Applications include:

   a. **N-FOCUS (Nebraska Family Online Client User System)** – a system that automates benefit/service delivery and case management for more than 30 Nebraska Department of Health and Human Services (DHHS) programs, including Child Welfare, Aid to Dependent Children, Supplemental Nutrition Assistance Program, and Medicaid

   b. **CHARTS (Children Have A Right To Support)** - a system used to maintain and enforce Nebraska Child Support

   c. **JOURNEY** – a system used to manage and deliver benefits and services for the DHHS WIC program and thirteen local WIC agencies

   d. **Other Backend Systems** – Information may be retrieved from other systems to handle the Newborn Screening, Early Hearing Detection, and Metabolic Food Program.

4. The solution must be compatible with the following interfaces:

   a. **API/Web Service Interface**
   Text messaging requests will be originated from the backend state applications and must be communicated to the texting solution via secure API/web service. Source information such as cell phone numbers and messages will be originated and stored in DHHS application data outside of the texting solution and sent to the texting solution. Status of the texting results and text responses must be communicated from the texting solution back to the State Applications via secure API/web service.

   b. **SFTP Interface**
   Text messaging requests will be originated from either a backend state application or DHHS user and sent via Secure File Transfer Protocol (SFTP), The texting request information will be in a predefined format contained in a file type of XML (Extensible Markup Language), JSON (JavaScript Object Notation), and CSV (Comma-separated Value) and must be transferred via SFTP to the texting solution. Texting results and responses must be available to the State Application or user via the same method.

   c. **Web Portal Interface**
   The texting solution must provide a secured web front end for designated staff to enter cell phone numbers, create text messages, and perform any administration or management of texting features. It must also allow manual upload of texting files and download of the texting results and responses via the web interface.

   d. **Data and Statistics**
   The texting solution must provide access to data and statistical information for reporting via a secured web front end. The solution must allow exporting and transferring of the data and statistical information in XML and CSV file formats via SFTP.

3 Solution Methodology

3.1 Use Case

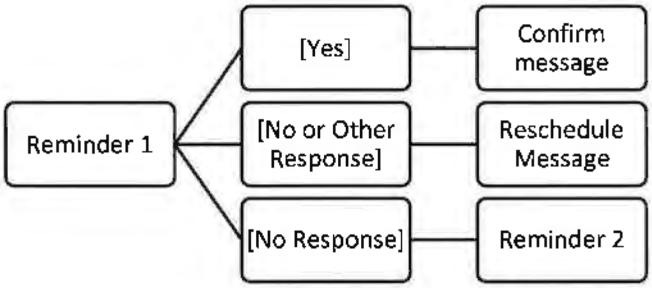
The use case description is the first step to implementing a solution for DHHS. The use-case is used to identify, clarify and organize solution requirements and includes a definition of a goal and the high-level interactions between members and DHHS to achieve that goal.

3.2 Member Experience

It is recommended that the member experience be defined early in the process. The desired member experience will drive business logic and dialogs and the required data elements.

3.3 Business Logic

Business logic will be defined in both the DHHS and mPulse Mobile platforms and will vary by use-case. The business logic will drive dialogs and data mappings.



3.4 Dialogs

Once the use-case, member experience and business logic have been defined, mPulse Mobile will work with DHHS to define the dialogs and message flows to be built in the mPulse Mobile platform.

3.5 Data

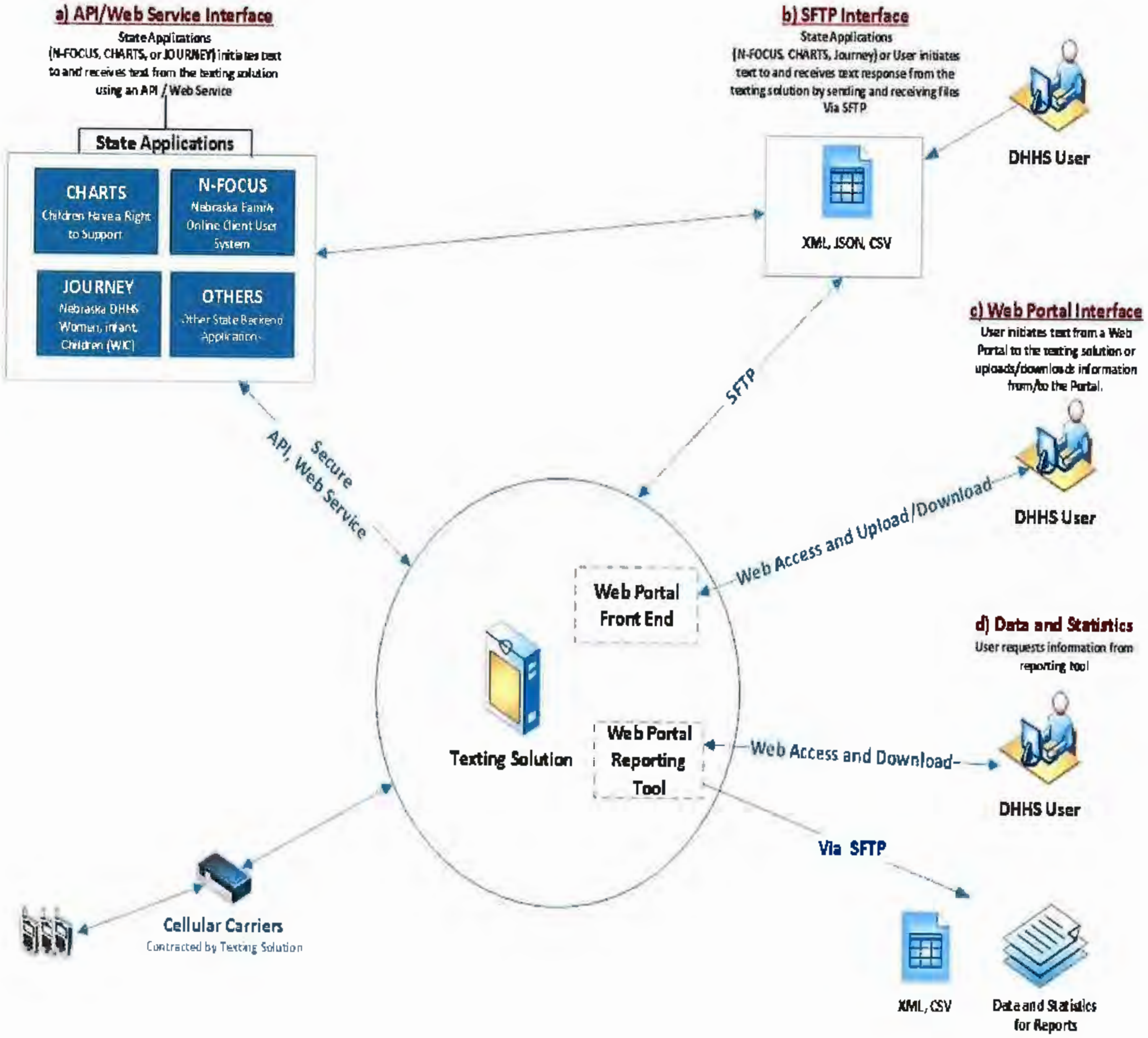
Data to support the dialogs is used for three purposes in the mPulse Mobile platform:

1. Identification – An email, mobile number or a member ID can be used to identify the message recipient.
2. Personalization – Member first name and other personal information can be included to personalize the message.
3. Segmentation – Member attributes can be used to segment workflows. For example, you may want dialogs to members over 60 years old to be defined differently than a dialog for members under 30.

3.6 API

The appropriate API calls and/or file-transfers are defined once the data and dialogs have been finalized.

4 Solution Overview



a) API/Web Service Interface
State Applications
(N-FOCUS, CHARTS, or JOURNEY) initiates text to and receives text from the texting solution using an API / Web Service

b) SFTP Interface
State Applications
(N-FOCUS, CHARTS, Journey) or User initiates text to and receives text response from the texting solution by sending and receiving files Via SFTP

c) Web Portal Interface
User initiates text from a Web Portal to the texting solution or uploads/downloads information from/to the Portal.

d) Data and Statistics
User requests information from reporting tool

State Applications
CHARTS
Children Have a Right to Support
N-FOCUS
Nebraska Family Online Client User System
JOURNEY
Nebraska DHHS Women, Infant, Children (WIC)
OTHERS
Other State Backend Applications
XML, JSON, CSV
DHHS User
SFTP
Secure API, Web Service
Web Access and Upload/Download
DHHS User
Web Portal Front End
Texting Solution
Web Portal Reporting Tool
Web Access and Download
DHHS User
Via SFTP
XML, CSV
Data and Statistics for Reports
Cellular Carriers
Contracted by Texting Solution

4.1 mPulse Engagement Console

4.1.1 User Access

4.2 Messaging Limitations

4.2.1 Common Limitations

4.2.2 CSV Limitations

4.3 Data Integration: Batch (CSV) Integration

4.3.1 CSV File Format and Fields

4.3.2 SFTP / File Transfer Details

SFTP Location	
Authorization	
Folder/Filename	
Time & Frequency	

4.3.3 mPulse File Processing

4.3.4 mPulse Return File

4.4 API Integration

4.4.1 Assumptions

4.4.2 mPulse API Overview

mPulse recommends using the following core APIs to support all use cases described.

Event Upload API	This API can be used to transmit one or more transactions related to a member. The Event Upload API can also be used for cancellation of an appointment reminder.
Audience API	This API allows mPulse clients to add and subscribe members to the platform that are part of a program to receive messages. Only members with a valid contact address (mobile number), will be accepted. All member profile information can be added and updated using this API. When a List is provided, the member is automatically subscribed unless they are previously unsubscribed. *mPulse does support overriding unsubscription status if required using the Audience API.*

4.4.3 API flow for Use Case 1

4.4.4 Event Upload API to For Use Case 1

Event Upload Request URL

Request Method	POST
Prod Request URL	https://ms-api.mpulsemobile.com/account/1257/uploadEvent

Event Upload Request Headers

Header	Required	Description
X-Ms-Format	Yes	Value must be “xml”.
X-Ms-Source	Yes	Value must be “api”.
Authorization	Yes	Value must be “Basic base64_encode({API_USERNAME}:{API_PASSWORD})”.
X-Ms-API-Version	Yes	Value must be “2.0”.
X-Ms-Verbosity	No	Value can be “simple” or “full”. If this header is not included, default value is “simple”. Sample API responses provided below using Full Verbosity.

Event Upload Request Body (Per API Request)

XML Tag	Batch File CSV Field Name	Notes
list_id	Parent level tag	*Specify list ID here*
events *Attributes*: name=”xxx”		

NOTE: XML is case-sensitive. I

Sample Request Body

```
<body>
  <listid>2960</listid>
  <events name="send_non_hbo_reminder">
    <event scheduled_on="+00:00" timezone="US/Pacific" evaluation_scope="no_rule">
      <client_member_id>lee_mrn</client_member_id>
      <correlationid>lee_appt_101</correlationid>
      <first_name>Lee</first_name>
      <appt_schedule_time>2018-01-08 22:40</appt_schedule_time>
      <appt_weekday_value>0</appt_weekday_value>
      <visit_date>2018-01-07</visit_date>
      <visit_time>2:40 PM</visit_time>
      <facility>Tallahassee Memorial Hospital Wound Care Center</facility>
      <facility_phone>555-555-5555</facility_phone>
    </event>
  </events>
</body>
```

Sample Successful Response:

```
<body>
  <results>
    <processed_event_instances>1</processed_event_instances>
    <scheduled_messages>1</scheduled_messages>
    <errors>0</errors>
    <details>
      <listid>2960</listid>
      <events event_definition_id="1240" event_definition_name="send_non_hbo_reminder">
        <event event_instance_request_index="0" correlationid="lee_appt_101"
memberid="12748419">
          <event_instance_body>
            <![CDATA[<body><event scheduled_on="+00:00" timezone="US/Pacific"
evaluation_scope="no_rule"><client_member_id>lee_mrn</client_member_id><correlationid>lee_appt_
101</correlationid><first_name>Lee</first_name><appt_schedule_time>2018-01-08
22:40</appt_schedule_time><appt_weekday_value>0</appt_weekday_value><visit_date>2018-01-
07</visit_date><visit_time>2:40 PM</visit_time><facility>Tallahassee Memorial Hospital Wound Care
Center</facility><facility_phone>555-555-5555</facility_phone></event></body>]]>
        </event_instance_body>
        <event_instance_id>13370229</event_instance_id>
        <scheduled_messages>
          <scheduled_message>
            <dialogue_id>243</dialogue_id>
            <scheduled_datetime>2018-01-06 03:42:00+00:00</scheduled_datetime>
          </scheduled_message>
        </scheduled_messages>
        <errors></errors>
      </event>
    </events>
  </details>
</results>
</body>
```

Sample Failed Response (member does not exist):

```
<body>
  <results>
    <processed_event_instances>1</processed_event_instances>
    <scheduled_messages>0</scheduled_messages>
    <errors>1</errors>
    <details>
      <listid>2960</listid>
      <events event_definition_id="1240" event_definition_name="send_non_hbo_reminder">
        <event event_instance_request_index="0" correlationid="lee_appt_101" memberid="None">
          <event_instance_body>
            <![CDATA[<body><event scheduled_on="+00:00" timezone="US/Pacific"
evaluation_scope="no_rule"><client_member_id>mrn000000</client_member_id><correlationid>lee_ap
pt_101</correlationid><first_name>Lee</first_name><appt_schedule_time>2018-01-08
22:40</appt_schedule_time><appt_weekday_value>0</appt_weekday_value><visit_date>2018-01-
07</visit_date><visit_time>2:40 PM</visit_time><facility>Tallahassee Memorial Hospital Wound Care
Center</facility><facility_phone>555-555-5555</facility_phone></event></body>]]>
            </event_instance_body>
            <scheduled_messages></scheduled_messages>
            <errors>
               <error>
                  <error_message>The member in the event instance is either null or is not a
valid member.</error_message>
                  <error_code>ERR-EVENT-008</error_code>
               </error>
            </errors>
         </event>
      </events>
   </details>
</results>
</body>
```

Audience API to Add and Subscribe Patients

Audience Request URL

Request Method	POST
Prod Request URL	https://ms-api.mpulsemobile.com/accounts/1257/members

Audience Request Headers

X-Ms-Format	Yes	Value must be "xml".
X-Ms-Source	Yes	Value must be "api".
Authorization	Yes	Value must be "Basic base64_encode({API_USERNAME}:{API_PASSWORD})".

Audience Request Body Details

Note: XML attributes are case sensitive

XML Tag	CSV Field Name	Notes
mobilephone	PatientPhone,PatientSecPhone	Provide comma-separated phone numbers in the order that you need to attempt to upload.
firstname	PatientFName	Proper casing preferred, as this value will be displayed in EC-2 console.

lastname	PatientLName	Proper casing preferred, as this value will be displayed in EC-2 console.

Sample Audience Request Body

```
<body>
        <listid>2960</listid>
        <member>
                <clientmemberid>patient_mrn</clientmemberid>
                <mobilephone>16194587718</mobilephone>
                <firstname>Jane</firstname>
                <lastname>Doe</lastname>
                <facility>Tallahassee Memorial Hospital Wound Care Center</facility>
                <facility_phone>333-333-3333</facility_phone>
        </member>
</body>
```

4.5 Reporting

5 Project Management

This section provides information on the project management methodology that mPulse will use to manage the API integration

5.1 Project Tracking Milestones

5.2 Project Timeline

Detailed tasks and dates are outlined in Rollout Plan Smart sheet

5.3 Project Teams

5.3.1 DHHS Team

Name	Role	Email

5.3.2 mPulse Team

Name	Role	Email

5.4 Training

Attachment 1

Attachment 1

mPulse Mobile's Functional Business/Technical Requirements Traceability Matrix

Request for Proposal Number 6111 Z1

Bidders are instructed to complete a Functional Business/Technical Requirements Traceability Matrix for RFP 6111 Z1 Text Messaging Solution. Bidders are required to describe in detail how their proposed solution meets the conformance specification outlined within each Functional Business/Technical Requirement.

The Traceability Matrix is used to document and track the project requirements from the proposal through testing to verify that the requirement has been completely fulfilled. The awarded Contractor will be responsible for maintaining the contract set of baseline requirements. The Traceability Matrix will form one of the key artifacts required for testing and validation that each requirement has been complied with (i.e., 100% fulfilled).

The Traceability Matrix should indicate how the bidder intends to comply with the requirement and the effort required to achieve that compliance. It is not sufficient for the bidder to simply state that it intends to meet the requirements of the RFP. DHHS will consider any such response to the requirements in this RFP to be non-responsive. The narrative should provide DHHS with sufficient information to differentiate the bidder's technical solution from other bidders' solutions.

The bidder must ensure that the original requirement identifier and requirement description are maintained in the Traceability Matrix as provided by DHHS. Failure to maintain these elements may be grounds for disqualification.

How to complete the Traceability Matrix:

Column Description	Bidder Responsibility
Req #	The unique identifier for the requirement as assigned by DHHS, followed by the specific requirement number. This column is dictated by this RFP and must not be modified by the bidder.
Requirement	The statement of the requirement to which the bidder should respond. This column is dictated by the RFP and must not be modified by the bidder.
(1) Comply	The bidder should insert an "X" if the bidder's proposed solution complies with the requirement. The bidder should leave blank if the bidder's proposed solution does not comply with the requirement. If left blank, the bidder should also address the following: • Capability does not currently exist in the proposed system, but is planned in the near future (within the next few months) • Capability not available, is not planned, or requires extensive source-code design and customization to be considered part of the bidder's standard capability • Requires an extensive integration effort of more than 500 hours
(a) Core	The bidder should insert an "X" if the requirement is met by existing capabilities of the core system or with minor modifications to existing functionality.
(b) Custom	The bidder should insert an "X" if the bidder proposes to custom develop the capability to meet this requirement. Indicate "custom" for those features that require substantial or "from the ground up" development efforts.

Column Description	Bidder Responsibility
(c) 3rd Party	The bidder should insert an "X" if the bidder proposed to meet this requirement using a 3rd party component or product (e.g., a COTS bidder, or other 3rd party). The bidder should describe the product, including product name, its functionality and benefits in their response.

Introduction

The State realizes that not all of the requirements stated in this specification may be in the bidder's solution. While it is hoped that many of the functions and tasks are available, the State encourages bidders to note any modifications necessary to provide the functions required in this specification, and to meet the design needs of the system.

Texting Software Functional Business/Technical Requirements

The functional requirements listed below are those that DHHS staff deem essential. Bidders should note if their application meets each specific requirement, and describe how their software will meet each requirement. Bidders should also define and describe any additional functionality available in their software, beyond what is listed in the functional requirements.

Each requirement is identified by the following first three characters:

GEN	General System Requirements
TXT	Texting System Requirements
RPT	Reporting Requirements
DBM	Database/Data Management Requirements
TEC	General Technical Requirements
ERR	Error Handling Requirements
BKP	Backup and System Recovery Requirements
SEC	Security Requirements
DOC	System and User Documentation
TRN	Training
PTT	Production, Test and Training Requirements
PER	System Performance Requirements

General System Requirements

This section represents the overall business requirements that apply to the software. Describe in the response how the proposed solution meets the requirement.

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
GEN-1	Describe overall functionality of the bidder's Short Messaging Service (SMS) Texting solution. Provide a description and diagram of the solution including the architecture, hardware, and software, including location of the solution (cloud solution, vendor site, host site, etc).	X	X		

Response:

mPulse Mobile is an enterprise-class cloud Communication Platform that delivers communications over SMS, Email, Push Notifications, Secure Messaging and Interactive Voice Response channels. The platform supports high-volume message delivery for healthcare clients with populations over ten million.

The platform is compliant for HIPAA 45 CFR Parts 1260, 162 and 164, in conjunction with NIST 800-53. The mPulse Mobile service is hosted exclusively in US-based SOC-II compliant Amazon AWS datacenters. All data at rest and motion is encrypted with AES-256/CBC. Data and production access is restricted by role, and limited to US-based employees only.

Language preferences: All international languages are supported by using the UCS-2 messaging template. Additionally, mPulse Mobile SMS channel supports a 450-character limit (standard SMS messages have a 160-character limit) by leveraging segmentation support available in most mobile devices. The larger message limit accommodates greater character usage by international languages.

Communication Channel preferences: Channel preferences are stored and managed at the individual consumer level. The consumer preferred channel is used whenever multiple channels can be used to deliver campaign content e.g. Appointment Reminders.

Campaign Opt-out preferences: Content areas are organized by campaigns. Consumer subscriptions to campaigns are managed to meet TCPA regulatory requirements. All TCPA-required Opt-out messages are supported, and the individual consumer campaign subscription profiles are updated automatically. Do-Not-Spam and Global Permanent Removal lists are maintained to ensure strict compliance at the short code or email account level.

At the Communicate Layer mPulse Mobile's platform delivers 1-way messages, notifications and compliance related response handling. A suite of trigger options can be configured to support a wide range of use cases e.g. time, date, recurrence and consumer profile change. In addition, messages can be triggered by highly configurable API-based customer triggers.

mPulse Mobile's platform documents all core delivery metrics by channel with real-time and asynchronous call-backs supported.

mPulse Mobile's Engagement Layer contains the Engagement Engine which runs automated SMS dialogues for large consumer populations. 2-way interactions are significantly more engaging for consumers, uncover powerful insights about them, and can be used to solve specific business problems.

Automated dialogues are 2-way messaging flows that employ rules and microservices (such as domain specific Natural Language Understanding (NLU), sentiment analysis and solution-based services e.g. AIR QUALITY, URGENT keyword text-ins) to intelligently respond to consumers' responses in real-time. mPulse Mobile's proprietary Engagement Engine is the core technology that powers the dialogues. The engine maintains the context of a consumer interaction to support branching logic based on user responses. The Engagement Engine also supports concurrent dialogues with the same member using prioritization algorithms. Furthermore, integration to the Engagement Engine allows clients to register callbacks at critical states within the dialogue. These callbacks provide the full context of the entire dialogue containing all messages sent and received.

mPulse Mobile has over 20 health topic-based NLU services. Consumer responses to specific open-ended questions can be interpreted automatically and used to determine the next action. Natural response handling can be incorporated into branching logic workflows to drive specific business outcomes. Additionally, mPulse Mobile incorporates NLU into conversational agent-based solutions for specific consumer health engagement challenges.

mPulse Mobile uses sentiment analyzers to assess consumer response to messaging programs at the individual consumer and population level. Responses are interpreted in relation to specific topic domains using a combination of machine learning and lexicon-based recognition. Sentiment analysis has proven to be an effective input for tailoring content to individuals, as well as uncovering strategic insights about consumer health beliefs.

mPulse Mobile's Engagement Console is a secure browser-based user interface that mPulse Mobile customers use to manage mobile engagement with their members. The console allows customer staff to view communication history at the individual level. Manual 1:1 interactions can be quickly initiated to take advantage of the consumer convenience of SMS or other communication channels. Customer staff can also launch automated dialogues, which has broad applications across Care Management, Health Coaching and Call Center functions.

Please see the attached *mPulseMobile Platform Architecture_mPulse.pdf* for more detail.

<table>
<tr><th>Req #</th><th>Requirement</th><th>(1)
Comply</th><th>(a)
Core</th><th>(b)
Custom</th><th>(c)
3rd Party</th></tr>
<tr><td colspan="6"></td></tr>
<tr><td>GEN-2</td><td>Describe the bidder's connectivity and relationship to Wireless Service Providers (Carriers). Include how the proposed solution handles message content, delivery scheduling, and message routing services via multiple cellular network carriers/vendors. Include a list of your current Carriers and any known gaps in coverage in the State of Nebraska.</td><td>X</td><td>X</td><td></td><td></td></tr>
<tr><td colspan="6">Response:
All SMS messages are delivered through mGage, the SMS aggregator that mPulse Mobile has been partnering with for over ten years. mGage offers connectivity to all of the major carriers in Nebraska (Verizon, AT&T, T-Mobile, Sprint) as well as Mobile Virtual Network Operators (MVNOs) such as Cricket Wireless, TracFone, Boost Mobile, MetroPCS, Straight Talk and others.</td></tr>
<tr><td>GEN-3</td><td>The bidder's solution must have the ability to interface with DHHS backend applications (NFOCUS, CHARTS, JOURNEY, and other identified systems) via API/ web service. DHHS will be managing the phone numbers and text messages within the DHHS applications and providing data to the texting solution. In return the texting solution must provide data (results and responses) back to the DHHS applications via the same method. Describe how your solution meets this requirement.</td><td>X</td><td>X</td><td></td><td></td></tr>
</table>

Response:

mPulse Mobile has system interfaces in-place with each of our customers.

The mPulse Mobile platform is configurable and built for interfacing with Nebraska DHHS through automated SFTP and web-based API. Please see the attached *mPulse Mobile - Integration and Security Overview v. 1.4.0 .pdf* for details. Furthermore, mPulse Mobile can provide specific development and custom API endpoints as needed to meet Nebraska DHHS needs as services for additional costs.

The mPulse Mobile Audience API allows you to manage your Member population with the following supported actions:

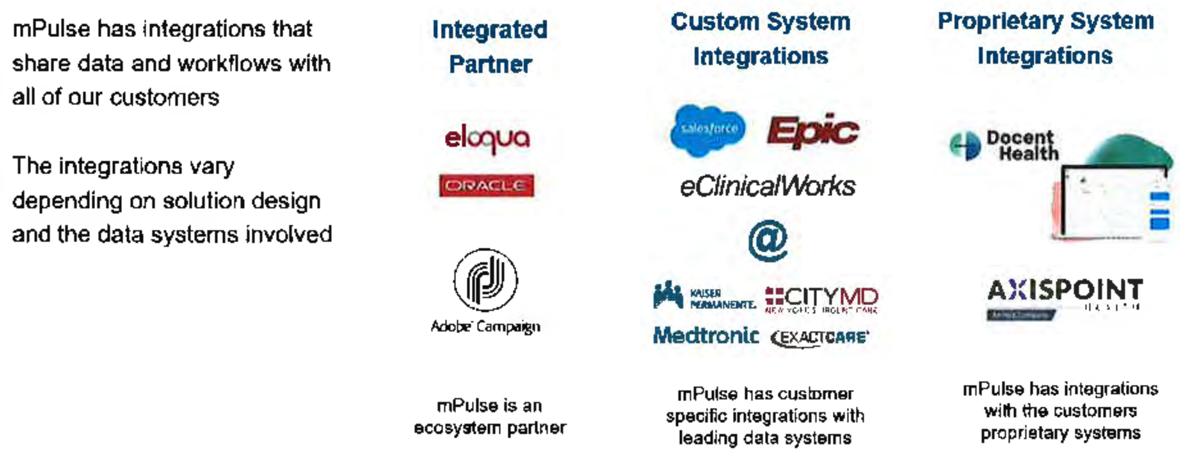
- Add
- Update
- Subscribe
- Resubscribe
- Unsubscribe
- Get information
- Delete

The Event Upload API is used to send messages or start dialogues. Either can be scheduled immediately, relative to the time the request is made, or for a specific date and time.

Callbacks allow you to sync updates to the mPulse Mobile platform database (i.e., events) with your database in real-time. mPulse provides callbacks for the following events:

- SMS responses (i.e., MOs)
- Subscriptions (all channels)
- Unsubscriptions (all channels)
- Link clicks (Email and Secure Message)
- Bounced messages (SMS and Email)
- Opened messages (Email, Secure Message, and Push)

The attached *mPulseMobile - Tech and Data.pdf* presents additional details and illustrations related to integrations.


mPulse has integrations that share data and workflows with all of our customers

The integrations vary depending on solution design and the data systems involved

Integrated Partner

mPulse is an ecosystem partner

Custom System Integrations

mPulse has customer specific integrations with leading data systems

Proprietary System Integrations

mPulse has integrations with the customers proprietary systems

GEN-4	The bidder's solution must provide an SFTP interface to allow text messaging requests from DHHS via a XML(Extensible Markup Language), JSON (JavaScript Object Notation), and CSV (Comma-separated Value) files. In return, the texting solution must provide a file with data (results and responses) back to DHHS via the same method. Describe how your solution meets this requirement.	X	X		

Response:

Events are used to trigger dialogues which can include multiple messages, responses and branches. In addition to the web API, automated SFTP is supported. Uploaded files may be JSON, XML or SFTP.

The following will occur when a file is uploaded from a source system:

1. The file format will be validated
2. Member information will be added / updated
3. Events will be scheduled
4. Log data will be written that includes any exceptions
   a. Members that could not be added/updated
   b. Invalid phone numbers

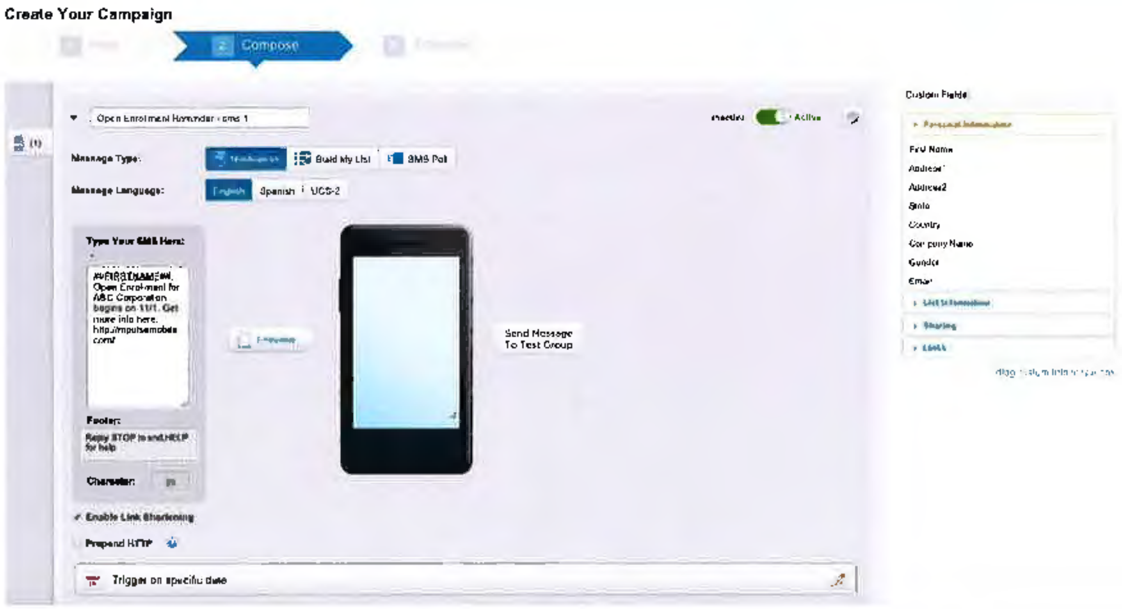
GEN-5	The bidder's solution must provide a secured, front-end Web Portal for the texting system. DHHS requires a front-end, web based system with an easy-to-use portal for authorized staff to create text messages, define receiving groups, define settings, and view or query information for reporting. The portal must also allow manual upload of texting files and download of the texting results and responses. Describe how the bidder meets the requirement. Please submit screenshots and descriptions of your solutions front end portal.	X	X		

Response:

The mPulse mobile Control Panel (CP) is a web-based portal that can be used to can manage Members, Communications, and your Account. The control panel is used to create messages and workflows to communicate with members and monitor how those campaigns are performing.

The Control Panel is a front-end, web based system with an easy-to-use portal for authorized staff to create text messages, define receiving groups, define settings, and view or query information for reporting. The control panel also allows manual upload of texting files and download of the texting results and responses.

Please see the attached *mPulse Platform Control Panel User Guide.pdf* for Control Panel details and screenshots.



Open Enrolment Reminder - sms 1

#FIRSTNAME#, Open Enrolment for ABC Corporation begins on 11/1. Get more info here. http://mpulsemobile.com/

Reply STOP to end,HELP for help

GEN-6	Describe how the bidder's proposed solution has the capability to notify DHHS staff if an interface is not available for any reason.	X	X		

Response: MPulse Mobile uses PagerDuty to intelligently alert mPulse Mobile personnel whenever an outage or degraded service is reported by the aggregator or observed within our systems. Our incident response and SLA details can be found in the attached *Incident Response Policy v1.3 (Signed).pdf* and *mPulse_SLA.pdf.*					
GEN-7	Describe any Federal and/or State entities that are currently using the bidder's solution(s) and how the solution is used by the entity.	X	X		
Response: mPulse Mobile works with a number of government entities and partnerships to deliver engagement solutions, including: - Delaware Health Information Network – Support for the Health Information Exchange's Community Health Record product - Cook County Care (IL) – Medicaid member engagement to close gaps in care, navigate benefits, and renew coverage - Pequot Health Care – Tribal health plan member engagement, plan navigation, wellness check reminders, and gaps in care closure					
GEN-8	Describe how the bidder's solution complies with regulations – TCPA (Telephone Consumer Protection Act), FCC (Federal Communications Commission), FTC (Federal Trade Commission), MMA (Mobile Marketing Association), and CTIA (Cellular Telecommunications Industrial Association).	X	X		
Response: Healthcare mobile messaging is primarily subject to three areas of regulation and oversight: 1) the Telephone Consumer Protection Act (TCPA), enforced by the Federal Communications Commission (FCC); 2) the Health Insurance Portability and Accountability Act of 1996 (HIPAA); and 3) wireless carrier industry standards, codified and enforced by The Wireless Association (CTIA). mPulse Mobile has a broad range of proven approaches to enroll healthcare consumers in text messaging programs that are TCPA, FCC, FTC, MMA and CTIA compliant. mPulse leverages its decade-long experience in health engagement to help our 90+ clients determine the most impactful opt-in strategy for their business and consumer needs. Please see the attached *Essential Guidebook for Healthcare Mobile Messaging.pdf* and*TCPA Policy 2018 Rev 1.3.pdf* for complete details.					
GEN-9	Describe any system or user customization preferences available with the bidder's proposed solution.	X	X		

Response:

The mPulse Mobile platform is configurable and built for interfacing with DHHS systems. Please see the attached *mPulse Mobile - Integration and Security Overview.pdf* for details. Furthermore, mPulse Mobile can provide specific development and custom API endpoints as needed to meet DHHS needs as services for additional costs.

For Text Message/SMS – The ability to customize text message communications, in mPulse technology offering, exists in two broad categories – individual level customization and group level customization. Following are the drivers of this customization:

Member Profile – Data in member profile is used in two ways. (A) Any field in a member's profile can be added with in the body of the message to customize messages. For example, the token ##first.name##, is used to include member's first name to personalize the message before it is sent to the member's phone number. (B) Certain profile fields becomes triggers for message customization. For example gender and age fields are used to customize messages, say for mammograms to women or prostate cancer examinations to men. Similarly, language preference is used to customize messages to members preferred language.

Event – An event is used to trigger a message specifically when certain condition are met for a member. For example, an appointment reminder or a medication reminder message will be sent to a member and only to that member, when their specific appointment is coming up or it's time for their medication, respectively .

Real-time customization based on Member Reponses – (A) Messages are customized on the basis of the messages texted back by the member. For example, in response to a poll about barriers to medication adherence, the sent messages are customized based on the member response to the poll query. Additionally, lack of response (engagement) by the member is an event in mPulse platform and leads to communication customized to that. (B) Messages texted in by the members are assigned sentiment scores based on the content of the messages and the responses from mPulse are customized based on the sentiment score.

Social determinants – When social determinants data is available for a specific population, communications are customized at group level based to those values. For example, for a Medicaid population, the messages are customized by health literacy level or for a population in a zip code without access to public recreation spaces, messages might be customized to indoor exercising tips.

Member Profile – Data in member profile is used in two ways. (A) Any field in a member's profile can be added with in the body of the PN message to customize messages. (B) Profile fields can also be leveraged as triggers for message customization.

The Communication layer is where all consumer communication information is managed, which includes preference management and campaign subscriptions. Preferences are managed and documented for language, communication channels and campaign opt-outs:

Language preferences: All international languages are supported by using the UCS-2 messaging template. Additionally, mPulse Mobile SMS channel supports a 450-character limit (standard SMS messages have a 160-character limit) by leveraging segmentation support available in most mobile devices. The larger message limit accommodates greater character usage by international languages.

Communication Channel preferences: Channel preferences are stored and managed at the individual consumer level. The consumer preferred channel is used whenever multiple channels can be used to deliver campaign content e.g. Appointment Reminders.

Campaign Opt-out preferences: Content areas are organized by campaigns. Consumer subscriptions to campaigns are managed to meet TCPA regulatory requirements. All TCPA-required Opt-out messages are supported, and the individual consumer campaign subscription profiles are updated automatically. Do-Not-Spam and Global Permanent Removal lists are maintained to ensure strict compliance at the short code or email account level.

At the Communicate Layer mPulse Mobile's platform delivers 1-way messages, notifications and compliance related response handling. A suite of trigger options can be configured to support a wide range of use cases e.g. time, date, recurrence and consumer profile change. In addition, messages can be triggered by highly configurable API-based customer triggers.

mPulse Mobile's Communicate Layer documents all core delivery metrics by channel with real-time and asynchronous call-backs supported.

<table>
<tr><td colspan="6">Please see the attached <i>mPulse Platform Control Panel User Guide.pdf</i> for more details on customization and preferences.</td></tr>
<tr><td>GEN-10</td><td>Describe the customer support availability and process for obtaining help from the bidder's proposed solution. For example, Help Desk, live chat, knowledge base, FAQs, video tutorials, etc. Include the hours that customer support is available.</td><td>X</td><td>X</td><td></td><td></td></tr>
<tr><td colspan="6">Response:
Details around SLA and escalation procedures can be found in the attached <i>mPulse_SLA.pdf</i>. An account manager and customer success manager will be assigned to DHHS to manage escalations. Live chat, knowledge base, FAQs and video tutorials may be developed as needed and support hours can be adjusted to meet DHHS requirements.</td></tr>
<tr><td>GEN-11</td><td>Describe the software licensing model of the solution, including any required third party licensing. Include a description of setup, a general description of what is included with the "base" product, system components or "extras". Describe if short codes are included with the bidder's proposed solution. Describe how the Bidder maintains licensed software no more than two supported versions behind the latest release and updated with latest security patches.</td><td>X</td><td>X</td><td></td><td></td></tr>
<tr><td colspan="6">Response:
The mPulse Mobile solution is priced as an annual license fee without the need for any third party licensing. That fee includes the HITRUST Certified Platform for HIPAA-compliant management of personal health information (PHI) and other sensitive data, adherence to TCPA regulations, and automated SFTP or API data transfer management systems. The solution provides capabilities for one-way and two-way automated and manual dialogues, with the ability for employees to access a web-based application for one-on-one communication and member data management. Initial setup includes the provisioning of a short code, the creation of the customer account in our systems, training for customer staff and the development of use cases (or program dialogues) to communicate with identified members. A certain number of use cases are included in the proposal with the ability to add additional use cases for a pre-determined fee. Additional user licenses, beyond the number included in the proposal, are also available for the web-based application.</td></tr>
</table>

Texting System Requirements

This section represents the overall texting requirements that apply to the software. Describe in the Response how the proposed solution meets the requirement.

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
TXT-1	The bidder's proposed solution must have the ability to support two-way communication both sending and receiving text messages. Describe how your solution meets this requirement.	X	X		

Response:

mPulse Mobile's ability to create and manage two-way dialogues is a distinction.

mPulse Mobile's Engagement Layer contains the Engagement Engine which runs automated SMS dialogues for large consumer populations. 2-way interactions are significantly more engaging for consumers, uncover powerful insights about them, and can be used to solve specific business problems.

Automated dialogues are 2-way messaging flows that employ rules and microservices (such as domain specific Natural Language Understanding (NLU), sentiment analysis and solution-based services e.g. AIR QUALITY, URGENT keyword text-ins) to intelligently respond to consumers' responses in real-time. mPulse Mobile's proprietary Engagement Engine is the core technology that powers the dialogues. The engine maintains the context of a consumer interaction to support branching logic based on user responses. The Engagement Engine also supports concurrent dialogues with the same member using prioritization algorithms. Furthermore, integration to the Engagement Engine allows clients to register callbacks at critical states within the dialogue. These callbacks provide the full context of the entire dialogue containing all messages sent and received.

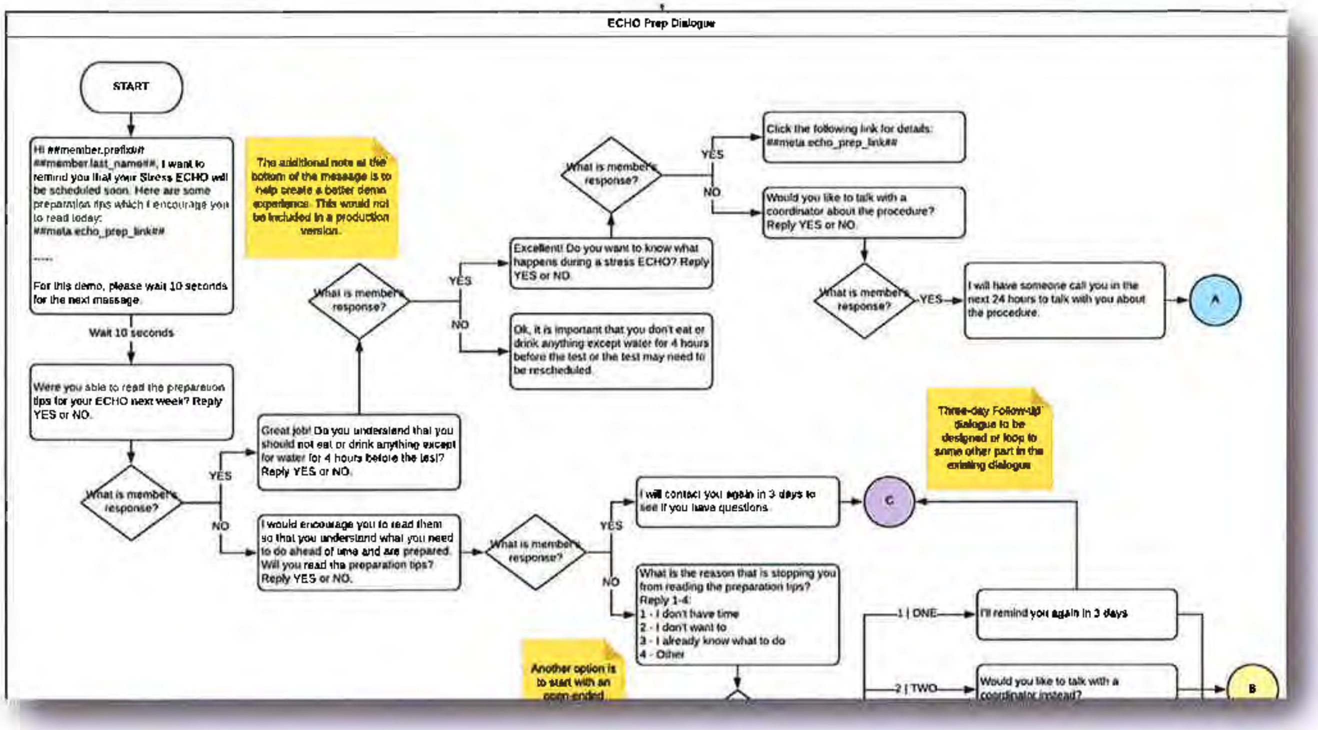
mPulse Mobile has over 20 health topic-based NLU services. Consumer responses to specific open-ended questions can be interpreted automatically and used to determine the next action. Natural response handling can be incorporated into branching logic workflows to drive specific business outcomes. Additionally, mPulse Mobile incorporates NLU into conversational agent-based solutions for specific consumer health engagement challenges.

mPulse Mobile uses sentiment analyzers to assess consumer response to messaging programs at the individual consumer and population level. Responses are interpreted in relation to specific topic domains using a combination of machine learning and lexicon-based recognition. Sentiment analysis has proven to be an effective input for tailoring content to individuals, as well as uncovering strategic insights about consumer health beliefs.

mPulse Mobile's Engagement Console is a secure browser-based user interface that mPulse Mobile customers use to manage mobile engagement with their members. The console allows customer staff to view communication history at the individual level. Manual 1:1 interactions can be quickly initiated to take advantage of the consumer convenience of SMS or other communication channels. Customer staff can also launch automated dialogues, which has broad applications across Care Management, Health Coaching and Call Center functions.

The attached *mPulseMobile - Tech and Data.pdf* provides additional illustrations that describe how two-way dialogues are enabled and developed.

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party


ECHO Prep Dialogue
START
Hi ##member.prefix## ##member.last_name##, I want to remind you that your Stress ECHO will be scheduled soon. Here are some preparation tips which I encourage you to read today: ##meta.echo_prep_link##

For this demo, please wait 10 seconds for the next message.
The additional note at the bottom of the message is to help create a better demo experience. This would not be included in a production version.
Wait 10 seconds
Were you able to read the preparation tips for your ECHO next week? Reply YES or NO.
What is member's response?
YES
NO
Great job! Do you understand that you should not eat or drink anything except for water for 4 hours before the test? Reply YES or NO.
I would encourage you to read them so that you understand what you need to do ahead of time and are prepared. Will you read the preparation tips? Reply YES or NO.
What is member's response?
YES
NO
Excellent! Do you want to know what happens during a stress ECHO? Reply YES or NO.
Ok, it is important that you don't eat or drink anything except water for 4 hours before the test or the test may need to be rescheduled.
What is member's response?
YES
NO
Click the following link for details: ##meta.echo_prep_link##
Would you like to talk with a coordinator about the procedure? Reply YES or NO.
What is member's response?
YES
I will have someone call you in the next 24 hours to talk with you about the procedure.
A
What is member's response?
YES
NO
I will contact you again in 3 days to see if you have questions.
C
Three-day Follow-up dialogue to be designed or loop to some other part in the existing dialogue
What is the reason that is stopping you from reading the preparation tips? Reply 1-4:
1 - I don't have time
2 - I don't want to
3 - I already know what to do
4 - Other
1 | ONE
I'll remind you again in 3 days
2 | TWO
Would you like to talk with a coordinator instead?
B
Another option is to start with an open-ended

TXT-2	The bidder's proposed solution must support both individual and broadcast messaging. Broadcast messaging is defined as the ability to send a message to thousands of clients. Describe how your solution meets this requirement.	X	X		

Response:

The mPulse Mobile solution supports broadcast messaging by subscribing members to a list, and either manually or through a pre-defined event, sending that message to the desired recipients. The mPulse Mobile platform supports broadcast messages to millions of recipients at once. We are on-pace to deliver over 200 million messages in 2019.

The platform has been tested to support throughput in the 500-1000 messages per second range. A sustained rate of 500 messages per second allows for a million messages to be delivered in under an hour. Factors that impact the maximum rate include features (such as link shortening) and the type of trigger used. For example, if a message is triggered as a result of an Audience Profile Update, it is slower than if it is triggered using the Event Upload API.

TXT-3	Describe how the bidder's proposed solution handles OPT IN and OPT OUT functionality.	X	X		

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
Response: mPulse Mobile has a broad range of proven approaches to enroll healthcare consumers in text messaging programs. mPulse leverages its decade-long experience in health engagement to help our 90+ clients determine the most impactful opt-in strategy for their business and consumer needs. Please see the attached *mPulse Opt-In Overview.pdf* for details on how OPT IN and OPT OUT functionality is managed.					
TXT-4	Describe how the bidder's proposed solution handles incoming texts from the client when no response is expected. For example, if a text response is received from a client that was not solicited. What happens and where does the text message go?	X	X		

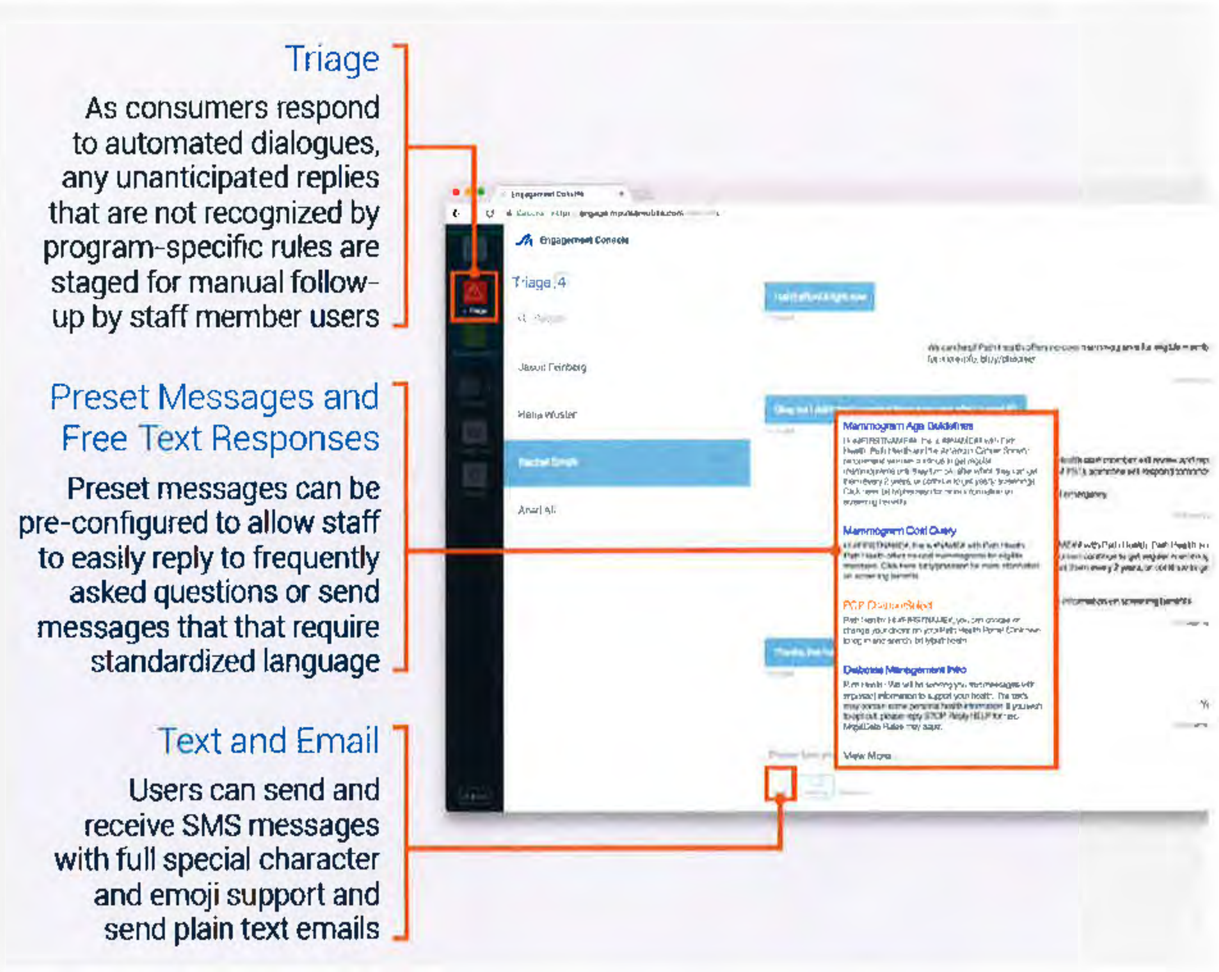
Response:

The mPulse Mobile platform has a number of options for unsolicited incoming texts.

1. All responses are available in an incoming text report (also known as a "Mobile Originated") report.
2. Auto responders can be setup to acknowledge the incoming text and to provide direction to the sender.
3. The mPulse Mobile platform is the only platform in the market that can route incoming texts (including unsolicited texts) to an Engagement Console.

mPulse Mobile's Engagement Console enables real-time 1-on-1 interaction with healthcare consumers by giving client staff a cloud-based console to send and receive text messages as part of the broader mPulse solution.

The mPulse Mobile Engagement Console supports both outbound 1:1 communication and inbound by alerting agents to incoming messages that are not handled by automation.

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
	 Engagement Console Triage 4 Mammogram Age Guidelines Mammogram Cost Query PCP Change/Select Diabetes Management Info View More Triage As consumers respond to automated dialogues, any unanticipated replies that are not recognized by program-specific rules are staged for manual follow-up by staff member users Preset Messages and Free Text Responses Preset messages can be pre-configured to allow staff to easily reply to frequently asked questions or send messages that that require standardized language Text and Email Users can send and receive SMS messages with full special character and emoji support and send plain text emails				
TXT-5	The bidder's proposed solution must provide a status on the delivery of the text messages to DHHS. The status must indicate whether the text was successfully delivered to the intended client phone number or unsuccessfully delivered. If any errors were encountered, the reason for the failure must be provided. Describe how your solution meets this requirement and how DHHS is notified of the status of text messages delivered.	X	X		

<table>
<tr><th>Req #</th><th>Requirement</th><th>(1)
Comply</th><th>(a)
Core</th><th>(b)
Custom</th><th>(c)
3rd Party</th></tr>
<tr><td colspan="6">Response:
A delivery status is available from mPulse for every SMS message sent. Carriers (Verizon, T-Mobile, etc.) do not reliably return a “delivered” status, so the mPulse Mobile platform records a message as SENT if a delivery error (bounce, invalid number or undeliverable) is not received.
The following status is available for each message sent:
<b>Delivered</b> (Sent) - Since SMS carriers inconsistently report a status of “delivered”, we assume messages have been delivered if we do not receive any delivery errors, which are described below.
<b>Soft Bounce</b> - Soft bounces are errors that are caused by failures that may not be persistent. A soft bounce indicates that you should attempt to resend the message. Examples of soft bounces are as follows:
• The subscriber has insufficient funds for the requested
transaction (from operator).
• The mobile subscriber’s message queue is full (from operator).
• Handset memory exceeded.
<b>Hard Bounce</b> - Hard bounces are errors that indicate a permanent failure. The number should be invalidated as a mobile number in your system, and you should not attempt to resend the message. Examples of hard bounces are as follows:
• Subscriber not provisioned.
• Subscription terminated by operator.
• The subscriber is not registered (from operator).</td></tr>
<tr><td>TXT-6</td><td>If a text message fails to get delivered to the intended recipient, describe if the text is retried, and if so, how many times?</td><td>X</td><td>X</td><td></td><td></td></tr>
<tr><td colspan="6">Response:
A hard bounce is a permanent failure, so those will not be retried by the mPulse Mobile platform. Soft bounces are reported by the carrier when message delivery fails for another reason which could be due to a transitory network issue or because a member needs to reload a pay-as-you-go plan. The mPulse Mobile platform will make one additional attempt after five minutes, then report a soft-bounce status.</td></tr>
<tr><td>TXT-7</td><td>The bidder’s solution must have the ability to schedule text messages to be sent at specific timeframes. Describe how your solution meets this requirement.</td><td>X</td><td>X</td><td></td><td></td></tr>
</table>

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party

Response:

Dialogues are event driven and can be triggered both externally (from DHHS systems) or internally with a campaign defined in the mPulse Mobile Communication Console. The following internal message triggers are available:

DATES

- Absolute Date: Send flu shot reminder on September 1
- Date relative to message: 15 days from last message
- Date relative to member attribute: Screening reminder 30 days before 50th birthday

EVENT

- Inbound text from member
- Event from your system

<table>
<tr><th>Req #</th><th>Requirement</th><th>(1) Comply</th><th>(a) Core</th><th>(b) Custom</th><th>(c) 3rd Party</th></tr>
<tr><td>TXT-8</td><td>The bidder's solution must be able to deliver text messages to the entire client base (approximately 100,000 text messages) within one hour. Describe how the bidder's proposed solution meets this requirement.</td><td>X</td><td>X</td><td></td><td></td></tr>
<tr><td colspan="6">Response:
The mPulse Mobile platform has been tested to support throughput in the 500-1000 messages per second range. A sustained rate of 500 messages per second allows for a million messages to be delivered in under an hour. Factors that impact the maximum rate include features (such as link shortening) and the type of trigger used. For example, if a message is triggered as a result of an Audience Profile Update, it is slower than if it is triggered using the Event Upload API.
Sending 100,000 text messages within an hour would require a throughput rate of approximately 28 messages per second which is well within the mPulse Mobile service parameters, and can be accommodated with the correct configuration and planning.</td></tr>
<tr><td>TXT-9</td><td>Describe any messaging limitations including the maximum number of characters that can be used for texts sent with the bidder's proposed solution.</td><td>X</td><td>X</td><td></td><td></td></tr>
<tr><td colspan="6">Response:
mPulse Mobile SMS supports a 450-character limit (standard SMS messages have a 160-character limit) by leveraging segmentation support available in most mobile devices. Note that this response is 408 characters, and would be considered a long message for a healthcare consumer to read, so our recommendation is that any SMS message sent be kept to well under 450 characters in order to remain user-friendly.</td></tr>
<tr><td>TXT-10</td><td>Describe how the bidder's proposed solution handles multiple text messages going to the same recipient during the same timeframe. Is there any ability to prioritize messages or setup a predetermined order? Does the solution limit the number of text messages sent to a client in a specified timeframe?</td><td>X</td><td>X</td><td></td><td></td></tr>
<tr><td colspan="6">Response:
Yes. The mPulse Mobile platform is capable of both prioritizing and limiting messages sent to a healthcare consumer over the same timeframe.
Content is tailored to the individual using mPulse Mobile's proprietary Activation Intelligence technology. Demographic, psychographic and behavioral inputs are processed by independent analytical data agents to determine the next optimal automated dialogue to initiate for the member. This AI-based engine incorporates collaborative filtering, statistical estimators and other learned models along with explicit rules that incorporate time, best-practices and similar logic-based rules. Each automated dialogue is stored using a variety of attributes describing the content and outcomes. The recommendation retrieves the most optimal automated dialogue by matching attributes of available dialogues in the content library against the generated content search vector. Consumer behavior and engagement as a result of the dialogues are fed back to improve future recommendations.</td></tr>
<tr><td>TXT-11</td><td>The bidder's proposed solution must allow for the use of short codes. Describe if the solution offers and works with both dedicated and shared short codes. Describe if the solution offers and works with both vanity and non-vanity short codes. Describe the estimated timeline for setting up new short codes. Describe how the bidder's proposed solution meets this requirement.</td><td>X</td><td>X</td><td></td><td></td></tr>
</table>

<table>
<tr><th>Req #</th><th>Requirement</th><th>(1)
Comply</th><th>(a)
Core</th><th>(b)
Custom</th><th>(c)
3rd Party</th></tr>
<tr><td colspan="6">Response:
The mPulse Mobile platform offers and works with both dedicated and shared shortcodes. It is recommended that at least one dedicated shortcode be provisioned for healthcare-related SMS messaging coming from DHHS.
mPulse Mobile manages the entire process of applying for, provisioning, and implementing short-codes. The application and provisioning process can take up to six weeks, but the quality of applications presented by mPulse Mobile allows for provisioning to occur in a shorter timeframe.
mPulse Mobile supports both vanity and non-vanity short codes.</td></tr>
<tr><td>TXT-12</td><td>The bidder's proposed solution must allow DHHS to designate a specific short code within the API/web service and SFTP interfaces when sending texts. Describe how the bidder's proposed solution meets this requirement.</td><td>X</td><td>X</td><td></td><td></td></tr>
<tr><td colspan="6">Response:
In order for an SMS message to be sent to a healthcare consumer, the consumer must be subscribed to a list. Every list is associated with a specific shortcode. Members can be (and often are) subscribed to multiple lists.
To specify the shortcode used for sending the message, DHHS simply has to specify the list being used as part of the message, dialogue, or campaign.</td></tr>
<tr><td>TXT-13</td><td>Describe how the bidder's proposed solution supports the use of long codes.</td><td>X</td><td>X</td><td></td><td></td></tr>
<tr><td colspan="6">Response:
SMS long codes are supported using the exact same mechanisms as SMS short codes. Note that there are two areas where SMS shortcodes are vastly superior to long codes when it comes to messaging healthcare consumers:
1. The carriers (Verizon, AT&T, etc.) are not obligated to deliver messages sent over long codes. If a carrier decides that a long-code is being used for unsolicited messages, they can unilaterally block the number. The regulated nature of shortcodes ensures that messages will be delivered.
2. The SMS delivery rate for longcodes is restricted to only 1-2 messages / second, so long-codes cannot be used for messaging members at scale.</td></tr>
<tr><td>TXT-14</td><td>The bidder's proposed solution must be able to support keyword responses from a client. Can keywords be customized? Are certain keywords included with the base solution? Is there a maximum number of keywords that can be used? Can the use of keywords be tracked in the solution?</td><td>X</td><td>X</td><td></td><td></td></tr>
<tr><td colspan="6">Response:
There is no limit to the number of keywords that can be configured as part of the solution. Keywords (except for the regulated keywords, STOP, HELP, etc.) are configurable. The use of keywords is tracked within in the system and can be reviewed via on-demand or delivered reporting.</td></tr>
</table>

<table>
<tr><th>Req #</th><th>Requirement</th><th>(1)
Comply</th><th>(a)
Core</th><th>(b)
Custom</th><th>(c)
3rd Party</th></tr>
<tr><td>TXT-15</td><td>The bidder's proposed solution must have the ability to send out an automated response or series of responses to a specific incoming text messages from a client. Describe how the bidder's proposed solution meets this requirement.</td><td>X</td><td>X</td><td></td><td></td></tr>
<tr><td colspan="6">Response:

mPulse Mobile's Engagement Layer contains the Engagement Engine which runs automated SMS dialogues for large consumer populations. 2-way interactions are significantly more engaging for consumers, uncover powerful insights about them, and can be used to solve specific business problems.

Automated dialogues are 2-way messaging flows that employ rules and microservices (such as domain specific Natural Language Understanding (NLU), sentiment analysis and solution-based services e.g. AIR QUALITY, URGENT keyword text-ins) to intelligently respond to consumers' responses in real-time. mPulse Mobile's proprietary Engagement Engine is the core technology that powers the dialogues. The engine maintains the context of a consumer interaction to support branching logic based on user responses. The Engagement Engine also supports concurrent dialogues with the same member using prioritization algorithms. Furthermore, integration to the Engagement Engine allows clients to register callbacks at critical states within the dialogue. These callbacks provide the full context of the entire dialogue containing all messages sent and received.

mPulse Mobile has over 20 health topic-based NLU services. Consumer responses to specific open-ended questions can be interpreted automatically and used to determine the next action. Natural response handling can be incorporated into branching logic workflows to drive specific business outcomes. Additionally, mPulse Mobile incorporates NLU into conversational agent-based solutions for specific consumer health engagement challenges.</td></tr>
<tr><td>TXT-16</td><td>Describe how the bidder's proposed solution avoids having a large batch of distributed messages caught in carriers' spam filter.</td><td>X</td><td>X</td><td></td><td></td></tr>
<tr><td colspan="6">Response:

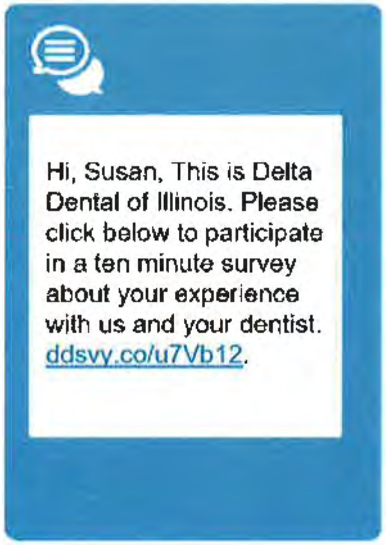
mPulse Mobile uses TCPA approved short-codes which guarantees SMS delivery to recipients.</td></tr>
<tr><td>TXT-17</td><td>Describe how the bidder's proposed solution allows an active URL link within the text that can direct clients to a website.</td><td>X</td><td>X</td><td></td><td></td></tr>
<tr><td colspan="6">Response:

URL links are formatted in mPulse Mobile SMS text messages such that links are automatically enabled on mobile devices. Furthermore, web links delivered to mobile devices can be automatically tokenized and tracked at the member level. Whether a link was clicked can be incorporated into dialogues and workflows, and can be reported back to DHHS.</td></tr>
<tr><td>TXT-18</td><td>Describe the bidder's proposed solution's capability to send surveys to clients and create reports of voting results and number of responses.</td><td>X</td><td>X</td><td></td><td></td></tr>
</table>

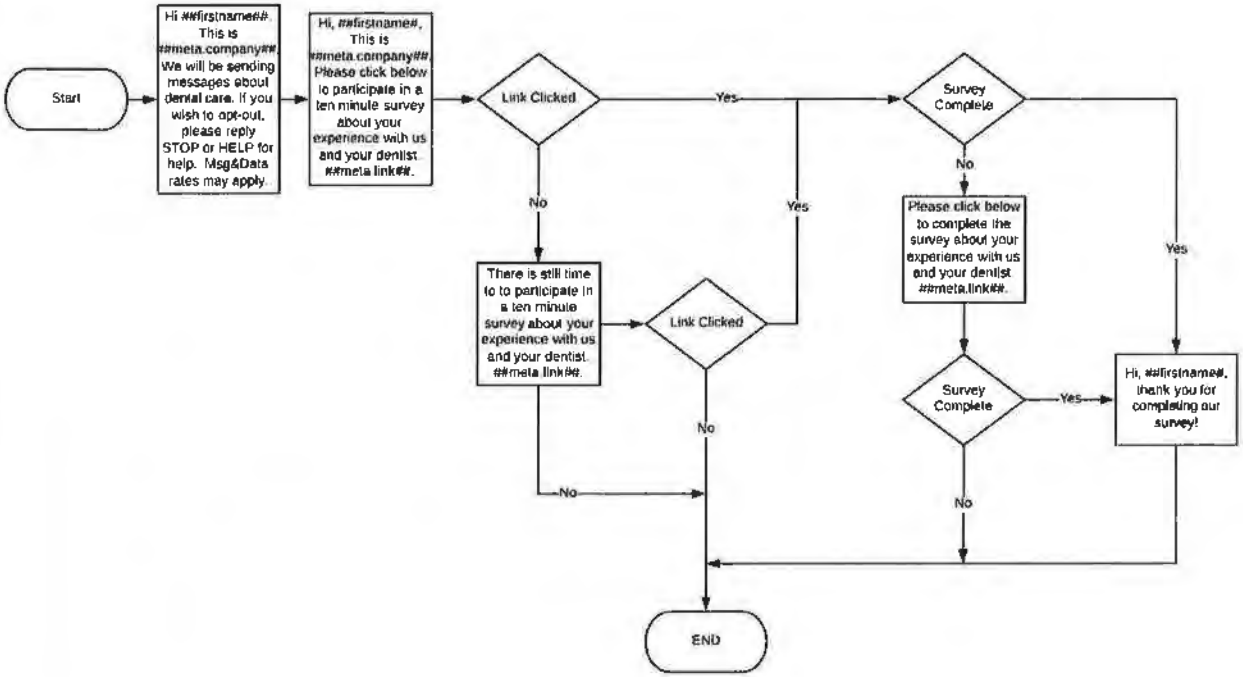
Response:

SMS surveys are supported with results going back to DHHS. In addition, tracked web surveys can be delivered via SMS and tracked. See examples below:

Hi, ##firstname#, This is ##meta.company##. Please click below to participate in a ten minute survey about your experience with us and your dentist. ##meta.link##.



Hi, Susan, This is Delta Dental of Illinois. Please click below to participate in a ten minute survey about your experience with us and your dentist. ddsvy.co/u7Vb12.

<table>
<tr><th>Req #</th><th>Requirement</th><th>(1)
Comply</th><th>(a)
Core</th><th>(b)
Custom</th><th>(c)
3rd Party</th></tr>
<tr><td colspan="6">

Hi ##firstname##. This is ##meta.company##. We will be sending messages about dental care. If you wish to opt-out, please reply STOP or HELP for help. Msg&Data rates may apply.
Hi, ##firstname#, This is ##meta.company##, Please click below to participate in a ten minute survey about your experience with us and your dentist ##meta link##.
There is still time to to participate in a ten minute survey about your experience with us and your dentist. ##meta link##.
Please click below to complete the survey about your experience with us and your dentist ##meta.link##.
Hi, ##firstname#, thank you for completing our survey!</td></tr>
<tr><td>TXT-19</td><td>The bidder's solution must support text messages sent and received in foreign languages. Describe how the bidder's solution supports this requirement and how it is setup for specific cell phone numbers. Describe the foreign languages supported.</td><td>X</td><td>X</td><td></td><td></td></tr>
<tr><td colspan="6">Response:
The mPulse Mobile platform supports all languages including double-byte languages such as Chinese, Japanese, and Korean.</td></tr>
<tr><td>TXT-20</td><td>Describe how the bidder's solution supports an unlimited number of contacts or contact groups within the web portal</td><td>X</td><td>X</td><td></td><td></td></tr>
</table>

<table>
<tr><th>Req #</th><th>Requirement</th><th>(1)
Comply</th><th>(a)
Core</th><th>(b)
Custom</th><th>(c)
3rd Party</th></tr>
<tr><td colspan="6">Response:
The mPulse Mobile solution supports extensive member attributes and member preferences options including language preference. A message template and dialogue supporting each language will be built. Healthcare consumers will be able to choose their preferred language and will receive the appropriate dialogue based on that preference.</td></tr>
<tr><td>TXT-21</td><td>Describe how the bidder's solution supports standard text messages to be stored in the web portal and available for use when sending out messages.</td><td>X</td><td>X</td><td></td><td></td></tr>
<tr><td colspan="6">Response:
The mPulse Mobile Event API can be configured so that standard text messages can be triggered from the web portal.</td></tr>
<tr><td>TXT-22</td><td>Describe all the information that is stored in the texting system database, and the length of time that the information is stored in the system database. Describe the bidder's ability to store message information (metadata) including but not limited to:
• Sender Telephone Number;
• Recipient Cellular Telephone Number;
• Message data that was sent/received;
• Date and time that the message was sent; and,
• Whether the text message was successful or failed to be received.</td><td>X</td><td>X</td><td></td><td></td></tr>
<tr><td colspan="6">Response:
All of the information described above is stored in the system database. The mPulse Mobile platform retains information for a minimum of seven years per HIPAA requirements and can implement alternative retention periods if needed.
mPulse Mobile is designed to manage and host sophisticated dialogues and campaigns that use member and event data for segmentation, dialogue branching and segmentation.
Member Attributes that comes from DHHS may be used to personalize messages. "Hi Mary, we have important information to send about your health." Member data can also be used for driving dialogues or to branch based on a member attribute. A dialogue may branch for example if a person's age is over 65 or under 30.
mPulse Mobile can also use engagement / sentiment to segment and to drive dialogues.
Event data / attributes that comes from DHHS as part of the Event object is used to trigger dialogues which can include many messages, responses and branches. One Event Definition can be defined for each dialogue type. When an event in your system indicates that a particular dialogue should be launched, Walmart will make an Event Upload API request to mPulse Mobile using the corresponding Event information.
Please see the attached <i>mPulse Mobile - Data Overview v. 1.0.0.pdf</i> for more detail.</td></tr>
</table>

Reporting Requirements

This section represents the reporting requirements that apply to the software. Describe in the Response how the proposed solution meets the requirement.

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
RPT-1	The bidder's solution must provide access to data and statistical information for reporting via a secured web front end. The solution must allow exporting and transferring of the data and statistical information in XML and CSV file formats to DHHS via SFTP. Describe how your solution meets this requirement.	X	X		
Response: The mPulse Mobile platform is configurable and built for interfacing with Nebraska DHHS through automated SFTP and web-based API. Please see the attached mPulse Mobile - Integration and Security Overview v. 1.4.0 .pdf for details. Reporting is available in both XML and CSV file formats. These reporting APIs allow clients to retrieve information about their members or messages sent or received by them. In addition to request-based API's, mPulse also provides real-time callbacks for several events such as member responses, delivery failures and subscriptions.					

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
RPT-2	Describe any online web based dashboards and metrics available in the bidder's proposed solution. Reporting should include overall totals as well as totals by short/long code. Reports should include the following, but not limited to: • Monthly inbound and outbound traffic reports; • Successful vs Failed Messages; • Uptime and downtime of services; • Error code messages; and, • Opt out rates.	X	X		

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party

Response:

The mPulse Mobile platform supports on-demand, interactive, and custom reporting available through scheduled reports, on-line user interfaces, and API's.

The following is a partial list of message statistics available:

Campaign Details
Campaign Message Details
Average Customer Response Time
Help Requests
Sentiment
Auto-Processed Messages
Messages Sent By Day And Time
Messages Received By Day And Time
Message Frequency
Customer Response Time
Activation Dialogues Initiated
Population Activated
Activation Score
Rules Triggered
Dialogues Initiated
Rule Counts
Members By Language / Age / Gender
Api Requests
Callbacks Sent / Failed

Please see the attached mPulseReporting.pdf for examples.

RPT-3	Describe how the bidder's solution has the ability to produce overall reports as well as reports by short/long code including, but not limited to: • DHHS clients that have "opted in" and "opted out" of receiving information via text message; and, • Keywords that are being used along with statistics on their use. • Number of text messages and broadcast messages sent by type of message (i.e. appointment reminders).	X	X		
Response: All of that information is available in the mPulse Mobile Insights Dashboard. Please see the attached mPulse Mobile Reporting Screenshots.pdf and InsightsDashboardOverview.pdf for additional detail and examples aside from up-time which is delivered as described below.					

Database/Data Management System (DBMS) Requirements

DHHS requires the benefits inherent with a relational database management system (RDBMS). The accessibility, flexibility and maintainability achieved through normalized data structures are essential to achieving the business objectives outlined in this RFP.

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
DBM-1	Describe what DBMS is used for storage of data with the bidder's proposed solution. If the bidder's proposed solution requires any DHHS data to be stored off-site (including data "in the cloud") describe how and where the data is secured and stored within the continental United States.	X	X		

<table>
<tr><th>Req #</th><th>Requirement</th><th>(1)
Comply</th><th>(a)
Core</th><th>(b)
Custom</th><th>(c)
3rd Party</th></tr>
<tr><td colspan="6">Response:
mPulse Mobile is a cloud-based solution which employs PostgreSQL as the primary database. All data is stored in the United States.
The mPulse Mobile Platform is on dedicated systems within AWS data centers. No processing or memory is shared with other AWS customers. Within our platform, strict logical controls are in place at the organizational level to restrict access. In addition:
All API URLs contain the account ID.
Access is only possible from whitelisted IP's that are provisioned at the account level.
API access requires Basic Authentication using a unique account-based access key and account name.
Each of our API's are individually controlled and provisioned at the account level, i.e, one account can have access to our Audience API but not receive real-time callbacks while another account can have access to both.
Individual user access to our Control Panel is provisioned at the account level.
Since all tables within the DB have the account id, removal of data within the database can be performed by using account id within the delete condition. This can be done without impact to any other account as all data is logically separable.
Please see the attached Information <i>Security Policy v1.0.9 (Signed).pdf</i> for additional detail.</td></tr>
<tr><td>DBM-2</td><td>Describe how the bidder's proposed solution maintains an automated history of all transactions, including but not limited to: date and time of change, "before" and "after" data field contents, and operator identifier or source of the update. Describe how long the history is maintained.</td><td>X</td><td>X</td><td></td><td></td></tr>
<tr><td colspan="6">Response:
Data field updates to transactional messaging data is not permitted. All before and after changes to member data is retained as part of the mPulse Mobile audit log. Please see the attached <i>Log Review Policy v1.2 (Signed).pdf</i> for more detail.</td></tr>
<tr><td>DBM-3</td><td>Describe the length of time that the text messaging data is maintained in the bidder's proposed solution.</td><td>X</td><td>X</td><td></td><td></td></tr>
<tr><td colspan="6">Response:
The mPulse Mobile platform retains information including text messaging data for a minimum of seven years per HIPAA requirements and can implement alternative retention periods if needed.</td></tr>
</table>

General Technical Requirements

This section presents the overall technical requirements that apply to the software. Describe in the Response how the proposed solution meets the requirement.

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
TEC-1	Describe how the proposed solution is scalable and flexible enough to accommodate any changes required by the State and/or federal statute, mandate, decision or policy. Describe the upgrade and maintenance process for the proposed solution.	X	X		
Response: mPulse takes a rigorous approach to fixes and upgrades as we support the platform. Therefore, we have an extensive deployment and quality control process including code review, automated, manual and functional testing, white-box and black-box testing, security risk review, and finally user acceptance testing. Once, QA has provided assurance that a release is production ready, we deploy using a rolling deploy-and-release model to minimize downtime. The latest mPulse Mobile roadmap can be presented to DHHS under NDA. The attached *Software Development Life Cycle.pdf* details how updates are prioritized and managed.					
TEC-2	Describe any redundancy built into the proposed solution to limit any downtime in the bidder's proposed solution.	X	X		
Response: Our production systems are hosted in the Amazon US West (N. California) Region and backup systems are kept in the Amazon US East (N. Virginia) Region. Please see the attached *Disaster Recover Policy (Signed)v2.2.pdf* for more detail.					
TEC-3	Describe what industry standard browsers are supported by the bidder's solution.	X	X		
Response: mPulse Mobile supports all modern browsers including IE, Microsoft Edge, FireFox, Chrome and Safari.					

Error Handling Requirements

The management of the system requires that all occurrences of errors be logged for review and that critical errors be accompanied by appropriate alerts. Authorized users need to be able to query and review the error log and configure the alerts.

<table>
<tr><th>Req #</th><th>Requirement</th><th>(1)
Comply</th><th>(a)
Core</th><th>(b)
Custom</th><th>(c)
3rd
Party</th></tr>
<tr><td>ERR-1</td><td>Describe how the bidder's proposed solution provides edits at the point of data entry in the web portal to minimize data errors and provide immediate feedback in order for incorrect data to be corrected before further processing.</td><td>X</td><td>X</td><td></td><td></td></tr>
<tr><td colspan="6">Response:
Field-level validation is used for all input within mPulse Mobile web tools to minimize data errors and provide immediate feedback in order for incorrect data to be corrected before further processing.</td></tr>
<tr><td>ERR-2</td><td>Describe how the bidder's proposed solution provides edits on text messages sending and receiving. The solution should provide a comprehensive set of error messages with unique message identifiers. Please provide a list of error messages.</td><td>X</td><td>X</td><td></td><td></td></tr>
<tr><td colspan="6">Response:</td></tr>
<tr><td>ERR-3</td><td>Describe how the bidder's proposed solution ensures all errors are written and categorized to an error log. Describe how the bidder's proposed solution allows for a user to view, filter, sort, and search the error log.</td><td>X</td><td>X</td><td></td><td></td></tr>
<tr><td colspan="6">Response:
As a cloud-based solution, the mPulse Mobile operations team monitors and reviews all log files for errors. As required, mPulse Mobile can deliver all errors related to DHHS for review.
Please see the attached <i>Log Review Policy v1.2 (Signed).pdf</i> for more detail.</td></tr>
<tr><td>ERR-4</td><td>Describe how the bidder's proposed solution provides for the generation of standard and customizable error reports.</td><td>X</td><td>X</td><td></td><td></td></tr>
</table>

<table>
<tr><th>Req #</th><th>Requirement</th><th>(1) Comply</th><th>(a) Core</th><th>(b) Custom</th><th>(c) 3rd Party</th></tr>
<tr><td colspan="6">Response:
The mPulse Mobile Log Review Policy has been formulated with the following goals in mind:
• Ensure security, reliability and privacy of mPulse Mobile's systems, networks and data, and the networks, systems and data of others.
• Protect mPulse Mobile's systems, networks and data from harm and interference.
• Ensure that mPulse Mobile, its employees and other users of its facilities comply with the law and avoid legal liability.
• Encourage the responsible use of resources, and discourage practices which degrade the usability of network resources or cause harm to resources or individuals.
• Maintain mPulse Mobile's reputation as a responsible organization.
• Access to online content via the network may be restricted in accordance with our policies and federal regulations.
Please see the attached <i>Log Review Policy v1.2 (Signed).pdf</i> for more detail.</td></tr>
</table>

Backup and System Recovery Requirements

<table>
<tr><th>Req #</th><th>Requirement</th><th>(1) Comply</th><th>(a) Core</th><th>(b) Custom</th><th>(c) 3rd Party</th></tr>
<tr><td>BKP-1</td><td>Describe the bidder's proposed Backup and System Recovery plan and readiness. Describe the bidder's Service Level Agreement (SLA) on returning the solution to service from a backup. Describe the bidder's proposed backup retention schedules – daily, weekly, monthly, quarterly, etc. Bidder must submit a copy of their SLA with their response.</td><td>X</td><td>X</td><td></td><td></td></tr>
<tr><td colspan="6">Response:
Please see the attached <i>mPulse_SLA.pdf</i> and <i>Disaster Recovery Policy v2.4 (Signed).pdf</i> for complete details.</td></tr>
<tr><td>BKP-2</td><td>Describe the bidder's proposed Disaster Recovery Plan. Describe the bidder's SLA on returning the solution back to operational service.</td><td>X</td><td>X</td><td></td><td></td></tr>
<tr><td colspan="6">Response:
mPulse Mobile estimates a 2-3 hours recovery time objective. Please see attached <i>Disaster Recovery Policy v2.4 (Signed).pdf</i></td></tr>
<tr><td>BKP-3</td><td>Describe how backups of the bidder's proposed solution are able to be scheduled without user intervention and without interruption to the system.</td><td>X</td><td>X</td><td></td><td></td></tr>
</table>

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
Response: mPulse Mobile manages all backup operations as part of the service with no involvement from or disruption to DHHS. Please see attached *Disaster Recovery Policy v2.4 (Signed).pdf.*					
BKP-4	Describe how the bidder's proposed solution provides testing and validation processes for all of the backup requirements listed previously (BKP-1, BKP-2, and BKP-3).	X	X		
Response: mPulse Mobile tests validates backups on a weekly basis and performs a full disaster recovery test annually as part of the HITRUST certification.					
BKP-5	If there is a backup failure or downtime, describe the bidder's proposed method and timing of communication to DHHS.	X	X		
Response: Any backup or recovery failure that results in a service disruption will be reported to DHHS per the attached *mPulse_SLA.pdf.*					

Security and Audit Requirements

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
SEC-1	Describe the bidder's proposed security safeguards integrated into their application and how these safeguards address DHHS security. Refer to DHHS Information Technology (IT) Access Control Standard (DHHS-IT- 2018-001B) for specific requirements: http://dhhs.ne.gov/ITSecurity	X	X		
Response: Please see the attached *Information Security Policy v1.0.9 (Signed).pdf.*					
SEC-2	Describe how the bidder's proposed solution meets the DHHS requirements for unique user ID access. Include: • Specification on configuration of the unique user ID; • How the unique user ID is assigned and managed; • How the unique user ID is used to log system activity; and, • How the system handles the creation of duplicate user ID accounts.	X	X		

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
Response: Please see the Authentication of Users section of the attached *Information Security Policy v1.0.9 (Signed).pdf.*					
SEC-3	Describe how the bidder's proposed solution meets the DHHS standard for administering passwords: • Initial Password assignment; • Strong Password Requirements; • Password reset process; • Password expiration policy; and, • Password controls for automatic lockout access to any user or user group after an administrator-defined number of unsuccessful log-on attempts.	X	X		
Response: Please see the Password Management section of the attached *Information Security Policy v1.0.9 (Signed).pdf.*					
SEC-4	Describe any security processes for managing security updates, and integrated components subject to vulnerability, including anti-virus.	X	X		
Response: Please see the attached *Patch Management Policy v1.1 (Signed).pdf* and the Anti-Virus section of the attached *Information Security Policy v1.0.9 (Signed).pdf.*					
SEC-5	Describe how the bidder's proposed solution provides the ability to maintain a directory of all personnel who currently use or access the system.	X	X		
Response:					

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
SEC-6	Describe how the bidder's proposed solution provides role-based security and allows restricted access to system features, function, screens, fields, database, etc. Role authentication may occur at the directory level, application level, or database level (depending on database solution). Describe the security administration functions integrated into the proposed system that manage role-based access to system functions, features, and data. Include a description of: • How and where the proposed system stores security attributes or roles; • How roles are created and security is applied to the role based on how and where security attributes are stored (if multiple options describe each); • How groups are defined and how roles and security are applied to each group; • How access limits are applied to screens and data on screens by role or group; • How users are created and assigned to one or more roles or groups; and, • How role and group creation and assignment activity is logged.	X	X		

Response:

Access to data is based on the principles of separation of duties with least privilege access rights enforced. User and system access is enforced by mandatory and role-based access controls (RBAC).

MPulse Mobile application roles restrict access to campaigns, administrative functions and member data.

Please see Section 5: Managing your Control Panel account of the attached *mPulse Platform Control Panel User Guide.pdf* for details on how RBAC is configured.

Please see the Roles and Responsibility section of the attached *Information Security Policy v1.0.9 (Signed).pdf* for details on how roles are managed at the organizational and system level at mPulse Mobile.

<table>
<tr><th>Req #</th><th>Requirement</th><th>(1) Comply</th><th>(a) Core</th><th>(b) Custom</th><th>(c) 3rd Party</th></tr>
<tr><td>SEC-7</td><td>Describe how the bidder's proposed solution provides the capability to monitor, identify, and report on events on the information system, detects attacks, and provides identification of unauthorized use and attempts of the system. Describe how the proposed solution alerts DHHS of potential violations.</td><td>X</td><td>X</td><td></td><td></td></tr>
<tr><td colspan="6">Response:
How mPulse Mobile monitors, identifies, and reports on events on the information system, detects attacks, and provides identification of unauthorized use and attempts of the system is best described in the following attachments:
The Intrusion Detection and Prevention section of the attached <i>Information Security Policy v1.0.9 (Signed).pdf</i>
The IDS escalation procedures section of the attached <i>Information Security Policy v1.0.9 (Signed).pdf</i>
The attached <i>Log Review Policy v1.2 (Signed).pdf</i>
The attached <i>Incident Response Policy v1.3 (Signed).pdf</i></td></tr>
<tr><td>SEC-8</td><td>Describe how the bidder's proposed solution has defined and deployed strong controls (including access and query rights) to prevent any data misuse, such as fraud, marketing or other purposes.</td><td>X</td><td>X</td><td></td><td></td></tr>
<tr><td colspan="6">Response:
mPulse Mobile is a HITRUST certified solution. In addition to the security controls described above, all employees undergo HIPAA security awareness training, CMS fraud and abuse training and OIG/LEIE screening.
Please see the attached <i>Security Awareness & Training Policy v1.2 (Signed).pdf</i></td></tr>
</table>

System and User Documentation Requirements

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
DOC-1	Describe how the bidder's proposed solution provides on-line Help for all web portal features, functions, and data element fields, as well as descriptions and resolutions for error messages, using help features including indexing, searching, tool tips, and context-sensitive help topics. A sample copy of five (5) screen shots must be included with bidder's response.			X	

<table>
<tr><th>Req #</th><th>Requirement</th><th>(1) Comply</th><th>(a) Core</th><th>(b) Custom</th><th>(c) 3rd Party</th></tr>
<tr><td colspan="6">Response:
Custom on-line help screens can be developed as needed for DHHS. Our solution has been developed with modern UX methods meant to minimize the need for on-line help.</td></tr>
<tr><td>DOC-2</td><td>Describe how the bidder's proposed solution provides an on-line User Manual with a printable version available. The documentation should include full mock-ups of all screens/windows and provide narratives of the navigation features for each window/screen. A sample copy of five (5) pages must be included with bidder's response.</td><td>X</td><td>X</td><td></td><td></td></tr>
<tr><td colspan="6">Response:
Please see the attached <i>mPulse Platform Control Panel User Guide.pdf.</i></td></tr>
<tr><td>DOC-3</td><td>Describe how the bidder's proposed solution will have an on-line Reporting Manual with a printable version available that includes descriptions, definitions, and layouts for each standard report. Include definitions of all selection criteria parameters and each report item/data element, all field calculations defined in detail, and field and report titles. A sample copy of five (5) pages must be included with bidder's response.</td><td>X</td><td>X</td><td></td><td></td></tr>
<tr><td colspan="6">Response:
Please see the attached <i>InsightsDashboardOverview.pdf.</i></td></tr>
<tr><td>DOC-4</td><td>Describe how the bidder's proposed solution will have an On-line Technical System Operation Manual with a printable version available. The documentation should include operating procedures to assist technical staff in operation and working with the Texting solution. A sample copy of five (5) pages must be included with bidder's response.</td><td>X</td><td></td><td>X</td><td></td></tr>
<tr><td colspan="6">Response:
Please see the attached <i>mPulse Platform Control Panel User Guide.pdf.</i></td></tr>
</table>

Training Requirements

This section presents the overall training requirements that apply to the software. They are not specific to any technology or platform.

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
TRN-1	Describe the bidder's proposed solution training plan. Describe how the bidder develops and provides training material to DHHS for initial training and updates to training material for enhancements and changes made to the system. The content of these materials should be consistent with the on-line Help, User Manual, and Reporting Manual.	X		X	

Response:

Please see the attached *mPulseTrainingPlanTemplate.pdf* and *Example - SJFMC Training Material - MEC.pdf*

The mPulse Mobile Account Management team plans training with customers as part of the onboarding process and then work with the customer to develop the training plan and training materials. Details for each training plan include:

- Who will be trained
- What information is needed for each person being trained
- How many trainings will be provided
- How long the training will be
- What days/times work best for the training
- What level of training will be provided (Admin, List manager, user)

Production, Test and Training Requirements

DHHS requires three environments (Production, Test, and Training) in order to work with the new software on an ongoing basis:

Test Environment – A test environment is required that mirrors the live production environment, including hardware and software. This test environment would be used to test application changes before they are deployed to production. This step is an important part of quality assurance, where all changes are tested to minimize the risk of adverse reactions in the production environment. While it is necessary to mirror all of the functions of the production environment, it is not necessary to maintain the same load capacity.

Training Environment – A training environment is also required that allows DHHS to provide hands-on training to users. This environment would allow DHHS to maintain unique data for use in training and conduct training without interference with the test and/or production environments. This environment would have occasional use.

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
PTT-1	The bidder's proposed solution must support several environments, i.e., production environment, test / training environment to allow for testing/training to occur outside of the production environment.	X	X		

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
Response: Separate accounts and environments outside of production can be setup for testing and training purposes.					
PTT-2	Describe how the bidder's proposed solution provides the ability to refresh any testing or training environment at the request of DHHS. Describe the refresh process and describe how the refresh process occurs.	X	X		
Response: Training and testing environments can be reconfigured and refreshed with testing and/or training data as required by DHHS. As a hosted solution, the mPulse Mobile Account management team will perform these tasks as needed on behalf of DHHS.					

System Performance Requirements

This section describes requirements related to the proposed systems' on-line performance, response times, and sizing from a system architecture standpoint.

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
PER-1	Describe the bidder's proposed system performance functionality and monitoring tools.	X	X		
Response: mPulse Mobile utilizes multiple pulse monitors (regular 1-minute) to check all applications and servers. New Relic is used to monitor application performance, and PagerDuty is used to intelligently alert our personnel whenever an outage or degraded service is reported by the aggregator or observed within our systems. mPulse has a variety of monitoring and alerting systems for the mPulse platform. This covers thresholds for system usage (CPU %, memory %, disk %), application error percentages, and queuing system thresholds. When any of these triggers – error or alert happen – we have alerts across email, SMS, and phone to developers and product managers. We also track uptime for all services and APIs.					
PER-2	Describe how the bidder's proposed solution captures system downtimes, along with the causes of the downtimes where applicable. Describe the bidder's proposed method and timing of communication to DHHS on downtimes.	X	X		
Response: Please see service level agreement (SLA) details in the attached mPulse_SLA.pdf. mPulse Mobile has met all SLA's since product launch in 2016.					

<table>
<tr><th>Req #</th><th>Requirement</th><th>(1)
Comply</th><th>(a)
Core</th><th>(b)
Custom</th><th>(c)
3rd Party</th></tr>
<tr><td>PER-3</td><td>Describe how the bidder's proposed solution supports concurrent users with minimal impact to response time, with the ability to increase the demand on the system by 50% without modification to the software or degradation in performance.</td><td>X</td><td>X</td><td></td><td></td></tr>
<tr><td colspan="6">Response:
We have tested our platform to support throughput in the 500-1000 messages per second range. A sustained rate of 500 messages per second allows for million messages to be delivered in under an hour.
Factors that impact the maximum rate include features (such as link shortening) and the type of trigger used. For example, if a message is triggered as a result of an Audience Profile Update, it is slower than if it is triggered using the Event Upload API.
mPulse mobile will scale out and validate the platform to ensure that it meets DHHS requirements.
mPulse Mobile is on-track to deliver over 200 million messages in 2019 for our current customers. The platform currently supports campaigns and messaging for customers whose member populations currently exceed the entire population for the state of Nebraska.</td></tr>
<tr><td>PER-4</td><td>Describe how the bidder's proposed solution is available online 24 hours a day and 7 days a week, 99.9% of the time each month. Describe any known timeframes or past instances where the system has been unavailable for use.</td><td>X</td><td>X</td><td></td><td></td></tr>
<tr><td colspan="6">Response:
Please see service level agreement (SLA) details in the attached <i>mPulse_SLA.pdf</i> which describes the 99.9% uptime guarantee. mPulse Mobile has met all SLA's since product launch in 2016.</td></tr>
<tr><td>PER-5</td><td>Describe how the proposed solution has the ability to generate reports and ad hoc queries without performance impact to user access or system response time.</td><td>X</td><td>X</td><td></td><td></td></tr>
<tr><td colspan="6">Response:
mPulse Mobile has implemented a dedicated reporting platform that is able to generate and deliver reports without impacting user access or system performance. The mPulse Mobile Insights Dashboard and reporting supports analysis, filtering and sorting. Ad-hoc queries can be supported by data exports for use in any data visualization tool.</td></tr>
</table>

PER-6	Describe how the bidder's proposed solution provides application performance monitoring and management capabilities, including any key performance indicators (KPI) or other metrics to measure and report system performance for the proposed system.	X	X		

Response:

mPulse Mobile has employed comprehensive monitoring and alerting systems. They cover thresholds for system usage (CPU %, memory %, disk %), application error percentages, and queuing system thresholds.

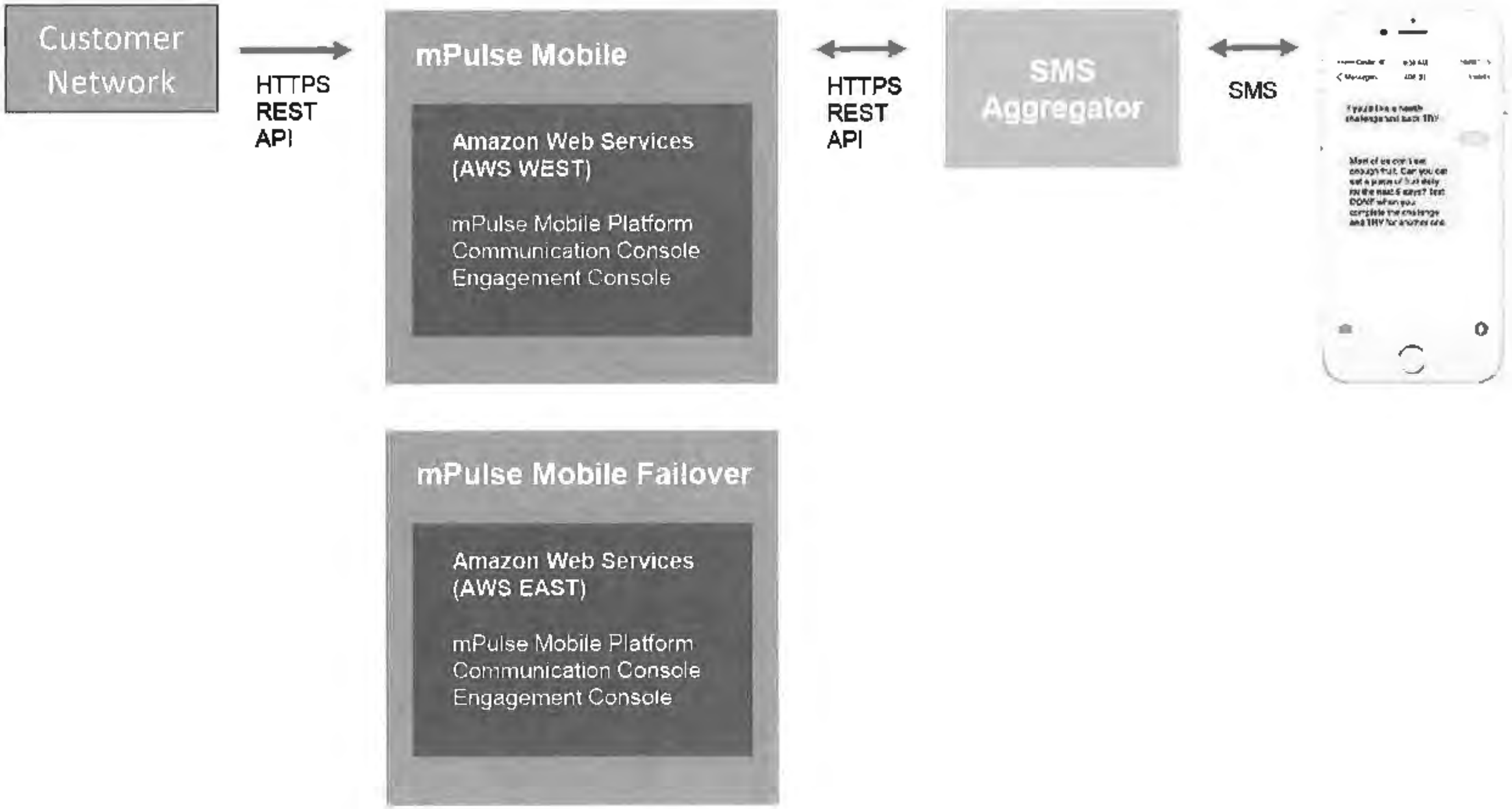
These components send alerts via email, SMS, and phone (depending on the severity) to the mPulse Mobile devops team. Uptime for all services and APIs are also tracked 24x7x365.

A

Exhibit A

mPulse Mobile Platform Architecture

Functional Architecture



Customer Network

HTTPS REST API

mPulse Mobile

Amazon Web Services (AWS WEST)

mPulse Mobile Platform
Communication Console
Engagement Console

HTTPS REST API

SMS Aggregator

SMS

If you'd like a health challenge text back TRY

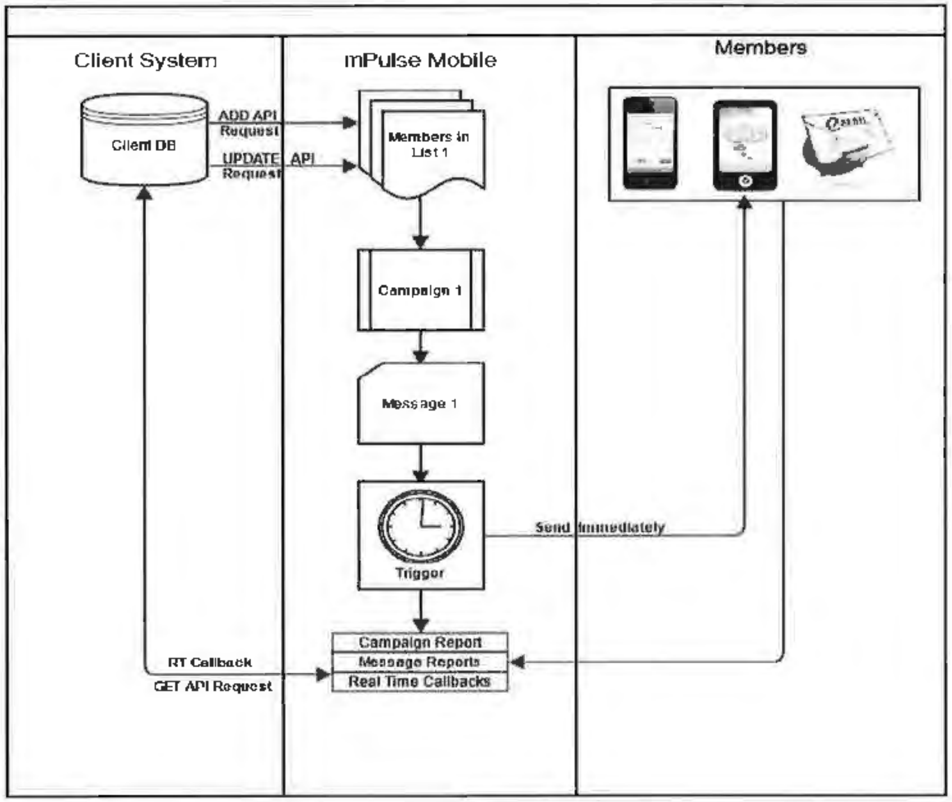
Most of us don't eat enough fruit. Can you eat a piece of fruit daily for the next 5 days? Text DONE when you complete the challenge and TRY for another one.

mPulse Mobile Failover

Amazon Web Services (AWS EAST)

mPulse Mobile Platform
Communication Console
Engagement Console

Data Flow



Client System

mPulse Mobile

Members

Client DB

ADD API Request

UPDATE API Request

Members in List 1

Campaign 1

Message 1

Trigger

Send Immediately

Campaign Report

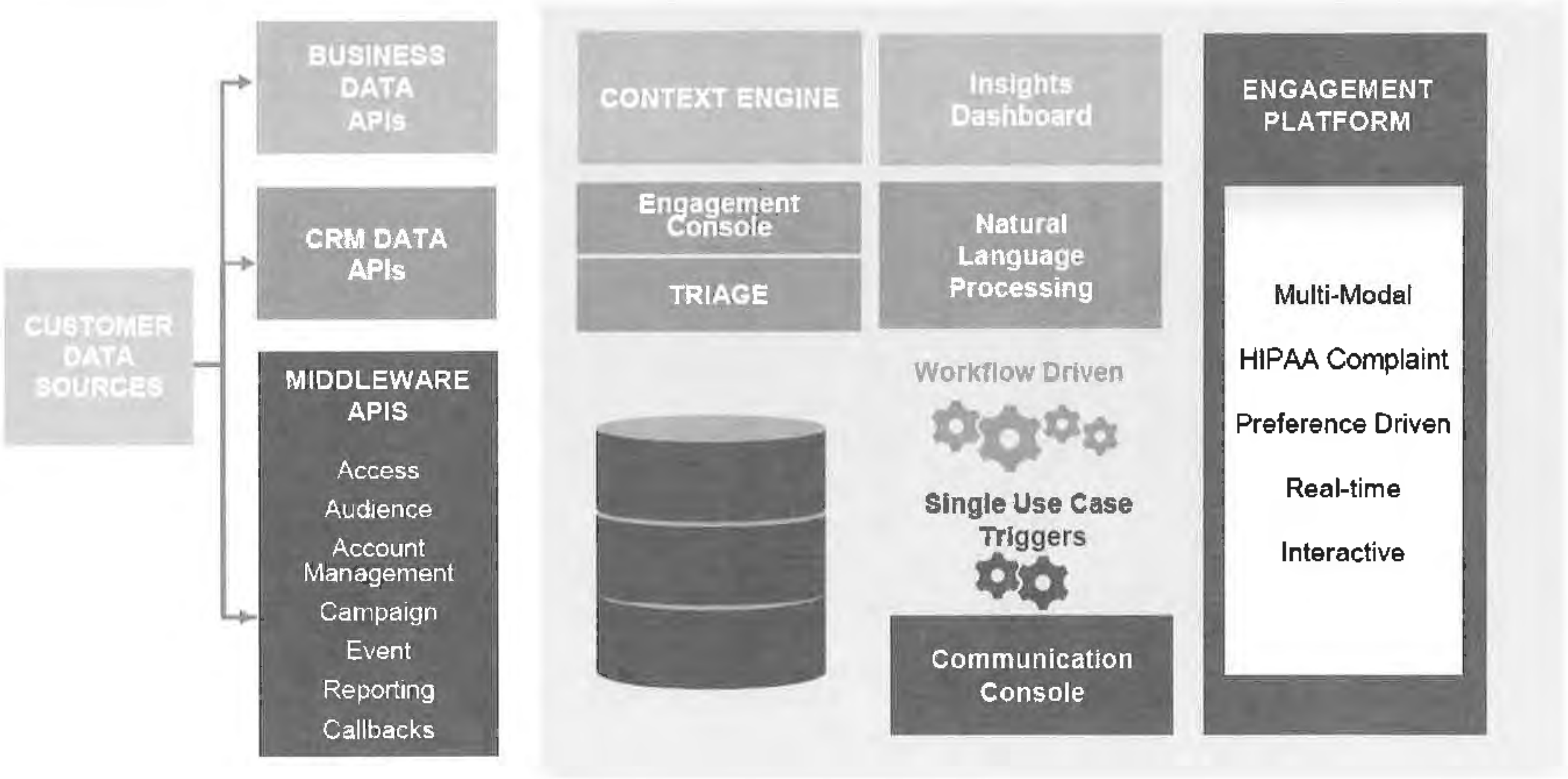
Message Reports

Real Time Callbacks

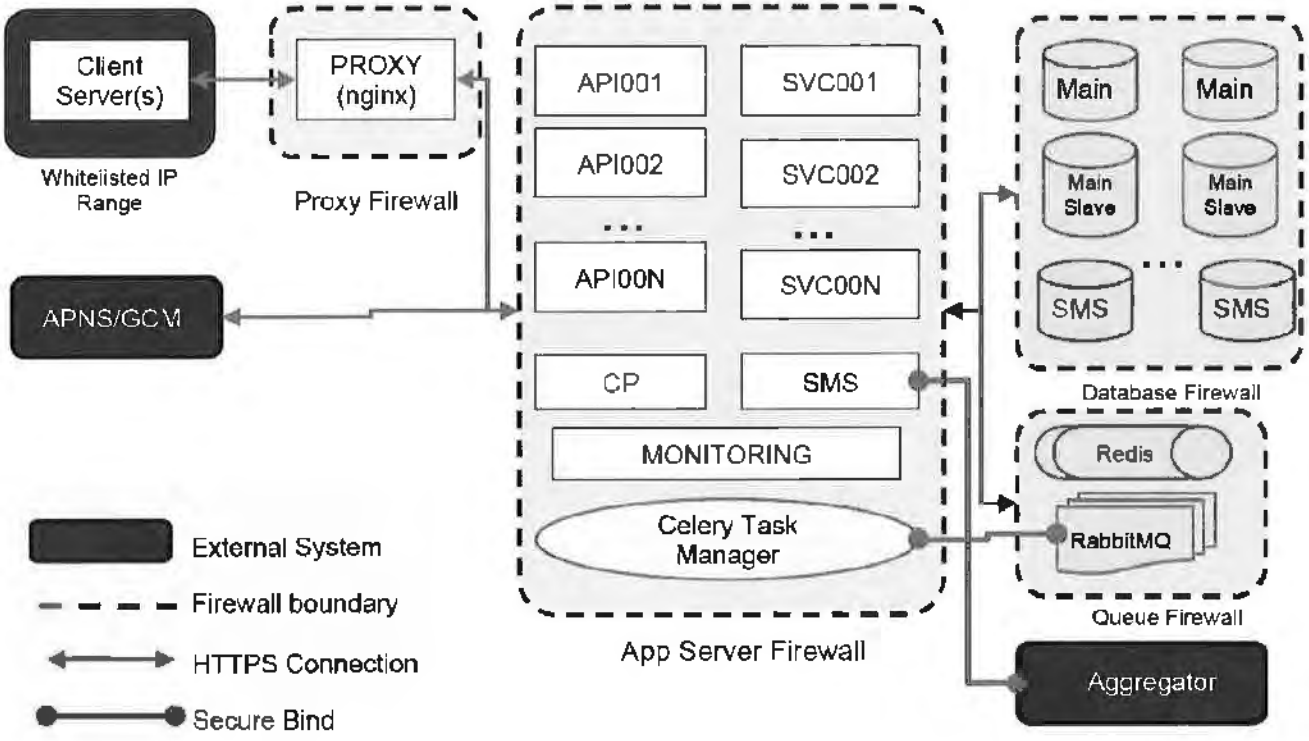
RT Callback

GET API Request

Platform Architecture



Technical Architecture



B

Exhibit B

mPulse Mobile Integration and Security Overview v1.4

Integration and Security Overview

mPulse Mobile's APIs make it easy to securely automate mobile healthcare engagement by allowing you to manage your Members' profiles and communication preferences and initiate campaigns or dialogues based on events in your systems. This document provides an overview of topics that are commonly addressed during initial discussions about API integrations.

Documentation

mPulse Mobile's API documentation is available online on our Public Access pege: https://mpulsemobile.atlassian.net/wiki/spaces/MPA/overview.

We recommend starting with the "Introduction to the mPulse Mobile Platform" document, which provides step-by-step instructions on adding a Member and sending them an SMS message.

Real-time Integration

Our RESTful APIs and callbacks support JSON and XML and allow you to sync your systems with your mPulse Mobile account.

Audience API

The Audience API allows you to manage your Member population. The endpoint is https://ms-api.mpulsemobile.com/accounts/{ACCOUNT_ID}/members.

The following actions are supported:

- Add
- Update
- Subscribe
- Resubcribe
- Unsubscribe
- Get information
- Delete

Event Upload API

The Event Upload API is used to send messages or start dialogues. Either can be scheduled immediately, relative to the time the request is made, or for a specific date and time.

The endpoint is https://ms-api.mpulsemobile.com/account/{ACCOUNT_ID}/uploadEvent.

Callbacks

Callbacks allow you to sync updates to the mPulse Mobile platform database (i.e., events) with your database in real-time. We have callbacks for the following events:

- SMS responses (i.e., MOs)
- Subscriptions (all channels)
- Unsubscriptions (all channels)
- Link clicks (Email and Secure Message)
- Bounced messages (SMS and Email)
- Opened messages (Email, Secure Message, and Push)

Security

HIPAA Compliance

We received our SOC2 Type II report on October 31, 2016 and completed our HITRUST certification in January 2018.

Authentication

mPulse Mobile's APIs use Basic Auth. In addition, only whitelisted IP addresses can access your account via API. Your Account Management team will provide you with your API credentials. These are different from your Control Panel account login credentials.

mPulse Mobile's callbacks support Basic Auth and client-authenticated SSO. mPulse Mobile will provide you with a self-signed certificate.

OAuth support is being rolled out on an API-by-API basis. Currently, OAuth is available for our Audience and Event Upload APIs.

Database Encryption

Client data are stored in a secure location that is encrypted using AES-256. Access to encrypted volumes is restricted to Data Processing personnel with a Secured Access Clearance status.

All activity is logged and reviewable by IT security. All connections to the mPulse Mobile platform and APIs are secured with TLS 1.2.

Scalability

mPulse Mobile's platform is a cloud-based solution that uses industry leading servers that rapidly scale. Performance is assessed on a weekly basis. Its service-oriented architecture (SOA) allows us to rapidly scale to meet increases in capacity demands. Last year (2017), we averaged over five million messages each month.

Test Environment

Your Account Management team can set up a test account for you in mPulse Mobile's production environment to which you can connect your QA or test environment. This means you will have two production mPulse Mobile accounts. You will point your test environment to one account and your production environment to the other.

There are several short and text-enabled toll-free number options available for test accounts. Please speak with your Sales Director or Account Manager to determine what will work best for you.

Mobile Phone Number Validation

Only valid mobile phone numbers (i.e., mobile phone numbers that will receive SMS messages sent from our platform) can be saved to our database. We support over 99.9% of mobile phone carriers in the United States. This represents all Tier 1 and 2 carriers and about 85% of Tier 3 carriers.

Member Record Identifiers

When Members are added to your mPulse Mobile account, the Audience API response includes a unique Member identifier that can be used in other API requests. You can also use your own unique Member identifier (e.g., Medical Record Number, Patient ID, etc.)

Member Contact Information

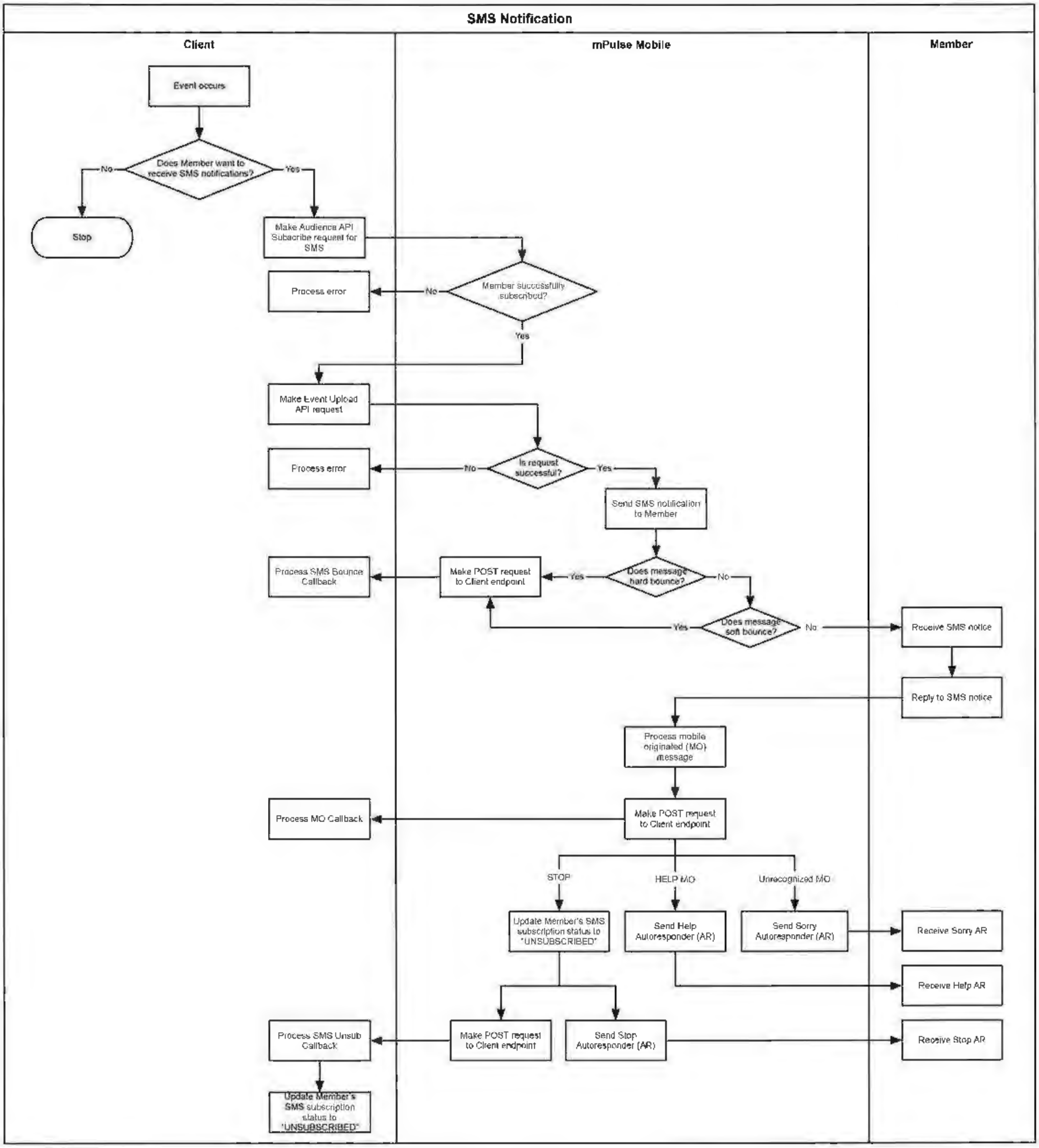
Each Member's Mobile Phone Number, Email Address, and App Member ID must be unique within your account and can be used to identify a Member record.

Personalizing Messages

Messages are personalized by including tokens (i.e., placeholders) that are populated from the Member profile or the Event Upload API request.

Sample Workflow Diagram

The workflow diagram below shows what a typical integration looks like. The workflow may be more or less complex depending on your business requirements.


SMS Notification
Client
mPulse Mobile
Member
Event occurs
Does Member want to receive SMS notifications?
No
Yes
Stop
Make Audience API Subscribe request for SMS
Member successfully subscribed?
No
Process error
Yes
Make Event Upload API request
Is request successful?
No
Process error
Yes
Send SMS notification to Member
Does message hard bounce?
Yes
Make POST request to Client endpoint
Process SMS Bounce Callback
No
Does message soft bounce?
Yes
No
Receive SMS notice
Reply to SMS notice
Process mobile originated (MO) message
Make POST request to Client endpoint
Process MO Callback
STOP
HELP MO
Unrecognized MO
Update Member's SMS subscription status to "UNSUBSCRIBED"
Send Help Autoresponder (AR)
Send Sorry Autoresponder (AR)
Receive Sorry AR
Receive Help AR
Make POST request to Client endpoint
Send Stop Autoresponder (AR)
Receive Stop AR
Process SMS Unsub Callback
Update Member's SMS subscription status to "UNSUBSCRIBED"

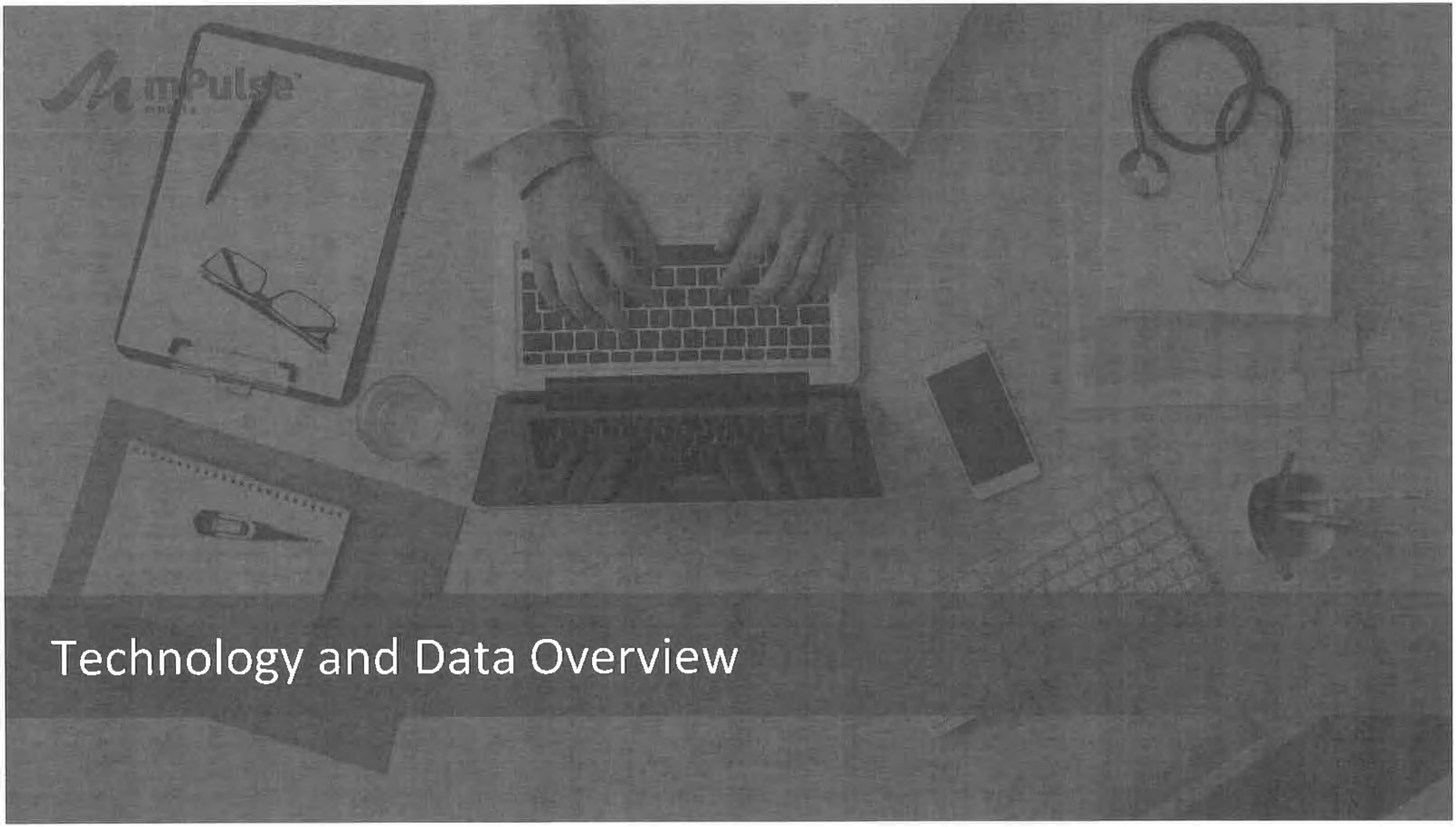
Additional Information

Please contact your Sales Director or Account Manager if you want to discuss these topics in more detail as they relate to your specific use case.

C

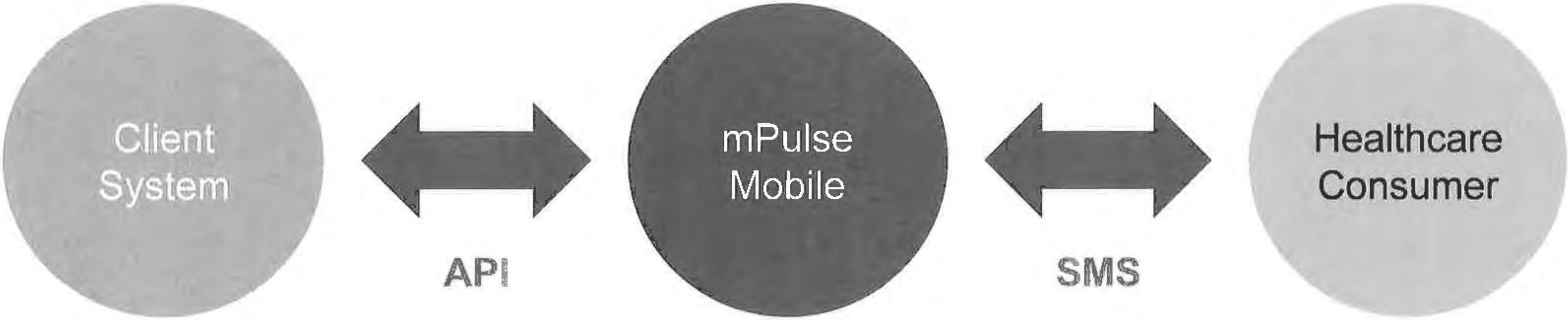
Exhibit C

mPulse Mobile Technology and Data



Technology and Data Overview

API



Methodology

1. Use Case

- Defining the use case is the first step towards implementing a mobile engagement program. The use case definition includes articulating a goal and the high-level interactions between healthcare consumers and your organization to achieve that goal.

2. Consumer Experience

- Designing the consumer experience is the next step. Together, the desired patient experience and the use case definition are used to identify, clarify, and organize solution requirements.

3. Solution / Business Logic

- Business logic will be defined in both customer and mPulse Mobile platforms and will vary by use case and by customer. The business logic will drive dialogues and data mappings.

4. Dialogues

- Once the use case, consumer experience, and business logic have been defined, mPulse Mobile will work with you to design the dialogues and message flows to be built in the mPulse Mobile platform.

5. Data

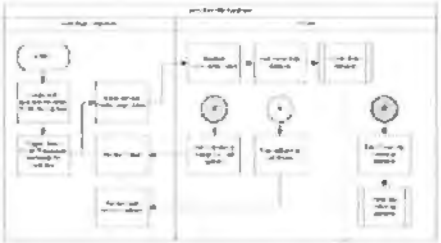
- Data sources and destinations to support the messaging program will be identified. Data elements include member and event attributes used for personalization, branching, and reporting. In this step, data going back to customer systems is also identified.

6. Reporting and Program Results

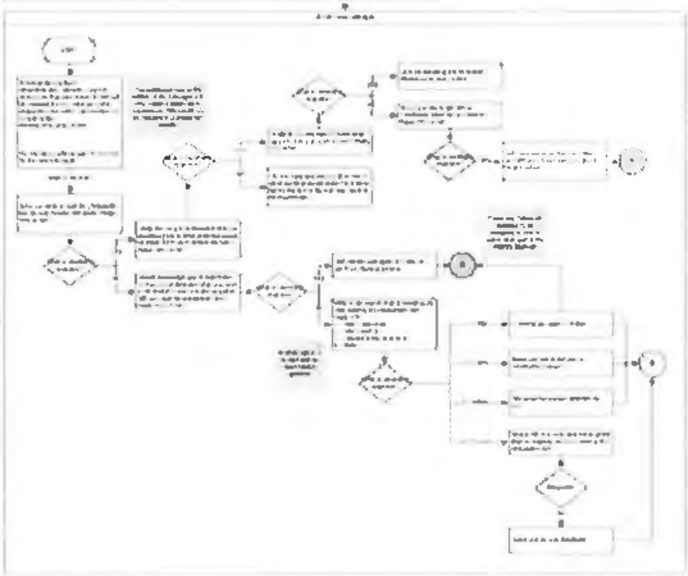
- Reporting is defined to support the use case and measure results.

Dialogue Development

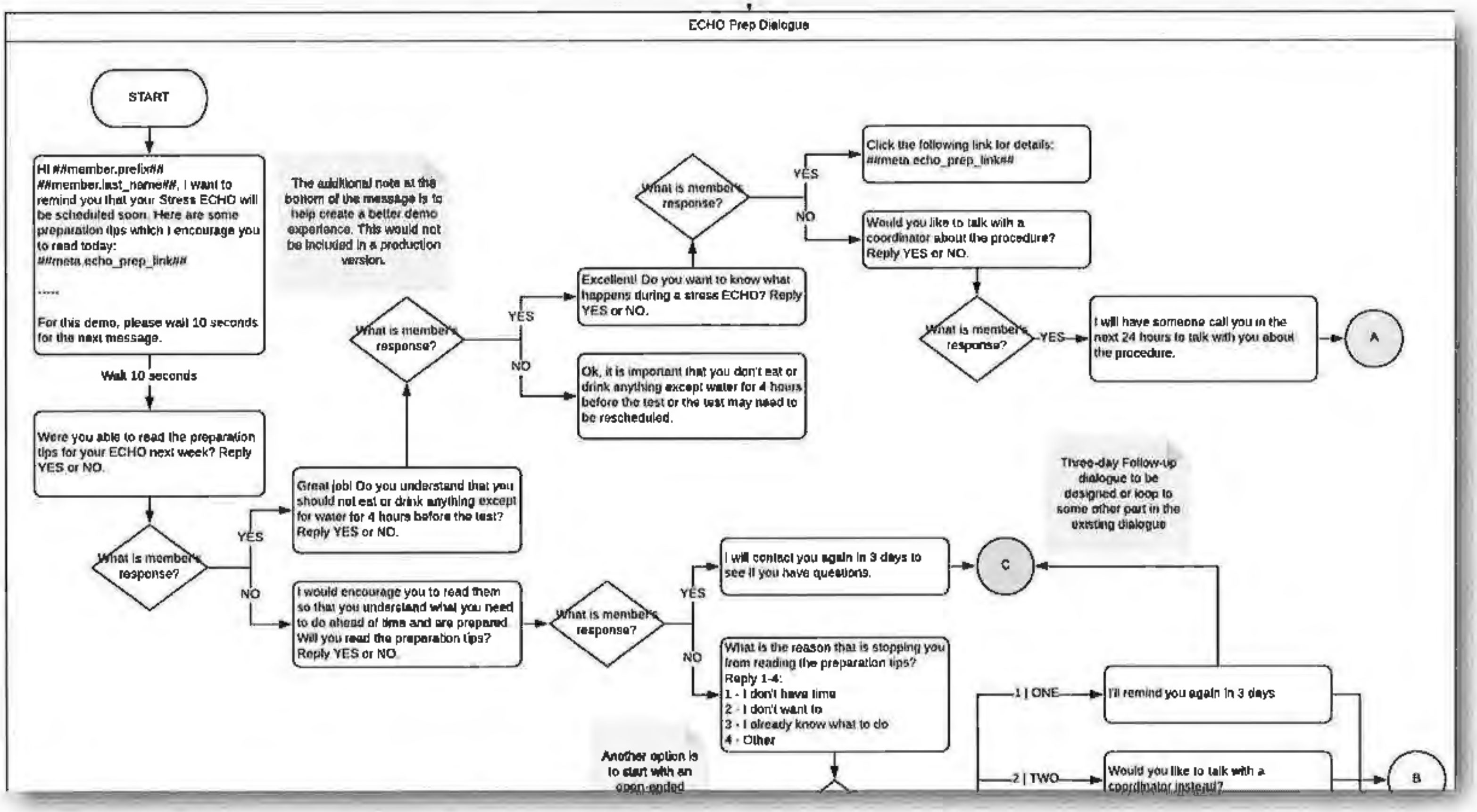
Customer Workflow



mPulse Dialogue



Dialogue Development



ECHO Prep Dialogue

START
Wait 10 seconds
What is member's response?
YES
NO
What is member's response?
YES
NO
What is member's response?
YES
NO
What is member's response?
YES
NO
What is member's response?
YES
A
C
B
1 | ONE
2 | TWO

Hi ##member.prefix## ##member.last_name##, I want to remind you that your Stress ECHO will be scheduled soon. Here are some preparation tips which I encourage you to read today: ##meta.echo_prep_link##

For this demo, please wait 10 seconds for the next message.

The additional note at the bottom of the message is to help create a better demo experience. This would not be included in a production version.

Were you able to read the preparation tips for your ECHO next week? Reply YES or NO.

Great job! Do you understand that you should not eat or drink anything except for water for 4 hours before the test? Reply YES or NO.

I would encourage you to read them so that you understand what you need to do ahead of time and are prepared. Will you read the preparation tips? Reply YES or NO.

Excellent! Do you want to know what happens during a stress ECHO? Reply YES or NO.

Ok, it is important that you don't eat or drink anything except water for 4 hours before the test or the test may need to be rescheduled.

Click the following link for details: ##meta.echo_prep_link##

Would you like to talk with a coordinator about the procedure? Reply YES or NO.

I will have someone call you in the next 24 hours to talk with you about the procedure.

Three-day Follow-up dialogue to be designed or loop to some other part in the existing dialogue

I will contact you again in 3 days to see if you have questions.

What is the reason that is stopping you from reading the preparation tips?
Reply 1-4:
1 - I don't have time
2 - I don't want to
3 - I already know what to do
4 - Other

I'll remind you again in 3 days

Would you like to talk with a coordinator instead?

Another option is to start with an open-ended

D

Exhibit D

mPulse Mobile Control Panel User Guide

mPulse Mobile Control Panel User Guide

Table of Contents

1 WHAT IS COVERED IN THIS GUIDE 3
1.1 WHAT IS NOT COVERED IN THIS GUIDE 3
2 LOGGING INTO THE MPULSE CONTROL PANEL 3
2.1 SETTING UP YOUR CONTROL PANEL ACCOUNT 3
2.2 LOGGING INTO THE CONTROL PANEL 4
3 CONTROL PANEL WALKTHROUGH: SENDING AN SMS MESSAGE 4
3.1 CREATING AN SMS-ENABLED LIST 4
3.2 SET UP AUTO-RESPONSE MESSAGES FOR YOUR LIST 5
3.3 ADDING MEMBERS TO A LIST 7
3.3.1 Importing members via CSV and other lists 7
3.3.2 Adding Members Manually 9
3.3.3 Unsubscribing members 10
3.4 CREATE A CAMPAIGN WITH SMS MESSAGES 10
4 MONITOR CAMPAIGN PERFORMANCE 14
4.1 VIEWING RESPONSES TO CAMPAIGN MESSAGES 14
4.2 VIEWING REPORTS AND DATA FROM A CAMPAIGN 15
5 MANAGING YOUR CONTROL PANEL ACCOUNT 17
APPENDIX 1: IMPORTANT TERMS 18
APPENDIX 2: CONTROL PANEL ACCOUNT ACCESS LEVELS 19
APPENDIX 3: FREQUENTLY ASKED QUESTIONS AND TROUBLESHOOTING 20
APPENDIX 4: CONTROL PANEL ACCOUNT ACCESS LEVELS .... ERROR! BOOKMARK NOT DEFINED.

1 What is covered in this guide

This document provides an overview of the core functionality of the mPulse Mobile Platform, administering your account on it, and instructions on how to send an SMS message. More detailed documentation about API integration and advanced functionality is available online at: https://mpulsemobile.atlassian.net/wiki/display/MPA/mPulse+Public+Access.

1.1 What is not covered in this guide

This guide is intended to cover the core functionality of the mPulse platform for account administrators. It does not detail functionality around certain advanced workflows, API integrations, member list segmentation, SMS poll questions, and custom fields. These topics should be covered with your main mPulse point of contact.

2 Logging into the mPulse Control Panel

The main interface for manually managing your mPulse account is The Control Panel (CP). From this web-based interface, you can manage your Members, Communications, and your Account. The Control Panel is used to manage lists of Members, create messages and workflows to communicate with them, and monitor how those campaigns are performing.

2.1 Setting up your Control Panel account

Data security and responsible messaging practices are high priorities for mPulse Mobile. As such, getting access to the Control Panel requires each user to take a few important steps once it has been determined that he or she should have access to the platform:

- First, **any computer trying to access the mPulse Platform must have its IP address "whitelisted" by mPulse Mobile for safe access**. Contact your mPulse Mobile Account Manager/Client Success Manager, or and give them your IP address so that it can be added to the safe list
    - NOTE: IP addresses are tied to the network you are connecting to mPulse from, not your computer itself. This means that users wanting to access the Control Panel from different locations/networks must white-list each IP address. mPulse recommends that **users who intend to access the platform frequently from different places use their organization's VPN**. To white-list a VPN IP address, contact your IT department to get the address (it is a different process than simply looking up a normal IP address) and pass that along to your Client Success Manager.

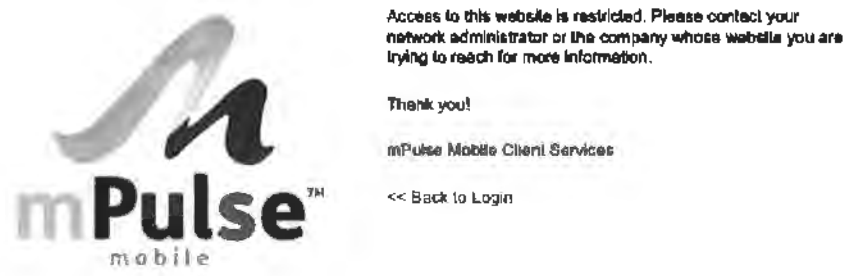
- Next, either **an existing administrator on your account, or your Client Success Manager, needs to add you to the Control Panel account**. To do this, they will need a name, email address, and mobile phone number (optional). If you are an administrator trying to add a new user, see section 5 of this guide.
    - Please note that there are no shared usernames and passwords i.e. a group user account similar to the current HRI group (Angelica Shea's team). You will need to create an excel file of all users on m5 with their access level, see Appendix 2 of this guide.

- Once you have been added, you will receive an email to the address you provided with a link that prompts you to create a password for the platform. This password must be at least 8 characters and must contain at least one upper case letter, lower case letter, a number, and a special character (.,!@#$% etc.)

2.2 Logging into the Control Panel

To log in, go to https://apps.mpulsemobile.com/. We recommend bookmarking this page. Your username is the email address you received the confirmation message at, and your password is the one you created via the link provided in the confirmation message.

- If you receive an error message when trying to log in, the most likely reason is that your IP address has not been whitelisted (see 2.1) This is the error message for an unrecognized IP Address. Contact your Account Manager or Client Success Manager if you see this and provide your IP address for whitelisting:



Access to this website is restricted. Please contact your network administrator or the company whose website you are trying to reach for more information.

Thank you!

mPulse Mobile Client Services

<< Back to Login

3 Control Panel Walkthrough: Sending an SMS Message

All communication sent through the mPulse platform takes the form of campaigns sent to lists of members. **Campaigns** are message workflows that can range from a simple announcement sent immediately to a list to complex and interactive messaging that are triggered under specific circumstances and can consist of dozens of messages sent over the course of months. **Members** are individuals identified on the platform by their unique cellphone numbers or email addresses and given a unique member ID. **Lists** are simply groups of members which are the recipients of different campaigns.

The Control Panel is the primary way to manually interact with the mPulse platform to create lists, add members, and message them in campaigns. From the Control Panel, you can:

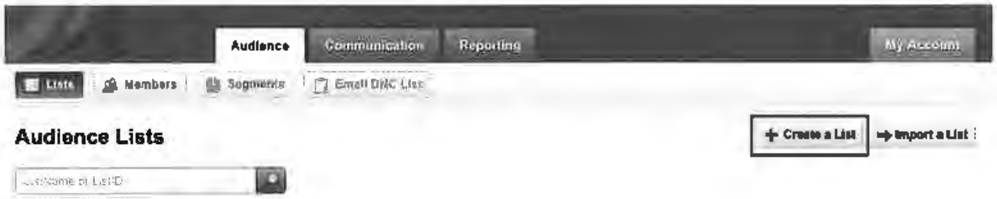
- Create lists of members
- Design and create communications campaigns for those members
- Launch and monitor those campaigns
- Generate and export reports with data on your campaigns.

This section will walk through how to do each of these core functions.

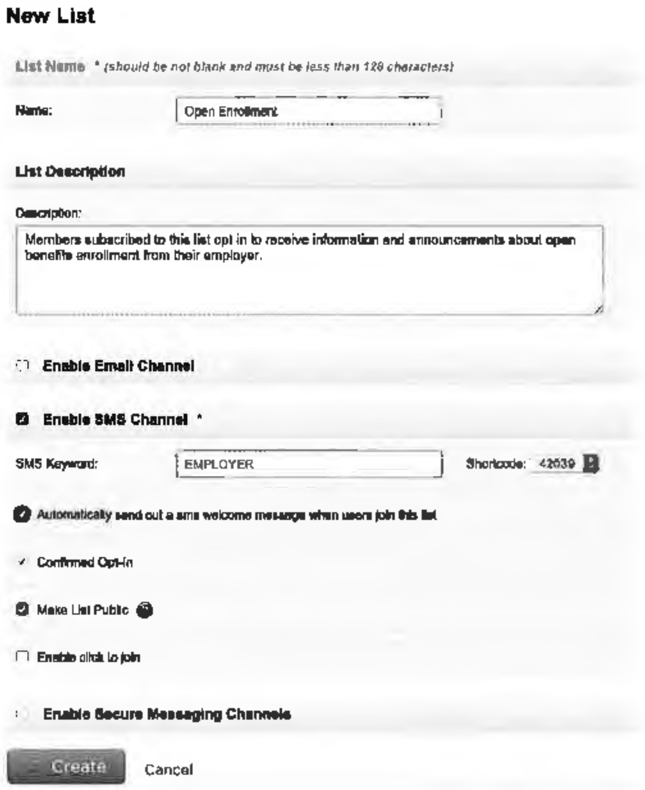
3.1 Creating an SMS-enabled list

In order to send an SMS message to a member, the member must be subscribed to SMS in a list. Therefore, we will first create an SMS-enabled list.

1. In Control Panel (CP), navigate to Audience > Lists, and click "+ Create a List".



2. Set up your list as shown below, with your preferred list name, description (optional) and keyword. The **keyword** is the string of letters and/or numbers a person can text to the short code and be added to the list. As such, you cannot use the same keyword for multiple lists on the same short code. Make sure to disable the email channel If you have more than one short code enabled on your account, select from the "Short code" dropdown menu the one you want to use. If you only have one enabled, then it will be selected by default. Click "Create" when done.



New List

List Name * (should be not blank and must be less than 128 characters)

Name: Open Enrollment

List Description

Description: Members subscribed to this list opt in to receive information and announcements about open benefits enrollment from their employer.

☐ Enable Email Channel

☒ Enable SMS Channel *

SMS Keyword: EMPLOYER   Shortcode: 42039

● Automatically send out a sms welcome message when users join this list

✓ Confirmed Opt-In

☑ Make List Public

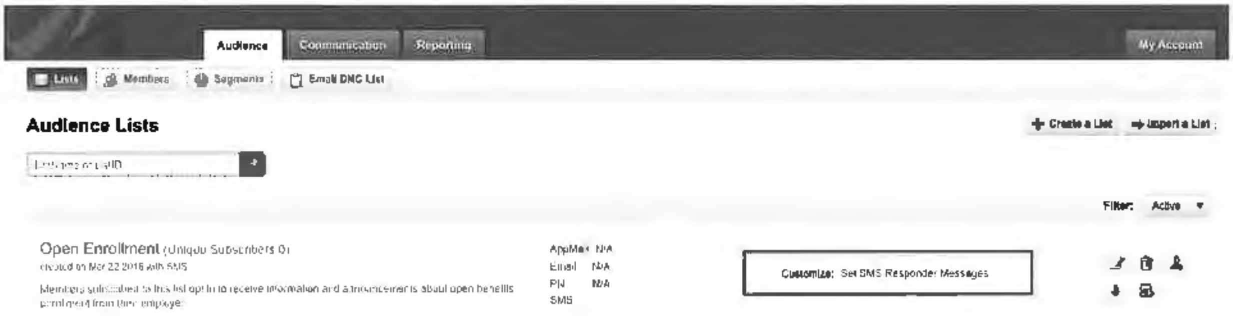
☐ Enable click to join

○ Enable Secure Messaging Channels

3.2 Set up auto-response messages for your list

With a list set up, you need to customize the messages that are automatically sent out to its members in different situations.

1. In the Audience view, click "Set SMS Responder Messages"



Audience Lists

Open Enrollment (Unique Subscribers 0)
created on Mar 22 2016 with SMS
Members subscribed to this list opt in to receive information and announcements about open benefits enrollment from their employer

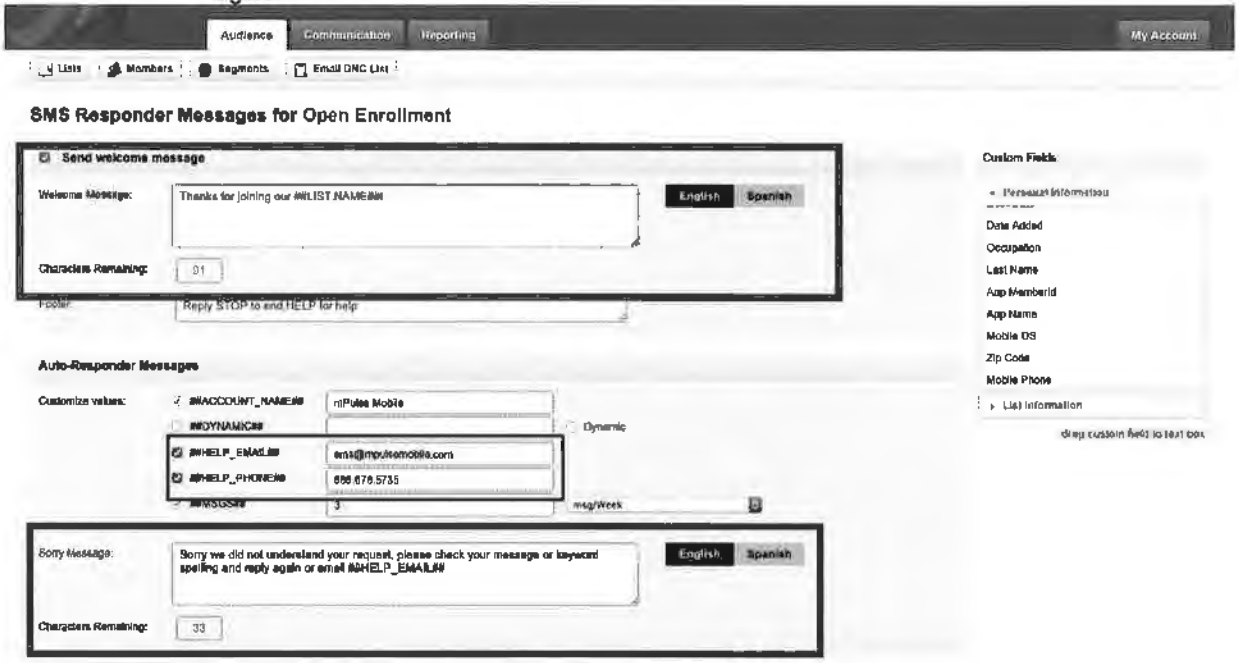
AppMax	N/A
Email	N/A
PN	N/A
SMS	

Customize: Set SMS Responder Messages

2. Review and edit (if needed) the welcome message at the top. This is automatically sent to members who text the list keyword to your short code. If you prefer to welcome new members through a campaign, you may disable this message by unchecking the box next to "Send welcome message" or by editing your list on the audience view and disabling the "Automatically send out a sms welcome message when users join this list" option. You should also review the "Sorry Message" in the middle of the panel, which is triggered when a member responds with something that is not recognized by any of the list's campaigns.

3. In both, there are variables surrounded by number symbols like "##LIST.NAME##" which is how the platform shows custom information. The default Welcome Message (shown below) is "Thanks for joining our ##LIST.NAME##!" which would read on a member's phone as "Thanks for joining our Open Enrollment!" in this case. To add different custom fields, you can drag and drop the desired information type from the box on the left into the desired message.

4. The only other area you should review on this screen is the Help Email and Help Phone fields. These should be consistent with your organization's policies and structure. For instance, an Open Enrollment list like the one in this example would might use an employer's HR help line and general HR/benefits inbox for members who have questions or difficulties. That help email is automatically included in the Sorry Message by default in the form of the variable "##HELP_EMAIL##". When the messages and help info are set up to your requirements, click "audience" to return to your list view. NOTE: the grayed boxes and options can all be customized via your mPulse client success manager.



SMS Responder Messages for Open Enrollment

☑ Send welcome message

Welcome Message: Thanks for joining our ##LIST.NAME##

Characters Remaining: 91

Footer: Reply STOP to end HELP for help

Auto-Responder Messages

Customize values:
✓ ##ACCOUNT_NAME## mPulse Mobile
□ ##DYNAMIC## ○ Dynamic
☑ ##HELP_EMAIL## ema@mpulsemobile.com
☑ ##HELP_PHONE## 888.676.5735
✓ ##MSGS## 3 msg/Week

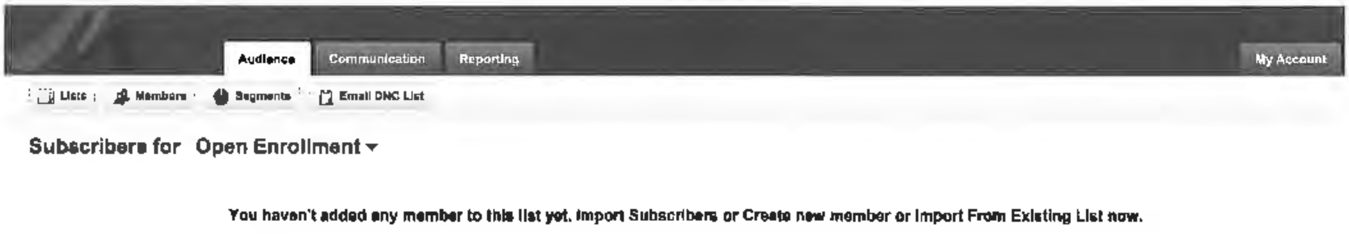
Sorry Message: Sorry we did not understand your request, please check your message or keyword spelling and reply again or email ##HELP_EMAIL##

Characters Remaining: 33

3.3 Adding members to a list

Now that our list is set up, we need members to send messages to. For an SMS message to be sent to a member, he or she must be both on the list associated with a messaging campaign, and subscribed to receive SMS messages on that list. This section will walk through the different ways to add members to a list. To begin, click the name of the list from the Audience Lists screen, which will take you to that list's set of subscribers. For lists that don't have any, you will see the following message that prompts you to pick one of the three ways to manually add members.

COMPLIANCE NOTE: Anytime you add a NEW member to a list, the Telephone Consumer Protection Act of 1991 (TCPA) REQUIRES you to send them a welcome message with the option of replying "STOP" to opt-out within 48 hours.



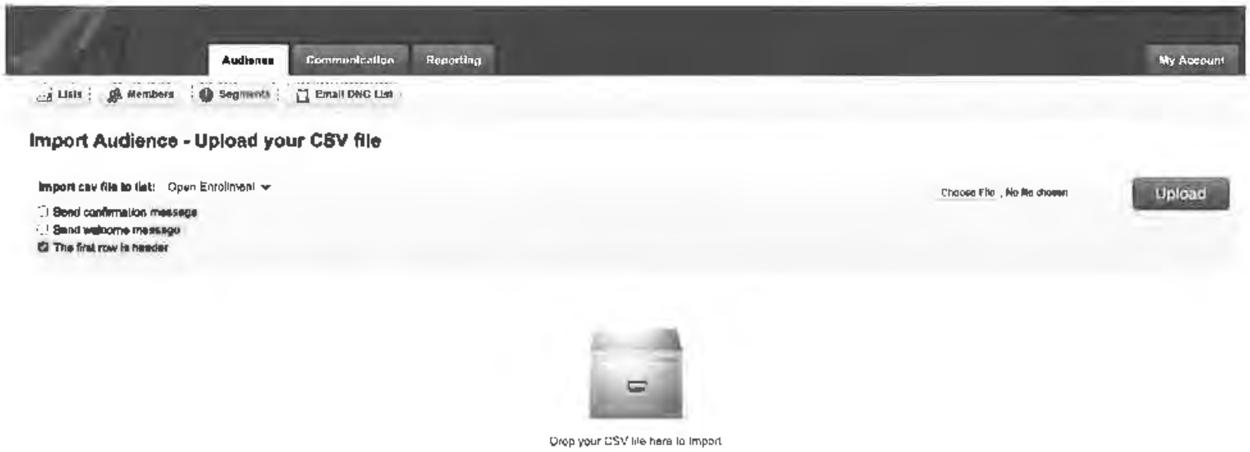
Subscribers for Open Enrollment ▾

You haven't added any member to this list yet. Import Subscribers or Create new member or Import From Existing List now.

3.3.1 Importing members via CSV and other lists

The fastest way to add a number of members to the platform is via an import from a spreadsheet file or from an existing list. To import from an existing list, click the prompt or the "add subscribers" button. Follow the prompts to select the list you want to copy members from and select whether to restrict the import to only active members, members who are subscribed to a particular channel (SMS), and if you want to update the subscriptions of the members who's phone number matches one you are attempting to import. The platform will not duplicate the number; selecting this option only means that the member's subscription to different channels on this list will be replaced with whatever it is on the other list you are importing from.

To import via CSV, click "Import Subscribers" and select a .csv file for upload. Note the options on the left, especially the "First row is header" column that lets the platform know to omit column labels when importing. The "Send welcome message" option will, if selected, send a welcome to NEW members only (not ones that are already on the list and have already been welcomed). As noted above, the TCPA requires new members to be welcomed within 48 hours of subscription to an SMS campaign.



Import Audience - Upload your CSV file

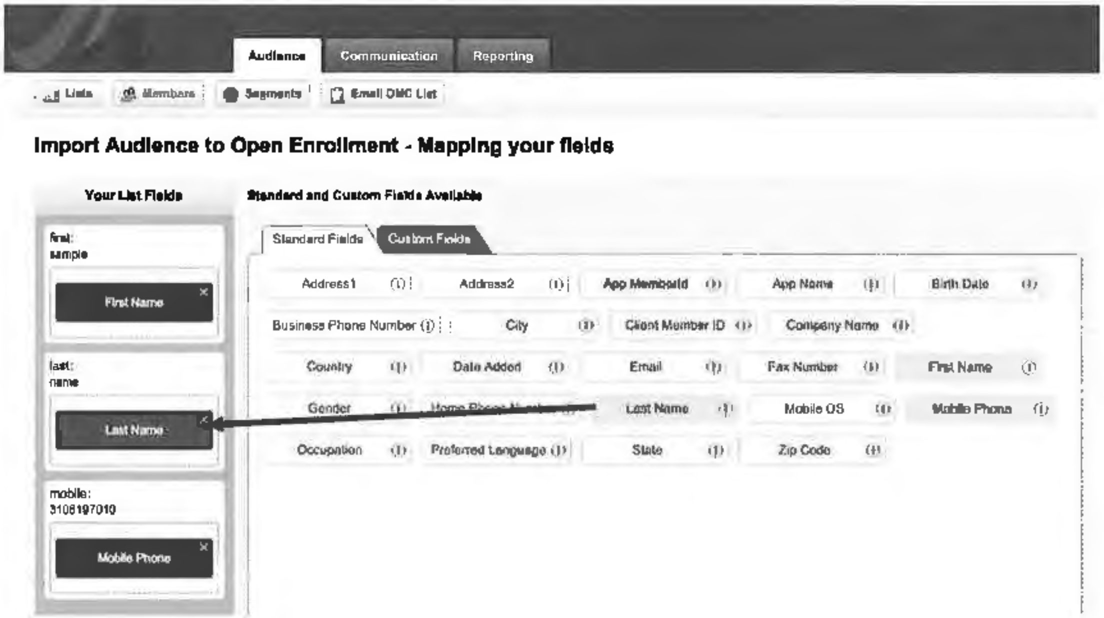
Import csv file to list: Open Enrollment ▾

□ Send confirmation message
□ Send welcome message
☑ The first row is header

No file chosen

Drop your CSV file here to import

After uploading a CSV, you will be taken to a page that allows you to map each column of your spreadsheet to a field in the member profile (e.g., you make the columns of first names in the file map to the "first name" field in the platform). Your list fields will display on the left hand side and you simply drag and drop standard or custom fields over to each column to match the data to the field (see below). Click complete to finish importing. This process can take a few minutes and you will receive an email notifying you when it is completed.



Import Audience to Open Enrollment - Mapping your fields

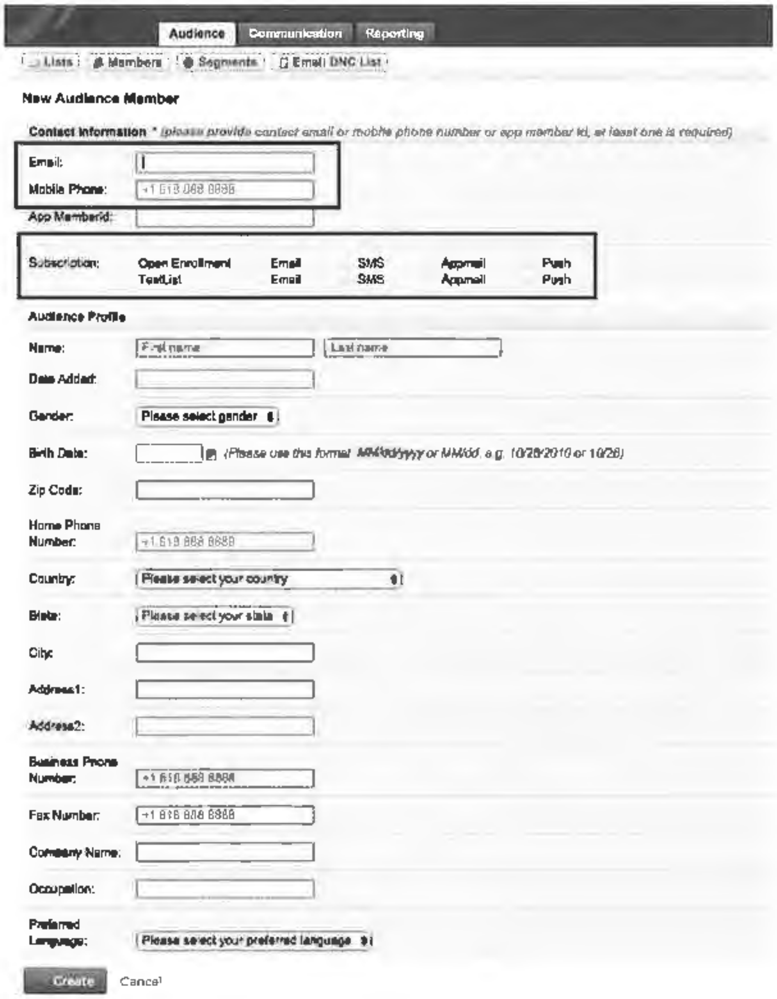
first:
sample

last:
name

mobile:
3108197010

3.3.2 Adding Members Manually

The other way to add members via the Control Panel is manually by inputting their information directly into the platform. To do this, click “new member” in the Audience Member view. You will be directed to a data sheet that looks like this:



New Audience Member

Contact Information * *(please provide contact email or mobile phone number or app member id, at least one is required)*

Email:

Mobile Phone: +1 619 888 8888

App Memberid:

Subscription:	Open Enrollment	Email	SMS	Appmail	Push
	TestList	Email	SMS	Appmail	Push

Audience Profile

Name: First name Last name

Date Added:

Gender: Please select gender

Birth Date: *(Please use this format: MM/dd/yyyy or MM/dd, e.g. 10/28/2010 or 10/28)*

Zip Code:

Home Phone Number: +1 619 888 8888

Country: Please select your country

State: Please select your state

City:

Address1:

Address2:

Business Phone Number: +1 619 888 8888

Fax Number: +1 619 888 8888

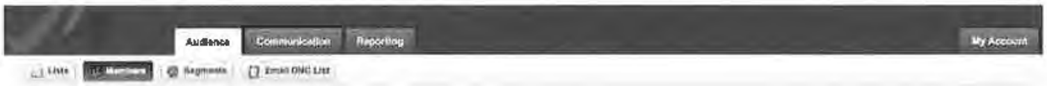
Company Name:

Occupation:

Preferred Language: Please select your preferred language

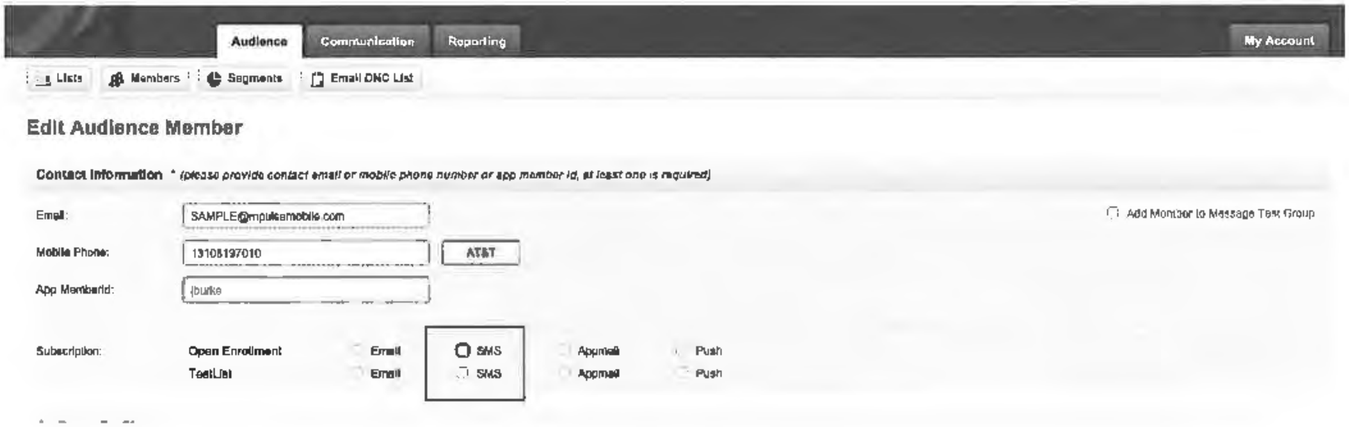
For the purposes of sending messages, the **platform will only need an email address or a mobile number to create a member** (except for secure messaging, which requires a specific AppID code). Other information like name, address, company name, etc. and any custom fields that your organization has set up via your Client Success Manger can be used for more specific member segmentation and more customized messaging. Ask your account manager or Client Success Manager about leveraging these options.

When finished entering a mobile number and any other necessary info, click create to finish. You can view and edit member details, or delete members from the platform, at any time by clicking the Audience tab and selecting “members” to see a list of them.



3.3.3 Unsubscribing members

If you need to remove a member from a list, the easiest way to do so is to find them on the member's section of the audience tab and click the pencil on his or her entry to edit. It is best practice not to delete the whole member profile. Rather, simply un-check the SMS channel boxes on the profile and click "update" at the bottom of the screen (see below).



Edit Audience Member

Contact Information * (please provide contact email or mobile phone number or app member id, at least one is required)

Email: SAMPLE@mpulsemobile.com

Mobile Phone: 13108197010

App MemberId: jburke

Subscription:

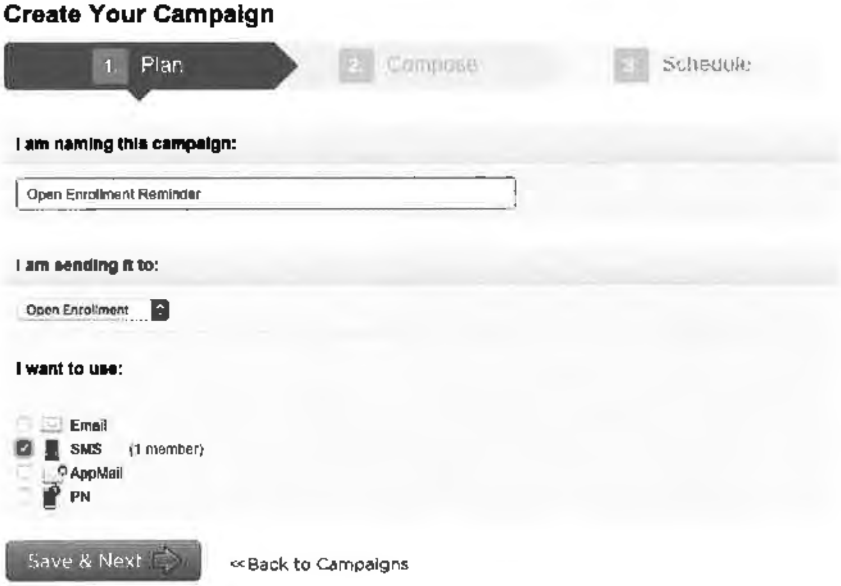
Open Enrollment	○ Email	○ SMS	○ Appmail	○ Push
TestList	○ Email	○ SMS	○ Appmail	○ Push

3.4 Create a campaign with SMS messages

We have a list of members, so now we need to create our messaging to them. As noted above, all communication in the mPulse platform takes the form of **campaigns.** We will create a campaign that will be sent to the list we just created. **Only Members subscribed to the List – and who are subscribed to the SMS channel – can be messaged.** The following is a walk-through of the process to create a campaign set to trigger immediately or on a set date/time.

1. In Control Panel, navigate to the Communication tab, click the Campaigns button, and select "+ New Campaign".

2. Plan your campaign as shown below, with an easily identifiable name and set to send to the correct list with the SMS channel selected:



Create Your Campaign

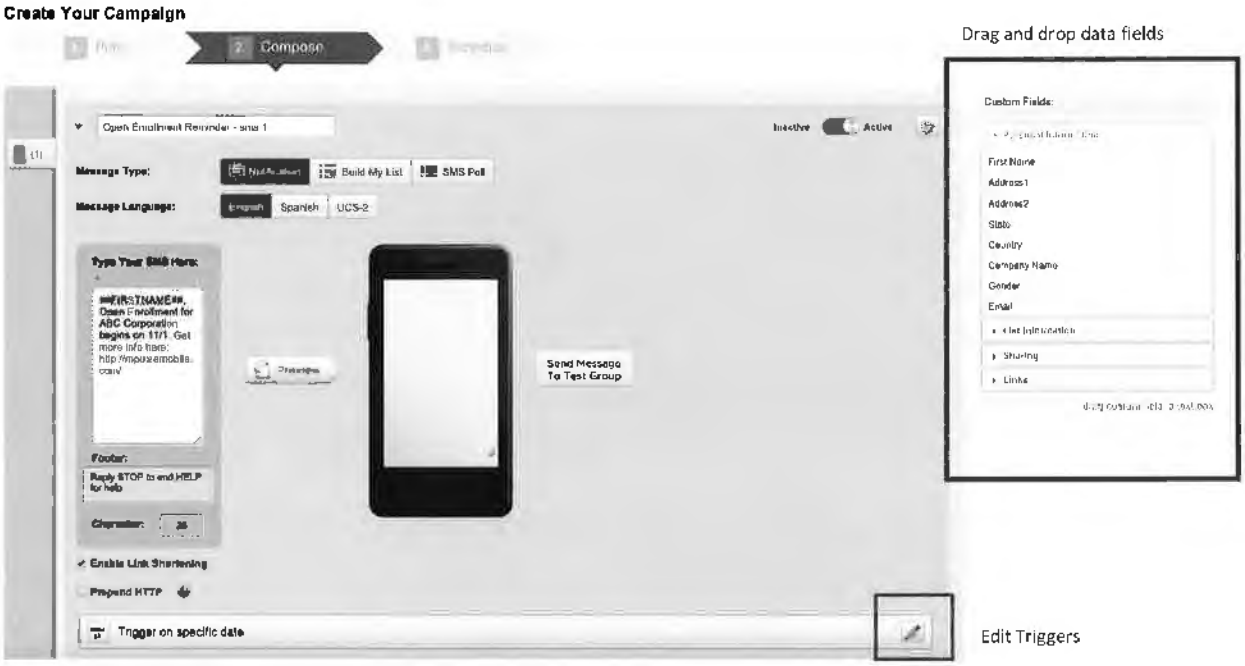
I am naming this campaign: Open Enrollment Reminder

I am sending it to: Open Enrollment

I want to use:

- □ Email
- ☑ SMS (1 member)
- □ AppMail
- □ PN

3. Compose your first message to fit your needs, as shown below. NOTE: it is best practice to Enable Link Shortening at the bottom of the compose field when including a link in a message. This allows the platform to track whether a member clicks a link you send in a message, allowing you to gather better engagement data and program messages to be sent to members based on whether they clicked a link in a previous message (see step 10 of this list).



Create Your Campaign

Open Enrollment Reminder - sms 1

Message Type: Notification

Message Language: English

Type Your SMS Here:

##FIRSTNAME##, Open Enrollment for ABC Corporation begins on 11/1. Get more info here: http://mpulsemobile.com/

Footer: Reply STOP to end HELP for help

✓ Enable Link Shortening

○ Prepend HTTP

Trigger on specific date

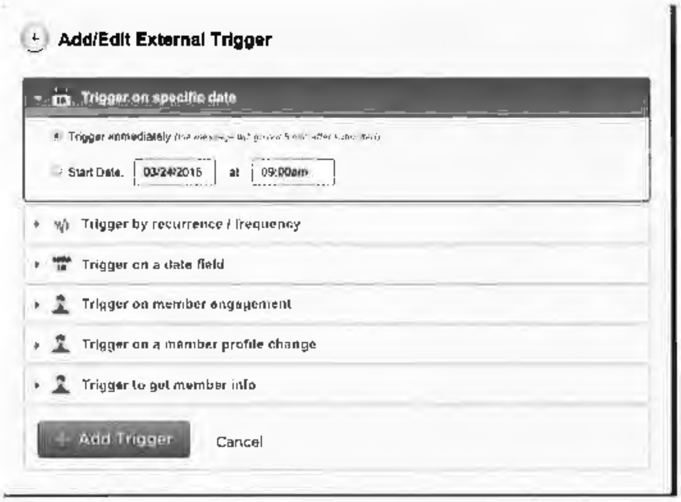
Drag and drop data fields

Edit Triggers

4. Values from the member profile field can be used to personalize messages by using variables (e.g., ##FIRSTNAME##) that you can drag over from the box on the right side of the compose screen. Variables are replaced with the field's value when compiling the actual message for a member. So in this example, the member would receive a text that reads: "Jim, Open Enrollment for ABC Corporation beings on 11/1. Get more info here: mp0.co/JBGd Reply STOP to end, HELP for help" (see highlighted box above).

5. Messages are sent when they are **triggered.** These triggers can be tied to customized events and interactions and integrated to your organization's other systems via API integrations. For this guide, we will outline how to send messages immediately, upon subscription, and on a specific date and time. To edit triggers, click the pencil in the bottom right of the compose screen.

6. The first, and most straightforward trigger is for a **specific date** (see below). You can set it to trigger immediately, which will send the message the moment that the campaign is launched, or select a specific date and time. (Note: if your organization spans multiple time zones and you are unsure which one your account uses by default, check with your Client Success Manager).



Add/Edit External Trigger

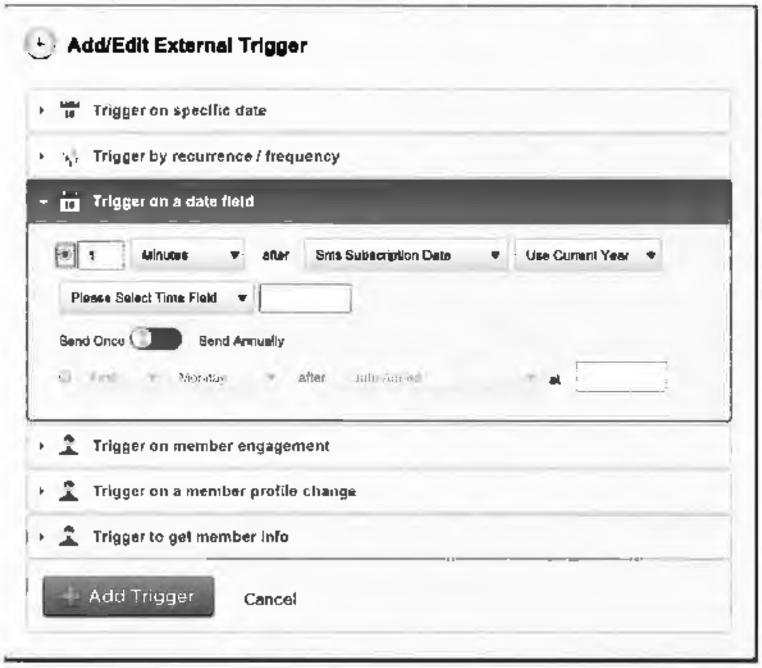
Trigger on specific date

● Trigger immediately

○ Start Date. 03/24/2015 at 09:00am

Trigger by recurrence / frequency
Trigger on a date field
Trigger on member engagement
Trigger on a member profile change
Trigger to get member info
Add Trigger
Cancel

7. The other primary way to trigger messages is on a "**date field**" (see below). This trigger sends messages once a particular date or time requirement has been met. The most common way to use this trigger is shown below, where it is set to send the message soon after (usually 0 or 1 minute) after a member is subscribed to the SMS channel on the list. In practice, a user could text the keyword in to the short code –which would both subscribe him or her to the list and also subscribe the number to the SMS channel – and would receive the message immediately after. This can take the place of the list's welcome message, which you would disable on the list screen (see 3.4, step 4).

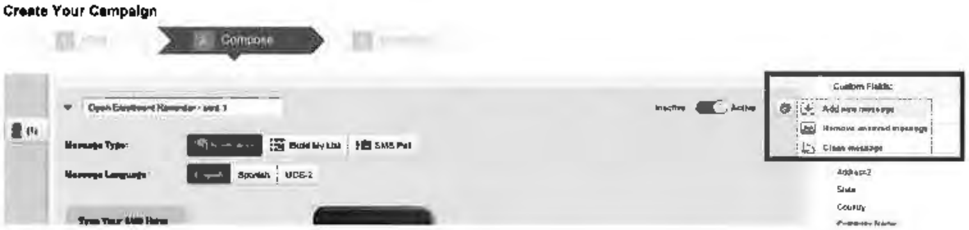

Add/Edit External Trigger
Trigger on specific date
Trigger by recurrence / frequency
Trigger on a date field
Trigger on member engagement
Trigger on a member profile change
Trigger to get member info
Add Trigger
Cancel

Trigger on a date field: 1 Minutes after Sms Subscription Date, Use Current Year

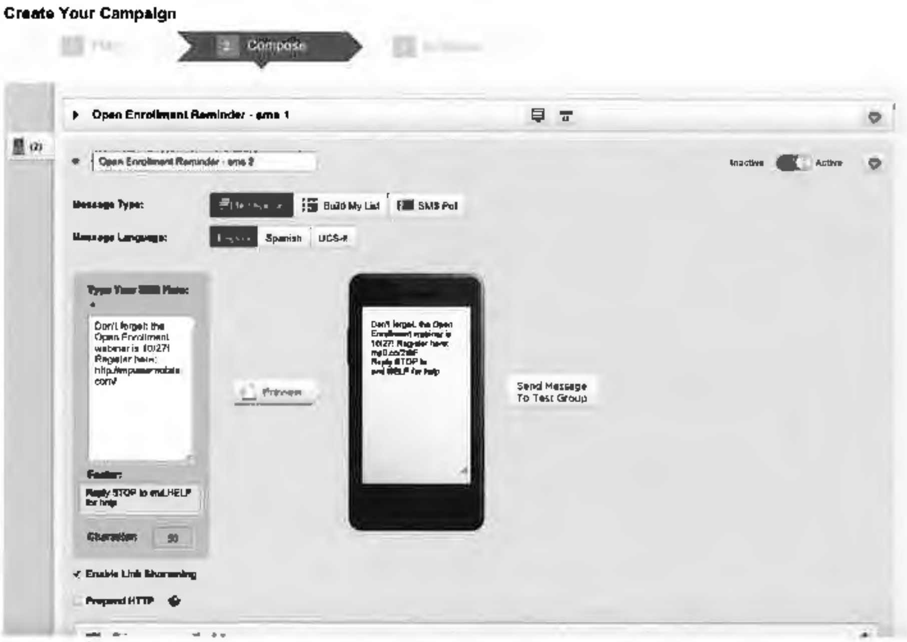
Please Select Time Field

Send Once / Send Annually

8. The next trigger we will cover is for messages in campaigns that have multiple SMS messages going out to members. To demonstrate, you will need to add a new message to the campaign. To add additional messages, click the gear symbol in the top right of the Compose field (see below)



9. Compose the second message to your liking:



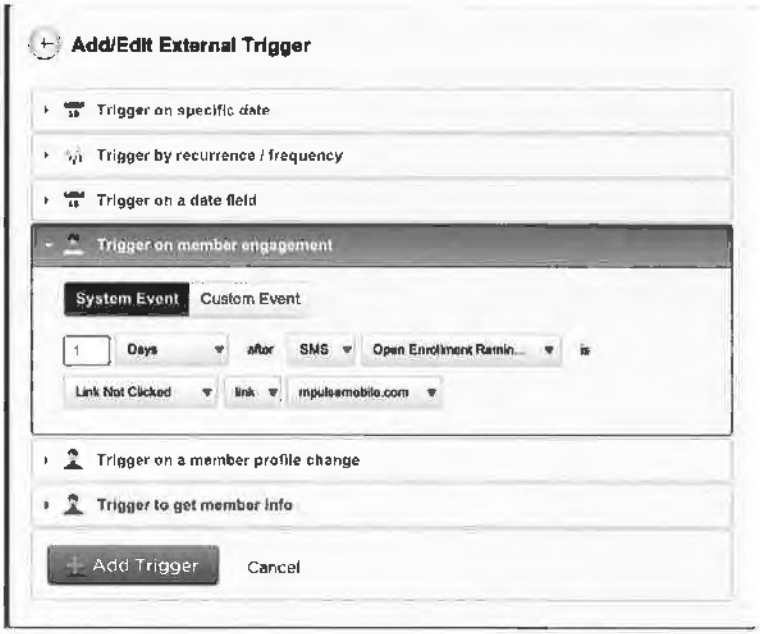
Create Your Campaign

Don't forget: the Open Enrollment webinar is 10/27! Register here: http://mpulsemobile.com/

Reply STOP to end,HELP for help

Don't forget: the Open Enrollment webinar is 10/27! Register here: mp0.co/2t6F Reply STOP to end HELP for help

10. Edit the trigger by clicking the pencil in the bottom right corner of the compose field and select **"Trigger on member engagement."** This trigger is often used to send messages tied to custom events that are sent to the platform via API integrations and require set up and training by your Account Manger or Client Success Manager. In this walk-through, we will use the standard system events. As shown below, you can set up this second SMS to be sent after a member engages with a previous message in the campaign in a certain way. The example here is for our second message to be sent one day after the first message, to the members who did not click the link in the first one.



Add/Edit External Trigger

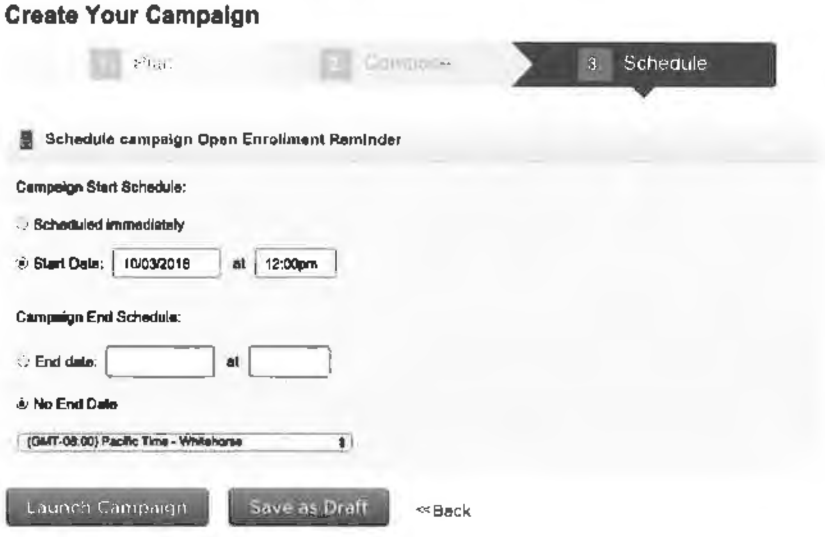
Trigger on specific date
Trigger by recurrence / frequency
Trigger on a date field
Trigger on member engagement
System Event
Custom Event

1 Days after SMS Open Enrollment Remin... is
Link Not Clicked link mpulsemobile.com

Trigger on a member profile change
Trigger to get member info
+ Add Trigger
Cancel

11. Click "+ Add Trigger" when done setting up each message's trigger and click "Next" when finished with all of the messages in the campaign.

12. This will take you to the "Schedule" field, where you can set the start and end date/time for your campaign. When it is set to your preference, you can launch the campaign or save it to be edited and launched later. NOTE: when you launch a campaign, there is an automatic 5-minute waiting period before the campaign is launched. During this time, you have the opportunity to halt the launch if you notice a mistake.



Create Your Campaign

1. Plan 2. Compose 3. Schedule

Schedule campaign Open Enrollment Reminder

Campaign Start Schedule:

○ Scheduled immediately

● Start Date: 10/03/2016 at 12:00pm

Campaign End Schedule:

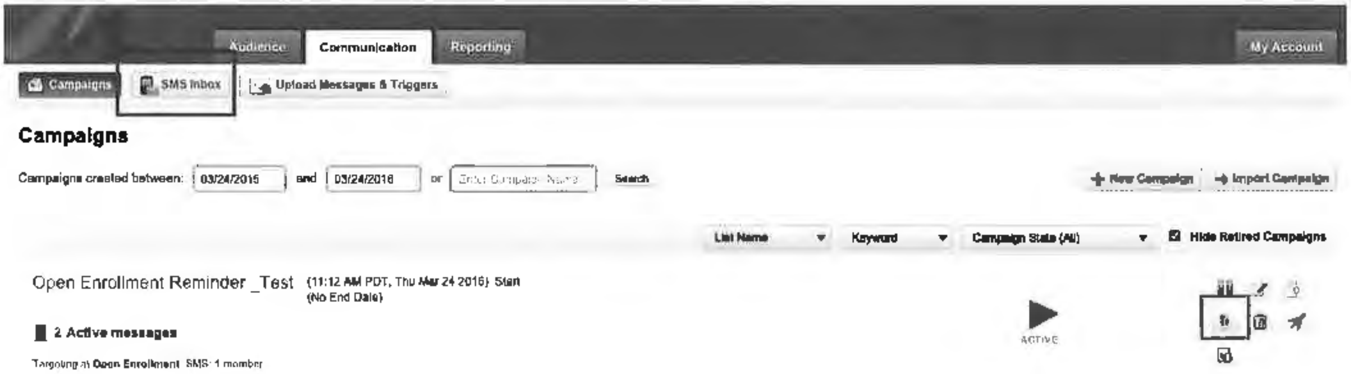
○ End date: at

● No End Date

(GMT-08:00) Pacific Time - Whitehorse

4 Monitor Campaign Performance

The Campaigns tab of the Control Panel allows you to create messaging workflows (see section 3.4) as well as track the results of those campaigns. This section will outline the key processes on the Control Panel to gather and review campaign data.



Campaigns

Campaigns created between: 03/24/2015 and 03/24/2016 or Enter Campaign Name Search

☑ Hide Retired Campaigns

Open Enrollment Reminder _Test (11:12 AM PDT, Thu Mar 24 2016) Start (No End Date)

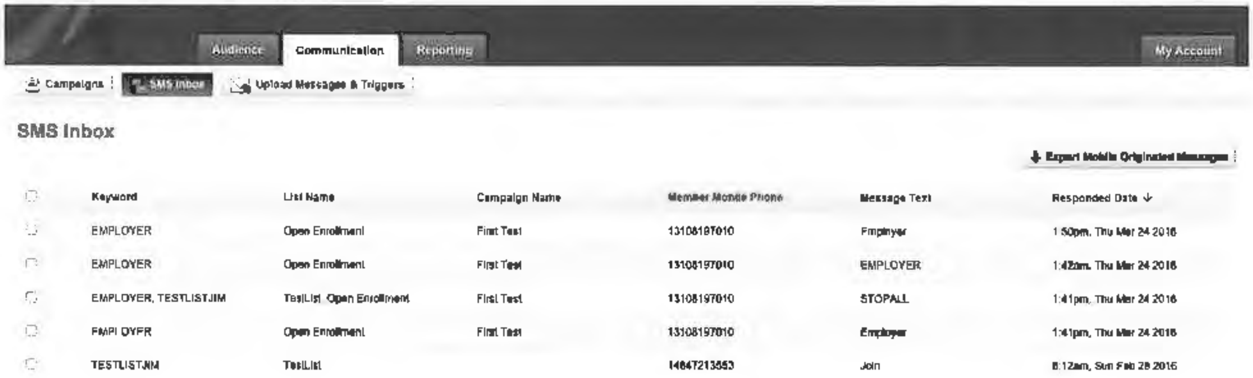
2 Active messages

Targeting at Open Enrollment SMS: 1 member

4.1 Viewing responses to campaign messages

To look at any and all responses from members who have received messaging while on one of your account's lists, click the **"SMS Inbox" button** near the top of the Communication tab. You will see a sortable, exportable list with the member's mobile number, the text he or she sent to your account, the date they texted your short code, and which campaigns and lists their response is related to (see below).

NOTE: The mPulse platform has advanced features that help understand, automate and streamline responses to members' texts to your short code. Contact your Client Success Manager if your organization anticipates a large volume of varied member responses to your campaign.

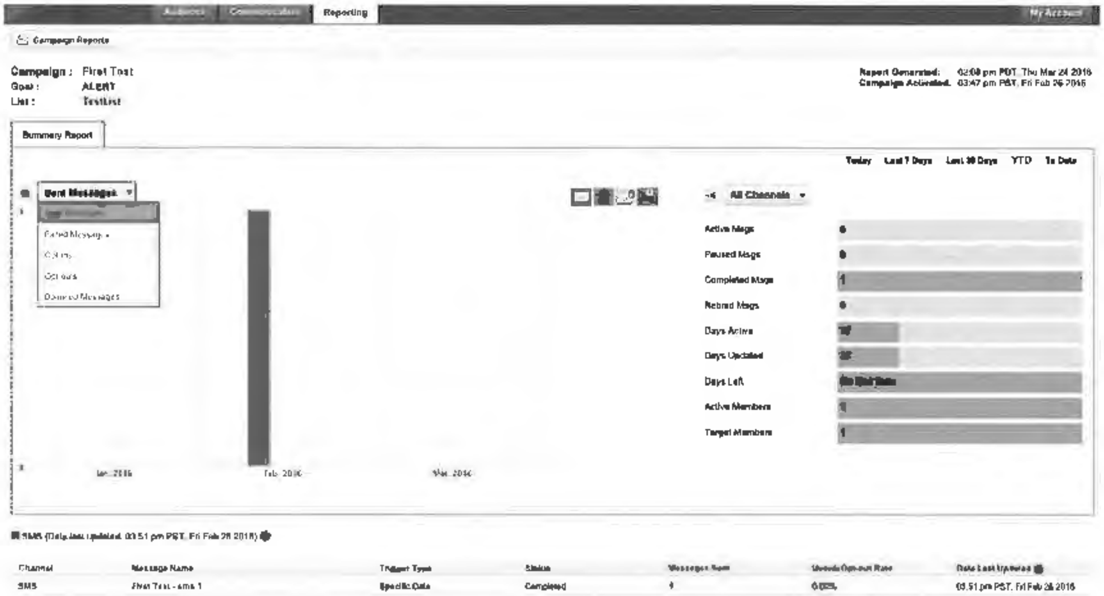


SMS Inbox

Keyword	List Name	Campaign Name	Member Mobile Phone	Message Text	Responded Date ↓
EMPLOYER	Open Enrollment	First Test	13108197010	Employer	1:50pm, Thu Mar 24 2016
EMPLOYER	Open Enrollment	First Test	13108197010	EMPLOYER	1:42am, Thu Mar 24 2016
EMPLOYER, TESTLISTJIM	TestList, Open Enrollment	First Test	13108197010	STOPALL	1:41pm, Thu Mar 24 2016
EMPLOYER	Open Enrollment	First Test	13108197010	Employer	1:41pm, Thu Mar 24 2016
TESTLISTJIM	TestList		14847213553	Join	8:12am, Sun Feb 28 2016

4.2 Viewing reports and data from a campaign

To generate, and review platform data about you campaign, you can click the bar chart logo next to your campaign on the Audience tab, or click to the "Reporting" tab at the top of the Control Panel and select "View Report" next to your desired campaign. You will be taken to a summary page that allows you to sort by channel, time frame, and data type (sent messages, failed messages, opt-outs, opt-ins, and bounced messages) to graph as well as specific statistics around each message in the campaign on a list below the chart.



Campaign : First Test
Goal : ALERT
List : TestList

Report Generated: 02:08 pm PDT, Thu Mar 24 2016
Campaign Activated: 03:47 pm PST, Fri Feb 26 2016

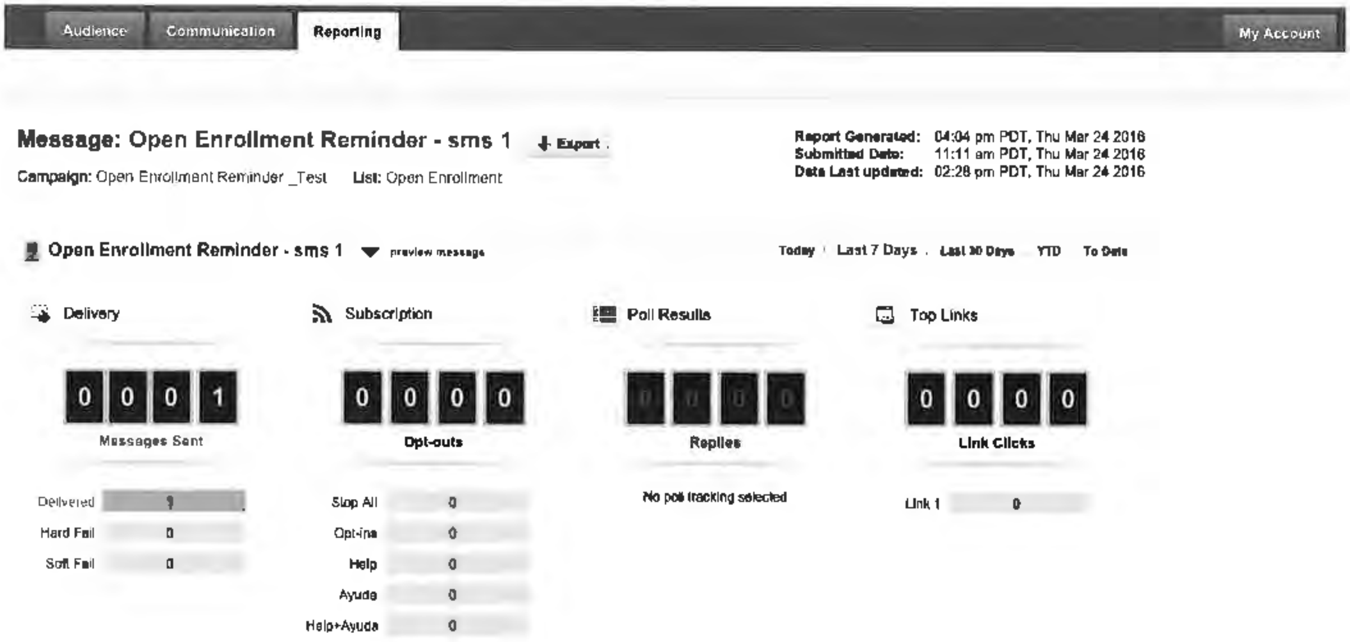
Active Msgs	0
Paused Msgs	0
Completed Msgs	1
Retired Msgs	0
Days Active	27
Days Updated	27
Days Left	No End Date
Active Members	1
Target Members	1

SMS (Data last updated: 03:51 pm PST, Fri Feb 26 2016)

Channel	Message Name	Trigger Type	Status	Messages Sent	Unsubs/Opt-out Rate	Date Last Updated
SMS	First Test - sms 1	Specific Date	Completed	1	0.00%	03:51 pm PST, Fri Feb 26 2016

To export this data, click on a message from that list. This will direct you to a dashboard (see below) that displays detailed statistics on delivery, opt-ins/outs, failure rates, and link clicks. This data can be exported at any time by clicking the "export" button at the top of this screen. NOTE: it is best practice to wait a full 24 hours after a message has been sent before reviewing and exporting this data. This is because certain cellular carriers take longer to report back their data to the mPulse platform, which makes reports that are run shortly after a message is sent sometimes incomplete or inaccurate until a full day has passed.

Clicking any of the categories will take you to a list of the members who fall into that category. These lists are also exportable, allowing you to generate an .xls file of, for instance, every member who has opted-out or who has clicked a link in the message.



Message: Open Enrollment Reminder - sms 1

Campaign: Open Enrollment Reminder _Test **List:** Open Enrollment

Report Generated:	04:04 pm PDT, Thu Mar 24 2016
Submitted Date:	11:11 am PDT, Thu Mar 24 2016
Data Last updated:	02:28 pm PDT, Thu Mar 24 2016

Open Enrollment Reminder - sms 1

Delivery

0 0 0 1

Messages Sent

Delivered	1
Hard Fail	0
Soft Fail	0

Subscription

0 0 0 0

Opt-outs

Stop All	0
Opt-ins	0
Help	0
Ayuda	0
Help+Ayuda	0

Poll Results

0 0 0 0

Replies

No poll tracking selected

Top Links

0 0 0 0

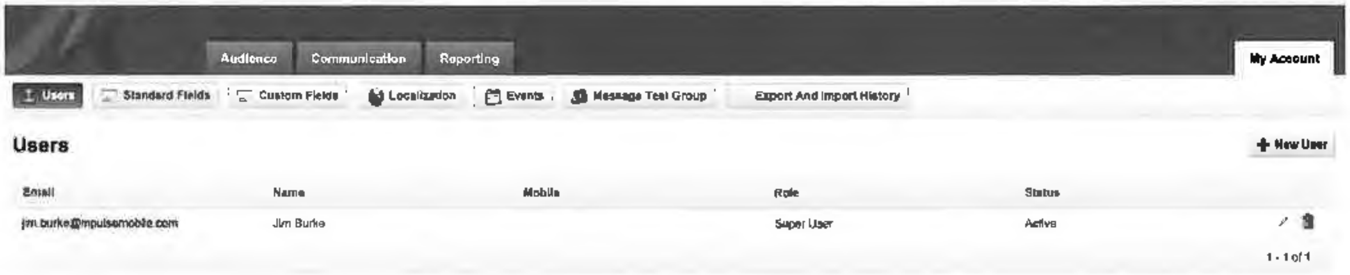
Link Clicks

Link 1	0

5 Managing your Control Panel account

The Control Panel supports as many individual user accounts as your organization needs. To fit with your organizational structure, Control Panel users can be set up to have different levels of access, visibility, and permissions – See Appendix 2 of this guide for a breakdown of every role, their permissions, and their restrictions. Every account on the mPulse platform has a designated "Super User" who has the highest level of control over the permissions and access of the other users on your account. If you have any questions about your level of access, contact your account's Super User, or your Account Manager or Client Success Manager.

To see all of the different users on your control panel account and to add, edit, and remove users (including your own account), click the "My Account" tab on the far right of the Control Panel. This will display a list of users with options to edit or remove the account on the right (see below). You can also click the "+ New User" button in the top left of this view and input the new Control Panel user's info. Note that, as mentioned in section 2.1 of this guide, a new user will need to use an IP address that has been white-listed by your mPulse Client Success Manger. Adding a member on this screen will send the new user a confirmation email to set up the account.



Users

Email	Name	Mobile	Role	Status
jim.burke@mpulsemobile.com	Jim Burke		Super User	Active

1 - 1 of 1

APPENDIX 1: Important Terms

The following terms are used throughout this document.

account ID
A unique identifier (a four-digit number) for each Control Panel Account that is required to use our APIs. Your Account Manager or Client Success Manager can provide you with your Account ID, or if you can see it when logged into the Control Panel, where it is displayed next to your Account Name in the upper left corner.

account name
The name assigned to your Control Panel Account. It is typically your company name. It is also used as the Username used to access your Account.

API access key
A string of letters, numbers, and symbols. It is the password used to access your account via our APIs. It is generated by your Client Success Manager.

campaign
A Campaign consists of one or more Messages and is targeted at one List.

Control Panel
Control Panel is the web-based interface used to manage your communication and members. It is the primary way you interact with the mPulse platform.

Event
An occurrence or thing that happens at a point in time.

Event definition
The parameters used to represent an Event with data.

Hard bounce
Indicates a permanent reason that an SMS message cannot be delivered. Mobile numbers that return a hard bounce to the mPulse platform are automatically unsubscribed from all lists and placed into a do-not-contact status. The most common reasons for a hard bounce are a disconnected phone number or a phone plan that does not allow short code communication.

list
A group of members, including their mobile numbers. All communication from the mPulse Platform is based on Lists. Lists are generally created around a certain topic or program using one or more channels. Each Campaign is sent to one List, and only Members subscribed to that List will receive messages from the Campaign. Lists can be set up so that members can be added to a list on the control panel and/or can add themselves by opting into a campaign.

list ID
A unique identifier for each List in the database that is automatically generated when a List is created.

member
A member in our database represents a person you would like to send messages to. Each member in our database must have a unique Mobile Phone Number, App Member ID, or Email Address.

member ID
When a member record is created in the database, a unique ID is generated for this record. This value does not change and is used to uniquely identify a member's record. It is often used in API requests.

member profile
Each member has a Member Profile, which stores data at the Member level. This data always includes their member ID and a mobile telephone number, but can also include data like names, email address and other custom fields.

mobile originated (MO) message
A message a Subscriber sends from his mobile phone to our Platform. Typically, just referred to as an "MO".

mobile terminated (MT) message
A message sent from the Platform to a Subscriber's mobile phone. Typically, just referred to as an "MT".

short code
A five- or six-digit number that is used to send and respond to text messages. It can either be a random set of numbers or a "vanity" number, which is tied to a specific brand or number pattern.

Soft bounce
Indicates a temporary delivery issue to a cell phone number. The mPulse platform attempts to deliver a message 10 times over the course of 24 hours before the number is labeled a soft bounce. The number is not unsubscribed, and can be messaged again in future campaigns. The most common reason for a soft bounce are phones that are roaming or outside of service areas.

subscriber
A Subscriber is a Member who has opted in to a list for one or more channels. Members can only be subscribed to a channel if we have the appropriate information to message them using that channel (e.g., a valid mobile phone number for SMS).

Variable
A placeholder used to personalize messages based on the recipient's Member Profile.

APPENDIX 2: Control Panel account access levels

- SUPER USER
  - Permissions:
    - May add and delete all other users on the account and controls whether users can add other users
    - Can set and change access levels for List Manager users
    - Full visibility of all lists and campaigns, with the ability to create and launch campaigns

- ADMINISTRATORS
  - Permissions:
    - May add and delete List Manager Users
    - Can set and change List Manager access levels
    - Full visibility of all lists and campaigns, with the ability to create and launch campaigns
  - Restrictions:
    - May not add or delete other Administrator users

- LIST MANAGERS
  - Permissions (NOTE: All of these permissions can be added or removed by an Administrator or Super User at any time- this list assumes all permissions are given):
    - May view the member lists that they are given access to
    - Can create Campaigns
    - Able to launch Campaigns
    - May view and edit other user's campaigns that have not been launched
    - Can delete list-level data from the account
    - May export data
  - Restrictions:
    - Cannot add any additional users (unless permitted to by a Super User)
    - Will not be able to view any new lists that are created in the account without an Administrator or Super User giving permission

- mPULSE MOBILE ADMINISTRATORS
  - Permissions:
    - Same as regular users in Administrator roles
    - Manages which IP addresses are white-listed for access to the platform
    - Provides access and information for any API integrations
    - May change the Super User
  - Restrictions:
    - Same as users in Administrator roles

APPENDIX 3: Frequently Asked Questions and Troubleshooting

- **What is the best method for testing a text messaging campaign?** – Best practice is to create a test version of any new workflow you want to deploy on the mPulse Platform first. To do so, follow all of the steps in section 3 of this guide but only using your own (and/or other testers') information in your audience list. Be sure to use your mobile phone to test all of your campaign's triggers as well as the various automatic responses. Text in all of your campaign's keywords, HELP, an intentionally unrecognizable collection of characters (to check the "sorry, we didn't understand" message) and STOP. Contact your Account Manager or Client Success Manager if you encounter unexpected problems or have any questions. If you are happy with your test campaign, you can use it in production by uploading your member info or distributing the keyword/short code info to the desired audience. You can also clone it by selecting the clone button on the right side of the Campaigns screen of the Communication tab to create a new campaign with the same structure and messaging as your test, which you can then edit and rename to your specifications before launching.

- **How do I incorporate advanced features like API integrations, custom event message triggers, audience segmentation, or natural language processing of incoming texts into my campaigns?** – If you need to use features of the mPulse platform that are beyond the messaging processes outlined in this guide, contact your Account Manager or Client Success Manager to schedule a meeting or to get more information and training.

- **What is the best practice on opting-in to SMS messaging?** In cases where members' mobile numbers are being uploaded into the platform, we generally recommend using a confirmation message automatically generated by the platform when a new member is added to the list. If you are already getting a member's opt-in via another method where the person is signing up to receive SMS messages, you can contact your Client Success Manager to have that confirmation message removed. That confirmation can also be removed via your Client Success Manager for cases where members are texting a keyword into the short code, since that member-originated messages acts as an opt-in. In general, you should check with your Account Manager or Client Success Manager regarding any questions you may have on opt-in strategy and Telecommunications Consumer Protection Act compliance.

E

Exhibit E

mPulse Mobile Incident Response Policy v1.3

mPulse Mobile
Incident Response Policy

This policy outlines the baseline behaviors required to ensure that employees, contractors and related constituents who use company resources for business do so in a safe, secure manner. It is designed to protect private and confidential data through creation, use, transmission and destruction. As a signed document, it is an addition to the library of acceptable use policies on file within Human Resources that allow employee behaviors to protect confidentiality of data.

Effective Date:	7/25/2018
Document Owner:	Ram Prayaga
Signature:	
Version:	1.3
Version Date Revision / Description Author:	7/7/2018 / Simon Leung

1. PURPOSE 3
2. SCOPE 3
3. INCIDENT REPORTING 3
3.1 WHO SHOULD REPORT INCIDENTS 4
3.2 HOW AND WHEN TO REPORT INCIDENTS 4
3.3 FORENSIC ANALYSIS 5
4. INCIDENT RESPONSE 7
4.1 AUTHORITY TO ACT 7
4.2 ACTIONS TO BE TAKEN 7
4.3 INTRUSION DETECTION POLICY 7
4.4 ASSIGN THE INCIDENT TO A HANDLER 7
4.5 COORDINATE INCIDENT RESPONSE TEAM 8
4.6 CONTAIN AND ERADICATE 9
4.7 CREATE EXECUTIVE AND TECHNICAL REPORT 10
4.8 STORE INCIDENT FILE AND EVIDENCE 10
4.9 NOTIFICATION 10
5.0 INCIDENT RESPONSE EXERCISES 10
5. COMPLIANCE AND SANCTIONS 11
6. APPLICABILITY AND ENFORCEMENT 11
7. REVISION HISTORY 11

1. Purpose

The mPulse Mobile Incident Response Policy has been formulated with the following goals in mind:

- Ensure security, reliability and privacy of mPulse Mobile's systems, networks and data, and the networks, systems and data of others.
- Protect mPulse Mobile's systems, networks and data from harm and interference.
- Ensure that mPulse Mobile, its employees, and other users of its facilities comply with the law and avoid legal liability.
- Encourage the responsible use of resources, and discourage practices which degrade the usability of network resources, or cause harm to resources or individuals.
- Maintain mPulse Mobile's reputation as a responsible organization.
- Access to online content via the network may be restricted in accordance with our policies and federal regulations.

2. Scope

This policy provides guidelines for permissible and impermissible actions regarding company information systems. This policy applies not only to mPulse Mobile's systems and networks, but to activities mPulse Mobile conducts on client systems and networks. This policy applies to any user of mPulse Mobile's systems, including, but not limited to, employees, interns, contractors, consultants, and temporaries (referred to in this policy as "users").

For the purposes of this document, the term incident is considered to be any adverse event that threatens the confidentiality, integrity, accessibility, or ability to audit company information resources. Information resources belonging to customers are expressly included in this definition, and covered by this policy.

These events include but are not limited to:

- Attempts (either failed or successful) to gain unauthorized access to a system or its data.
- Unwanted disruption or denial of service.
- Unauthorized use of a system for the transmission, processing, or storage of data.
- Changes to system hardware, firmware, or software characteristics without the company's knowledge, instruction or consent.
- Attempts to cause failures in infrastructure or services.

3. Incident Reporting

Incidents can be reported through manual detection techniques, through employee reports, or through the automated Intrusion Detection system. Incidents must be reported to the appropriate governmental entity when the law requires and to pertinent groups or agencies as necessary. The following incidents should be reported:

- Unauthorized Access
- Malicious Code
- Denial of Service (DoS)
- Scan and Probes
- Rogue Wifi
- Loss of EPHI data
- Breach of personally identifiable information (PII)
- Information system failures and loss of service
- Errors resulting from incomplete or inaccurate business data
- Breaches of confidentiality and integrity
- Disclosures of unprotected health information
- Misuse of information systems
- Identity theft
- Insider threat

3.1 Who should report incidents

mPulse Mobile requires mPulse Mobile Workforce to report any suspected Security Incidents. mPulse Mobile investigates all reports of suspected Security Incidents to determine whether an actual Security Incident occurred and, if it did, the extent to which the Security Incident resulted in the unauthorized access, use, disclosure, modification, or destruction of e-PHI. If a Security Incident is found to have occurred, mPulse Mobile also takes steps to mitigate the impact of the Security Incident.

mPulse Mobile notifies each affected Client whose e-PHI has been, or is reasonably believed by mPulse Mobile to have been, successfully accessed, acquired, used, or disclosed as a result of a Security Incident. The notice is made without undue delay and in accordance with the terms and conditions of the Business Associate Agreement and other contractual arrangements between mPulse Mobile and the affected Client.

3.2 How and when to report incidents

Security incidents should be directly reported to the employee's immediate supervisor and the Chief Technology Officer (or deputy or Helpdesk).

Urgent Incidents
Urgent incidents should be reported immediately or as close to the time of discovery as is possible.

Examples of urgent incidents include:

- Unauthorized access to mission critical servers, routers, firewalls, or any systems or networks involved in hosting company resources.
- Production outages due to Denial-of-Service attacks.
- Any mission critical (production) application failures.
- Attacks (successful or otherwise) on mission critical (production) infrastructure.
- Any virus or worm activity on mission critical (production) servers.
- Widespread damaging virus or worm activity on non-production systems.
- Breach of cardholder information or personally identifiable information (PII) or EPHI data.

Non-Urgent Incidents
Non-urgent incidents should be reported no later than one business day following detection.
Examples of non-urgent incidents
Scans and probes
Single incident or non-damaging virus or worm activity on non-production systems.

Virus Incidents
Single incidents of virus or worm activity outside the production environment are non-urgent unless there is significant risk of the virus or worm spreading.
Employees are required to exercise all reasonable means to prevent virus infection in accordance with the company security policies.

3.3 Forensic Analysis

Forensic analysis will vary greatly from incident to incident, but the methodology should be consistent. The goal of forensic analysis is to discover evidence that proves:

- What happened
- Where it happened
- When it happened
- Who did it
- How they did it

In particular cases, forensic evidence will be used in criminal or civil legal cases against the perpetrator. Since it may not be apparent at the beginning of an incident investigation that the outcome will be a legal case, the company must treat every investigation as if it will lead to a court case. The incident response process will establish and maintain an evidentiary chain for all electronic and physical evidence collected during the investigation. Detailed logs of actions and findings will be kept. Do not include company confidential information unless it is necessary.

To maintain an evidentiary chain the following information needs to be recorded:

- Where, when, and who discovered the evidence.
- Who has handled or examined the evidence and when.
- Who has had custody of the evidence, during what time period, and where it was stored/secured.
- If the evidence has changed custody, how and when the transfer occurred (include shipping numbers etc.).

Contact Information

- Name (who detected the incident)
- Email address
- Phone number(s)
- Who was the incident reported to

Description of incident

- Date & time incident was detected
- Date & time incident actually occurred (if different from above)
- Type of incident (e.g., defacement, DoS, etc.)
- Method of intrusion (e.g., vulnerability exploited?)
- Level of unauthorized access (e.g., root, administrator, user, etc.)
- Log extracts as appropriate
- Any other relevant information

Affected Systems(s)

- IP address and hostname
- Purpose of system

Operating system and software versions

- Type of protection that is in place

Source of Incident

- IP address and hostname
- Internal or External source

Damage assessment

- Impact of attack on business
- Staff time to detect, handle and recover from the incident
- Costs due to information loss, downtime, etc.

4. Incident Response

4.1 Authority to Act

The authority to respond to incidents lies with the CIO and his appointees. Upon notification of an incident the CTO will appoint an appropriate Incident Response team. Appointees are subject to ad hoc change on a per incident basis.

4.2 Actions to be taken

The Incident Response team shall take all necessary steps to respond to the incident. Such steps shall include appropriate notification, containment, damage assessment, and recovery. At all times, actions taken in response to incidents shall conform to the company's Information Security policy.

After the incident is handled, the IT department will review what occurred and develop action items to stop future incidents and learn from the activity.

4.3 Intrusion Detection Policy

- Normal logging processes are enabled on all host and server systems.
- Alarm and alert functions, as well as logging, of any firewalls and other network perimeter access control systems are enabled.
- All critical servers shall have additional monitoring tools.
- System integrity checks of the firewalls and other network perimeter access control systems are performed on a routine basis.
- Audit logs from the perimeter access control systems are reviewed.
- Audit logs for servers and hosts on the internal, protected network are reviewed.
- Unless critical systems have been compromised, the organization will first make an attempt to track intruders before correcting systems.
- At logical network concentration points, IDS tools are installed which monitor for traffic patterns consistent with known attacks.

4.4 Assign the Incident to a Handler

Assign the incident to an on-call Incident Handler (IH) and contact the IH immediately. If the Incident Handler cannot be reached or does not confirm that they are responding to the incident in the necessary time, and then use the following escalation tables:

High and Medium Risks

Role	Contact	Number	Email	Escalation Time
Technical Product Manager	Josh Levitan	888 678 5735 x746	Josh.Levitan@mpulsembile.com	15 minutes
Production and Client Success Manager	Dianna Hicks	888 678 5735 x712	Dianna.Hicks@mpulsemobile.com	30 minutes
DevOps Manager	Abhineet Raj	888 678 5735 x754	Abhineet.Raj@mpulsemobile.com	45 minutes
Development Manager	Kunal Agrawal	888 678 5735 x720	Kunal.Agrawal@mpulsemobile.com	45 minutes
Chief Technology Officer (CTO)	Ram Prayaga	888 678 5735 x702	Ram@mpulsemobile.com	60 minutes
Chief Financial Officer (CFO)	Brian Chudleigh	888 678 5735 x700	Brian@mpulsemobile.com	60 minutes

Low Risk

Role	Contact	Number	Email	Escalation Time
DevOps Engineer	Justine Espinoza	888 678 5735 x724	Justine@mpulsemobile.com	8 hours
Senior Manager Production and Client Success	Dianna Hicks	888 678 5735 x712	Dianna.Hicks@mpulsemobile.com	16 hours
Senior Operations and Compliance Manager	Jeff Martinez	888 678 5735 x719	Jeffrey.Martinez@mpulsemobile.com	32 hours

When an IH has been confirmed, contact the person who reported the event and give them the name and contact information for the assigned IH if it is a high or medium incident.

4.5 Coordinate Incident Response Team

The IH assigned to the incident is responsible for coordination of the response and investigation, and therefore will be the Primary Incident Handler (PIH) for the remainder of the investigation. The first task of the PIH is to review the incident documentation and associated event reports. The PIH should verify as much information as possible from the event report(s), verify the assigned severity level based on the available information, and acquire the resources necessary to respond to the incident. The PIH should then go to the location of the incident if appropriate.

Law enforcement should be informed at the discretion of Company's CIO. There are many factors to weigh including the severity of the incident, the scope of the compromise, cost to the company of supporting a criminal investigation, and the proprietary and confidential company information that would become public if a criminal investigation occurs. It will be up to the Incident Response team to decide whether the incident warrants legal action. It is recommended that Company's legal counsel be present in all meetings with law enforcement relevant to ongoing investigations.

The organization shall implement an insider threat program that includes a cross-discipline insider threat incident handling team.

4.6 Contain and Eradicate

The primary goal of the Incident Response team is to maintain/restore business continuity, so containment of a security incident is vital. Containment and eradication methods are highly dependent on the type and scope of the security incident, therefore only sample scenarios and methods are provided. Ideally, the appropriate method can be extrapolated from the sample methods. The containment phase is also where the bulk of evidence will be preserved. Always keep the following in mind:

- Preserve as much evidence in its original form as possible.
- Take detailed notes on your actions and the actions of those around you, including the time of the action. Include your reason for taking the action. Sign and date the bottom of each page of notes.
- Record each piece of evidence you find, including a description, location, time found, and other distinguishing attributes. If it is physical evidence, record who handled the evidence before it came into your possession. If it is electronic evidence, record any processing of the evidence that occurred prior to your possession of the evidence. This data will help maintain an evidentiary chain and record of possible modification.
- Restrict information about the incident on a need to know basis. Only management and technical personnel (system administrators, network engineers, development, etc.) that can significantly contribute to the resolution or investigation of the incident should be informed. Only disclose information that is immediately needed to solve the problem or task at hand.

4.7 Create Executive and Technical Report

After the incident has been contained, eradicated, and analyzed, create an executive level report for all incidents that contains:

- A high-level description of the incident and its scope
- The impact on the company
- Actions taken to prevent further occurrences
- Recommendations for further action

The technical report should contain detailed information about the event, investigation, and conclusions. All data used in the report should reference evidence collected and be verifiable. The report should be suitable for use in court for either civil or criminal cases.

4.8 Store Incident File and Evidence

All evidence, logs, and data associated with the incident should be placed in tamper resistant containers, grouped together, and put in limited access secure storage. Only incident investigators, executive management, and legal staff should have access to the storage facility. If and when evidence is turned over to law enforcement, create an itemized inventory of all the items, verify the inventory with the law enforcement representative, and have the representative sign and date the inventory list for our records. Give the original records to the Legal department, and save a copy for the security records. It is recommended that company's legal counsel be present in all meetings with law enforcement relevant to ongoing investigations.

4.9 Notification

The company will follow all legal notification requirements in conjunction with the Legal department.

5.0 Incident Response Exercises

Incident Response exercises are scheduled annually as part of the plan development process. During Incident Response exercise, events are analyzed against baseline to assess the likelihood of abnormalities and damages. Participants coordinate areas of improvements given specific, or ad hoc events. Planned exercises ensures that Incident Response teams are familiar with their assignments.

5. Compliance and Sanctions

All users are expected to comply with this policy and other mPulse Mobile policies. Anyone found in violation of this policy, may be subject to disciplinary action up to and including termination and criminal and civil prosecution.

All users are required and expected to report any information concerning violations or suspected violations of this policy to mPulse Mobile.

6. Applicability and Enforcement

This document is part of the company's comprehensive set of policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

This policy will be enforced by the IT Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

Any questions about this Policy should be sent via e-mail to Compliance@mpulsemobile.com

7. Revision History

Revision	Name	Date
1.0 – Initial	Ram Prayaga	12/15/2015
1.1 – Updated contacts	Simon Leung	7/20/2017
1.2 – Updated cover page with signature and effective date. contacts. Included section on Incident Response exercises.	Simon Leung	1/10/2018
1.3 – Updated contacts and titles to reflect changes.	Simon Leung	7/7/2018

F

Exhibit F

mPulse Mobile SLA

EXHIBIT "A"

Schedule A-1 - SLA

I. Service Level Agreements

Additional Definitions. When used in this Schedule, the following terms have the following definitions. Other terms used in this Schedule and not defined in this Schedule shall have the meaning specified in the Agreement to which this Schedule is attached.

"**End User**" means Client Customers that have obtained access to and use of the Platform pursuant to executed Customer Contracts.

"Client User" means an entity or individual that is authorized by Client to obtain access to the Platform pursuant to Section 7.4 of the Agreement.

"Transactions" means requests from Client Users and End Users.

For the avoidance of doubt, the term "**Platform**" as used in this Schedule shall have the meaning specified in the Agreement and shall include, without limitation, processing of Transactions, and include individual elements and components of the Platform.

A. Service Levels

Uptime

mPulse shall provide and make available the Platform with at least ninety-nine and nine tenths percent (99.9%) Uptime (as defined below) measured over each calendar month ("**Uptime Guarantee**").

Uptime for a calendar month is calculated in accordance with the following formula:

$$\text{"Uptime"} = \frac{(\text{Total minutes per month} - \text{Total minutes } \textit{Downtime} \text{ per month})}{(\text{Total minutes per month})}$$

"**Downtime**" is defined as the inability (i) for Client, Client Users or End Users to access or use the Platform or (ii) for the Platform to receive requests for Transactions or fully process Transactions in accordance with the SLA Specifications, the mPulse Documentation or the terms of the Agreement or this Schedule. For the avoidance of doubt, the term "Downtime" includes the time during which a Priority 1 or Priority 2 incident (as defined below) is being experienced. The SLA Specifications as of the Effective Date are set forth in Section II (SLA Specifications) of this Schedule.

Downtime (a) commences as of the earlier of (i) the time mPulse or its third party monitoring service identifies Downtime, including if Downtime is reported to mPulse by another mPulse customer, or (ii) the time that Client or an End User notifies mPulse of Downtime, and (b) ends when the Platform, the services and Transaction processing, as the case may be, is fully restored in a manner that complies with the SLA Specifications and mPulse Documentation or a workaround is identified and implemented and that overcomes the particular issue that caused the Downtime. The term "**workaround**" means an automatic, system generated (where technically possible) patch or manual procedure that mPulse has implemented or reasonably (as determined by Client in its sole discretion) recommends that Client implement, that allows the Platform to meet the Uptime Guarantee and in order to remove the adverse effects of an incident.

The parties will update the foregoing as the services provided by mPulse to the Client include new services.

Downtime shall not include any period of unavailability of the Platform due to Planned Maintenance (as defined below), including Planned Maintenance to implement upgrades which require mPulse to perform maintenance on any redundant environments contemporaneously, or force majeure events as set forth in Section 15.2 of the Agreement (including without limitation acts of God, terrorism, natural disaster, war, riots, and labor strife), provided that in the case of a force majeure event mPulse has implemented its then current disaster recovery and business continuity plans to address any such event. For clarity if there is any such event beyond the control of mPulse, the failure by mPulse to implement its disaster recovery and business continuity plans shall result in Downtime and will be subject to the payment of Service Credits to Client as provided in this Schedule. The foregoing shall be in addition to any other remedies at law or in equity under the Agreement in connection with mPulse's failure to implement its disaster recovery and business continuity plans.

mPulse will notify Client via email at least eight (8) business days in advance of any scheduled maintenance which will result in scheduled downtime ("**Planned Maintenance**") to the Platform. Each individual period of Planned Maintenance shall not exceed four (4) hours. All Planned Maintenance must also comply with the SLA Specifications. Any period of maintenance that does not comply with the terms in this paragraph shall be "Downtime" if such maintenance results in the inability (i) for Client, Client Users or End Users to access or use the Platform or (ii) for the Platform to fully process Transactions in accordance with the SLA Specifications, the mPulse Documentation or the terms of this Schedule.

Without limiting any other terms or conditions in this Schedule or the Agreement, mPulse agrees to take reasonable industry standard precautions to mitigate the risk of Downtime, including but not limited to (a) use of anti-virus and anti-trojan software; (b) installation of available hardware and software patches; (c) implementation of industry standard firewalls; (d) implementation of backup power generation facilities, security systems, scheduled backups, and fire protection systems; and (e) maintaining redundant internet providers. mPulse shall support the current "general availability" release of Microsoft Explorer, Safari, Google Chrome and Mozilla Firefox for access to the Platform provided that it is understood that there are certain End User variable settings that may adversely impact compatibility, such as *End User* browser configuration, firewalls, etc. mPulse will promptly notify Client in writing of any such End User variable settings that may adversely impact compatibility.

Priority Definition

- **Impact** - The impact of the incident on the business. This is typically determined by the number of Client Users or End Users affected. However it is also important to assess the number of services affected, potential business impact (reputation, loss of End User, etc.), or potential health risks.
    - **High** - An incident that has a high impact is an incident that is affecting many users, services, environments, or has a significant impact to the business (ex. Availability of production services).
        - Platform is unable to receive, process and respond to Client User or End User requests according to the SLA Specifications, the mPulse Documentation, the terms of the Agreement or this Schedule
        - User interface is not representing Client's brand in any of the production GUIs

        - All service slowdowns surrounding the 7 days before and after a product launch day

        Key Internal Functions (inclusive of, but not exclusive to)

        - APIs are not responsive or returning/updating incorrect data
        - APIs are not meeting the speed defined in the implementation plan
        - Data handoffs to other systems are not accurate and/or working
        - Client is unable to upload/create/modify items
        - Data and/or security is compromised

    - **Medium** - An incident that is only affecting a small number of users, services, or environments (ex. reports of slowness, intermittent connectivity, etc.).

    - **Low** - An incident with very little to no impact to the business

- **Urgency** - How quickly does the incident need to be resolved. Client will determine, in its reasonable discretion, the Urgency of each incident based on the nature of the incident, the impact on End Users and the Client and the following factors.

    - **High** - The incident is extremely urgent and needs to be resolved as quickly as possible.

    - **Medium** - The service is available but impaired (ex. slow download speeds).

    - **Low** - The service isn't performing as expected but the End User or Client User is still able to use the service successfully (ex. a redundant power supply failed.).

- **Priority** - Priority is derived from the determination of impact and urgency as seen in the chart below.

Priorty Coding System

		Impact		
		High	Medium	Low
Urgency	High	P1	P2	P3
	Medium	P2	P3	P4
	Low	P3	P4	P4

mPulse shall resolve issues in accordance with the following table, based on the severity of such issue as defined below. For purposes of this Schedule the terms "**issue**", "**incident**" and "**problem**" shall mean (i) any failure of the Platform to comply with the SLA Specifications, the mPulse Documentation, the terms of the Agreement or this Schedule or (ii) Downtime.

Client shall initially classify the issue Impact reported by the Client and mPulse shall initially classify the issue Impact discovered by or reported to mPulse or its third party provider. In addition mPulse may, upon written notice to Client, propose a reclassification of the issue Impact as fixes are rendered and/or implemented. As noted above, the Client will determine the Urgency for each incident.

In the event Client disagrees with mPulse's classification or reclassification of the issue Impact, as appropriate, the Parties shall confer as soon as possible to discuss when a further reclassification of the issue Impact is appropriate.

Priority	Acknowledgement	Updates	Resolution	Reports
P1 Considered service interruption	15 minutes	Every 60 minutes	6 hours	Incident report within 24 hours of resolution. RCA (defined below) report within 10 days
P2 Considered service interruption	120 minutes	Every 12 hours	48 hours	Incident report within 2 business days RCA (defined below) report within 15 days
P3	8 business hours	Daily	72 hours	Incident report within 3 business days of resolution RCA (defined below) report within 15 days
P4	Best effort	Weekly and as needed	10 business days	

Root Cause Analysis ("RCA"). In every case of a Priority 1, 2 or 3 incident, mPulse will conduct a RCA to determine the cause of the incident and will provide Client the results of such RCA as part of the incident and problem reports furnished in accordance with the time frames set forth above. Each report will identify the origin or root cause of each incident and identify corrective action taken by mPulse to correct or remedy the incident and the actions to be taken to prevent the re-occurrence of any Priority 1, 2 or 3 incident (collectively, a "**Post Mortem Report**"). Post Mortem Reports must be sent to Client via email. Post Mortem Reports shall be provided to Client in two stages, as follows.

- **Stage 1 Post Mortem Report - Incident Report.** Each Stage 1 Post-Mortem Report will include the following: (i) a summary of the incident, including a short description of the incident, together with a detailed summary of the history of the incident, including the date that the Incident was reported to or discovered by mPulse, (ii) the results of the root cause investigation referenced above and (iii) corrective action and a proposed remediation plan for creating a permanent fix that will prevent the re-occurrence of such incident, including the timing for developing and deploying the permanent fix. mPulse will promptly implement any plan therein and develop the permanent fix at no additional cost to Client. The term "**permanent fix**" means an update or upgrade developed and deployed by mPulse in response to an incident that allows the Platform to meet the Uptime Guarantee and in order to remove the adverse effects of an incident.
- **Stage 2 Post Mortem Report – Problem Report.** Each Stage 2 Post-Mortem Report will include the following: (i) any updates to the results of the root cause investigation identified in the Stage

1 Post-Mortem Report, if any, together with substantiating written documentation for such updates, (ii) a certification that the permanent fix was implemented by mPulse in accordance with the Stage 1 Post-Mortem Report (or, if not so implemented as described in the Stage 1 Report, the reason for mPulse's deviation from the Stage 1 Post-Mortem Report in connection with the permanent fix), (iii) documentation evidencing, to the reasonable satisfaction of Client, that the permanent fix will prevent the re-occurrence of the incident, and (iv) a proposal for a remediation plan for any corrective action to be taken by mPulse (in addition to providing Client with the permanent fix) to prevent the re-occurrence of the incident, if any. mPulse will promptly implement any plan therein at no cost to Client.

mPulse represents, warrants and covenants that mPulse will have, during the term of the Agreement, the systems, processes, procedures and information necessary and appropriate to measure, substantiate, calculate and report on (i) performance against the Uptime Guarantee, including without limitation the calculation and measurement of Downtime, (ii) the duration of Downtime and incidents and (iii) the service credits payable as described in this Schedule.

Service Credits

In the event that mPulse fails to achieve the Uptime Guarantee or if mPulse fails to meet the acknowledgement or resolution service levels noted above in a calendar month or both, Client shall be entitled to service level credits as follows ("**Service Credits**"):

Cumulative Length of Downtime (outside 99.9% Uptime Guarantee)	Fee credit towards all Fees for the calendar month
0-60 minutes	5%
61-120 minutes	10%
121-360 minutes	15%
>360 minutes	30%

% of incidents Over the initial Acknowledgement response time	Fee credit towards all Fees for the calendar month
<25%	0.1%
25-50%	0.5%
>50%	1.0%

% of incidents Over Resolution time	Fee credit towards all Fees for the calendar month
<25%	0.1%
25-50%	0.5%
>50%	1.0%

Service Credits will be calculated monthly, will be accumulated for each calendar month for reporting and tracking purposes and will be deducted from the next invoice sent by mPulse to the Client, or if the next invoice will not be issued by mPulse for more than thirty (30) days after the end of the calendar month, then mPulse will pay the Service Credit to the Client within fifteen (15) days after the end of the calendar month.

With respect to Service Credits related to Downtime, such Service Credits will be calculated from the commencement of the Downtime until the Downtime is resolved (i.e., the number of minutes and partial minutes that elapse between the start of the Downtime and the end of the Downtime (i.e., a workaround or permanent fix is deployed)).

<u>Notifications Regarding Downtime</u>

In case of Downtime, an email will be sent to inform Client of the incident consistent with the acknowledgement periods specified above. Another email will be sent to Client when the Platform is back online.

A preliminary incident analysis report shall be sent to Client by email on the business day immediately after the occurrence of Downtime. A final incident analysis report shall be sent to Client by email within five (5) business days after the incident.

Downtime shall not be used for routine or preventive maintenance.

B. Continuation of Support and Maintenance.

Because of the critical importance of the support services to be performed by mPulse as described in this Schedule, mPulse assumes an independent obligation to continue performance of its support services obligations hereunder in all respects, unless Client is in material breach of this Agreement or Client is not paying undisputed Fees due mPulse.

C. Extended Failures

In the event of an Extended Failure (as defined below), Client shall have the right, but not the obligation, to terminate the Agreement upon thirty (30) days' written notice to mPulse without penalty or other financial obligation. "**Extended Failure**" means any of the following:

(a) Priority 1: (i) a Priority 1 incident continues for more than six (6) hours, or (ii) there are more than six (6) hours of Priority 1 incidents in any thirty (30) day period, or (iii) there are more than two (2) Priority 1 incidents in any 180 day period; or

(b) Priority 2: (i) a Priority 2 incident continues for more than 72 hours, or (ii) there are more than five (5) Priority 2 incidents in any 30 day period, or (iii) more than three (3) times in any thirty (30) day period, Priority 2 incidents continue for more than 24 hours.

D. Service Level Changes

This Schedule may only be amended by the mutual written consent of mPulse and Client, except that Client may update its email notification addresses at any time by written notice to mPulse.

[End of Section I]

II. SLA Specifications

1.1 Performance Level

1.1.1 Availability

Requirements	Description	Commitment
Overall system uptime	Describes the time in a defined period (e.g. monthly) when all services were available, over the total possible available time during the period, expressed as a percentage	99.9% Uptime Guarantee
Percentage of successful requests	Describes the number of requests processed by the service without an error over the total number of submitted requests, excluding retries of failed requests, expressed as a percentage.	99.9%
Number of successful operations	Describes the number of operations which fail after n numbers of retries	If the first 3 attempts fail, the 4th unsuccessful attempt shall be an incident and may be a high impact, high urgency incident
Percentage of timely service requests	Describes the number of service requests completed within a defined time period (e.g., seconds or milliseconds (ms) over the total number of service requests, expressed as a percentage.	GUI: • 90% less than 10 second • 100% less than 20 seconds API (within the mPulse system) per member update/insert request: • 90% less than 100ms • 100% less than 500ms

1.1.2 Capacity

Requirements	Description	Commitment
Number of simultaneous End Users and Client Users, respectively.	Refers to a target for the maximum number of separate End Users and Client Users that	GUI non-admin: - 1000 End Users

	can be using the Platform at one time.	GUI admin: 100 Client Users

1.1.3 Capability Indicators

Capability indicators are service level objectives which promise specific functionality relating to the Platform.

Requirements	Description	Commitment / Comment
External connectivity	Specifies capabilities of the Platform to connect to systems and services which are external to the Platform. The systems and services involved may be other cloud services or they may be outside cloud computing.	Comment: Covered by capacity for service throughput (E2E)

1.1.4 Support

Requirements	Description	Commitment/ Comment
Non-Emergency Support hours	Specifies the hours during which mPulse provides Client Users a support interface that accepts general inquiries and requests from Client Users via email and telephone.	8am-9pm EST Time (5am-6pm PST) M-F, excluding holidays.
Client Escalation process	Process by which Client escalates either the priority or the response/resolution time of an issue	1st: Product support - prodsupport@mpulsemobile.com -1-(888)-mpulse5 Once client emails or calls into the toll free number a case number will be generated with an auto email back to (insert client support email) for tracking purposes until resolution.
mPulse incident communication process	Refers to the process mPulse will follow to notify the Client of an issue	For incidents and updates: Contact the NOC by email and/or phone: prodsupport@mpulsemobile.com (888) mpulse5

1.1.5 Reversibility and the Termination Process

Requirements	Description	Commitment
Data retrieval period	Specifies the length of time during which the Client can retrieve a copy of its End User data from mPulse and the Platform.	Length of the Agreement + 5 years
Data retention period	Refers to the length of time during which mPulse will retain backup copies of the Client User data, End User data and Transaction data during the termination process (in case of problems with the retrieval process or for legal purposes).	Length of the Agreement + 5 years

1.1.6 Outage, Severity, and Response Definitions

Requirements	Description	Commitment
Scope Scheduled Maintenance	Describe how scheduled Planned Maintenance occurs.	• 8 business days advanced notice of Planned Maintenance • No longer than 2 hours of End User-facing downtime (GUI and API) associated with Planned Maintenance • No longer than 4 hours of system downtime (reporting and administration) associated with Planned Maintenance • Any outages, slowdowns, etc. outside of these commitments will be Downtime • All downtime due to maintenances without 8 business days advanced written notice is Downtime

1.2 Security Service Level Objectives

1.2.1 Service Reliability

Service reliability is the property of the Platform to perform its function correctly and without failure, typically over some period of time. This category is usually related to the security controls implementing business continuity management and disaster recovery in frameworks like ISO/IEC 27002 (Relevant security frameworks include in particular ISO/IEC 27001 and ISO/IEC 27002). Allowable downtime, which accounts for Planned Maintenance and force majeure, should be taken into account for this SLA.

Requirements	Description	Commitment

Level of redundancy.	Describes the level of redundancy of the Platform supply chain, possibly taking into account the percentage of the components or service that have a fail over mechanism.	100% of all components need to be redundant with a failover capability. E.g. data center
Service reliability (MTBF)	Describes the ability of the Platform to perform its function correctly and without failure over some specified period.	No more than 1 total failure across all components per calendar month for up to 7.4 minutes (i.e., consistent with the 99.5% Uptime Commitment)

1.2.2 Authentication & Authorization

Authentication is the verification of the claimed identity of an entity (typically for cloud computing the entity is an End User).

Authorization is the process of verifying that an entity has permission to access and use a particular resource based on predefined user privileges.

Authentication and authorization are key elements of information security which apply to the use of the Platform.

Requirements	Description	Commitment
Mean time required to revoke a Client User's access	Is the arithmetic average of the times required to revoke a Client Users' access to the Platform on request over a specified period of time.	The global account system is the authority for all Transactions. The mPulse implementation has to be in sync at all times. Administrative access for Client Users must be revoked immediately when Client removes or revokes access to the Platform.
Third party authentication support	Specifies whether third party authentication is supported by the Platform and defines which technologies can be used for third party authentication. Other authentication SLAs may become less relevant if authentication if performed by a 3rd party.	Need to support and mirror the Client global account system for End User authentication.

1.2.3 Security Incident management and reporting

An information security incident is a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations or threatening information security. Information security incident management is the processes for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents.

Requirements	Description	Commitment
Percentage of timely incident responses	Describes the defined incidents that are assessed and acknowledged by mPulse in a timely fashion in accordance with the service levels set forth in this Schedule. This is represented as a percentage by the number of defined incidents assessed and acknowledged by mPulse within a predefined time limit in accordance with the service levels set forth in this Schedule after discovery, over the total number of defined incidents to the Platform within a predefined period. (i.e., month, week, year, etc.)).	100% acknowledge and response for all P1 or P2 incidents within the time period specified in Section I of this Schedule.
Percentage of timely incident resolutions	Describes the percentage of defined incidents against the Platform that are resolved within a predefined time limit after discovery.	100% resolution for all P1 or P2 incidents within the time period specified in Section I of this Schedule.

1.2.4 Logging and Monitoring

Logging is the recording of data related to the operation and use of the Platform. Monitoring is defined as determining the status of one or more parameters of the Platform. Logging and monitoring are ordinarily the responsibility of mPulse.

Requirements	Description	Commitment
Logs retention period	Describes the period of time during which logs are available for analysis (e.g. the period of time that log files are available for use by Client Users).	30 calendar days
Log access availability	Describes what log file entries that Client Users have access to.	All logs

1.2.5 Vulnerability Management

Vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat.
Management of vulnerabilities means that information about technical vulnerabilities of information systems being used should be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

Requirements	Description	Commitment
Percentage of timely vulnerability corrections	Describes the number of vulnerability corrections performed by mPulse, and is represented as a percentage by the number of vulnerability corrections performed within a predefined time limit, over the total number of vulnerability corrections to the Platform which are reported within a predefined period (i.e. month, week, year, etc.).	100% corrections for all Priority 1 and Priority 2 vulnerabilities incidents within the time period specified in Section I of this Schedule.
Percentage of timely vulnerability reports	Describes the number of vulnerability reports by mPulse to the Client, and is represented as a percentage by the number of vulnerability reports within a predefined time limit, over the total number of vulnerability reports to the Platform which are reported within a predefined period (i.e. month, week, year, etc.).	A vulnerability report once per calendar quarter for external systems. Such report to be delivered to Client within thirty (30) calendar days after the end of each quarter.
Reports of vulnerability corrections	Is a description of the mechanism by which mPulse informs the Client of vulnerability corrections applied to the Platform, including the frequency of the reports.	A report delivered securely within 24 hours post remediation of all Priority 1 and Priority 2 vulnerabilities.

1.3 Data Management Service Level Objectives ("SLO") Overview

1.3.1 Platform End User Data Mirroring, Backup & Restore

This SLO category deals with the actual mechanisms used to guarantee that the End Users' data is available (online or offline) in case of failures forbidding access to it. The mechanisms falling under the scope of this SLO are divided in two widely-used categories: (i) data mirroring, and (II) backup/restore (defined in ISO/IEC 27002).

Requirements	Description	Commitment
Data Mirroring Latency	Refers to the difference between the time data is placed on primary storage and the time the same data is placed on mirrored storage.	Operational/Primary DB's • Under 3 seconds Reporting/Mirrored DB's: • Under 1 min.
Data Backup Frequency	Refers to the period of time between complete backups of the Platform, Client User data and End User data.	In addition to escrow (when required) maintenance back-ups will occur on the following schedule: Platform: Daily Client User data: Daily End User data: Daily
Maximum Data Restoration time	Refers to the committed time taken to restore the Platform, Client User data and End User data from a backup.	Meantime to operation (MTTO) which requires data restore = 8 hours total
Percentage of Successful Data Restorations	Refers to the committed success rate for data restorations, expressed as the number of data restorations performed without errors over the total number of data restorations, expressed as a percentage.	100% - no data loss.

1.3.2 Data Portability

The following list of SLOs is related with mPulse's capabilities to export data, so it can still be used by the Client, e.g., in the event of expiration or termination of the Agreement.

Requirements	Description	Commitment
Data portability format	Specifies the electronic format(s) in which Platform data can be transferred to/accessed from the Platform.	Gzip SQL
Data portability interface	Specifies the mechanisms which can be used to transfer Platform data to and from the Platform. This specification potentially includes the specification of transport protocols and the specification of APIs or of any	Flatfile to SFTP Zone

	other mechanism that is supported.	

EXHIBIT B

Privacy and Data Security

1. Statement of Purpose

mPulse takes privacy and data security seriously and will comply with all applicable laws governing the use and disclosure of Client Data and other applicable data security standards to which mPulse is required or has elected to comply (collectively, "**mPulse Security Standards**").

2. Client Data

mPulse will not use any Client Data, other than to perform its respective obligations pursuant to this Agreement or as otherwise expressly permitted herein.

mPulse acknowledges that applicable data privacy and protection laws in the United States are subject to change. mPulse shall reasonably cooperate with Client to amend the terms of this Agreement to the extent necessary for Client's, or its affiliates', compliance with applicable data privacy and protection laws.

Unless otherwise prohibited by law, mPulse will promptly notify the Client about any legally binding request for disclosure of Client Data and any request received directly from a Customer, prior to responding to any such request.

3. Security

mPulse agrees that all Client Data will be secured from unauthorized access, use, disclosure, and loss using commercially reasonable security practices and technologies. Without limiting the foregoing, mPulse represents and warrants that it has in place a comprehensive information security program designed to protect the information under its custody, management or control, including all Client Data, that all mPulse personnel with access to Client Data are provided appropriate training to ensure their compliance with mPulse's obligations and restrictions under this Agreement, with applicable laws and with mPulse's information security program, and that mPulse's information security program complies with the requirements of data security laws applicable to mPulse. mPulse also represents and warrants that it regularly, and at least once per calendar year, audits mPulse's information security program and information systems, to confirm compliance with mPulse Security Standards and applicable laws. Upon request, mPulse shall provide Client with a network diagram that outlines mPulse's information network relevant to the services provided under this Agreement and will permit Client to review its applicable information security policies. mPulse agrees that all Client Data will be stored and processed by the mPulse Platform in the United States, unless the Parties agree otherwise in writing. In the event that Client desires to market and sell any Client Solution outside of the United States, Client shall notify mPulse in writing and the Parties may mutually agree on a plan for providing such Client Solution outside of the United States.

4. Breach of Security

If there is an actual or suspected Breach of Security involving Client Data that is stored by Client, Client will notify the mPulse personnel within 12 hours of becoming aware of such occurrence via the following method: Contact email and phone: Jeffrey Martinez, jeffrey.martinez@mpulsemobile.com, 805-200-4823.

If there is an actual or suspected Breach of Security involving Client Data stored, managed or received by, or transmitted to, mPulse pursuant the Agreement, mPulse will notify the Client within 12 hours of becoming aware of such occurrence, via both of the following methods: email & phone.

For purposes of this Agreement, a "***Breach of Security***" shall mean: (a) any unauthorized possession, use, access, acquisition or knowledge of Client Data by any person, or (b) any attempt by any person to gain possession of Client Data without authorization or to use or acquire knowledge of any Client Data without authorization, where such attempt materially compromises the security of the Client Data.

In the event of an actual or suspected Breach of Security, Client and mPulse will cooperate to take all steps reasonably necessary to investigate and remediate the effects of such occurrence, ensure the protection of those Customers that are affected or likely to be affected by such occurrence, prevent the re-occurrence, and comply with mPulse Security Standards and other applicable laws. Client shall be responsible for determining whether any notification of Customers or others is necessary in response to a Breach of Security, and shall make any such required notifications to Customers.

The Party that is responsible for a Breach of Security will promptly reimburse the other Party for the reasonable and documented costs actually incurred by such Party in addressing and responding to such occurrence, including but not limited to any such costs associated with the notification of Customers (including any credit monitoring program or identity theft insurance offered to end users) and any audit conducted in response to a Breach of Security.

5. Records Retention

In connection with the mPulse Security Standards, mPulse has adopted a records retention policy in which mPulse expunges and deletes from its systems, records, and back-ups any personally identifiable information that has not been used by mPulse for a period of 18 months or more.

mPulse™
mobile

Exhibit G

mPulse Mobile Essential Guide Book for Healthcare Mobile Messaging

mPulse mobile

The Essential Guidebook for Healthcare Mobile Messaging

Best Practices for Compliant Healthcare Text Messaging

OCTOBER 2018

This guidebook outlines the key regulatory requirements and associated best-practices to develop and deliver fully compliant healthcare messaging programs.

The guidebook provides a review of the three key areas of regulation that apply to healthcare text messaging: TCPA law, the CTIA Guidelines and HIPAA. It defines typically compliant approaches for a range of healthcare use cases. However, regulatory compliance can vary depending on the facts and circumstances involved, therefore an organization should assess each of its healthcare messaging use cases individually with a compliance professional to confirm compliance with all applicable regulations. Therefore, following this guidebook is no guarantee that a healthcare messaging program is compliant.

TABLE OF CONTENTS

GOVERNING BODIES 04
FCC
CTIA
HIPAA

HEALTHCARE MESSAGING 05
HHS Definition of Healthcare
TCPA Consent Requirements for Non-Healthcare Telemarketing and Information Calls
The Healthcare Exemption
Legal Challenges and Risk
Text Messaging and Protected Health Information
Business Associates
Employers and Business Associates

COMPLIANCE DOCUMENTATION AND GUIDES............ 08

CLASSIFICATION OF MESSAGE PROGRAMS 09

SHORT CODES AND TOLL-FREE LONG CODES 10
Short Codes
Toll-Free Long Codes

MONITORING AND AUDITS 12
CTIA Audit Notices Severities Description
TCPA Violations

COMPLIANCE PRINCIPLES 14
CTIA Guiding Principles
Choice and Consent
Healthcare Messaging Context
Opt-In Requirements for Healthcare Messaging
Common Opt-In Approaches
Opt-In Considerations for Sensitive Healthcare Topics
Opt-Out
Identity Verification for Reassigned Mobile Phone Numbers
Customer Care
Program Content
Program Name and Product Description
Use of Keywords
Ages of Message Recipients
International Languages

FREE TO END USER HEALTHCARE MESSAGING........... 19

USE CASES... 21
Healthcare Assumed Opt-In
Healthcare Double Opt-In
Keyword Text-In
Single Message Program
Recurring Message Program

GLOSSARY 26

REFERENCES 27

GOVERNING BODIES

Healthcare mobile messaging is primarily subject to three areas of regulation and oversight: 1) the Telephone Consumer Protection Act (TCPA), enforced by the Federal Communications Commission (FCC); 2) the Health Insurance Portability and Accountability Act of 1996 (HIPAA); and 3) wireless carrier industry standards, codified and enforced by The Wireless Association (CTIA).

FCC

FCC is the governing body that enforces the TCPA. The TCPA restricts automated telephone solicitations and establishes the requirements for the use of text messaging, automatic dialing systems and fax machines.

CTIA

The CTIA (formerly known as the Cellular Telephone Industries Association) is the industry trade group for wireless telecommunications companies. As part of its responsibilities the CTIA monitors the short code programs that run on the wireless carriers. It has an industry handbook the specifically outlines messaging program requirements. Within the CTIA is the CSCA (Common Short Code Administration), which manages the provisioning of short codes. CTIA also publishes a best practices guide for text messaging.

CTIA guidelines are not legal requirements and mobile carriers may or may not follow them. Indeed, they may have additional requirements.

HIPAA

The Health Insurance Portability and Accountability Act of 1996 specifies the requirements for the protection and confidential handling of protected health information. Text messaging compliance requirements are covered within the Security Rule.

HEALTHCARE MESSAGING

HHS Definition of Healthcare

The term "healthcare" is defined broadly under the Department of Human and Health Services' (HHS) regulations to mean anything related to "care, services, or supplies related to the health of an individual including (1) preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual that affects the structure or function of the body; and (2) sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription." (45CFR160.103)

TCPA Consent Requirements for Non-Healthcare Telemarketing and Information Calls

For non-healthcare telemarketing calls and text messages (which are regulated the same way under the TCPA) made to consumers' cell phones, the TCPA generally requires callers to obtain the "express written consent" of called parties prior to calling them. This consent, which can be obtained via email, telephone key press, website click or text message under the federal E-SIGN act, must be clear and specific to receiving calls or texts from the caller.

Telemarketing messages can be broadly defined as messages that promote a product or service. Informational messages can be broadly defined as messages that contain information that does not relate to the sales or promotion of a product; e.g. weather forecast updates and information relating to a specific transaction. Healthcare messaging contains content that relates to care, services, or supplies related to the health of an individual.

The Healthcare Exemption

The TCPA (paragraph (a)(2) of 47 CFR 64.1200) clearly articulates different regulatory requirements for informational healthcare messages. Specifically, these calls and texts can be made with the prior "express consent" of called parties, and do not require express written consent to comply with the TCPA. These messages must be informational and non-telemarketing in nature.

The TCPA recognizes the protections that HIPAA creates for consumer health information and the control it gives consumers in how they can obtain important personal health information from entities covered under HIPAA. The FCC has ruled that "provision of a phone number to a healthcare provider constitutes prior express consent for healthcare calls subject to HIPAA by a HIPAA-covered entity and business associates acting on its behalf, as defined by HIPAA, if the covered entities and business associates are making calls within the scope of the consent given, and absent instructions to the contrary." (FCC 15-72 paragraph 141). This statutory language, first introduced in the FCC's 2012 TCPA ruling and commonly referred to as the TCPA's "Healthcare Exemption," both codifies the importance Congress places in making sure healthcare consumers receive important information about their health and protects HIPAA-covered entities and business associates from the TCPA's stricter consent requirements for telemarketing messages.

An example would be a patient providing their mobile phone number when enrolling at a new doctor's office. The FCC, supported by multiple federal courts (see below) have consistently found the provision of a cell phone number in such a case to constitute express consent to receive informational healthcare messages – like an appointment reminder or wellness message from the doctor's office or the health system that it is a part of.

Legal Challenges and Risk

Since the introduction of the TCPA in 1991 there have been relatively few challenges by recipients of text messages relating to healthcare content. The vast majority of TCPA litigation results from 'telemarketing' messages, with few cases relating to purely informational or emergency messages.

The following case relates to healthcare messaging where all TCPA-compliant processes were followed:

Hudson v. Sharp Healthcare - Southern District of California (2014)
Plaintiff asserted defendant hospital violated the TCPA by sending autodialed calls to her cellphone to collect on unpaid hospital bills. It was ruled that providing one's phone number in the hospital intake process constituted "prior express consent". The case was dismissed.

Latner v. Mount Sinai Health System – 2nd Circuit (2018)
The plaintiff had provided his cell phone number to a clinical facility while there for a routine exam in 2003. In 2011, the system contracted with a vendor to send an automated text message to his phone with a flu shot reminder and brought a TCPA claim against the health system. Both the district and appeals courts ruled that the message only required express consent under the FCC's 2012 TCPA ruling's "Healthcare Exemption" and that the plaintiff's provision of his cell phone number to the system consitituted appropriate express consent to receive calls and texts related to his care, such as a vaccine reminder.

Zani v. Rite Aid – 2nd Circuit (2018)
The plaintiff, a pharmacy customer who had provided his cell phone number to Rite Aid and received a flu shot the previous year, received an informational, auto-dialed call reminding him to get another annual flu vaccination. The plaintiff argued that, because the content of the messaged matched advertisements that Rite Aid had created, the message was marketing in nature and should have required his express written consent. The district and appeals courts disagreed, ruling that the 2012 FCC order created a "Healthcare Exemption" that exempted healthcare messages from other marketing-related messages. Because the call delivered a healthcare message, it was exempt, the courts said, regardless of whther it had a marketing purpose.

Wilkes v. CareSource Indiana, Inc. – Northern District of Indiana (2018)
Plaintiffs had been CareSource members but cancelled their plans and received automated phone calls about wellness and plan benefits to their cell phones after cancelling. After plaintiff called CareSource again to ask to be placed on a do-not-call list, the calls stopped. The court found in favor of CareSource and held that: 1) the provision of phone numbers as part of the plaintiffs' insurance applications to the Indiana Healthcare Exchange constituted their prior express consent to be called by CareSource and its business associate and 2) calling to cancel insurance coverage did not constitute a revocation of that consent, which was only revoked when the plaintiffs called to specifically opt out of calls.

The following healthcare-related cases are examples where TCPA-compliant processes were not followed:

Kolinek v. Walgreens Co. – Northern District of Illinois (2015)
The plaintiff asserted the defendant violated the TCPA by making prescription refill reminders to her phone after she had only provided her phone number for identity verification purposes. The case settled for $11million. In this example, the defendant company did not follow appropriate process for collecting the phone number. The plaintiff was informed by a Walgreen's pharmacist 'that the number was needed for potential identity verification purposes.' The number was not collected for the purpose of contacting the customer about healthcare-related topics, so the 'prior express consent' opt-in was not applicable.

Griffith v. Outcome Health – Northern District of Illinois (2018)
The plaintiff asserted the defendant violated the TCPA by not honoring her repeated opt-out requests. The plaintiff initially enrolled to receive messages with nutrition tips. She later replied 'STOP' which was the stated way to revoke consent to receive text messages. Despite continued attempts at replying STOP she continued to receive nutrition tip messages on an almost daily basis. The case settled for $2.9M.

The example cases highlight the importance of rigorously following TCPA compliant processes to minimize risk exposure. TCPA violation insurance coverage can add additional levels of risk management. Leading mobile messaging vendors have policies that client organizations can subscribe to.

Text Messaging and Protected Health Information (PHI)

SMS text messaging falls under HIPAA's Security Rule for disclosing PHI, which defines the requirements for disclosing PHI in electronic form. Importantly, HIPAA does not explicitly prohibit the use of SMS text messaging to transmit electronic PHI. Instead, the Security Rule requires covered entities and their Business Associates to take appropriate administrative, physical and technical measures to safeguard the transmission and storage of PHI. HIPAA provides a guidelines framework to assess the risks associated with use of the text channel:

- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards
- Organization Safeguards
- Policies and procedures and documentation requirements

The decision to include PHI in text content should take into account the degree of sensitivity associated with the PHI. For example, an individual's first name is technically PHI but has little risk associated with it, whereas specific information about an individual's medical condition has much more risk associated with it.

Additionally, inclusion of certain PHI in text workflows can be dependent on consumer expressed written consent to receive PHI.

When assessing a mobile messaging vendor for healthcare messaging, entities should assess organizations on two broad levels:

1. The extent that the messaging provider has assessed and audited security risks, starting at cell phone number collection and storage, transfer to mobile messaging vendor, delivery of messages to aggregators to carriers and then finally to the cell phone owner.
2. The experience the vendor has at delivering mobile messaging workflows that could potentially contain PHI and adherence to appropriate best practices.

Business Associates

The FCC's TCPA rules defer to HIPAA guidelines for authorization of Business Associates (BA) to engage with individuals for whom the BA does not directly have prior express consent. It acknowledges the privacy protections afforded under HIPAA, and exempts from TCPA consent compliance requirements all identification, time-of-day and opt-out requirements.

As specified in HIPAA guidelines, covered entities must enter into a contract with entities that meet the definition of business associate that create, receive, maintain or transmit PHI to ensure they have satisfactory assurances from the business associate that it will appropriately safeguard PHI. (FCC-12-21 paragraph 61)

Employers and Business Associate Agreements (BAA) with Health Plans

If an employer provides terms and conditions and a privacy policy that specifies the individual has provided their phone number so that they can be contacted about issues relating to their employment and health, then it is appropriate for a health plan to contact the individual if the employer has provided the individuals information to the health plan and a BAA is in place.

COMPLIANCE DOCUMENTATION AND GUIDES

The full TCPA legislation: click here for link.

The CTIA provides voluntary guidelines that outline messaging program requirements. This includes the Messaging Principals and Best Practices guidebook, which focuses on maintaining a wireless messaging environment largely free of unwanted messages: click here for link.

The CTIA also provides specific guidelines on Short Code use in its CTIA Short Code Monitoring Handbook: click here for link.

CLASSIFICATION OF MESSAGE PROGRAMS

The CTIA differentiates Application-to-Person (A2P) and Person-to-Person (P2P) messaging. P2P Messaging describes low-volume exchanges of messages between end users. Which the CTIA defines as consistent with typical human operation. This guidebook does not provide any guidelines to cover P2P messaging within the healthcare space. A2P describes all messaging that falls outside the definition of P2P (i.e. traffic that is not consistent with human operation). Common usages are:

- Enterprises texting multiple consumers simultaneously
- Call center scenarios
- Alerts and notifications

The Messaging Principals and Best Practices guidebook sets out to protect consumers from unwanted messages, particularly high volume A2P traffic.

A2P messages are most commonly delivered using short codes. The short code platform was developed to accommodate higher volume SMS traffic with upfront consumer protections from unwanted messaging traffic and review procedures to ensure appropriate use of the platform. Toll-free long codes can also be used for some healthcare text messaging use cases.

SHORT CODES AND TOLL-FREE LONG CODES

Short Codes

Short Codes

A2P messages are most commonly delivered using Common Short Codes (commonly referred to as short codes). The short code platform was developed to accommodate higher volume SMS traffic with upfront consumer protections from unwanted messaging traffic and review procedures to ensure appropriate use of the platform. Short codes can be used to deliver all types of healthcare related A2P messages including alerts, reminders and transactional messages. A short code is a 5 or 6-digit number that is used by businesses to send messages to their customers, and for healthcare organizations to send messages to their patients and health plan members. The numbers can be assigned randomly, or in the case of 'vanity' short codes they are selected. Vanity short codes allows organizations to have specific digits, or for the number to spell out a word.

Provisioning a Short Code

Short codes are acquired though the CSCA website: https://www.usshortcodes.com. The CSCA assigns short codes to applicants which allows the recipient to use the number across all wireless service providers.

- Messaging vendors typically coordinate the application for a short code on behalf of their customers
- Short codes can be renewed for 3,6 or 12 months at a time

To ensure a timely approval of a short code application the following information should be available for program submission:

- Terms and Conditions URL
- Estimated total messages
- Estimated number of participants per month
- URL for customer information/help page
- Opt-In Keyword
- Privacy Policy

Provisioning Time
It typically takes 6-8 weeks for a new short code to be provisioned.

Vanity vs Random
Normally the 5 or 6 digits of a short code are randomly assigned. When the digits are chosen, it is termed a vanity short code. The digits can spell out a more memorable number or a word e.g. HEALTH. Vanity short codes can help with number recollection, and also become a brand asset.

Ongoing Short Code Program Maintenance
The messaging service provider is responsible for maintaining accurate records with the carrier systems and the CSCA registry. If a service provider requires a modification to a messaging program, these changes must be submitted to the carriers for review and then update any relevant carrier records. Programs being used in the market, must match the program details that were approved.

Toll-Free Long Codes

Toll-free long codes are 10-digit toll-free phone numbers that are provisioned so that they can send and receive texts. Toll-free long codes are toll-free for telephone calls only. The end user does get charged for sending texts to and from a toll-free long code. Toll-free long codes can only be used for care management and call center type interactions. They are not meant to be used for large volume alert, reminder and transactional messages.

Provisioning a Toll-Free Long Code
Toll-free numbers are provisioned through toll-free service providers for use within the North American Numbering Plan (NAMP). After which, an Aggregator provisions the toll-free number to be text enabled.

- Messaging vendors typically coordinate the application for a toll-free long code on behalf of their customers.
- Once provisioned for texting, the toll-free long code does not need to be renewed.

To ensure a timely approval of a toll-free long code application the following information should be available for program submission:

- Terms and conditions URL
- Estimated total messages
- Estimated number of participants per month
- URL for customer information/help page
- Opt-in keyword
- Privacy policy

Provisioning Time
It typically takes 1-2 weeks for a new toll-free long code to be provisioned.

When to Use a Toll-Free Long Code Rather Than a Short Code
The vast majority of A2P messaging is delivered using the short codes platform. The short code platform has higher delivery capacity than toll-free long codes which means many more messages can be delivered per second, and the per message cost is lower for short codes. Importantly, any large volume alerts, reminders and transactional messages should only be sent using short codes.

For care management and call center type interactions, toll-free long codes have several advantages. They take 5-6 weeks less time to provision, so if a short time to launch is an important requirement, toll-free long code programs can be set up in a shorter time. Toll-free long codes do not have a monthly license fee. This means it may be more cost effective for low volume messaging programs to use a toll-free long code and spend more per message, but avoid paying a monthly license fee. Lastly, when a toll-free number is already being used for consumer telephone calls, there may be situations where a company wants to deliver text messaging on the same number as the toll-free telephone line for continuity of experience.

MONITORING AND AUDITS

Provisioning of a short code is done with the expectation that the owner of the short code will follow the guides for short code use as outlined in the CTIA Short Code Monitoring Handbook. The CTIA conducts in-market monitoring of short code use to ensure compliance levels are maintained. Audits are triggered when programs do not compliance requirements which are identified by the CTIA's in-market monitoring tool.

The penalty for not meeting the CTIA's compliance requirements is having the short code shut down by the carriers. There is no specific legal penalties if the CTIA's guidelines are not adhered to.

CTIA Audit Notices Severities Description

Severity	Definition	Cure Date	Penalties
0	Extreme consumer harm	Immediate	**CTIA:** Immediate registry suspension harm **Carriers:** Vary by case; immediate suspension or termination possible
1	Serious consumer harm	5 business days	**CTIA:** Unresolved audits; possible registry harm suspension **Carriers:** Vary by case
2	Moderate consumer harm	5 business days	**CTIA:** Vary by case consumer harm **Carriers:** Vary by case

TCPA Violations

The TCPA does not conduct audits of mobile messaging providers. However, this statute can be enforced in court or by the FCC. In such cases an individual might challenge the legal basis for receiving a text and the matter would be resolved legally. See section 'Legal Challenges And Risk' (Page 6) for an example of case law relating to Healthcare text messaging.

For TCPA cases brought in court, someone initiating unlawful messages could be liable anywhere from $500.00 to $1500.00 per call (or text), or recover actual monetary loss, whichever is greater. (47 U.S. Code § 227)

HEALTHCARE MESSAGING COMPLIANCE PRINCIPLES

The CTIA Short Code Rule Book provides extensive detail on messaging program compliance. Its guidelines are not legal requirements. Mobile operators may or may not follow the CTIA guidelines, and indeed, they may have additional requirements. The CTIA guidelines cover compliance for a broad range of messaging types with a focus on telemarketing messages, whereas this guidebook is focused specifically on healthcare messages. Therefore, this section includes specific areas of CTIA compliance that are highly relevant for healthcare messages and incorporates rules from the TCPA and HIPAA.

CTIA Guiding Principles *(Section A.1 in the CTIA Short Code Rule Book)*

The CTIA guidebook outlines four guiding principles for messaging programs. These are focused specifically towards telemarketing messages, which have more rigorous compliance requirements than healthcare messages. But since these principles form the basis for general messaging compliance requirements, they have been included in this guidebook:

1. **Display clear calls-to-action**: All programs must display a clear call-to-action. Customers must be made aware of what exactly they are signing up to receive.
2. **Offer clear opt-in mechanisms**: Customers must consent clearly to opt into all recurring-messages programs. Requiring a customer to enter a mobile phone number does not constitute a compliant opt-in. Instead, customers must understand they will receive messages and consent to receive them.
3. **Send opt-in confirmation messages:** A confirmation message must be sent to customers ***always***. For recurring-messages programs, confirmation messages must include clear opt-out instructions.
4. **Acknowledge opt-out requests:** Short code service providers must acknowledge and act on all opt-out requests. Monitoring procedures confirm successful opt-out.

Choice and Consent *(Section A.2 in the CTIA Short Code Rule Book)*

Short code programs are expected to deliver sufficient value so consumers elect to participate with full transparency into the delivery conditions.

Healthcare Messaging Context

No component of program advertising or messaging may be deceptive about the underlying program's functionality, features, or content. All disclosures present in calls-to-action, advertisements, terms and conditions, and messages must remain clear and consistent throughout the user experience.

Opt-In Requirements for Healthcare Messaging

Consent is assumed when an individual provides the health organization with their telephone number, most commonly in relation to a specific transaction i.e. new patient enrollment, signing-up to a new health plan. As they fall under the TCPA's informational message category, Healthcare messaging programs do not require prior express written consent from the mobile phone owner. The TCPA requires 'prior express consent'. 'Prior express consent' is not defined by the TCPA; however, in 1992 when the law was established the FCC stated "persons who **knowingly release** their phone number have in effect given their invitation or permission to be called at the number which they have given, **absent instructions to the contrary**."

Common Opt-In Approaches

Assumed Opt-In *(Prior express consent)*
The assumed opt-in approach is a compliant approach for healthcare messages. To the extent a customer releases his telephone number to a healthcare provider or insurance company for treatment or insurance purposes—for example, on a hospital intake form, an insurance application, or a HIPAA authorization form—the company is deemed to have the necessary consent to send that customer informational text messages. Program terms and conditions, including complete opt-out information, and privacy policy should be provided to the individual if requested. When a messaging program is initiated the healthcare organization sends an Opt-in Confirmation Message (or initial text) that expresses who the text is from, describes the general content of messages and provides opt-out functionality, support functionality and details of messaging rates.

Double Opt-In *(equivalent to express written consent)*
The double opt-in approach adds an additional level of consent to the assumed opt-in approach. For example, it can be used if the message program could contain marketing content.

The double opt-in approach sends an initial message to the number that the individual provided. The initial message specifies who the message is from, describes the general content of messages, opt-out and support functionality. In addition, it specifically requests the individual responds to the message with a specified keyword to be opted in. The individual is only considered opted-in, if they reply to the keyword.

If an individual has not provided their mobile phone number to a healthcare organization, the organization can use a range of approaches to drive opt-in from consumers. For example, this could relate to a health plan that does not have an individual's mobile number but wants to deliver information about plan benefits and services. In addition, in exigent medical situations, the Free to End-User approach can be used, which is highlighted in section Free to End-User Healthcare Messaging (Page 19).

Keyword Text-In *(equivalent to express written consent)*
The short code number is displayed with a keyword and key information about the message program. When the individual texts in the keyword to the number they are considered opted-in. Details of the program could be displayed on a website, bill board or promotional materials. Program information needs to be clearly articulated: who runs the messaging program, a description of the messaging topics, details of messaging rates, where Terms and Conditions and Privacy Policy documents can be accessed. In the initial message that is sent out after opting-in, the following information should be included who the text is from, describes the general content of messages and provides opt-out functionality, support functionality and details of messaging rates.

Submitted Mobile Number *(equivalent to express written consent)*
Information about the messaging program

is displayed and there is functionality for the individual to submit their mobile phone number. Typically, key program information is displayed on a web page, and there is a form where the individual can enter their mobile phone information and key personal information. Key program information needs to be clearly articulated; who runs the messaging program, a description of the messaging topics, details of messaging rates, where Terms and Conditions and Privacy Policy documents can be accessed. In the initial message that is sent out after opting-in, the following information should be included who the text is from, describes the general content of messages and provides Opt-out functionality, support functionality and details of messaging rates.

Use of IVR systems fall into the submitted mobile number approach, where a message program is advertised with a corresponding phone number. If an individual calls in, the IVR takes them through a workflow where they can opt-in to a messaging program.

The submitted opt-in approach is appropriate for single message and recurring message programs.

Express Written Consent Formats

Some messaging programs and use cases may need to operate with the express written consent of consumers. The FCC has defined such consent as a written agreement that includes "clear and conspicuous disclosure informing the person signing that by executing the agreement, such person authorizes the seller to deliver or cause to be delivered to the signatory telemarketing calls using an automatic telephone dialing system or an artificial or prerecorded voice."

There are two key considerations around gaining express written consent. First, healthcare organizations should remember that express written consent is only required for telemarketing programs that promote the sale of a good or service. Second, the FCC has noted that consent obtained in compliance with the E-SIGN Act will satisfy the requirements of their rules on express written consent, including permission obtained via an email, website form, text message, telephone keypress, or voice recording (2012 TCPA Order, 27 FCC. Rcd. at 1844).

Opt-In Records

All opt-in requests must be retained from the time a user initiates opt-in until a minimum of 6 months after the user has opted out of the program. For the assumed opt-in approach, the record of customer consent is captured in the documentation when the customers phone number was initially captured. Other opt-in approaches, such as keyword text-ins require the messaging service provider to capture a record of the opt-in and manage the record handling in coordination with the healthcare organization for which the messaging program is being managed.

Identity Verification

Some opt-in approaches do not provide information about who the individual is e.g. when a customer texts in a keyword to a short code number. For many healthcare messaging programs this is not an issue, as the messaging program is based on general information that is not specific to the individual. For example, if a hospital advertises a keyword text-in to get the hospital's emergency department wait time.

However, there are situations when it is important to verify the identity of the phone owner who texted in, as the messaging program content is tailored to the specific customer. For example, if a mobile health engagement program is advertised on a health plan ID card and a customer texted in with a number that was not on record. In these situations the healthcare company should have a process developed for identity verification prior to launching the program.

Opt-In Considerations for Sensitive Healthcare Topics

Although the lowest requirements of consent is appropriate for all healthcare messages, there are certain topics where it may be appropriate to adopt increased levels of consent, even if no PHI is included in the text. For example message programs relating to:

- Depression and mental health
- HIV
- Sexual health

In these situations, individuals may prefer to actively consent to engaging on such topics.

Opt-Out

Functioning opt-out mechanisms are crucial for all text messaging programs. Programs must always acknowledge and respect customers' requests to opt out of programs. Short code programs must respond to, at a minimum, the universal keywords STOP, END, CANCEL, UNSUBSCRIBE, and QUIT by sending an opt-out message and, if the user is subscribed, by opting the user out of the program. Subsequent text, punctuation, capitalization, or some combination thereof must not interfere with opt-out keyword functionality. Consumers can legally revoke their consent to receive text message using any reasonable means. Once revoked, a new consent would need to be obtained before sending any additional messages.

Recurring-messages programs must display opt-out instructions at program initiation and at least once every 30 days in message content or service messages. A program may deliver one final message to confirm a user has opted out successfully, but no additional messages may be sent after the user indicates a desire to cancel a short code program.

Identity Verification for Reassigned Mobile Phone Numbers

Mobile numbers can change ownership, which may mean a mobile number that was previously owned by an individual who had consented to receive text messages from a healthcare organization is transferred to an individual who has not consented to receive text messages from the healthcare organization. In this situation, the healthcare organization would likely have no knowledge that the number had changed ownership. If the healthcare organization sends a message to the new mobile number owner, they would be in effect sending a message to someone who had not opted into their messaging program. Based on a ruling from the U.S. Court of Appeals for the D.C. Circuit in March 2018, liability cannot be assigned to companies that mistakenly texted a reassigned number after a one call 'safe harbor' without any notice that the number has been reassigned or an opt-out from the number's new owner. However, no specific guidance was provided on how such reassigned numbers should be handled. Currently the FCC is making progress towards creating a comprehensive database of reassigned numbers. (ACA Int'l, et al. v. FCC, et al. 2018)

Without clear guidance, it becomes paramount to ensure consumers can revoke their consent to receive text message using any reasonable means, which includes directly through the text channel, orally and in writing.

Customer Care (Section A.3 in the CTIA Short Code Rule Book)

Customer care contact information must be clear and readily available to help users understand program details as well as their status with the program. Customer care information should result in users receiving help. Programs must always respond to customer care requests, regardless of whether the requester is subscribed to the program. At a minimum, the HELP keyword must return the program name and further information about how to contact service providers. Short code programs should promote customer care contact instructions at program opt-in and at regular intervals in content or service messages, at least once per month.

Program Content (Section A.4 in the CTIA Short Code Rule Book)

All content associated with short code programs must promote a positive user experience. The CTIA Short Code Rulebook identifies specific areas such as unapproved or illicit substances and controlled substances that should not be included in a Short Code program.

Privacy Policy and Terms and Conditions *(Section A.5 in the CTIA Short Code Rule Book)*

Privacy related to PHI is covered in the section Text Messaging and Protected Health Information above. Even when messages do not contain PHI, measures must be taken to protect the privacy of user information. Service providers are responsible for protecting the privacy of user information and must comply with applicable privacy law. Service providers should maintain a privacy policy for all programs and make it accessible from the initial call-to-action. When a privacy policy link is displayed, it should be labeled clearly.

Use cases might require different disclosures in the full terms and conditions. In all cases, terms and conditions and privacy policy disclosures must provide up-to-date, accurate information about program details and functionality.

Program Records and Product Description *(Section A.6 in the CTIA Short Code Rule Book)*

Consistent program names and product descriptions in advertisements and messages help consumers connect all parts of the short code experience. All short code programs are required to disclose program names, product description, or both in service messages, on the call-to-action, and in the terms and conditions. The program name is the sponsor of the short code program, often the brand name or company name associated with the short code. The product description describes the product advertised by the program.

Program Names and Functionality *(Section A.7 in the CTIA Short Code Rule Book)*
Service providers assume responsibility for maintaining accurate records in carrier systems and the Common Short Code Administration (CSCA) registry. Service providers wishing to modify a program must submit changes to the carriers for review and must update relevant carrier records. Programs promoted in the market must match the programs approved.

Use of Keywords

Keywords need to be at least at least 2 characters long, have no spaces and cannot include any special characters. Typically, they cannot be system keywords. This prevents use of common terms like HELP, STOP and YES.

All mandatory keywords must be processed correctly, regardless of MO message format (e.g., keywords must function whether sent by MMS or SMS). Service providers must scan MO message logs regularly to identify opt- out attempts and must terminate those subscriptions, regardless of whether the subscribers used the correct opt- out keywords or methods.

Ages of Message Recipients

With parent's permission the youngest age a message can be sent to is 13 years old. Consent requires documented written expressed consent from a parent for a covered entity to directly contact their child if under 18 years of age, but 13 years or older. Any age under 18 but older than 13 requires parental consent.

International Languages

All required message program information must be made available in all international languages that the program is available in. This includes Terms and Conditions and Privacy Policy.

STOP and HELP commands must work in all international languages the messaging program is available in. This explicitly means an error message cannot be returned if an international STOP or HELP command is made. Additionally, the follow-up response must be written in the language that the original command was made.

FREE TO END USER HEALTHCARE MESSAGING

Free to end user messages are text messages that are delivered with no charges to the recipient to receive the text.

Free-to-end user healthcare messaging was an additional healthcare carve out made by the TCPA in 2015. A healthcare organization can text an individual who has not previously provided their mobile phone number if the message content is considered expedient and the message is free to the end user. In addition to being free to the called party: the following conditions must be met:

1. The messages must be sent only to the number provided by the individual
2. The messages must state the name and contact information for the healthcare organization (for calls, at the outset)
3. The messages must be strictly limited in purpose to the eight exempted types of messages ((1) appointment and exam confirmations and reminders; (2) wellness checkups; (3) hospital per-registration instructions; (4) pre-operative instructions; (5) lab results; (6) post-discharge follow-up intended to prevent readmission; (7) prescription notifications; and (8) home healthcare instructions) be HIPAA-compliant, and may not include "telemarketing, solicitation, or advertising content, or billing, debt-collection, or other financial content"
4. The messages must be concise (for calls generally one minute or less, and for texts, 160 characters or less)
5. The messages must be limited to one per day and three per week from a specific healthcare provider
6. The messages must include "an easy means to opt out" (an interactive voice and/or key-press activated option for answered calls, a toll-free number for voicemail, and instructions to use "STOP" for texts)
7. The opt-out requests must be honored "immediately." (FCC 15-72 paragraph 125)

The TCPA does not specifically define when free to end user messaging should be considered over standard healthcare messaging. An interpretation is as follows: when a healthcare company that does not have a relationship with the individual is enlisted to provide care services by a healthcare organization that does have a relationship with the patient and there is not a clearly defined Business Associate arrangement between the two companies. Using this free to end user approach would remove any uncertainty about calls and messages made to the individual by the enlisted company.

HEALTHCARE ASSUMED OPT-IN USE CASES

	Description	**Requirements**
Call-to-Action	During a transaction the individual is asked to provide a mobile phone number as a way for them to be reached for matters that relate to the transaction	Terms and conditions must be available if requested Privacy Policy must be available if requested
Terms & Conditions	Terms and conditions must be readily available if requested	Terms and conditions should be hosted on the company website.
Opt-in	Opt-in is assumed when the individual provides their mobile phone number when requested	The individual provides their mobile phone number
Message Flow	Recurring-messages programs confirming opt-in with a single text message MUST state explicitly to which program the user enrolled and provide clear opt-out instructions in the Opt-In Confirmation MT.	Opt-In Confirmation MT • Program (brand) name OR product description • Opt-out information • Customer care contact information • Product quantity or recurring-messages disclosure • "Message and data rates may apply" disclosure HELP MT • Program (brand) name OR product description • Additional customer care contact information Opt-Out MT • Program (brand) name OR product description • Confirmation that no further messages will be delivered

HEALTHCARE DOUBLE OPT-IN USE CASE

	Description	**Requirements**
Call-to-Action	During a transaction the individual is asked to provide a mobile phone number as a way for them to be reached for matters that relate to the transaction. A Opt-in message is sent that requires the individual to text back a Keyword to be opted into the message program	Terms and conditions must be available if requested Privacy Policy must be available if requested
Terms & Conditions	Terms and conditions must be readily available if requested	Terms and conditions should be hosted on the company website.
Opt-In	Opt-in is achieved when the individual replies to the short code with the correct keyword	The individual provides their mobile phone number and responds to an opt-in text
Message Flow	Recurring-messages programs confirming opt-in with a single text message MUST state explicitly to which program the user enrolled and provide clear opt-out instructions in the Opt-In Confirmation MT.	Opt-In Confirmation MT • Program (brand) name OR product description • Opt-out information • Customer care contact information • Product quantity or recurring-messages disclosure • "Message and data rates may apply" disclosure HELP MT • Program (brand) name OR product description • Additional customer care contact information Opt-Out MT • Program (brand) name OR product description • Confirmation that no further messages will be delivered

KEYWORD TEXT-IN USE CASE

	Description	Requirements
Call-to-Action	During a transaction the individual is asked to provide a mobile phone number as a way for them to be reached for matters that relate to the transaction. A Opt-in message is sent that requires the individual to text back a Keyword to be opted into the message program	Terms and conditions must be available if requested Privacy Policy must be available if requested
Terms & Conditions	Terms and conditions must be readily available if requested	
Opt-in	Opt-in is achieved when the individual texts in a specific keyword to the short code number	The individual provides their mobile phone number and responds to an opt-in text
Message Flow	Recurring-messages programs confirming opt-in with a single text message MUST state explicitly to which program the user enrolled and provide clear opt-out instructions in the Opt-In Confirmation MT.	Opt-In Confirmation MT • Program (brand) name OR product description • Opt-out information • Customer care contact information • Product quantity or recurring-messages disclosure • "Message and data rates may apply" disclosure HELP MT • Program (brand) name OR product description • Additional customer care contact information Opt-Out MT • Program (brand) name OR product description • Confirmation that no further messages will be delivered

SINGLE MESSAGE PROGRAM USE CASES

	Description	Requirements
Call-to-Action	The call-to-action for a single-message program can be simple. The primary purpose of disclosures is to ensure a consumer consents to receive a text message and understands the nature of the program.	Product description Complete terms and conditions or link to terms and conditions Privacy policy or link to privacy policy "Message and data rates may apply"disclosure
Terms & Conditions	Comprehensive terms and conditions may be presented in full beneath the call-to-action, or they may accessible from a link or a pop-up presented near the call-to-action	Program (brand) identification Product description Customer care contact information "Message and data rates may apply" disclosure
Opt-in	The consumer must actively opt into single-message programs.	Consumer's affirmative opt-in message programs.
Message Flow	Although single-message programs are not required to display HELP and STOP keywords, they should support HELP and STOP commands, as described in the Universal Compliance Principles.	Opt-In Confirmation MT • Program (brand) name OR product description HELP MT • Program (brand) name OR product description • Additional customer care contact information Opt-Out MT • Program (brand) name OR product description • Confirmation that no further messages will be delivered

RECURRING MESSAGE PROGRAM USE CASE

	Description	Requirements
Call-to-Action	Because of their ongoing touch points with consumers, recurring-messages programs require the most disclosures among use cases. The primary purpose of disclosures is to ensure the consumer consents to receive text messages and understands the nature of the program.	• Product description • Service delivery frequency or recurring-messages disclosure • Complete terms and conditions or link to complete terms and conditions • Privacy policy or link to privacy policy • "Message and data rates may apply" disclosure
Terms & Conditions	Comprehensive terms and conditions might be presented in full beneath the call-to- action, or they might be accessible from a link or a pop-up presented near the call-to- action.	• Program (brand) name • Service delivery frequency or recurring-messages disclosure • Product description • Customer care contact information • Opt-out instructions in bold type • "Message and data rates may apply" disclosure
Opt-in	Consumers must provide prior express written consent to enroll in all text message programs (i.e., single-message programs or recurring-messages programs). Recurring-messages programs must send one message confirming opt-in consent. Double opt-in is optional.	Consumer's affirmative opt-in
Message Flow	Recurring-messages programs confirming opt-in with a single text message MUST state explicitly to which program the user enrolled and provide clear opt-out instructions in the Opt-In Confirmation MT.	Opt-In Confirmation MT • Program (brand) name OR product description • Opt-out information • Customer care contact information • Product quantity or recurring-messages disclosure • "Message and data rates may apply" disclosure HELP MT • Program (brand) name OR product description • Additional customer care contact information Opt-Out MT • Program (brand) name OR product description • Confirmation that no further messages will be delivered

GLOSSARY

Audit Notice
Report issued to noncompliant short code programs detailing the specific violations and actions required to bring the program into compliance

Call-to-Action
Language urging a customer to opt into a short code program, and the mechanism (e.g., button displaying "buy now") allowing them to do so

Compliance Audit
Test performed to determine the compliance of a short code program

Confirmation Message
Sent at the start of message campaigns. It must contain specific details of the messaging program. It can also be referred to as a Welcome Message

Consent
Act of agreeing to opt into a short code program and the terms and conditions associated with the purchase

Content Message
Text message delivering purchased content or displaying instructions for how to access purchased content

Message Platform
Application through which messages are received and sent

Mobile Originated (MO)
Text message sent from a user's mobile device

Mobile Terminated (MT)
Text message sent to user in response to user texting a keyword

Service Message
Text message offering details about the short code program, including opt-in instructions, opt-out instructions, summary terms and conditions, and support information (e.g., helpline)

REFERENCES

Telephone Consumer Protection Act. Title 47 Chapter 5

Health Insurance Portability and Accountability Act. 45 CFR Part 160, Part 162, and Part 164

Messaging Principles and Best practices. CTIA

Short Code Monitoring Handbook. CTIA Short Code Monitoring Program

45CFR160.103

FCC-12-21 paragraph 57

FCC-12-21 paragraph 61

47 U.S. Code § 227

FCC 15-72 paragraph 125

ACA Int'l, et al. v. FCC, et al., No. 15-1211 (D.C. Cir. 2018)

Hudson v. Sharp Healthcare, No. 3:2013cv01807 - Document 56 (S.D. Cal. 2014)

Kolinek v. Walgreen Co. – Case No. 13 C 4806, (N.D. Ill. 2014)

Griffith v. ContextMedia, LLC d/b/a Outcome Health – Civil Case No.: 16-2900 (N.D. Ill DC 2016)

Ferencz v. International Clinic Consultants - Case No. 13-215314-9 SEA (Wash. Sup. Ct. 2014)

mPulse™
mobile

About mPulse Mobile

mPulse Mobile, the leader in Conversational AI solutions for the healthcare industry, drives improved health outcomes and business efficiencies by engaging individuals with tailored and meaningful dialogue. mPulse Mobile combines behavioral science, analytics and industry expertise that helps healthcare organizations activate their consumers to adopt healthy behaviors. With over a decade of experience, 70+ healthcare customers and more than 150 million conversations annually, mPulse Mobile has the data, the expertise and the solutions to drive healthy behavior change.

To ask a question or request a call, go to: mpulsemobile.com/contact

mpulsemobile.com

Version History
1.0 - June 2017
1.5 - April 2018
2.0 - October 2018

H

Exhibit H

mPulse Mobile TCPA Policy

mPulse Mobile, Inc.
TCPA POLICIES AND PROCEDURES

To whom does this Policy apply?

This Policy applies to all mPulse employees, and any third-party contractors or agents, to the extent that such employees, third-party contractors or agents are involved in or facilitate the transmission of telephone calls or text messages to healthcare patients on mPulse's customers behalf.

Background on legal framework and application to mPulse Mobile

The Federal Communications Commission (the "FCC") has by order implementing the Telephone Consumer Protection Act (the "TCPA") adopted rules, including those set forth in 47 CFR § 64.1200, (together with the TCPA, the "TCPA Rules"), prohibiting the initiation of telephone calls (other than a call made for emergency purposes or made with the prior express consent of the called party) using automatic telephone dialing systems or an artificial or prerecorded voice to telephone numbers assigned to, among other services, cellular telephone service or any service for which the called party is charged for the call.

Further, the Federal Trade Commission (the "FTC") has by order implementing the Telemarketing Consumer Fraud and Abuse Prevention Act (the "Telemarketing Act") adopted rules, including those set for in 16 CFR § 310, establishing the National Do-Not-Call Registry (DNC Registry), prohibiting sellers and telemarketers from calling a person whose telephone number is on the DNC Registry unless the seller or telemarketer has an Established Business Relationship ("EBR") with the person or has prior written consent to contact the person.

mPulse offers mobile engagement technology solutions to its customers in the healthcare industry so that they can engage their patients and others (collectively, "individuals") to achieve successful healthcare outcomes. As a result, many of the TCPA Rules and DNC Registry requirements are inapplicable to the informational healthcare messages mPulse customers initiate through the mPulse services, nor are they directly applicable to mPulse as a conduit of its customers' messages that they are ultimately responsible for. Nevertheless, mPulse, as a matter of policy, requires all mPulse customers to represent and warrant that they have the prior express consent of the individuals they choose to contact through the mPulse services and are otherwise fully compliant with their obligations under all applicable consumer protection laws, such as the TCPA and the Telemarketing Act.

This Policy is designed to complement our Terms of Service – which is binding on all of our customers' use of mPulse services – by outlining the procedures we use to monitor our customers' compliance with our Terms of Service and any applicable legal requirements, and to provide a backstop to their compliance obligations when necessary. **If you have any questions regarding this policy, or suspect any mPulse customer is utilizing the mPulse services in a manner inconsistent with the law or our Terms of Service, contact the Chief Operating Officer immediately at 888-678-5735 or compliance@mpulsemobile.com.**

What do we do if a patient asks to be removed from a customer calling list?

The mPulse platform fully recognizes all commonly used opt-out requests that individuals may respond with to any message they receive from an mPulse customer. In certain circumstances, an individual may communicate their desire not to receive any additional messages from an mPulse customer directly to mPulse or its agents. If any person receives such a notification from a patient, always direct the individual to reply to the last message they have received with "STOP" if possible.

Nevertheless, mPulse shall maintain an internal Do Not Call (DNC) list for such circumstances for each individual mPulse customer, and which will be readily available for viewing and communicated to the applicable customer. *No individual who is listed on an internal DNC list shall be messaged unless the Chief Operating Officer has provided written consent to override the internal DNC list.*

- If any mPulse employee or agent receives a notification, whether oral or written, from an individual that they no longer wish to receive messages sent by or on behalf of an mPulse customer, such person shall enter that individual's telephone number into mPulse's internal DNC list for the applicable mPulse customer, along with the individual's name, if provided, when such a notification is received. If such mPulse employee or agent is not able to directly record such a notification directly into mPulse's internal DNC list, such person shall notify the Chief Operating Officer within one (1) business day of receiving such a notification and provide the individual's telephone number and, if provided, the individual's name.

- If it cannot be determined which particular customer is responsible for initiating the message that the individual no longer wishes to receive, the individual's telephone number will be placed on the global DNC list maintained by mPulse.

- mPulse's IT Department shall ensure that all records of DNC requests shall be retained for a period of no less than four (4) years from the date any such request was made.

When is it acceptable to send a message to an individual?

All routine, non-emergency messages initiated by mPulse customers should ordinarily be placed during normal business hours based on the individual's location, as determined by the individual's area code if no address is on file for the individual. The foregoing calling time restrictions do not apply in the case of an emergencies.

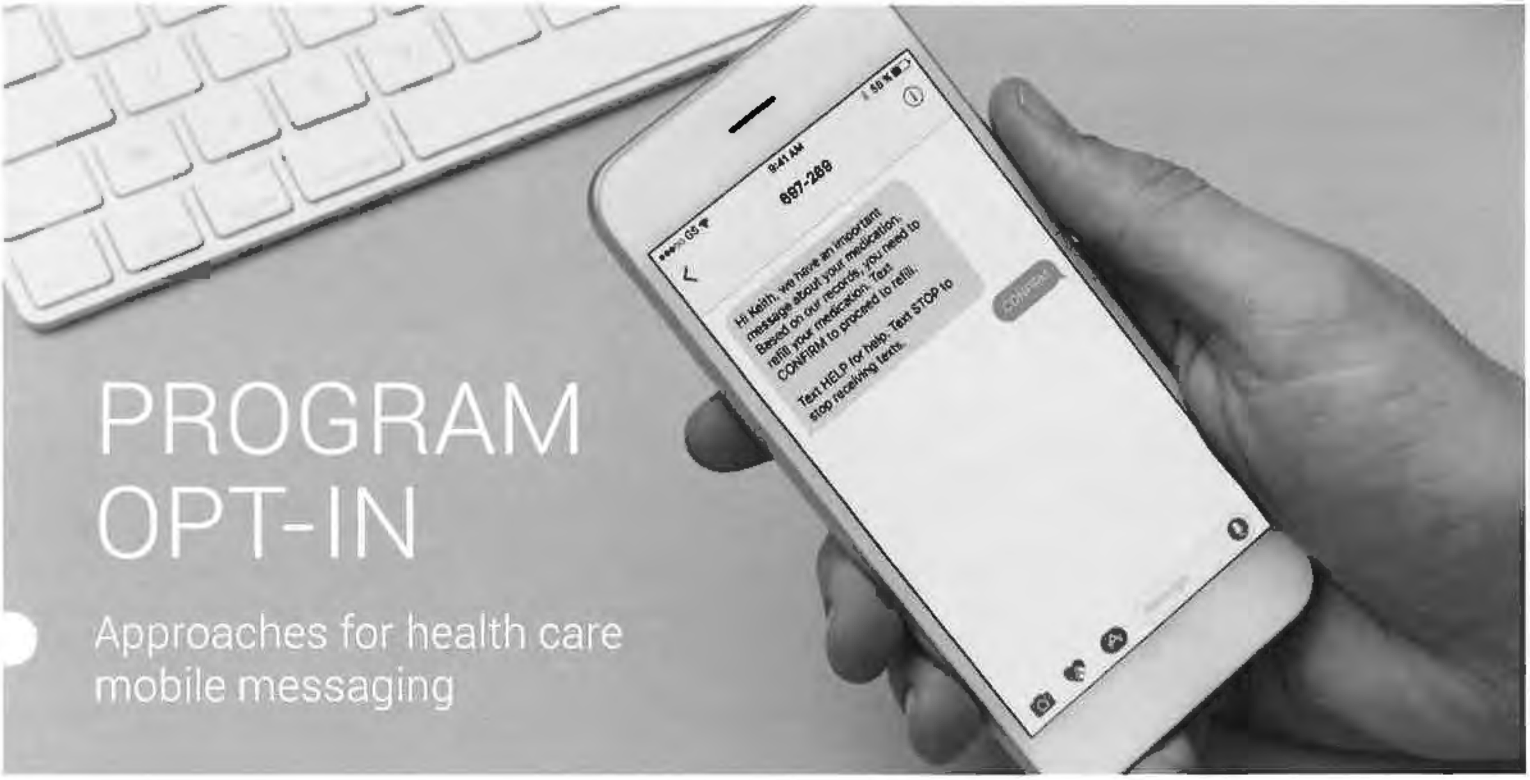
How do I report a violation of the Policy?

TCPA compliance violations can be costly. Any violations of this Policy shall be reported to the Chief Operating Officer promptly. Any individual complaint regarding possible violations of this Policy shall also be reported promptly to the Chief Operating Officer for coordination and handling.

I

Exhibit I

mPulse Mobile Opt-in Overview



PROGRAM OPT-IN

Approaches for health care mobile messaging

Hi Keith, we have an important message about your medication. Based on our records, you need to refill your medication. Text CONFIRM to proceed to refill.

Text HELP for help. Text STOP to stop receiving texts.

mPulse Mobile has a broad range of proven approaches to enroll healthcare consumers in text messaging programs. mPulse leverages its decade-long experience in health engagement to help our 70+ clients determine the most impactful opt-in strategy for their business and consumer needs.

Prior Express Consent

Maintains TCPA compliance for healthcare informational messaging via the express opt-in of consumers that have provided their mobile number to the healthcare organization

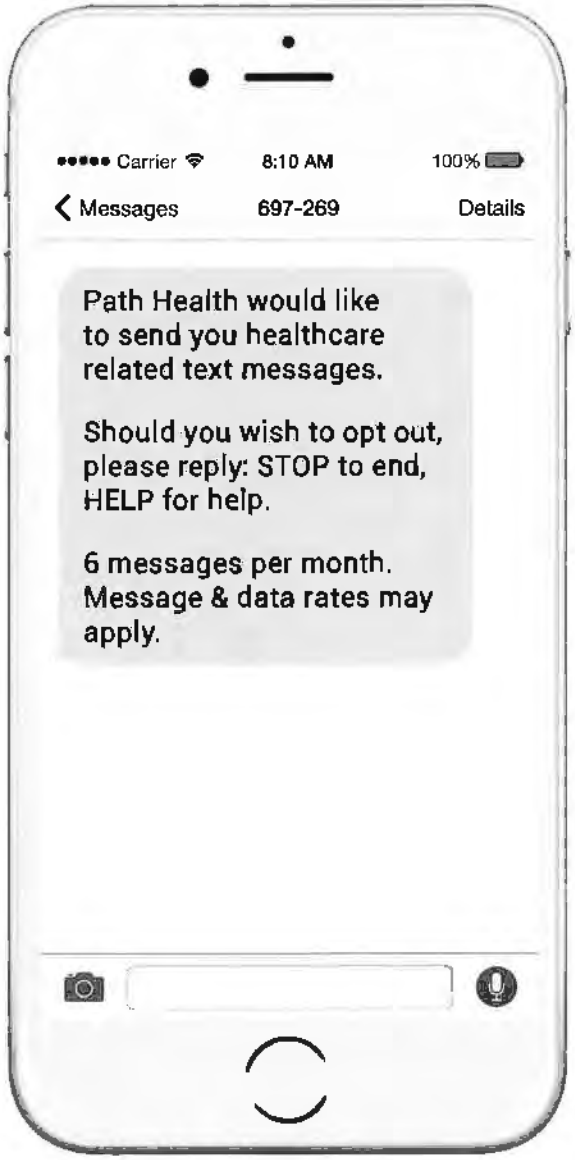
ASSUMED OPT-IN

Opt-In Process

Send an initial welcome message with program information and opt-out instructions to consumers that have provided a mobile number as a way to contact them

Consumer Adoption

Very high program adoption rates, typically only 2-5% of consumers opt-out



Path Health would like to send you healthcare related text messages.

Should you wish to opt out, please reply: STOP to end, HELP for help.

6 messages per month. Message & data rates may apply.

Learn More

Additional information on TCPA-compliant healthcare messaging can be found in mPulse Mobile's *Essential Guidebook for Healthcare Mobile Messaging*

Express Written Consent: Inbound Methods

Maintains TCPA compliance for all forms of automated text messaging through the express written opt-in of consumers

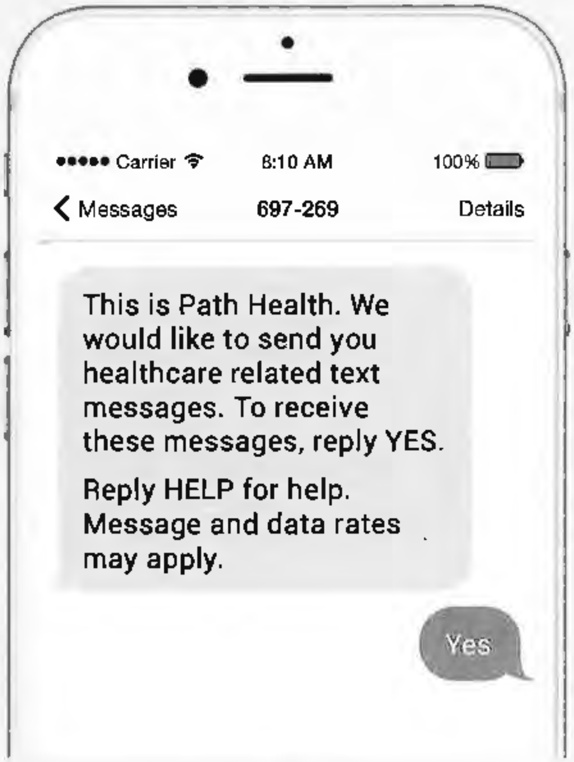
DOUBLE OPT-IN

Opt-In Process

Send an initial welcome message to consumers and ask for an additional opt-in confirmation via text before any further messaging
Falls under the ESIGN Act as an electronic signature

Consumer Adoption

The additional confirmation step can have an adverse impact on enrollment when compared to an assumed opt-in



This is Path Health. We would like to send you healthcare related text messages. To receive these messages, reply YES.

Reply HELP for help. Message and data rates may apply.

Yes

INBOUND IVR

Opt-In Process

Offer consumers on inbound calls the option to join the text program, either by keypress on the call or via texting in to the short code

Consumer Adoption

Relies on inbound call volume and proactive consumer action to drive enrollment results

"To receive text message updates from Path Health, press one and enter your ten-digit cell phone number. Message and data rates may apply."

"You can also text 'Path' to the number 22987 to join."

Express Written Consent: Inbound Methods (continued)

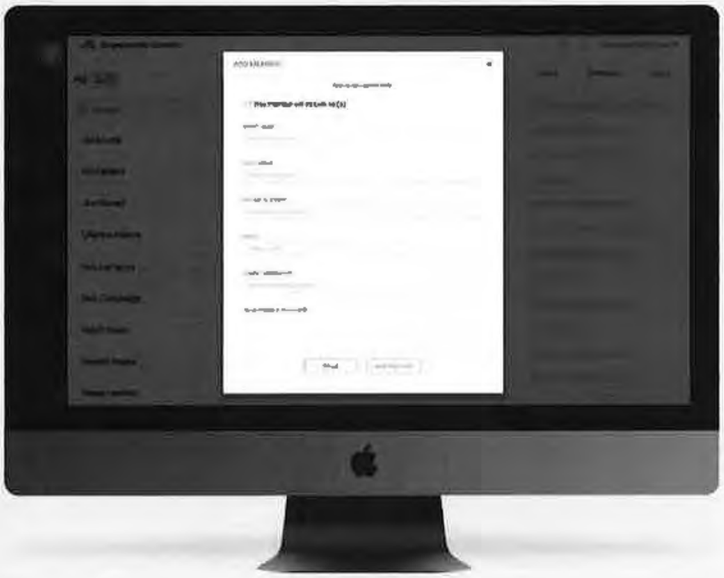
LIVE AGENT

Opt-In Process

Give consumers on live inbound calls the option to join the text program, and manually add them via preference management or mPulse's Engagement Console

Consumer Adoption

Requires high inbound call volume to be effective



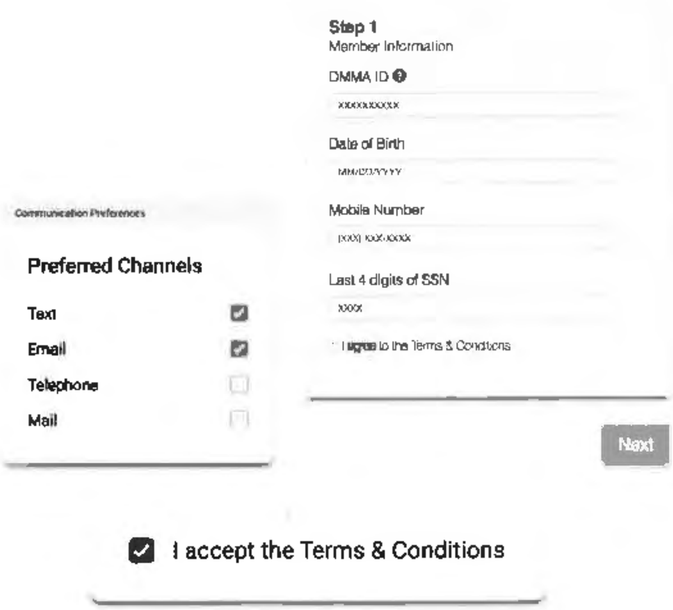
HOSTED PREFERENCE MANAGEMENT PAGE

Opt-In Process

Allow consumers to directly opt in to programs by entering their mobile numbers into a dedicated web page
Can be hosted by mPulse or client company

Consumer Adoption

Relies on consumers to navigate to the page via inbound web traffic or outbound channels (eg email)



Communication Preferences

Preferred Channels

Text	☑
Email	☑
Telephone	□
Mail	□

Step 1
Member Information

DMMA ID
XXXXXXXXXX

Date of Birth
MM/DD/YYYY

Mobile Number
(XXX) XXX-XXXX

Last 4 digits of SSN
XXXX

□ I agree to the Terms & Conditions

Next

☑ I accept the Terms & Conditions

Express Written Consent: Outbound

Leverages existing outreach channels to drive program adoption

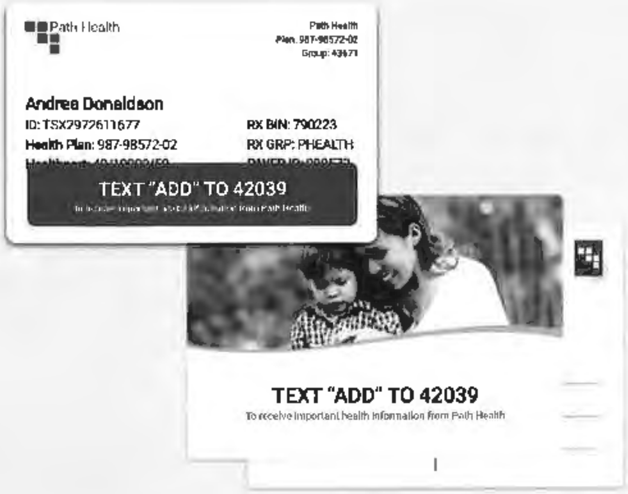
PHYSICAL MAIL

Opt-In Process

Place a call to action in a dedicated postcard or with important consumer materials for consumers to text in to the short code

Consumer Adoption

Opt-in rates vary by mailer type (e.g. ID cards vs informational postcards) and depend on consumers opening and reading mail before proactively responding on different channels



Path Health

Path Health
Plan: 987-98572-02
Group: 43671

Andrea Donaldson

ID: TSX2972611677	RX BIN: 790223
Health Plan: 987-98572-02	RX GRP: PHEALTH

TEXT "ADD" TO 42039

To receive important health information from Path Health

TEXT "ADD" TO 42039

To receive important health information from Path Health

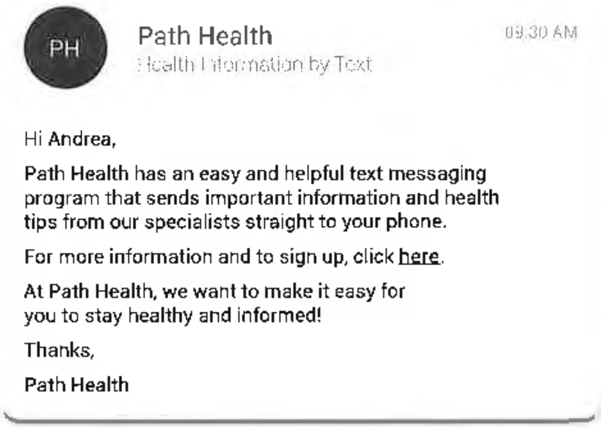
EMAIL

Opt-In Process

Direct consumers to text in or link to a sign-up or preference management page (see above)

Consumer Adoption

Dependent on email opens and link-clicks to drive opt-in rates



PH

Path Health

Health Information by Text

09:30 AM

Hi Andrea,

Path Health has an easy and helpful text messaging program that sends important information and health tips from our specialists straight to your phone.

For more information and to sign up, click here.

At Path Health, we want to make it easy for you to stay healthy and informed!

Thanks,

Path Health

OUTBOUND IVR

Opt-In Process

Launch dedicated opt-in campaigns via voice with an explanation of the program and the option to opt in over the phone

Outbound IVR calls are generally subject to the same TCPA regulations as text messaging

Consumer Adoption

Relies on consumers to answer live phone calls and then keypress on the call to gain opt-in

"This is an automated message from Path Health. To get updates and information from Path Health via text message, press five, followed by your ten digit cell phone number, or text "join" to the number 22987."

Opt-In Method Requirements

During the opt-in process, and when the program is running, there are core opt-in and opt-out management responsibilities handled by client healthcare companies, and others that are managed by mPulse Mobile.

	PRIOR EXPRESS CONSENT	EXPRESS WRITTEN CONSENT
CLIENT RESPONSIBILITIES	• Gather or use consumer cellphone numbers that have been obtained directly from the consumer and in a context where the messaging program is considered relevant. • Document when and how cellphone number was obtained. • Monitor non-mPulse channels for consumer opt-outs and promptly inform mPulse when a consumer asks to opt out.	• Gather consumer cellphone numbers specifically for the messaging program, working with mPulse to design and support the opt-in campaign via express, written channels. • If using the text-in-based approach, promote the text in keyword and short code across consumer communications. • Monitor non-mPulse lines of communication for consumer opt-outs and promptly inform mPulse when a consumer asks to opt out.
MPULSE MOBILE RESPONSIBILITIES	• Monitor all programs and short codes for text-based opt-outs and immediately honor them. • Accept and honor forwarded opt-out requests that consumers make directly to the healthcare organization. • Follow CTIA and FCC best practices for TCPA compliance and always offer opt-in and opt-out functionality.	

mPulse Mobile Capabilities

mPulse Mobile is committed to maintaining industry-leading program compliance capabilities. In addition to meeting all standard TCPA compliance requirements, mPulse Mobile:

- Utilizes Natural Language Understanding (NLU) to discover non-standard opt-out or preference requests automatically
- Recognizes all foreign languages and special characters
- Carefully follows CTIA guidelines on honoring variations of the "STOP" opt out command (eg. "end," "cancel," "unsubscribe")
- Leverages over 10 years of experience in mobile messaging compliance
- Offers clients and partners access to its TCPA liability insurance if required
- Actively monitors changes and updates to FCC regulations and TCPA case law

Summary

	Assumed Opt-In	Double Opt-In	Inbound IVR	Live Agent	Preference Management	Physical Mail	Email	Outbound IVR
Description	Welcome text with opt out as an option	Asks for text confirmation of consent	Allows inbound phone callers to opt in	Can manually add consenting callers to text program	Allows consumers to directly opt in online	Invites consumers to text in to the program	Link or text in to consent	Call consumers to drive text-ins
Consent Obtained	Express	Express Written	Express Written	Express Written	Express Written	Express Written	Express Written	Express Written
Adoption Rate	Highest	Medium	Lower	Lower	Lower	Lower (eg ID Card) Very Low (eg Letter)	Very Low	Very Low

Legal Overview

This overview summarizes the key law and rulings that guide healthcare text messaging. For more information, contact your mPulse Mobile account team or email info@mpulsemobile.com.

- FCC regulations (47 CFR 64.1200) forbid persons or entities from initiating "any telephone call that includes or introduces an advertisement or constitutes telemarketing, using an automatic telephone dialing system or an artificial or prerecorded voice," to a cell phone number, "other than a call... that delivers a 'health care' message made by, or on behalf of, a 'covered entity' or its 'business associate,' as those terms are defined in the HIPAA Privacy Rule, 45 CFR 160.103"
- The FCC's 2015 Declaratory Ruling elaborated that the "provision of a phone number to a healthcare provider constitutes prior express consent for healthcare calls subject to HIPAA473 by a HIPAA-covered entity and business associates acting on its behalf, as defined by HIPAA, if the covered entities and business associates are making calls within the scope of the consent given, and absent instructions to the contrary."
- This exception for healthcare messaging has been consistently upheld in case law:
  - Zani v. Rite Aid Headquarters Corp., 17-1230-cv (2nd Cir. February 21, 2018)
  - ACA International Et. Al v. Federal Communications Commission, No. 15-1211 (9th Cir. March. 16, 2018)
  - Bailey v. CVS Pharmacy, inc. 3:17-cv-11482 (US District Southern NJ, August 14, 2018)
- For all messaging outside these healthcare-related exemptions, the FCC and the TCPA require the call or text to be "made with the prior express written consent of the called party" (47 CFR 64.1200)
  - Any auto-dialed call that "includes or introduces any advertisement or constitutes telemarketing," require prior express written consent from the telephone subscriber. - Rules & Regs. Implementing the TCPA of 1991, 27 FCC Rcd. 1830, 1838-44 (2012) ("2012 TCPA Order"); 47 C.F.R. § 64.1200(a)(2).
  - FCC regulations define prior express written consent as a written agreement that includes "clear and conspicuous disclosure informing the person signing that by executing the agreement, such person authorizes the seller to deliver or cause to be delivered to the signatory telemarketing calls using an automatic telephone dialing system or an artificial or prerecorded voice." 2012 TCPA Order, 27 FCC Rcd. at 1855.
  - The FCC further noted that "consent obtained in compliance with the E-SIGN Act will satisfy the requirements of our revised rule, including permission obtained via an email, website form, text message, telephone keypress, or voice recording." 2012 TCPA Order, 27 FCC. Rcd. at 1844

This material is intended for general information purposes only and does not constitute legal advice. For legal issues that arise, the reader should consult legal counsel. Compliance with the Telephone Consumer Protection Act and other relevant laws and regulations will depend on the individual program and organizations should always consult with TCPA and, if applicable, HIPAA compliance professionals prior to launching a mobile messaging program.

mPulse™ mobile

About mPulse Mobile

mPulse Mobile, the leader in mobile health engagement, drives improved health outcomes and business efficiencies by engaging individuals with tailored and meaningful dialogue. mPulse Mobile combines technology, analytics and industry expertise that helps healthcare organizations activate their consumers to adopt healthy behaviors.

With 9 years of experience, 70+ healthcare customers, and more than a hundred million messages sent annually, mPulse Mobile has the data, the expertise and the technology to drive healthy behavior change.

To ask a question or request a call, go to: mpulsemobile.com/contact

✉ in 🐦

mpulsemobile.com

J

Exhibit J

mPulse Mobile Data Overview

Data Overview

mPulse Mobile makes it easy to transfer data between customers' systems and mPulse Mobile's HITRUST-certified platform. This document provides an overview of the available data transfer methods and data types.

Data Transfer Methods

mPulse Mobile provides customers with a variety of data transfer methods to support their different resource levels and requirements.

APIs and Callbacks

Real-time integrations are enabled by mPulse Mobile's RESTful APIs and callbacks that support JSON and XML formats.

The Audience API allows you to manage member data, and the Event Upload API allows you to send us events, as they occur or in batches, to drive dialogues immediately or in the future.

For more information about our APIs and callbacks, please ask your Sales Director or Account Manager for our "Integration and Security Overview".

Automated Secure File Transfer Protocol (SFTP)

Automated SFTP is often the best data transfer solution for customers who do not require real-time updates to drive messaging programs. While the processing of files is automated on the mPulse Mobile side, files can be manually or automatically posted on the customer side.

This method allows for a much faster implementation than APIs and provides the flexibility to quickly iterate. Many customers start with an automated SFTP approach and then integrate once they are happy with the overall data flow design.

Manual Batch File Uploads

CSV files can be manually uploaded using our web-based applications.

Manual Entry

Data can be manually managed using our web-based applications.

Data Types

Member

The most important piece of member data is the message destination (e.g., mobile number, email address, etc.) It is the minimum data required to create a member record because it is necessary to send a message. In addition to the message destination, we recommend providing First Name, Gender, Date of Birth, and ZIP Code. First Name is used for personalization, and the other three are used for analysis and tailoring.

Generally, member profile data change infrequently and are used for personalization (e.g., first name), tailoring (e.g., different age groups receive different content for the same type of campaign), segmentation (e.g., targeting a subgroup of the larger population for specific types of correspondence), and branching within dialogues (e.g.,

Member data come from several sources: client systems (e.g., electronic medical records [EMRs], customer relationship management [CRM] tools, etc.), social determinants of health, and interactions with consumers.

Event

Event data are generally transactional and can be sent to mPulse Mobile as events occur. Based on the messaging program design, dialogues can be immediately triggered or scheduled for the future.

Event-level data can also be used for personalization and tailoring. In addition, event data can include information that is necessary for reporting purposes only (e.g., internal tracking information such as Transaction ID or Appointment ID).

Member Engagement Data

Responses

Incoming SMS messages (i.e., responses) are called mobile originated (MO) messages. MOs provide a wealth of information. In addition to those that we expect, consumers often send in messages about other topics. These messages give customers insight into consumers' needs that might not otherwise be uncovered.

Other Actions

In addition to responses, other actions help drive messaging and determine engagement. Other actions include things like link clicks, message opens, completed surveys, and opt-outs.

Non-actions

Non-actions can be just as important as actions and are also used to drive messaging. For example, if an email is not opened for a week after being sent, we can follow up with an SMS message.

Reporting

Each service layer (Communicate, Engage, and Activate) brings with it its own reporting metrics, building on what the previous layer offers.

Communicate

Operational level data live at the Communicate Layer. Reporting includes metrics on consumer reach: total members, total subscribers, messages sent, bounced messages, and response data.

Engage

At the Engage Layer, we start to provide more insight into the consumer experience with metrics like sentiment, dialogue activity and results, and customer user statistics for customers leveraging the Engagement Console.

Activate

Finally, the Activate Layer brings with it the Activation Profile and Activation Score, which is correlated with behavior change. Client data (e.g., EMR), public data (e.g., community need index [CNI]), and consumer engagement data (e.g., responses, response times, non-actions, etc.) are all used to develop the Activation Profile to tailor dialogues and content to the individual to drive higher Activation Scores.

Business Objectives

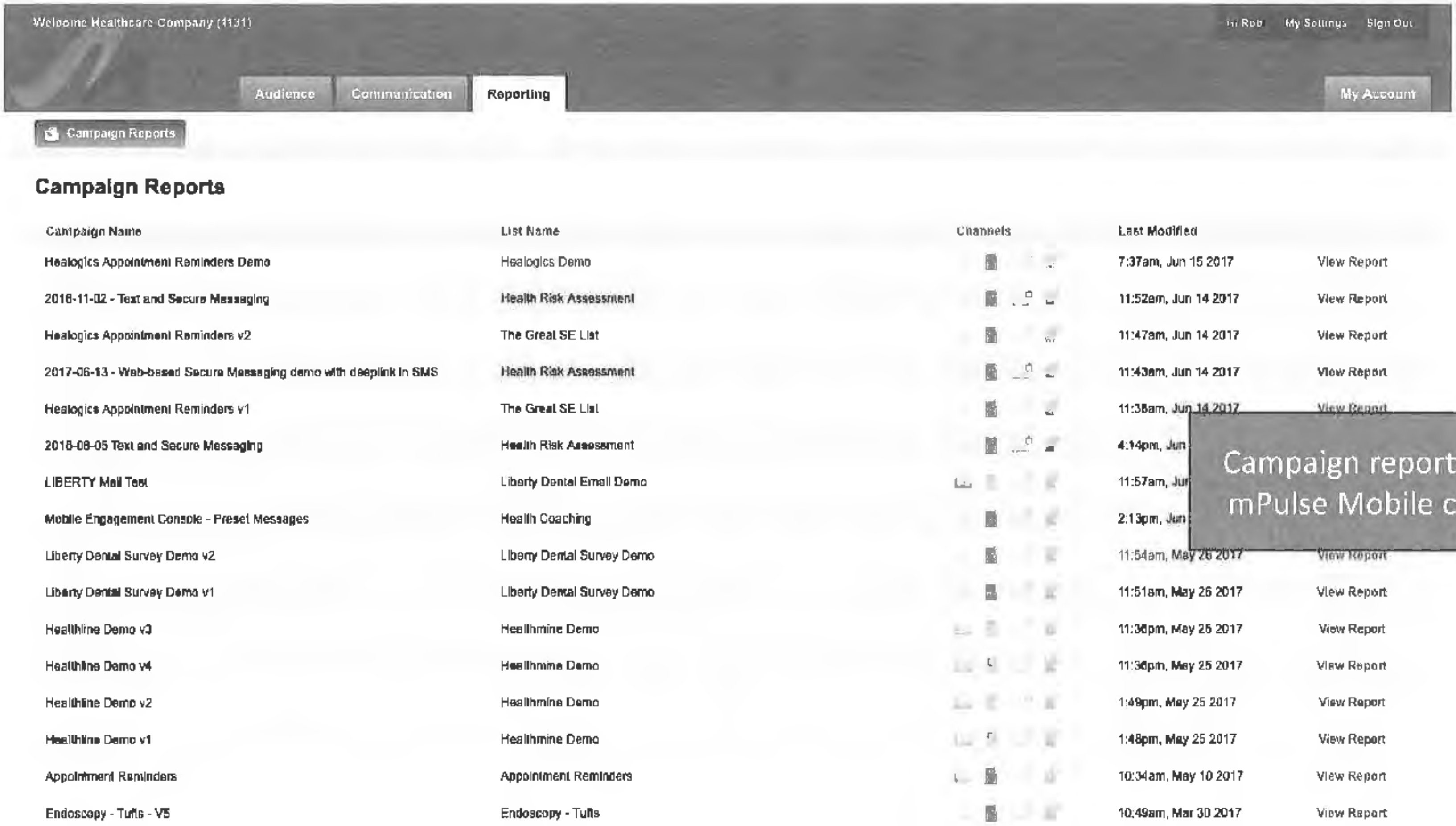
Tying messaging programs back to the desired business outcome metric or metrics is the best way to determine the success and value of a messaging program. In many cases customers are able to provide these data, and in others, self-reported data or proxy measures to determine program success is used. Additional Information

Please contact your Sales Director or Account Manager if you want to discuss these topics in more detail as they relate to your specific use case.

K

Exhibit K

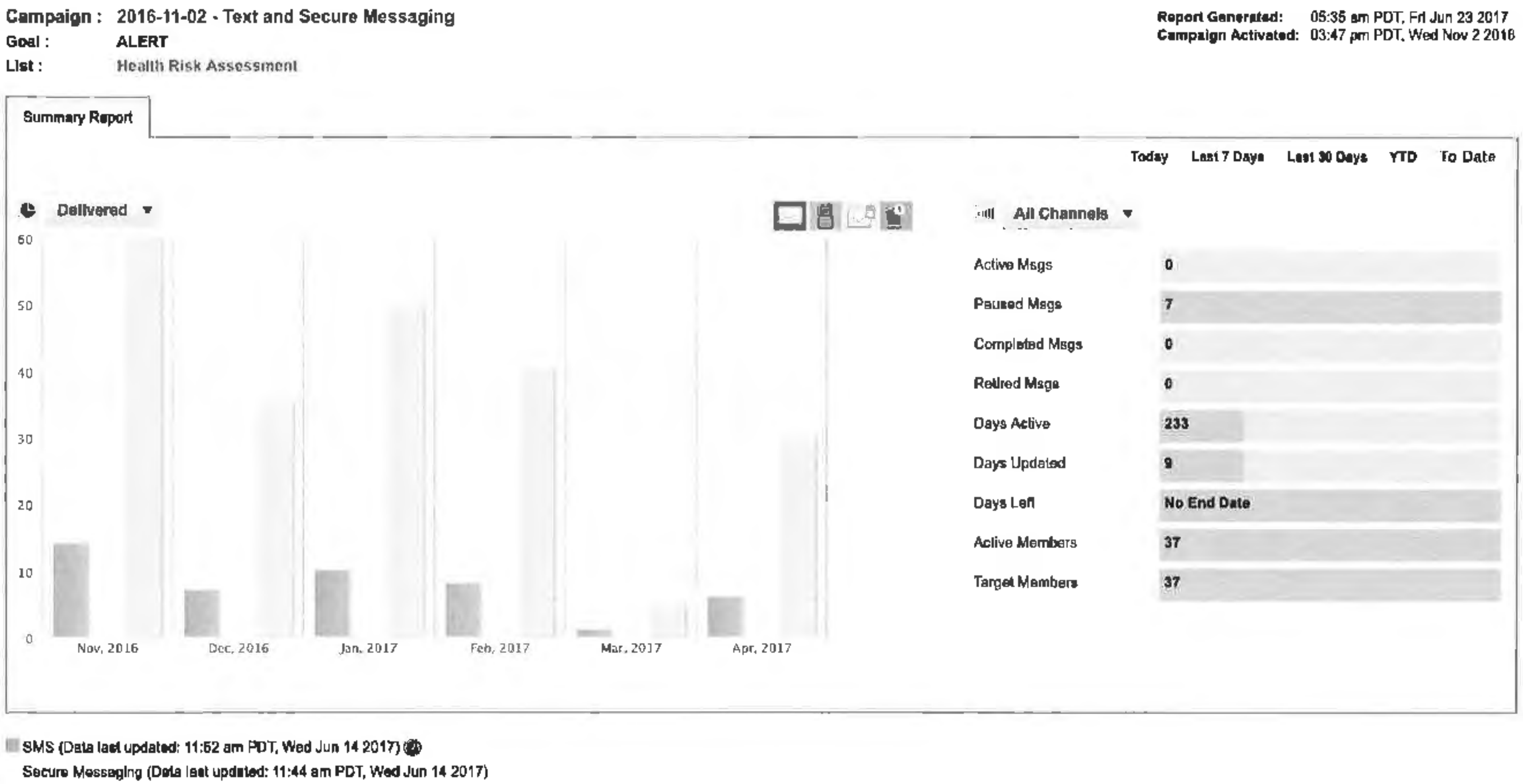
mPulse Mobile Reporting Screenshots



Campaign Reports

Campaign Name	List Name	Channels	Last Modified	
Healogics Appointment Reminders Demo	Healogics Demo		7:37am, Jun 15 2017	View Report
2016-11-02 - Text and Secure Messaging	Health Risk Assessment		11:52am, Jun 14 2017	View Report
Healogics Appointment Reminders v2	The Great SE List		11:47am, Jun 14 2017	View Report
2017-06-13 - Web-based Secure Messaging demo with deeplink in SMS	Health Risk Assessment		11:43am, Jun 14 2017	View Report
Healogics Appointment Reminders v1	The Great SE List		11:38am, Jun 14 2017	View Report
2016-08-05 Text and Secure Messaging	Health Risk Assessment		4:14pm, Jun	
LIBERTY Mail Test	Liberty Dental Email Demo		11:57am, Jun	
Mobile Engagement Console - Preset Messages	Health Coaching		2:13pm, Jun	
Liberty Dental Survey Demo v2	Liberty Dental Survey Demo		11:54am, May 26 2017	View Report
Liberty Dental Survey Demo v1	Liberty Dental Survey Demo		11:51am, May 26 2017	View Report
Healthline Demo v3	Healthmine Demo		11:38pm, May 25 2017	View Report
Healthline Demo v4	Healthmine Demo		11:36pm, May 25 2017	View Report
Healthline Demo v2	Healthmine Demo		1:49pm, May 25 2017	View Report
Healthline Demo v1	Healthmine Demo		1:48pm, May 25 2017	View Report
Appointment Reminders	Appointment Reminders		10:34am, May 10 2017	View Report
Endoscopy - Tufts - V5	Endoscopy - Tufts		10:49am, Mar 30 2017	View Report

Campaign reports are listed in mPulse Mobile control panel.



Campaign : 2016-11-02 - Text and Secure Messaging
Goal : ALERT
List : Health Risk Assessment

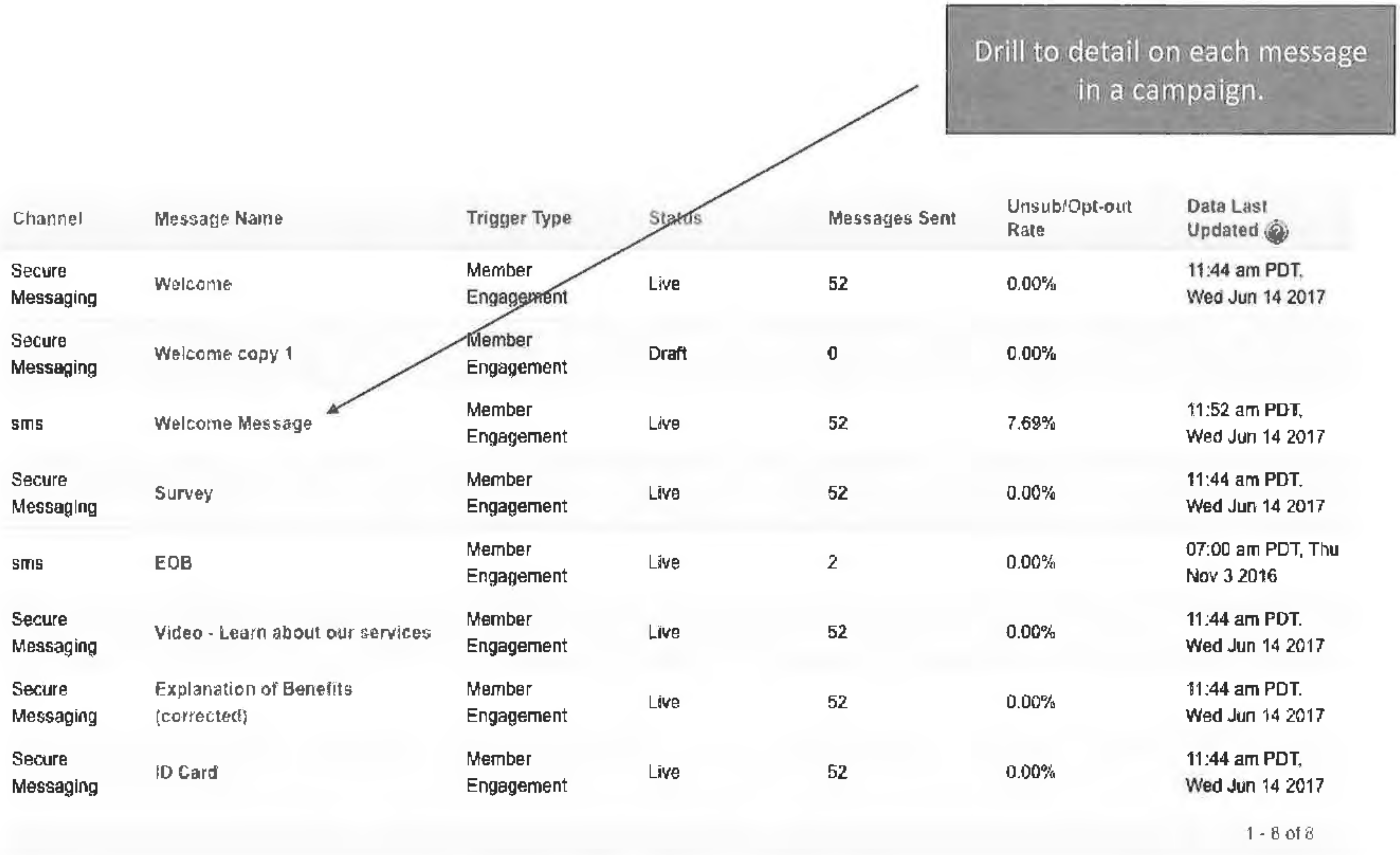
Report Generated: 05:35 am PDT, Fri Jun 23 2017
Campaign Activated: 03:47 pm PDT, Wed Nov 2 2016

Summary Report

Today Last 7 Days Last 30 Days YTD To Date

Active Msgs	0
Paused Msgs	7
Completed Msgs	0
Retired Msgs	0
Days Active	233
Days Updated	9
Days Left	No End Date
Active Members	37
Target Members	37

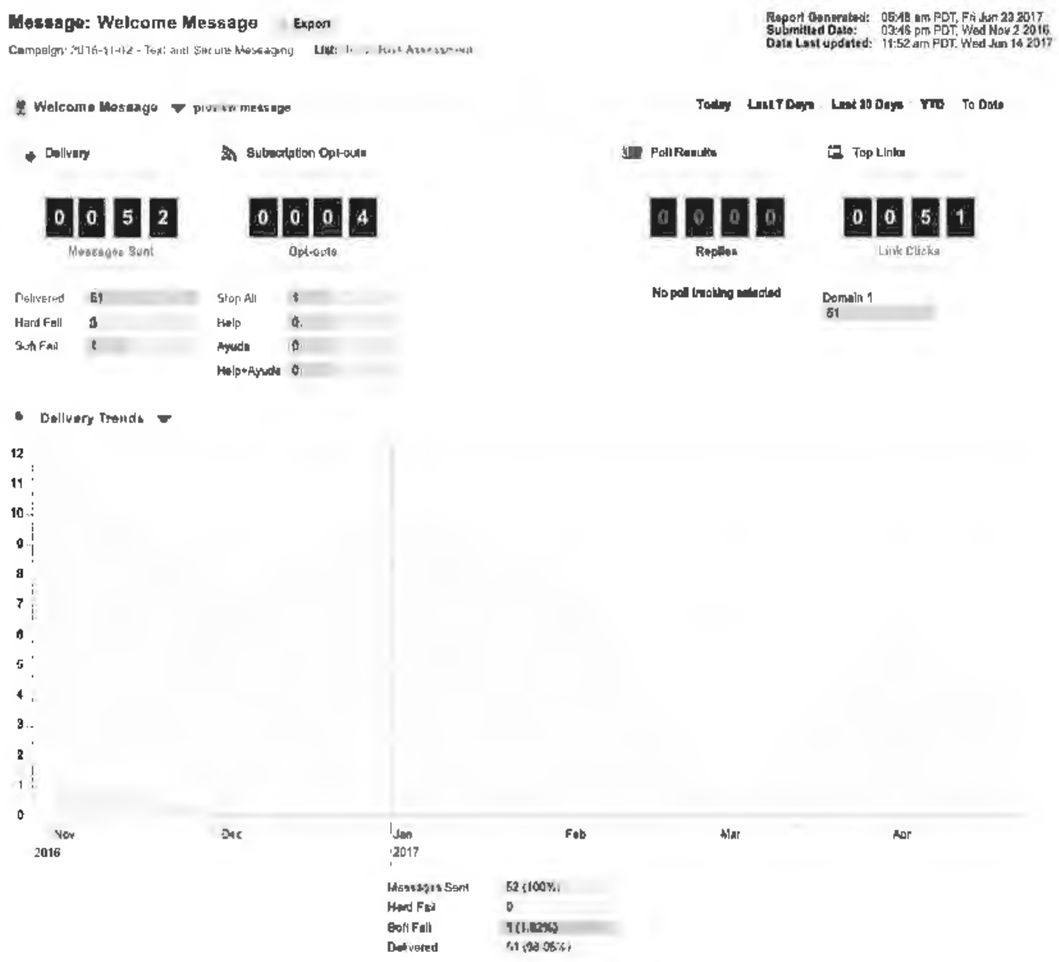
▨ SMS (Data last updated: 11:52 am PDT, Wed Jun 14 2017)
Secure Messaging (Data last updated: 11:44 am PDT, Wed Jun 14 2017)



Drill to detail on each message in a campaign.

Channel	Message Name	Trigger Type	Status	Messages Sent	Unsub/Opt-out Rate	Data Last Updated
Secure Messaging	Welcome	Member Engagement	Live	52	0.00%	11:44 am PDT, Wed Jun 14 2017
Secure Messaging	Welcome copy 1	Member Engagement	Draft	0	0.00%	
sms	Welcome Message	Member Engagement	Live	52	7.69%	11:52 am PDT, Wed Jun 14 2017
Secure Messaging	Survey	Member Engagement	Live	52	0.00%	11:44 am PDT, Wed Jun 14 2017
sms	EOB	Member Engagement	Live	2	0.00%	07:00 am PDT, Thu Nov 3 2016
Secure Messaging	Video - Learn about our services	Member Engagement	Live	52	0.00%	11:44 am PDT, Wed Jun 14 2017
Secure Messaging	Explanation of Benefits (corrected)	Member Engagement	Live	52	0.00%	11:44 am PDT, Wed Jun 14 2017
Secure Messaging	ID Card	Member Engagement	Live	52	0.00%	11:44 am PDT, Wed Jun 14 2017

1 - 8 of 8



Message: Welcome Message Export

Campaign: 2016-11-02 - Text and Secure Messaging List: [illegible] Risk Assessment

Report Generated: 05:48 am PDT, Fri Jun 23 2017
Submitted Date: 03:46 pm PDT, Wed Nov 2 2016
Data Last updated: 11:52 am PDT, Wed Jun 14 2017

0052 Messages Sent

Delivered	51
Hard Fail	0
Soft Fail	1

0004 Opt-outs

Stop All	4
Help	0
Ayuda	0
Help+Ayuda	0

0000 Replies

No poll tracking selected

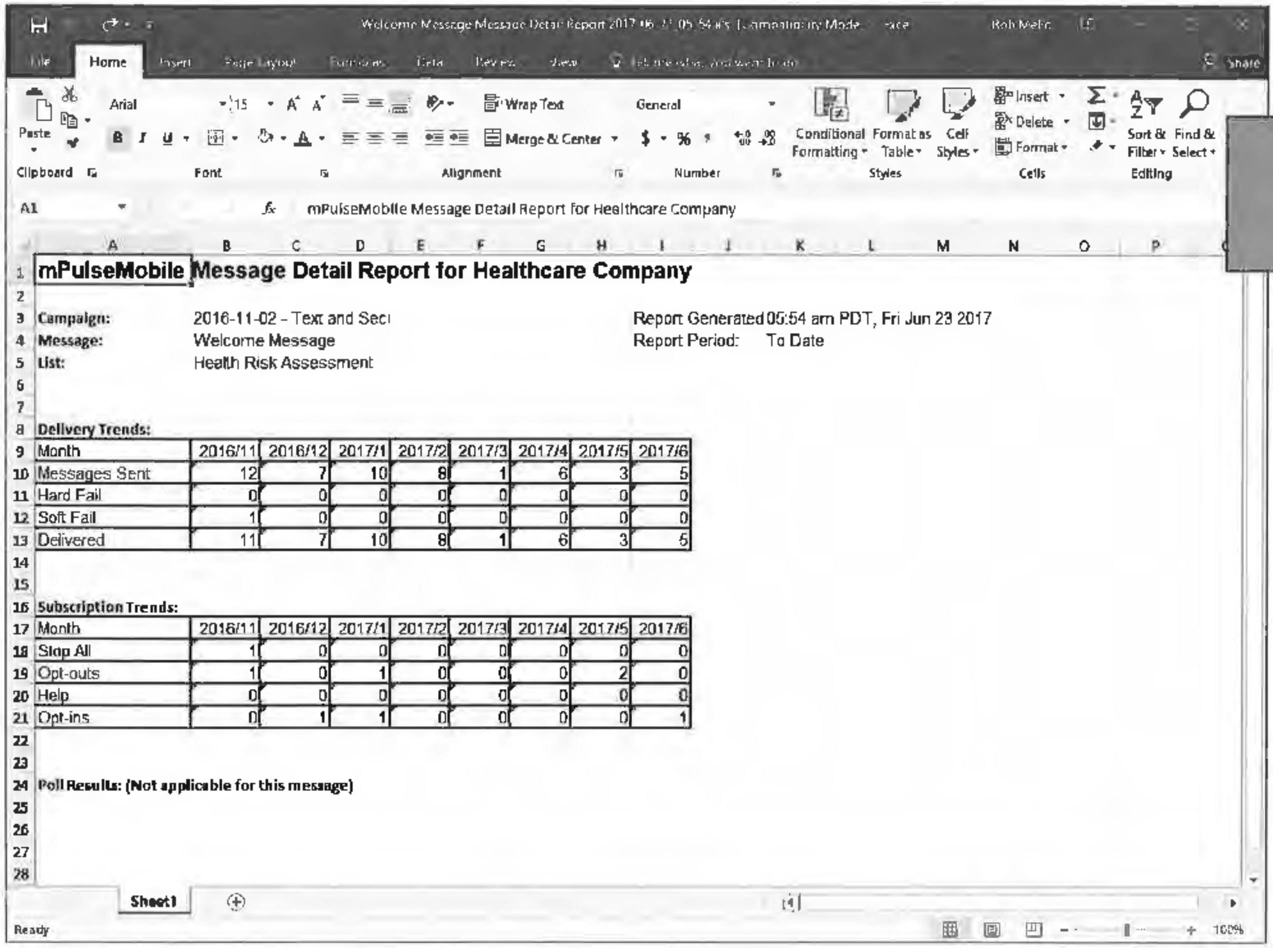
0051 Link Clicks

Domain 1
51

Messages Sent	52 (100%)
Hard Fail	0
Soft Fail	1 (1.92%)
Delivered	51 (98.08%)

Detail for a single message.

Message Detail Export



mPulseMobile Message Detail Report for Healthcare Company

mPulseMobile Message Detail Report for Healthcare Company

Campaign: 2016-11-02 - Text and Sec

Message: Welcome Message

List: Health Risk Assessment

Report Generated 05:54 am PDT, Fri Jun 23 2017

Report Period: To Date

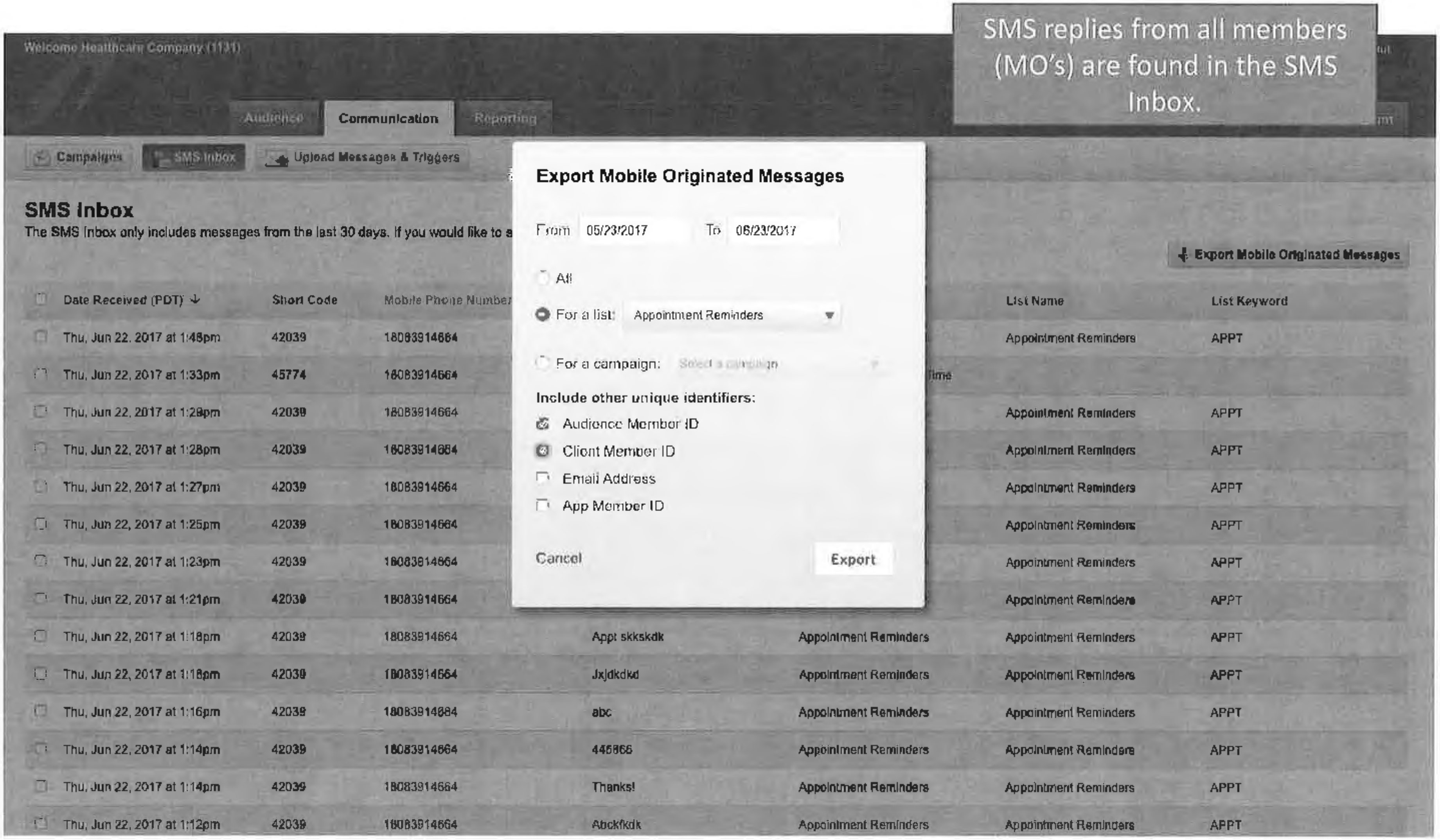
Delivery Trends:

Month	2016/11	2016/12	2017/1	2017/2	2017/3	2017/4	2017/5	2017/6
Messages Sent	12	7	10	8	1	6	3	5
Hard Fail	0	0	0	0	0	0	0	0
Soft Fail	1	0	0	0	0	0	0	0
Delivered	11	7	10	8	1	6	3	5

Subscription Trends:

Month	2016/11	2016/12	2017/1	2017/2	2017/3	2017/4	2017/5	2017/6
Stop All	1	0	0	0	0	0	0	0
Opt-outs	1	0	1	0	0	0	2	0
Help	0	0	0	0	0	0	0	0
Opt-ins	0	1	1	0	0	0	0	1

Poll Results: (Not applicable for this message)



SMS replies from all members (MO's) are found in the SMS Inbox.

Welcome Healthcare Company (1131)
Audience
Communication
Reporting
Campaigns
SMS Inbox
Upload Messages & Triggers
Export Mobile Originated Messages

SMS Inbox

The SMS Inbox only includes messages from the last 30 days. If you would like to s

Export Mobile Originated Messages

From 05/23/2017 To 06/23/2017

○ All

● For a list: Appointment Reminders ▼

○ For a campaign: Select a campaign

Include other unique identifiers:

☑ Audience Member ID

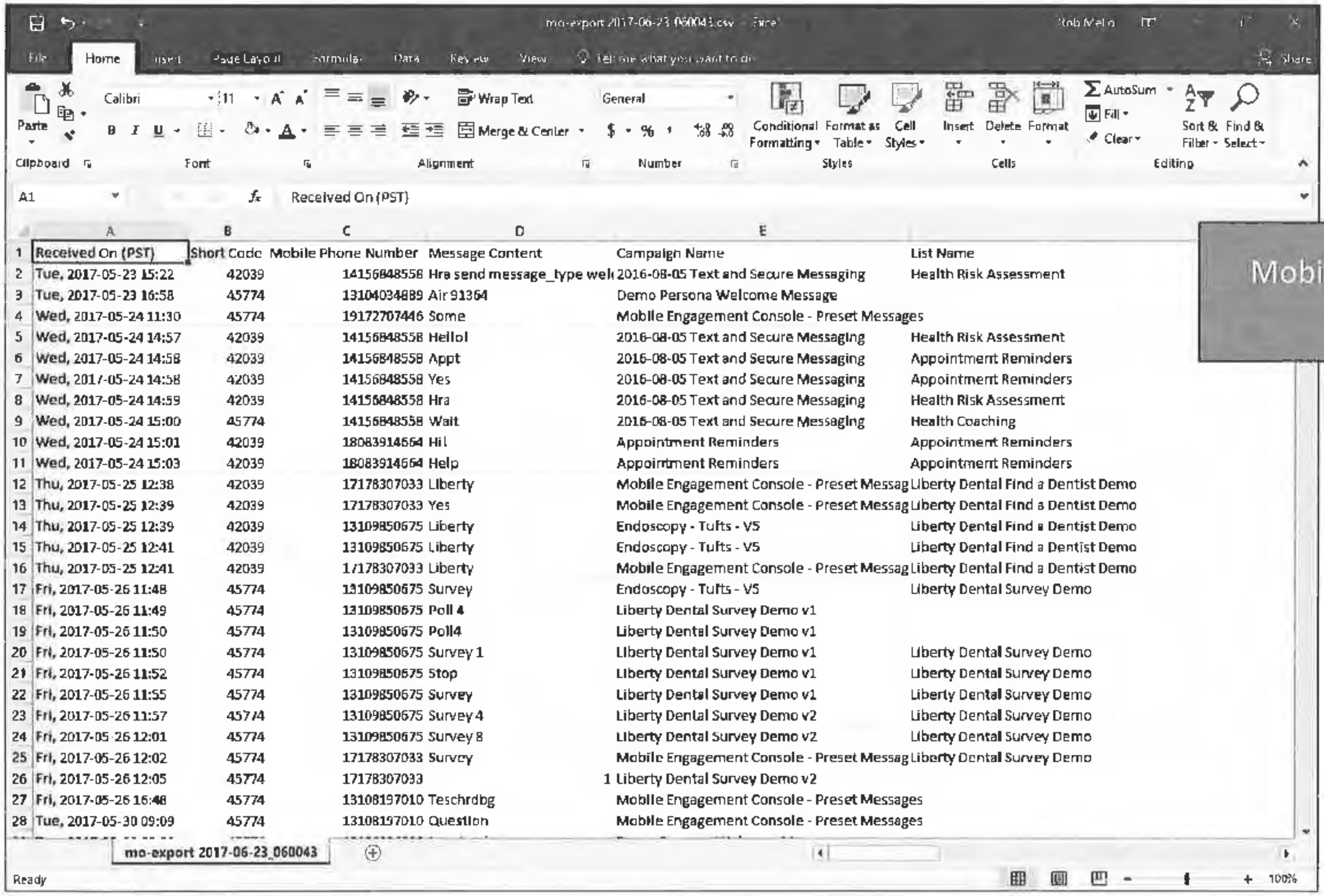
☑ Client Member ID

☐ Email Address

☐ App Member ID

Date Received (PDT) ↓	Short Code	Mobile Phone Number			List Name	List Keyword
Thu, Jun 22, 2017 at 1:48pm	42039	18083914664			Appointment Reminders	APPT
Thu, Jun 22, 2017 at 1:33pm	45774	18083914664		Time		
Thu, Jun 22, 2017 at 1:28pm	42039	18083914664			Appointment Reminders	APPT
Thu, Jun 22, 2017 at 1:28pm	42039	18083914664			Appointment Reminders	APPT
Thu, Jun 22, 2017 at 1:27pm	42039	18083914664			Appointment Reminders	APPT
Thu, Jun 22, 2017 at 1:25pm	42039	18083914664			Appointment Reminders	APPT
Thu, Jun 22, 2017 at 1:23pm	42039	18083914664			Appointment Reminders	APPT
Thu, Jun 22, 2017 at 1:21pm	42039	18083914664			Appointment Reminders	APPT
Thu, Jun 22, 2017 at 1:18pm	42039	18083914664	Appt skkskdk	Appointment Reminders	Appointment Reminders	APPT
Thu, Jun 22, 2017 at 1:18pm	42039	18083914664	Jxjdkdkd	Appointment Reminders	Appointment Reminders	APPT
Thu, Jun 22, 2017 at 1:16pm	42039	18083914684	abc	Appointment Reminders	Appointment Reminders	APPT
Thu, Jun 22, 2017 at 1:14pm	42039	18083914664	446666	Appointment Reminders	Appointment Reminders	APPT
Thu, Jun 22, 2017 at 1:14pm	42039	18083914664	Thanks!	Appointment Reminders	Appointment Reminders	APPT
Thu, Jun 22, 2017 at 1:12pm	42039	18083914664	Abckfkdk	Appointment Reminders	Appointment Reminders	APPT

Mobile Originated Message Export



	A	B	C	D	E	
1	Received On (PST)	Short Code	Mobile Phone Number	Message Content	Campaign Name	List Name
2	Tue, 2017-05-23 15:22	42039	14156848558	Hra send message_type welc	2016-08-05 Text and Secure Messaging	Health Risk Assessment
3	Tue, 2017-05-23 16:58	45774	13104034889	Air 91364	Demo Persona Welcome Message	
4	Wed, 2017-05-24 11:30	45774	19172707446	Some	Mobile Engagement Console - Preset Messages	
5	Wed, 2017-05-24 14:57	42039	14156848558	Hello!	2016-08-05 Text and Secure Messaging	Health Risk Assessment
6	Wed, 2017-05-24 14:58	42039	14156848558	Appt	2016-08-05 Text and Secure Messaging	Appointment Reminders
7	Wed, 2017-05-24 14:58	42039	14156848558	Yes	2016-08-05 Text and Secure Messaging	Appointment Reminders
8	Wed, 2017-05-24 14:59	42039	14156848558	Hra	2016-08-05 Text and Secure Messaging	Health Risk Assessment
9	Wed, 2017-05-24 15:00	45774	14156848558	Wait	2016-08-05 Text and Secure Messaging	Health Coaching
10	Wed, 2017-05-24 15:01	42039	18083914664	Hi!	Appointment Reminders	Appointment Reminders
11	Wed, 2017-05-24 15:03	42039	18083914664	Help	Appointment Reminders	Appointment Reminders
12	Thu, 2017-05-25 12:38	42039	17178307033	Liberty	Mobile Engagement Console - Preset Messag	Liberty Dental Find a Dentist Demo
13	Thu, 2017-05-25 12:39	42039	17178307033	Yes	Mobile Engagement Console - Preset Messag	Liberty Dental Find a Dentist Demo
14	Thu, 2017-05-25 12:39	42039	13109850675	Liberty	Endoscopy - Tufts - V5	Liberty Dental Find a Dentist Demo
15	Thu, 2017-05-25 12:41	42039	13109850675	Liberty	Endoscopy - Tufts - V5	Liberty Dental Find a Dentist Demo
16	Thu, 2017-05-25 12:41	42039	17178307033	Liberty	Mobile Engagement Console - Preset Messag	Liberty Dental Find a Dentist Demo
17	Fri, 2017-05-26 11:48	45774	13109850675	Survey	Endoscopy - Tufts - V5	Liberty Dental Survey Demo
18	Fri, 2017-05-26 11:49	45774	13109850675	Poll 4	Liberty Dental Survey Demo v1	
19	Fri, 2017-05-26 11:50	45774	13109850675	Poll4	Liberty Dental Survey Demo v1	
20	Fri, 2017-05-26 11:50	45774	13109850675	Survey 1	Liberty Dental Survey Demo v1	Liberty Dental Survey Demo
21	Fri, 2017-05-26 11:52	45774	13109850675	Stop	Liberty Dental Survey Demo v1	Liberty Dental Survey Demo
22	Fri, 2017-05-26 11:55	45774	13109850675	Survey	Liberty Dental Survey Demo v1	Liberty Dental Survey Demo
23	Fri, 2017-05-26 11:57	45774	13109850675	Survey 4	Liberty Dental Survey Demo v2	Liberty Dental Survey Demo
24	Fri, 2017-05-26 12:01	45774	13109850675	Survey 8	Liberty Dental Survey Demo v2	Liberty Dental Survey Demo
25	Fri, 2017-05-26 12:02	45774	17178307033	Survey	Mobile Engagement Console - Preset Messag	Liberty Dental Survey Demo
26	Fri, 2017-05-26 12:05	45774	17178307033	1	Liberty Dental Survey Demo v2	
27	Fri, 2017-05-26 16:48	45774	13108197010	Teschrdbg	Mobile Engagement Console - Preset Messages	
28	Tue, 2017-05-30 09:09	45774	13108197010	Question	Mobile Engagement Console - Preset Messages	

L

Exhibit L

mPulse Mobile Insights Dashboard Overview

Insights Dashboard Overview

The Insights Dashboard is a browser-based application that provides visualizations of mPulse Mobile information through actionable metrics and trends related to mobile engagement, activation and dialogues.

Channel Filter and Date Range

Results for all visualizations are filtered by channel and date range to narrow the data being analyzed. The system remembers the last setting so that users are viewing the defaults that are most meaningful to them.

from 02/08/2017 to 11/07/2017

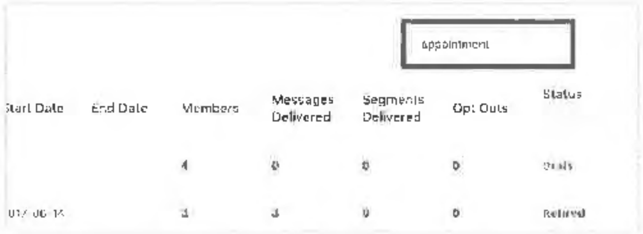
Navigation

Graphic elements displayed on the insights dashboard are interactive. Users can drill-down on summary elements to view detail and can hover over graphs to see daily totals.

Textual elements include search and export capabilities. Users can search on data fields and can export data to CSV format.

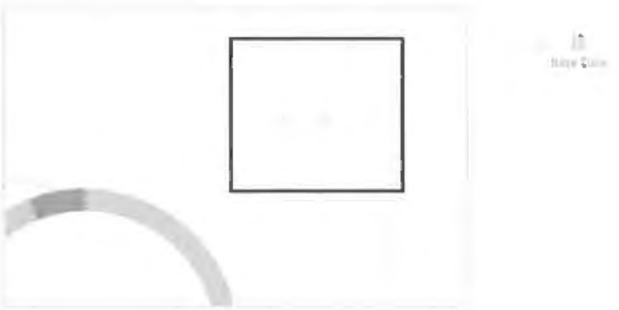
Search and Export

The search tool is shown at the top of each table.


appointment

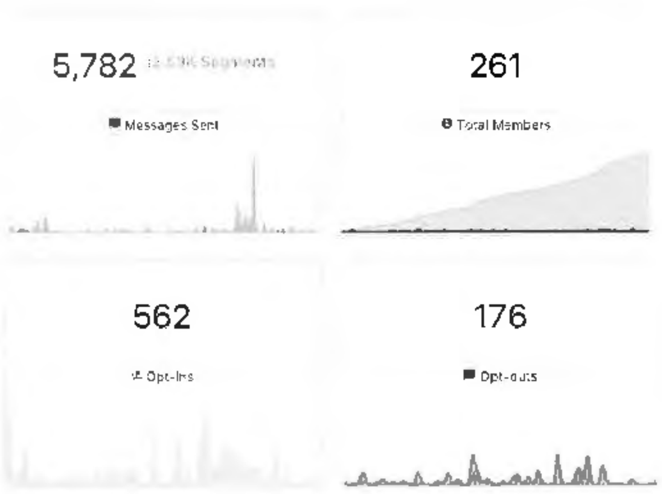
Start Date	End Date	Members	Messages Delivered	Segments Delivered	Opt Outs	Status
		4	0	0	0	[illegible]
[illegible]		3	3	0	0	Retired

Data displayed in tables and in most visualizations may be downloaded for further analysis in other tools such as Excel. The download button can be found in the upper right of each dashboard element.



Communicate Layer

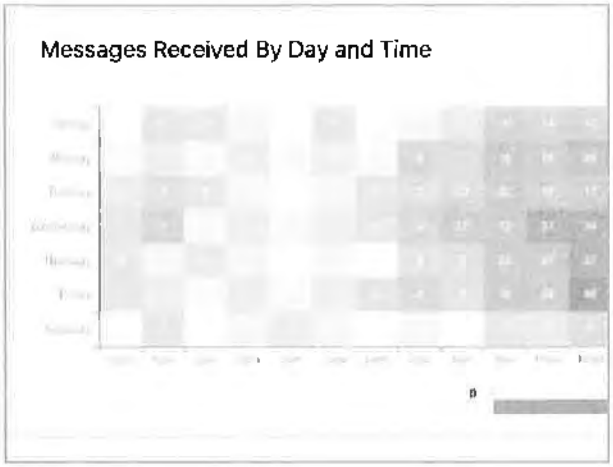
The communicate section displays member and messaging metrics such as messages sent, opt-ins, opt-outs along with information about one-way communicate layer campaigns.

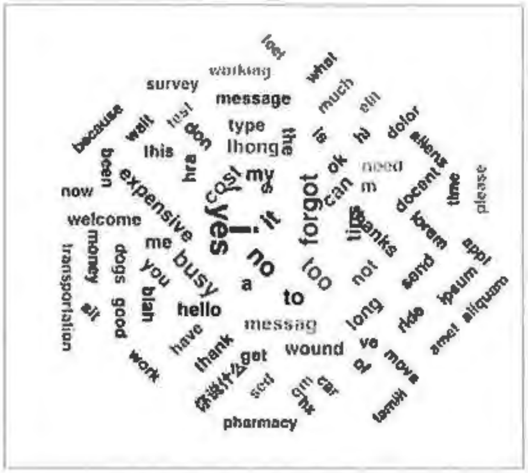


Engage Layer

The Engage Section displays metrics related to responses and healthcare consumer engagement. Visualizations include information such as response time, sentiment score, and the number/percentage of messages that were automatically processed.

Also included in the Engage section is a heatmap that shows the number of messages sent and received by day and time and a word-cloud that shows word frequency at a glance.

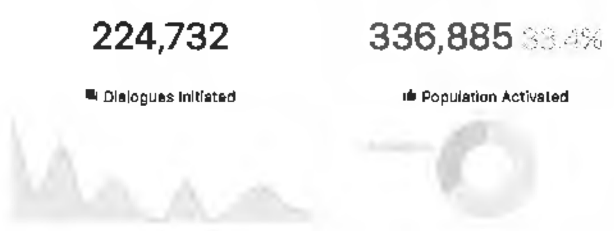




Activate Layer

The Activate Section helps you to analyze how many healthcare consumers are participating in and completing Activate dialogues.

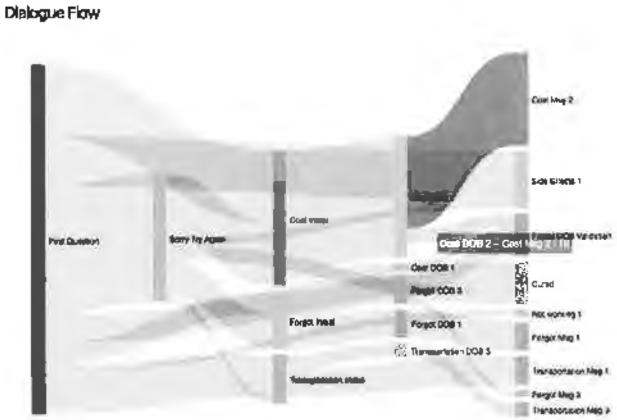
Visualizations include information such as response time, sentiment score, and the number/percentage of messages that were automatically processed.



224,732
Dialogues Initiated

336,885 33.4%
Population Activated

Dialog Flow is a Sankey diagram that shows how members are flowing through multi-branch dialogues. Thicker paths in the dialogue diagram represent the number of members flowing through that stage.



Member Lookup

The Member Lookup tool allows you to view a member's history. Each column may be sorted and searched, and the data may be exported.

Member Message History

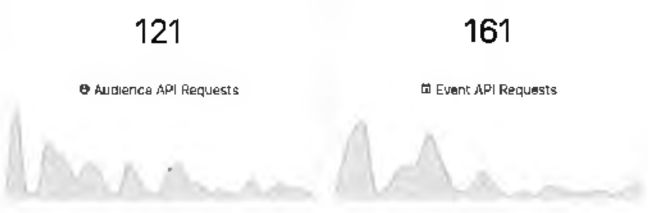
Member Insights

Member visualizations include a heat map of the Community Needs Index (CNI) by ZIP Code. Clicking on an area displays the city, ZIP Code, CNI, Health Literacy rating, and member count.

mPulse
Santa Cruz, CA
Zipcode:
CNI:
Health Literacy:
Member Count: 1

System Information

The System Information section of the dashboard displays interface details such as API requests and successful and failed callbacks for system administrators.



121
Audience API Requests

161
Event API Requests

Version History

Version	Date	Author	Comments
	2018-06-29	Rob Mello	Draft

M

mPulse™
mobile

Exhibit M

mPulse Mobile Information Security Policy v1.0.9

mPulse Mobile

Information Security Policy

This policy outlines the baseline behaviors required to ensure that employees, contractors and related constituents who use company resources for business do so in a safe, secure manner. It is designed to protect private and confidential data through creation, use, transmission and destruction. As a signed document, it is an addition to the library of acceptable use policies on file within Human Resources that allow employee behaviors to protect confidentiality of data.

Effective Date:	9/10/2018
Document Owner:	Ram Prayaga
Signature:	
Version:	1.0.9
Version Date Revision / Description Author:	9/5/2018 / Simon Leung

1. PURPOSE ... 5
2. SCOPE ... 5
3. ROLES & RESPONSIBILITIES ... 5
   A. DEPARTMENT MANAGERS ... 6
   B. SYSTEMS ADMINISTRATORS ... 6
   C. HUMAN RESOURCES ... 6
   D. USERS ... 7
4. IT CHANGE CONTROL POLICY APPLICABILITY ... 7
   CHANGE REQUEST SUBMISSION ... 7
   CHANGE REQUEST APPROVAL ... 8
   CHANGE TESTING ... 8
   CHANGE IMPLEMENTATION ... 8
5. DATA CLASSIFICATION & RETENTION POLICY ... 9
   DATA CLASSIFICATION INTRODUCTION ... 9
   A. INFORMATION CATEGORIES ... 9
   B. DATA RETENTION REQUIREMENTS ... 9
   SENSITIVE DATA ... 9
   AUDIT LOGS ... 10
   DISPOSAL REQUIREMENTS ... 10
   DISPOSAL PROCESS ... 10
   APPROVED UTILITIES ... 10
   AUTHENTICATION OF USERS ... 10
   CUSTOMER ACCOUNTS ... 11
   PASSWORD MINIMUM STANDARDS ... 11
   SYSTEMS ... 11
6. LOGICAL SEPARATION ... 11
   DEPARTMENT MANAGER RESPONSIBILITIES ... 12
   SYSTEM ADMINISTRATOR RESPONSIBILITIES ... 12
   CONNECTED ENTITIES ... 13
   STANDARDS ... 13
   PROCEDURES ... 13
7. REMOTE ACCESS ... 14
   APPROVAL ... 14
   ACCEPTABLE USE ... 14
   AUTHENTICATION ... 14

Device Identification 14
Permitted Locations 14
Approved Products 15
Session Disconnect 15
Personal Firewalls 15
Facilities 15
Employee Access 15

8. ELECTRONIC MEDIA POLICIES STORAGE 15

Electronic Media 15
Destruction 16

9. ENCRYPTION & KEY MANAGEMENT POLICY 16

Transmission over Un-trusted Networks 16
Key Generation 16
Key Storage 17

10. ANTI-VIRUS POLICY 17

Software Configuration 17
Signature Updates 17
Software Logging 17

11. BACKUP POLICY 17

Backup Media 17
Transport 18
Audit 18
Media Destruction 18

12. LOGGING POLICY 18

Logging 18
Events Logged 19
Log Security 19
System Administrator 19
Configuration Changes 19
Allowed Network Connection Paths 20
Configuration Review 20

13. SYSTEM STANDARDS POLICY 20

System Purpose 20
System Configuration Standards 20
System Configuration Process 21
Standard Software 21
Network Time Protocol (NTP) 21

14. VULNERABILITY & SECURITY TESTING POLICY....................21

Vulnerability Identification 21
Scanning and Audit 22
Intrusion Detection and Prevention 22
IDS Escalation Procedures 22

15. INCIDENT RESPONSE POLICY....................23

What is an Incident?.................... 23
Purpose 23
Incident Response Goals 23
Incident Definition.................... 24
Incident Planning 24
Incident Response 25
Response Strategy 26
Automated Detection Systems 27
Containment 28
Remediation.................... 29
Post Mortem Process.................... 29

16. REVISION HISTORY 30

1. Purpose

The mPulse Mobile Information Security Policy has been formulated with the following goals in mind:

- Ensure security, reliability and privacy of mPulse Mobile's systems, networks and data, and the networks, systems and data of others.
- Protect mPulse Mobile's systems, networks and data from harm and interference.
- Ensure that mPulse Mobile, its employees, and other users of its facilities comply with the law and avoid legal liability.
- Encourage the responsible use of resources, and discourage practices which degrade the usability of network resources, or cause harm to resources or individuals.
- Maintain mPulse Mobile's reputation as a responsible organization.
- Access to online content via the network may be restricted in accordance with our policies and federal regulations.

2. Scope

This policy provides guidelines for permissible and impermissible actions regarding company information systems. This policy applies not only to mPulse Mobile's systems and networks, but to activities mPulse Mobile conducts on client systems and networks. This policy applies to any user of mPulse Mobile's systems, including, but not limited to, employees, interns, contractors, consultants, and temporaries (referred to in this policy as "users").

For the purposes of this document, the term incident is considered to be any adverse event that threatens the confidentiality, integrity, accessibility, or ability to audit company information resources. Information resources belonging to customers are expressly included in this definition, and covered by this policy.

These events include but are not limited to:

- Attempts (either failed or successful) to gain unauthorized access to a system or its data.
- Unwanted disruption or denial of service.
- Unauthorized use of a system for the transmission, processing, or storage of data.
- Changes to system hardware, firmware, or software characteristics without the company's knowledge, instruction or consent.
- Attempts to cause failures in infrastructure or services.

3. Roles & Responsibilities

The Chief Compliance Officer is responsible for coordinating and overseeing compliance with policies and procedures regarding the confidentiality, integrity and security of its information assets.

Specific responsibilities include:

- Making high-level decisions pertaining to the information security policies and their content. Approving exceptions to these policies in advance on a case-by- case basis.
- On an annual basis, coordinating a formal risk assessment to identify new threats and vulnerabilities and identify appropriate controls to mitigate any new risks.
- Annually review the Information Security policies and procedures to maintain adequacy in light of emergent business requirements or security threats.
- Maintain and distribute incident response and escalation procedures.

a. Department Managers

Department Managers are responsible for ensuring that access to systems and data is granted on a need to know basis and that systems are maintained in a way consistent with corporate policies. Corporate Departments include:

- Human Resources
- Client Services
- Technology & Product Management
- Operations
- Sales, Marketing and Business Development

Specific responsibilities of department managers include:

- Approving user access requests to systems and applications
- Approving major changes to systems that may impact business process

b. Systems Administrators

Systems Administrators are dedicated to security planning, implementation and systems administration. Specific responsibilities include:

- Monitoring and analyzing security alerts and distributing information to appropriate information security, technical and business unit management personnel.
- Create new information security policies and procedures when needs arise. Maintain and update existing information security policies and procedures.
- Applying information security policies and procedures as applicable to all information assets.
- Administering user account and authentication management

c. Human Resources

Due to their direct and constant relationship with existing employees, as well as their unique position of having the first and last interactions with new/terminated employees, the Human Resources Department has an important role with regards to information security.

Specific responsibilities include:

- Perform background checks on ALL potential employees.
- Disseminating security awareness information to ALL users. The security awareness training consists of an initial session when hired, then annual training thereafter.
- Administer sanctions and disciplinary action relative to violations of Information Security Policy
- Work with Systems Administrators to direct Authorization Requests for new employees.
- Notify Access Management personnel when any employee is terminated. Additional information regarding the Authorization Request process is available in the corporate wiki.
- Ensure the signed Security Awareness and Acceptable Use Policy Acknowledgment Form is filed in each employee's personnel file.

d. Users

Each user of company computing and information resources must realize the fundamental importance of information resources and recognize their responsibility for the safekeeping of those resources. Users must guard against abuses that disrupt or threaten the viability of all systems.

The following are specific responsibilities of all users:

- Embrace the policy that "Security is everyone's responsibility"
- Understand what the consequences of their actions are with regards to computing security practices and act accordingly
- Maintain awareness of the contents of the information security policies
- Read and sign the Security Awareness and Acceptable Use Policy
- Maintain the confidentiality of all sensitive and private data

Policy Exemptions

No exceptions allowed.

4. IT Change Control Policy Applicability

All proposed changes to network devices, systems and application configurations within the production data center must follow this policy.

Change Request Submission

All change requests, at a minimum, must contain the following information. This facilitates the workflow of the request, approval, implementation and review of the change requests.

Resources Affected by Change (customers) – If a change could impact the functionality of customers this item must be completed. This documentation must include changes to features, applications and procedures that will be different from the existing system. Included in this documentation are any upgrades that the customer needs to perform to the operating system or other required 3rd party software or hardware.

- Back out Procedures – If the change does not go as intended a plan must be in place that describes the process of reverting the environment to its original configuration.
- Test Plan - A set of planned tests must be developed to verify that the change accomplished what it was supposed to do, and does not adversely affect other system components or create a weakness in the security posture of the environment. This plan may be specific to each change

Change Request Approval

After all planning and documentation is complete management and concerned parties must sign off on the requested change. The request is submitted to the appropriate department manager for approval.

Change Testing

Prior to implementing changes within the production environment, all changes must first be tested in a test or QA environment.

Change Implementation

All changes must be implemented according to the documented change procedures that were tested successfully. Any discrepancies between expected results and actual results that impact the network, systems, applications, business requirements or support procedures must result in the immediate invocation of the documented back out procedures.

5. Data Classification & Retention Policy

Data Classification Introduction

All data stored on computing resources must be assigned a classification level based on data characteristics. The following information categories outline the criteria for classifying data. This level is used to determine which users are permitted to access the data and how that data must be handled.

a. Information Categories

Data is grouped into the following categories:

- DOD- Applies to business information classified under Department of Defense (DoD) data protected by the Privacy Act of 1974. Access to information in this specific group is relegated to verified U.S. citizens only.
- Critical Sensitive – Applies to business information which is intended strictly for use within the organization. Unauthorized disclosure will seriously and adversely impact the company, stockholders, business partners, and/or its customers. Examples of critical information include the HHS HIPAA Privacy and Security Final Rule.
- Sensitive - Applies to business information which is intended strictly for use within the organization. Unauthorized disclosure could seriously and adversely impact the company, stockholders, business partners, and/or its customers. Examples of sensitive information include: customer data, passwords, encryption keys, etc.
- Private - Applies to business information which is intended for use internally. Unauthorized disclosure could adversely impact the company, its stockholders, its business partners, and/or its customers. Examples of private information includes: client names, contract terms, contact information, industry relationship details, business strategy, etc.
- Public - Applies to all other information which does not clearly fit into the sensitive or private classifications. Unauthorized disclosure isn't expected to seriously or adversely impact the company. Any release of this information must be authorized by the Marketing department.

b. Data Retention Requirements

Sensitive Data

All sensitive data, regardless of storage location, will be retained only as long as required for legal, regulatory and business requirements. The specific retention length will be established by the data creator or Security Director. All private data, regardless of storage location, will be retained only as long as required for legal, regulatory and business requirements.

Audit Logs

All application and network audit logs must be retained for a minimum of 3 months which are kept available for immediate use. Log files older than 3 months will be archived offline.

Disposal Requirements

All sensitive data when no longer needed for legal, regulatory or business requirements must be removed or destroyed using an approved method documented in this policy. This requirement includes all data stored in systems, temporary files or contained on storage media.

Disposal Process

Media containing sensitive data that should no longer be retained must be disposed of in a secure and safe manner as noted below:

- Tape media: degauss, shred, incinerate, pulverize or melt.
- Allowed USB "thumb" drives, smart cards, and digital media: incinerate, pulverize or melt.

Before servicing or disposal, all sensitive information must be destroyed or sanitized according to the approved methods in this policy. Applies to computers, or communications equipment repurposed for another employee and devices sent to a vendor for trade-in.

Approved Utilities

The following is a list of currently approved utilities for disposing of sensitive data.

- The Linux utility, Shred, and DoYourData Super Eraser is approved for sanitizing hard disk media. All data sanitization is required to use a 7-pass binary wipe (DoD 5220.22-M ECE).

Authentication of Users

Each user's access privileges shall be authorized, according to business need.

Every user must have a single unique user ID and a personal secret password for access to systems and information. Users must not share their User ID or personal secret password.

Customer Accounts

All user accounts which are provided to customers of mPulse Mobile must follow and adhere to the same account requirements as outlined in the password minimum standards.

Password Minimum Standards

Password credentials on all systems are required to meet the following standards:

- Passwords must be at least 8 characters in length.
- Passwords must be complex and include lowercase letters, uppercase letters, digits and symbols
- Require that new passwords cannot be the same as the previously used passwords.
- Passwords must be reset at least every ninety (90) days. Users will be notified and prompted to reset their password prior to password expiration date.
- Initial user passwords must comply with these standards and must be changed immediately upon the user's next login.
- Where system level accounts are used a minimum password length of 12 alphanumeric characters must be utilized.

Systems

Each computer system shall have an automated or procedural access control process. The process must:

- Identify each User through a unique User identifier (user ID).
- Shared or group user IDs are never permitted for user-level access.
- Authenticate each user ID with a password.
- Enforce minimum password standards.
- Lock out accounts after not more than three invalid logon attempts.
- Require that once a user account is locked out, it remains locked until the System Administrator resets the account
- Require system/session idle timeout of 15 minutes. Systems and applications must authenticate using a password or token entry.

6. Logical Separation

The mPulse Mobile Platform is on dedicated systems within AWS data centers. No processing or memory is shared with other AWS customers. Within our platform, strict logical controls are in place at the organizational level to restrict access.

- All API URLs contain the account ID.

- Access is only possible from whitelisted IP's that are provisioned at the account level.
- API access requires Basic Authentication using a unique account-based access key and account name.
- Each of our API's are individually controlled and provisioned at the account level, i.e, one account can have access to our Audience API but not receive real-time callbacks while another account can have access to both.
- Individual user access to our Control Panel is provisioned at the account level.
- Since all tables within the DB have the account id, removal of data within the database can be performed by using account id within the delete condition. This can be done without impact to any other account as all data is logically separable.

Department Manager Responsibilities

The department manager shall provide access authorization according to job responsibility following a "need to know" perspective. Request and approval tracking is facilitated thru our online Jira. Each request for access must contain electronic evidence of approval by the appropriate department manager.

Quarterly audits of resource authorizations will be performed to monitor and confirm that access privileges are appropriate.

System Administrator Responsibilities

Account creation requests must specify access either explicitly or via a "role" that has been mapped to the required access. New accounts created by mirroring existing user accounts must be audited against the explicit request or roles for appropriate access rights.

Access must be denied immediately upon notification that access is no longer required. Written procedures must be in place to ensure that access privileges of terminated or transferred users are revoked as soon as possible.

Contractor accounts should be configured to expire at the end of the defined contract period.

User IDs shall be removed after ninety (90) days of inactivity. These requirements may not apply to certain specialized accounts (e.g., Administrator, Admin, root). In those instances, the Systems Administrator must document these accounts and the access controls in place to use these accounts.

Connected Entities

mPulse Mobile maintains connectivity with 3rd party vendors for delivering business services to our clients. All 3rd party vendors contractually agree that to receive sensitive data from mPulse Mobile they required to comply with HIPAA regulations.

Connectivity to the system operated by these vendors must be managed and evaluated on a quarterly basis to ensure compliance and connectivity methods have not changed between review periods.

The complete list of connected entities is maintained within the wiki system. Each connection request is initiated in the form of a Connected Entity Change ticket. This request includes the following information:

- Entity name and contact information.
- Connection type and details covering which portion of the mPulse Mobile platform will be accessed.
- Connection start date and end date or term or the connection.
- Reason for requiring the connection.

Standards

- Every connection from an external entity must be documented and authorized by the Security Director before allowing access to the internal system. Proper due diligence required to be conducted prior to connecting to the entity.
- If the external entity is connecting to any system within the environment, it to transmit sensitive data it must be verified that the entity complies with the HIPAA
- Access to the internal system must be allowed only for the time requested and the connection must be monitored.

Procedures

Connections between external entities and our internal systems are facilitated by our System Administrator staff with the oversight of our Security Director.

The following procedures are strictly followed to ensure proper execution of the requests.

- Staff member initiates the Connected Entity Change request through Jira.

The Security Director will review the request and evaluate the necessity and perform proper due diligence on 3rd party.

- Once approved, System Administrator staff will evaluate the necessary environment changes and follow standard system change request procedures.
- Once connectivity is established, daily monitoring and quarterly review of the

connection will be implemented.

- Once the duration of the request expires, System Administrator staff will follow standard system change request procedures to remove connectivity with 3rd
- party system.
- Disconnecting the connected entity will ensure that proper permissions and accounts are removed at the Firewall, Device and Application levels.

7. Remote Access

Approval

The security Director must explicitly approve any use or deployment of special technologies. For general user application, this includes: VPN access.

Special Technologies will be defined as, any piece of software and or hardware which is not provided by mPulse Mobile.

Acceptable Use

Acceptable use of special technologies is limited to those restrictions put forth in the Security Awareness and Acceptable Use Policy.

Authentication

User authentication mechanisms, where possible, must be integrated into the current authentication systems. Under no circumstances may the user authentication requirements be less strict than currently defined policies and procedures (i.e.: complex passwords, password change interval, etc).

All remote access to the network using these technologies must be authenticated via a two-factor, strong authentication scheme.

Device Identification

All special technology devices must be labeled, including owner, contact information, and device purpose.

Permitted Locations

All special technology devices' placement must be authorized by the security director

Approved Products

The security Director must approve special technologies or devices may be deployed into the network. Currently, wireless and modem use is prohibited to access the corporate and production networks.

Session Disconnect

All systems must be configured to automatically disconnect sessions after fifteen (15) minutes of inactivity.

Personal Firewalls

All mobile and/or employee-owned computers with direct connectivity to the Internet (e.g., laptops used by employees), and which are used to access the network, must have personal firewall software installed and activated.

Facilities

Data center locations are required to have a Visitor Logs in place. In addition, data center locations must contain biometric readers, lockable racks and or a private cage to ensure no passer by can tap into and or disrupt data workflow.
All visitors must present a form of government issued photo identification; complete the sign in log providing: name, firm represented, and the employee authorizing physical access (escort). This log must be retained for a minimum of 3 months.

Employee Access

Employees must request and be approved for access to physical and network resources. Access requests are processed thru the online Jira . Employees are required to submit access requests thru this tool to their manager for approval. Access requests to sensitive data areas must also be approved by the security Director.

8. Electronic Media Policies Storage

Electronic Media

Electronic media containing sensitive information (i.e.: CD, DVD, floppy disk, hard disk, tape, etc.) when approved for use is subject to the following storage guidelines:

- Sensitive information should never be copied onto removable media without authorization from the security director. At no time is electronic media containing sensitive information to be removed from any secure office environment, with the exception of computer system backups.
- At no time is electronic media containing sensitive information to be removed from any data center or computer room without prior authorization from the Security Director
- Electronic media containing sensitive data are to be physically retained, stored or archived only within secure office environments, and only for the minimum time deemed necessary for their use.
- All electronic media containing sensitive information must be stored on media in an encrypted file format. At no point should sensitive information should be stored in a clear format.
- All removable, sensitive electronic media must be stored securely.

Destruction

Hard copy and electronic media must be destroyed as outlined in the Data Disposal Policy

9. Encryption & Key Management Policy

Transmission over Un-trusted Networks

Sensitive information being transmitted must use secure means of communication when being transmitted to and from mPulse Mobile. Communication to external networks is required to implement:

- Secure Socket Layer version 3 or greater (SSL)
- Virtual Private Network (VPN)

Other sensitive data handling considerations:

- Email Transmission of sensitive data is prohibited.
- Unencrypted ePHI data is not to be sent via end-user messaging technologies (i.e.,email, instant messenger, etc.)
- No wireless networks of infrastructure can be connected to any systems with sensitive information

Key Generation

For the storage and transmission of secure message a AES-256 -CBC encryption method is used to encrypt and protect data while at rest or in motion.

Key Storage

Key management procedures ensure only authorized users can access and decrypt encrypted data using controls that meet operational needs and comply with data retention requirements. Regular audits review encryption management.

Key management is fully automated. Encryption keys and the equipment to generate, store and archive keys are protected against modification, loss, destruction and disclosure. Private keys are kept confidential. Management of keys must ensure that data is available for decryption when needed.

10. Anti-Virus Policy

Software Configuration

All workstations must be configured with approved anti-virus software. Anti-virus software is procured by the Information Technology department and will be installed on all applicable devices that connect to the corporate and production networks. All workstations must be configured to scan for viruses in real-time and end users must not be able to configure or disable the software. All servers must be configured to scan for viruses on a daily basis.

Signature Updates

All workstations must be configured to update virus signatures on a daily basis.

Software Logging

Anti-virus software must have logging enabled and alert system administrators if a virus is detected. Retention of Anti-virus software logs will be in accordance with the Data Retention Policy.

11. Backup Policy

Backup Media

Backup media is considered sensitive and should be handled appropriately at all times.

Transport

Offline storage media utilized for archival or back-up purposes will at all times be handled and retained in a secured environment such that only authorized personnel and contracted storage facility personnel have access to the archival media. All media couriers, and transport mechanisms, must be certified by the Security Director.

Positive log-out and log-in of archive media will take place during all archive media transfers. All media that is transferred from one location to another should be logged as being transferred, by whom, where, and was it properly received, with signature from management in the Backup Media Transfer Log.

All media containing sensitive data must be labeled as such prior to transfer, as detailed in the Paper and Electronic Media Policy.

Audit

All media used will be labeled and assigned a unique ID. All media must be registered for tracking prior to use.

Inventories of all stored media will take place on at least a quarterly basis. The systems administrators will compare the list of in-use media with records at the storage facility using the media inventory log.

Media Destruction

All media that is no longer needed or has reached end-of-life must be destroyed or rendered unreadable so that no data may be extracted. Information on acceptable destruction techniques is detailed in the Data Disposal Process.

12. Logging Policy

Logging

Logging is a critical component of the Information Security Program. Systems or applications handling sensitive information should be configured to provide detailed logging and audit capabilities. Logging must provide clear visibility into who accessed what data from which device during what period of time.

Events Logged

Automated audit trails must be implemented for all system components to reconstruct the following events:

- All administrative actions utilizing user IDs with significant privileges above a general user (e.g. root, user IDs with Administrator group privilege, oracle, etc)
- Access or initialization of audit log files
- Any user or administrator authentication attempts (both valid and invalid)
- Creation or deletion of system-level objects.
- Invalid logical access attempts

Log Security

All event logs must be collected in a centralized location or media that is difficult to alter and protected from unauthorized access. The logs will be further protected by TripWire file integrity monitoring software that alerts upon unauthorized modifications to the logs.

System Administrator

System administrators are responsible for the administration and oversight of firewall and network infrastructure.

- Document all firewall security rules and changes.
- Ensure appropriate logging of firewall events and active monitoring of the logs.
- Assure that security rules applied to the firewalls are sufficient to protect networks and corporate assets from external attacks and unauthorized access.
- Review all firewall security rule change requests for policy compliance prior to submission through the change management process.
- Actively monitor firewall security events.
- Conduct quarterly review of all firewall policies.

Configuration Changes

Any firewall changes must follow the Change Control Process. These changes include but are not limited to:

- Firewall rule additions, deletions, and modifications.
- Firewall software or system modifications.
- Firewall software or system upgrades, patches, or hot-fixes.

The change control process involves the creation of a Firewall Change request ticket using JIRA. The request will include the intended ACL rule change details, the reason for the change, and outline any back-out procedures in the event that the change does not have the intended effect. All Firewall Change requests must be approved by the Security Director prior to be implemented.

Allowed Network Connection Paths

All Internet-based inbound traffic is only permitted to the demilitarized zone (DMZ) network. In all cases, this traffic should be limited to HTTP and HTTPS where possible. Perimeter routers should not be configured with a route to internal address space, with the exception of the DMZ.

Anti-spoofing technologies must be configured on perimeter devices, denying or rejecting all traffic with a:

- Source IP address matching internally allocated or company owned address space.
- Source IP address matching RFC 1918 address space.
- Destination IP address matching RFC 1918 address space.

Cross-segment traffic from internal production systems must only be allowed to predefined connect to pre-approved networks. Additionally, this traffic should be restricted to only required protocols and services. Inbound connections to internal production systems, and originating from wireless networks, are not permitted.

Configuration Review

At least quarterly, a thorough review each firewall rule set must be performed. The review must include the removal, when merited, of unused, or unnecessary access paths. All proposed changes identified as result of this review must go through the current change control process prior to implementation.

13. System Standards Policy

System Purpose

All computing systems should be designated for a single primary purpose. Exceptions to single purpose deployments require approval from the security director.

System Configuration Standards

All systems, prior to deployment in the production environment, must conform to the System Configuration Standards. A valid business justification must exist for all deviations from published configuration standards. Any such deviations require written approval by the Security Director.

System Configuration Process

All new system deployments will follow the following high level procedure:

- Install operating system.
- Update all operating system software per vendor recommendations.
- Install system specific applications and software.
- Configure Network Time Protocol (NTP).
- Update all application software per vendor recommendations.
- Configure application parameters according to build document (application hardening).
- Standard Software The following list should be considered standard installed software on all applicable systems.

Standard Software

The following list should be considered standard installed software on all applicable systems.

- Trip Wire File Integrity software. Setup and configuration for production servers
- Anti-Virus
- Personal Firewall software
- VPN Client software

Network Time Protocol (NTP)

With exception of the NTP servers, all production systems must be configured to use one of the internal NTP servers to maintain time synchronization with other systems in the environment.

The NTP system will at all times be running the latest available version of the software.

14. Vulnerability & Security Testing Policy

Vulnerability Identification

Members of the systems administration teams must be informed of information security issues and vulnerabilities applicable to computing systems.

The primary method for identifying new threats as they arise will be through vendor and security specific Internet mailing lists. Although not complete, the following lists should be subscribed to as well as other vendor lists applicable to specific software packages and systems:

- CERT Security Bulletins
- Centos/RedHat Linux Vulnerability lists
- Apache Vulnerability list
- SANS.org Consensus Security Alerts

System Configuration Standards must be updated to reflect measures required for protection from any newly discovered vulnerability.

Scanning and Audit

In addition to the above informational alerts, internal network vulnerability scans must be performed at least quarterly and after any significant change in the network (e.g., new system component installations, changes in network topology, firewall rule modifications, product upgrades). This process includes identifying rogue wireless devices on the network. Penetration tests at both the application and network layer will be performed annually or after any significant change in the network.

All potential vulnerabilities identified through vulnerability scans and penetration exercises will be communicated to appropriate personnel for applicability and remediation. All high-level vulnerabilities must be corrected, subject to Change Control Policy. Follow up scans will be initiated to confirm compliance with security standards.

An additional annual risk assessment process that identifies threats, vulnerabilities, and results in a formal risk assessment must be conducted to ensure assets are adequately protected.

All critical security patches, hot-fixes, and service packs identified by the System Administrators, and found to be applicable, must be applied to systems within 30 days. As with any change to the environment, the change management procedure must be followed.

Intrusion Detection and Prevention

Networks and systems that fall under HIPAA scope will also be monitored by an intrusion system that alerts personnel of potential compromises. When events with high confidence are triggered, personnel must be notified for review and analysis. All events triggered by these systems will warrant immediate attention.

IDS Escalation Procedures

In the event that an intrusion system identifies non-normal activity within the network, the following escalation procedures are followed:

- Intrusion system is monitored 24/7 by qualified, trained staff. Currently we utilize Snort for monitoring IDS activity.

- Once an event or sequence of events is identified, a member of the staff will open a ticket outlining the event. This will send a notification to the security director and System administrators.
- The System Administrator and Security Director will review the recommended action and determine the proper course of action.

15. Incident Response Policy

What is an Incident?

An incident is defined as any issue that could affect the sensitivity, integrity of availability of networks, systems, or data.

This incident response plan defines what constitutes a security incident and outlines the incident response phases. This incident response plan document discusses how information is passed to the appropriate personnel, assessment of the incident, minimizing damage and response strategy, documentation, and preservation of evidence. The incident response plan will define areas of responsibility and establish procedures for handling various security incidents at mPulse.

Purpose

This policy is designed to protect mPulse resources against intrusion.

Incident Response Goals

mPulse defines the goals of our plan to identify, research, schedule, and remediate all recognized incidents. These goals include:

- Verify that an incident occurred. Maintain or Restore Business Continuity. Reduce the incident impact.
- Determine how the attack was done if one is uncovered. Prevent future attacks or incidents.
- Improve security and incident response. Prosecute illegal activity.
- Keep management informed of the situation and response.

Incident Definition

mPulse defines an incident as any one or more of the following:

- Loss of information confidentiality (data theft)
- Compromise of information integrity (damage to data or unauthorized modification).
- Theft of physical IT asset including computers, storage devices, printers, etc. Damage to physical IT assets including computers, storage devices, printers, etc. Denial of service.
- Misuse of services, information, or assets.
- Infection of systems by unauthorized or hostile software. An attempt at unauthorized access.
- Unauthorized changes to organizational hardware, software, or configuration.
- Reports of unusual system behavior. Responses to intrusion detection alarms.

Incident Planning

Team roles and responsibilities are defined in the Contingency Planning Matrix.
The Incident Response Report template is shared within the organization and with clients. Past Incident Response notifications are archived and organized by year.
Security Vulnerability Advisory notifications and procedure processes. Client Notification information and terms based on agreed SLA's.

Incident Severity levels are defined as follows:

Level	Description	Resource	Reaction
Level I	100% System Down	All hands on deck (IRP-PA)	Work on current iteration is interrupted and refocused to immediately address this issue
Level II	Partial System Failure	All hands on deck (IRP-PB)	Work on current iteration is interrupted and refocused to immediately address this issue
Level III	Major Bug Located	Development Staff and IT	Research is conducted in the iteration. Work may be executed within the current iteration or prioritized in the following iteration.

Incident Response

Discovery: Someone discovers something not right or suspicious. This may be from any of several sources:

- Clients
- Customer Support mPulse staff
- mPulse development
- 3rd party software vendors (Gazzang) Intrusion detection system (OSSEC)
- Our system administrator
- A firewall administrator (Amazon)
- mPulse monitoring team (IT/Dev)
- mPulse Security Officer
- An outside source.

Notification

Outside sources will generally contact our Customer Support department or mPulse Manager. Internal staff will create a Jira security ticket and schedule within the current iteration.

Analysis and Assessment

Many factors will determine the proper response including:

a) Is the incident real or perceived?
b) Is the incident still in progress?
c) What is the impact on the business should the attack succeed? Minimal, serious, or critical? This criterion is used to assist the Incident Response Team in evaluating the priority of the remediation.
d) What systems are in scope for the incident?
e) Is the incident inside the trusted network?
f) What data or property is threatened and how critical is it?
g) Was data integrity or confidentiality breached?

I. Severity Level 1 (HIGH)

Serious attempt to breach security (e.g. multi- pronged attack, denial of service attempt, virus outbreak, etc.) or a second Level 2 attack.

II. Severity Level 2 (MEDIUM)

One instance of a clear attempt to obtain unauthorized information or access (e.g. download password files, access restricted areas, single computer successful virus infection, successful buffer or stack overflow attempt, etc.) or a second Level 3 attack.

III. Severity Level 3 (HIGH)

One instance of potentially unfriendly activity (e.g. finger, unauthorized telnet, port scan, corrected virus detection, etc.).

h) Are services unavailable?

I. Severity Level 1 (HIGH)

Gateways are down, external interfaces are unavailable or connectivity. Or a second Level 2 attack.

II. Severity Level 2 (MEDIUM)

One instance of a clear attempt to obtain unauthorized information or access (e.g. download password files, access restricted areas, single computer successful virus infection, successful buffer or stack overflow attempt, etc.) or second Level 3 attack.

III. Severity Level 3 (LOW)

Serious attempt to breach security (e.g. multi- pronged attack, denial of service attempt, virus outbreak, etc.)

Response Strategy

A. Is the response urgent?

B. All external communication responses are deemed urgent, however, only defined and confirmed information will be shared. Response path will include the following steps:

   a. Once an incident notification is presented by a client or outside party, the account manager or response ticket recipient will formally acknowledge receipt via email. Once the incident has been researched and a cause is determined, clients may be

   b. notified if the remediation can be accomplished through client action or process change.

   c. If remediation involves mPulse effort / development, then notification to clients will be held off until a full assessment, analysis and remediation plan is set.

   d. Once set, the account manager will communicate with the client via email as well as by phone to address the issue and communicate the remediation plan.

C. Can the incident be quickly contained?

   a. If the response can be quickly contained (defined as executable within the current iteration), then mPulse may elect to bypass the communication of the remediation plan and only communicate the incident response and remediation to the client after work has been completed. Incident response communication will follow the above mentioned template.

Responses to Severity Level I:

1. Contain the intrusion and decide what action to take.
2. Collect and protect information associated with the intrusion via offline methods. In the event that forensic investigation is required, the Infrastructure team will work with legal and management to identify appropriate forensic specialists.
3. Notify management of the situation and maintain notification of progress at each following step.
4. Eliminate the intruder's means of access and any related vulnerabilities.
5. Research the origin of the connection.
6. Contact ISP and ask for more information regarding attempt and intruder, reminding them of their responsibility to assist in this regard.
7. Research potential risks related to or damage caused by intrusion method used.

Responses to Severity Level II:

1. Collect and protect information associated with the intrusion.
2. Research the origin of the connection.
3. Contact ISP and ask for more information regarding the attempt and intruder.
4. Research potential risks related to intrusion method attempted.
5. Upon identification of intruder, inform intruder of our knowledge of his actions and warn against future recriminations if attempt is repeated.

Responses to Severity Level III:

1. If possible, record the user, IP address, and domain of intruder.
2. Maintain vigilance for future break-in attempts from this user or IP address.

Automated Detection Systems

All automated detection systems within the environment, including intrusion detection sensors, audit logs, and file integrity checking systems, will be configured to automatically notify the System Administrators of the network. An engineer will be available on a 24/7 basis to initiate the incident response if warranted.

Containment

In the event of a system compromise or of a suspected compromise, the security Director should be notified. With the exception of steps outlined below, it is imperative that any investigative or corrective action be taken only by approved personnel or under the oversight of Incident Response personnel to assure the integrity of the incident investigation and recovery process.

When faced with a potential situation, system users should do the following:

- Do not alter the state of the computer system.
- The computer system should remain on and all currently running computer programs left as they are. Do not shutdown the computer or restart the computer.
- Immediately disconnect the computer from the network.
- Report the security incident.
- No one should communicate with anyone outside of their team about any details or generalities surrounding any suspected or actual incident.
- Security incidents should be immediately reported to the security Director who will work with local police and other law enforcement agencies as necessary to help resolve the incident.
- Document any information you know while waiting for the Incident Response Team to respond to the incident. This must include date, time, and the nature of the incident, if known. Any information you can provide will aid in responding in an appropriate manner.

In the event of an intrusion part of the containment process is to implement steps to prevent re- intrusion or re-infection.

- Determine how the intrusion happened. Determine the source of the intrusion whether it was email, inadequate training, attack through a port, attack through an unneeded service, attack due to unpatched system or application.
- Take steps to prevent an immediate re-infection which may include one or more of:
    - Close a port on a firewall
    - Patch the affected system
    - Shut down the infected system until it can be re-installed
    - Re-install the infected system and restore data from backup. Be sure the backup was made before the infection.
    - Change email settings to prevent a file attachment type from being allow through the email system.
    - Plan for some user training.
    - Disable unused services on the affected system.

Remediation

Be sure to preserve evidence against the intruder by backing up logs or possibly the entire system. Depending on the situation, restoring the system could include one or more of the following:

a) Re-install the affected system(s) from scratch and restore data from backups if necessary. Be sure to preserve evidence against the intruder by backing up logs or possibly the entire system.

b) Make users change passwords if passwords may have been sniffed.

c) Be sure turning off or uninstalling unused services has hardened the system.

d) Be sure the system is fully patched.

e) Be sure real time virus protection and intrusion detection is running.

f) Be sure the system is logging the correct items

Post Mortem Process

a) The Incident Report documentation must be augmented with the following pieces of information:

I. Evidence Collected and Preserved in the Jira ticket as part of the research efforts. This includes copies of logs, email, and other documentable communication. Keep lists of witnesses.

II. Notification documentation including communication with external agencies including the police if prosecution of the intruder is possible.

III. Assessments of damages to the organization and estimate both the damage cost and the cost of the containment efforts.

b) Review response and update policies

- Consider whether an additional policy could have prevented the intrusion.
- Consider whether a procedure or policy was not followed which allowed the intrusion, then consider what could be changed to be sure the procedure or policy is followed in the future.
- Was the incident response appropriate? How could it be improved?
- Was every appropriate party informed in a timely manner?
- Where the incident response procedures detailed and cover the entire situation? How can they be improved?
- Have changes been made to prevent a re-infection of the current infection? Are all systems patched, systems locked down, passwords changed, anti-virus

updated, email policies set, etc.?

- Have changes been made to prevent a new and similar infection?
- Should any security policies be updated?
- What lessons have been learned from this experience?

16. Revision History

Revision	Name	Date
1.0.0 Migration to Google Docs	Ram Prayaga	4/30/2015
1.0.1 Addition of Key Management to Data encryption policy	Ram Prayaga	1/29/2016
1.0.2 Fixed Typo in Disposal Process	Ram Prayaga	2/2/2016
1.0.3 Addition of lowercase letters, uppercase letters, digits and symbols in Password Minimum Standards	Jeff Martinez	8/8/2016
1.0.4 Addition of Critical Sensitive – Applies to business information which is intended strictly for use within the organization. Unauthorized disclosure will seriously and adversely impact the company, stockholders, business partners, and/or its customers. Examples of critical information include: Department of Defense (DoD) data protected by either the Privacy Act of 1974, as amended, or the HHS HIPAA Privacy and Security Final Rule. Access to information in this specific group is relegated to verified U.S. citizens only. Added attestation page	Jeff Martinez	3/2/2017
1.0.5 Added Logical Separation (page 7)	Jeff Martinez	3/9/2017
1.0.6 Changed description of Computing Systems, layout, and page	Simon Leung	11/2/2017
1.0.7 Removed Department of Defense (DoD) data protected by either the Privacy Act of 1974, as amended from Critical Sensitive and created a new section called DOD.	Jeff Martinez	12/18/2017

1.0.8 Modified Encryption & Key Management Policy and Vulnerability & Security Testing Policy to reflect updates. Fixed typo in Incident Response section.	Simon Leung	1/31/2018
1.0.9 Corrected order of severity categories under Analysis and Assessment, Incident Response. Fixed typo under Scanning and Audit.	Simon Leung	9/5/2018

N

Exhibit N

mPulse Mobile Log Review Policy v1.2

mPulse Mobile
Log Review Policy

This policy outlines the baseline behaviors required to ensure that employees, contractors and related constituents who use company resources for business do so in a safe, secure manner. It is designed to protect private and confidential data through creation, use, transmission and destruction. As a signed document, it is an addition to the library of acceptable use policies on file within Human Resources that allow employee behaviors to protect confidentiality of data.

Effective Date:	9/10/2018
Document Owner:	Ram Prayaga
Signature:	
Version:	1.2
Version Date Revision / Description Author:	8/17/2018 / Simon Leung

1. PURPOSE 3

2. SCOPE 3

3. ROLES AND RESPONSIBLITIES 3

4. INCIDENT RESPONSE 3

4.1 REVIEW OF LOGS 3
4.2 REVIEW OF VPN/LDAP, DATABASE LOGS 4
4.3 AWS LOGS 4
4.4 ROUTING AND FIREWALL LOGS 4
4.5 MOBILE COMPUTING AND COMMUNICATION 5
4.6 LOG RETENTION 5

5. APPLICATION AND ENFORCEMENT 5

6. REVISION HISTORY 6

1. Purpose

The mPulse Mobile Log Review Policy has been formulated with the following goals in mind:

- Ensure security, reliability and privacy of mPulse Mobile's systems, networks and data, and the networks, systems and data of others.
- Protect mPulse Mobile's systems, networks and data from harm and interference.
- Ensure that mPulse Mobile, its employees and other users of its facilities comply with the law and avoid legal liability.
- Encourage the responsible use of resources, and discourage practices which degrade the usability of network resources or cause harm to resources or individuals.
- Maintain mPulse Mobile's reputation as a responsible organization.
- Access to online content via the network may be restricted in accordance with our policies and federal regulations.

2. Scope

This procedure covers all logs generated for mPulse Mobile systems within the production environment, based on the flow of e-PHI data over mPulse Mobile service, including mPulse Mobile Platform.

3. Roles and Responsiblities

mPulse Mobile ops team shall review logs of access and activity of electronic protected health information (ePHI) applications, systems, and networks and address standards set forth by the HIPAA Security Rule to ensure compliance to safeguarding the privacy and security of ePHI.

mPulse Mobile management team is Responsible for monitoring the implementation of this procedure.

4. Incident Response

4.1 Review of Logs

The authority to respond to incidents lies with the Chief Information Security Officer (CSIO) and designated appointees. Upon notification of an incident the CSIO will appoint an appropriate Incident Response team. Appointees are subject to ad hoc change on a per incident basis.

A log review may be done to investigate an incident, as a periodic event, as a result of a client compliant, or suspicion of unsanctioned workplace practice. Review of activities shall also take into consideration mPulse Mobile's information system risk analysis results. The internal process shall review mPulse Mobile information system access and activity in mPulse Mobile SIEM, Graylog (e.g., log-ins, file accesses, and security incidents).

All logs are maintained in Graylog, which allows for the selectable criteria for logs generated by mPulse Mobile's information systems, such as:

- Source(s) of the log records
- Time
- Network address
- Application or service
- User
- Other details surrounding the incident

4.2 Review of VPN/LDAP, Database Logs

In mPulse Mobile Graylog console the ops team will look for:

- Any additions, modifications or deletions of user accounts.
- Any failed or unauthorized attempt at user logon.
- Any modification to system files.
- Any access to the server, or application running on the server.
- Actions taken by any individual with Administrative privileges.
- Any user access to audit trails.
- Any unauthorized access to e-PHI

4.3 AWS Logs

In the AWS CloudTrails the operations team will look for:

- Anomalies in Key Usage
- Admin level system changes

4.4 Routing and Firewall Logs

In the Graylog console the ops team will look for:

- Any vulnerabilities listed in the Common Vulnerability Entry (CVE) database.
- Any generic attack(s) not listed in CVE
- Any known denial of service attack(s).
- Any traffic patterns that indicated pre-attack reconnaissance occurred.
- Any attempts to exploit security-related configuration errors.
- Any authentication failure(s) that might indicate an attack.
- Any traffic to or from a back-door program.
- Any traffic typical of known stealth attacks.

4.5 Mobile Computing and Communication

mPulse Mobile monitors for unauthorized connections of mobile devices.

This applies to the corporate network controlled by Sonicwall and the cloud environment which is managed by perimeter controls including whitelisting of devices.

Monitoring is performed using perimeter control devices.

4.6 Log Retention

Logs are recorded for a minimum period of 30 days and archived for 10 years, as defined in the Log Retention Procedure.

See Audit Logs for details.

5. Application and Enforcement

This document is part of the company's comprehensive set of policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

This policy will be enforced by the IT Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

Any questions about this Policy should be sent via e-mail to Compliance@mpulsemobile.com

6. Revision History

Revision	Name	Date
1.0 – Initial	Ram Prayaga	12/15/2015
1.1 – Layout update	Simon Leung	7/20/2017
1.2 – Update cover page with signature field and effective date	Simon Leung	8/17/2018

O

Exhibit O

mPulse Mobile Software Development Life Cycle

Software Development Life Cycle

Confidentiality Notice:
The information contained in this document is proprietary, confidential and protected by copyright. Any dissemination, distribution, or reproduction of such information is strictly prohibited.

Version Information

1.0	Initial version	1/16/2016	Ram Prayaga
1.1	Updated Logo	7/20/2017	Simon Leung

Purpose and Objective

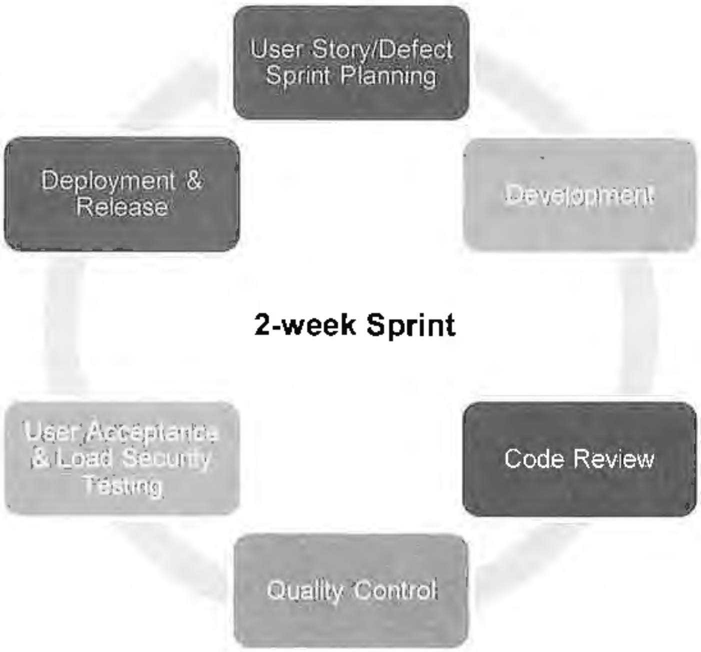
This document describes the high-level software development process followed by mPulse Mobile, Inc. This document is authored and maintained by the CTO to establish key software development controls and policies to ensure reliability, quality and maturity within the development process.

Items covered within this document:

- Development and release cycle.
- Access control.
- Approved storage locations and storing methods.
- Code management.

Software Development Life Cycle

As you see in the workflow cycle, a user story must be created first and all feature and acceptance criteria must be defined beforehand so that developers have a clear scope of what's required.


User Story/Defect Sprint Planning
Development
Code Review
Quality Control
User Acceptance & Load Security Testing
Deployment & Release
2-week Sprint

User Story/Defect & Sprint Planning

From there user stories are then prioritized by the product owner along with the Scrummaster so that a prioritized workflow can presented to off-shore development teams. Development teams can then work upon the prioritized goals during the work lifecycle.

Development

Once requirements from the user stories have been fully determined and agreed upon, a sprint planning session with the entire development commences. After unit testing by the developer, the code is checked into the Git repository and a senior member most familiar with the component and feature is assigned a code review task within JIRA.

Code Review

The code review, organized by a senior member, includes other peers and the QA manager. The primary objective of the review is used to ensure that coding standards and code quality standards have been successfully followed. It is also used for knowledge sharing with fellow team members for impact analysis. The code review includes (but is not limited to):

- Commenting, naming and general code readability
- Code reusability and impact analysis
- Performance and optimization considerations
- Security and compliance considerations

The review might result in some remediation items, which are documented in the code review task and is assigned to the developer to perform the necessary changes.

Quality Control

Once all tickets for a release are marked complete, QA deploys the code to the QA server for a rigorous functional and integration testing. They use automated and manual testing, tracking the test runs using a test management tool. And changes that fail a QC test, will be reported and reassigned to the developer.

User Acceptance Testing, Load Testing and Security Testing

Once finished with the quality control, a system admin ticket is created to deploy the completed release to the User Acceptance and Load Testing environment. This deployment process ensures the separation of responsibilities and serves as a dry run for production deployment. System Admin will review, perform and document all activities requested in the ticket including, database migrations and necessary infrastructure changes to support the release.

Once deployment, QA, product managers, account managers, client support specialists perform various UA testing to ensure usability and usefulness of the new release.

Security testing is also performed by QA and ensures that basic security considerations have been followed. Currently this is performed on a manual testing and the OWASP Top-10 list is used to evaluate and perform the necessary tests.[1]

Additionally, the QA engineers perform load tests on the load test environment to establish any performance impacts. Load tests are sometimes performed earlier if the primary purpose of the release is performance improvement. In general, load tests are used to ensure that existing baseline performance metrics are still met.

Deployment Release

Upon a successful build, regression testing and secure scans of the proposed software release must be presented to the QA Lead and an evaluation must be made to further continue the release process.

[1] mPulse is considering using an external automated tool to perform this scans.

Upon obtaining a positive review from the QA Lead, the following steps are conducted:

The development team creates a PGP key which seals the build so that no new code changes can be introduced. A Production Push Document is created documenting each step, which allows for a clean deployment of the latest build.

Should a rollback be needed, the steps are located within the PPD which consists of simply changing the sym-link back to the previous version.

- Once all the steps are documented and the tickets listed, a dry run will be conducted by the system administration on the UAT system.
- Once a proper build has been identified and a successful dry run has been executed, a production deployment date is assigned.
- Client notification is then sent out typically 2 weeks prior to the production release notifying the client of changes to the environment along with time, date and maintenance downtime.

Access Control

The development team has access to:

- Desktops to allow packages to be installed to enhance their work productivity.
- Developers have limited access to QA. They may inspect log files on the QA Environment, while System Administrators install fully vetted and approved applications on to QA.
- Developers have access to UAT for any log files. If needed, Developers will provide logs upon a documented JIRA request.

Code Management

All code management is kept within mPulse's version control system (a local git repository) located within the Amazon cloud and is backed up daily to ensure the latest codebase is intact. In addition, the development team's solutions architect has been assigned as the manager of the codebase to ensure that there are no commit issues when different teams come together.

P

Exhibit P

mPulse Mobile Disaster Recovery Policy v2.4

mPulse Mobile

Disaster Recovery Policy

This policy outlines the baseline behaviors required to ensure that employees, contractors and related constituents who use company resources for business do so in a safe, secure manner. It is designed to protect private and confidential data through creation, use, transmission and destruction. As a signed document, it is an addition to the library of acceptable use policies on file within Human Resources that allow employee behaviors to protect confidentiality of data.

Effective Date:	9/10/2018
Document Owner:	Ram Prayaga
Signature:	
Version:	2.4
Version Date Revision / Description Author:	8/15/2018 / Simon Leung

1. **PURPOSE** 4

2. **POLICY STATEMENT** 4

3. **OBJECTIVES** 4

4. **NOTIFICATION PROCESS** 5

INTERNAL – DISASTER RECOVERY TEAM 5
EXTERNAL – KEY CLIENT AND NOTIFICATION CONTACTS 6

5. **PLAN OVERVIEW** 6

PLAN UPDATING 6
PLAN DOCUMENTATION STORAGE 6
BACKUP STRATEGY 6
DATA BACKUP & REALTIME REPLICATION 7
RISK MANAGEMENT 7

6. **EMERGENCY RESPONSE** 8

ALERT, ESCALATION AND PLAN INVOCATION 8
a. Plan Triggering Events 8
b. Assembly Points 8
c. Activation of Emergency Response Team 8
DISASTER RECOVERY TEAM 9
EMERGENCY ALERT, ESCALATION AND DISASTER RECOVERY PLAN ACTIVATION 9
a. Emergency Alert 9
b. Disaster Recovery Procedures for Management 10
c. Contact with Employees 10
d. Backup Staff 10
e. Recorded Messages / Updates 10
f. Alternate Recovery Facilities / Hot Site 10
g. Personnel and Family Notification 10

7. **IT SYSTEMS** 11

FAILURE OF A SINGLE APPLICATION SERVER 11
RECOVERY OF DATABASE FAILURE 11
CATASTROPHIC FAILURE RECOVERY 11
EMERGENCY ACCESS 12

8. **MEDIA** 12

Media Contact 12
Media Strategies 12
Media Team 12
Rules for Dealing with Media 13

9. FINANCIAL AND LEGAL ISSUES 13

Financial Assessment 13
Financial Requirements 13
Legal Actions 13

10. DISASTER RECOVERY PLAN EXERCISES 13

11. APPLICATION AND ENFORCEMENT 14

12. REVISION HISTORY 14

13. APPENDIX – SUGGESTED FORMS 15

Damage Assessment Form 15
Management of DR Activities Form 15
Disaster Recovery Event Recording Form 16
Disaster Recovery Activity Report Form 16
Mobilizing the Disaster Recovery Team Form 17
Mobilizing the Business Recovery Team Form 17
Monitoring Business Recovery Task Progress Form 18
Preparing the Business Recovery Report Form 18
Communications Form 19
Returning Recovered Business Operations to Business Unit Leadership 19
Business Process/Function Recovery Completion Form 20

1. Purpose

To establish the process for mPulse Mobile regarding the appropriate action to take in the event an emergency or other occurrence that disrupts or damages e-PHI, e-PHI Systems or other repositories of PHI. This Plan also supports the mPulse Mobile Contingency Plan and Incident Response Policy.

This document delineates our policies and procedures for technology disaster recovery, as well as our process- level plans for recovering critical technology platforms and infrastructure. This document summarizes our recommended procedures. In the event of an actual emergency situation, modifications to this document may be made to ensure physical safety of our people, our systems, and our data.

Our mission is to ensure information system uptime, data integrity and availability, and business continuity.

2. Policy Statement

Corporate management has approved the following policy statement:

- The company shall develop a comprehensive IT disaster recovery plan.
- A formal risk assessment shall be undertaken to determine the requirements for the disaster recovery plan.
- The disaster recovery plan should cover all essential and critical infrastructure elements, systems and networks, in accordance with key business activities.
- The disaster recovery plan should be periodically tested in a simulated environment to ensure that it can be implemented in emergency situations and that the management and staff understand how it is to be executed.
- All staff must be made aware of the disaster recovery plan and their own respective roles.
- The disaster recovery plan is to be kept up to date to take into account changing circumstances.

3. Objectives

The principal objective of the disaster recovery program is to develop, test and document a well-structured and easily understood plan which will help the company recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts information systems and business operations. Additional objectives include the following:

- The need to ensure that all employees fully understand their duties in implementing such a plan

- The need to ensure that operational policies are adhered to within all planned activities
- The need to ensure that proposed contingency arrangements are cost-effective
- The need to consider implications on other company sites
- Disaster recovery capabilities as applicable to key customers, vendors and others

4. Notification Process

Internal – Disaster Recovery Team

Name, Title	Contact Option	Contact Number
Chris Nicholson Chief Executive Officer	Work	888-678-5735 x701
	Mobile	310-309-2480
	Home	310-309-2480
	Email Address	Chris@mPulseMobile.com
	Alternative Email	CNicholson2020@gmail.com

Name, Title	Contact Option	Contact Number
Ram Prayaga Chief Technology & Product Officer	Work	888-678-5735 x702
	Mobile	310-403-4889
	Home	818-594-0678
	Email Address	Ram@mPulseMobile.com
	Alternative Email	Ram@CafeThink.com

Name, Title	Contact Option	Contact Number
Brian Chudleigh Chief Financial Officer & Head of Human Resources	Work	888-678-5735 x700
	Mobile	805-750-0468
	Home	805-750-0468
	Email Address	Brian@mPulseMobile.com
	Alternative Email	

Name, Title	Contact Option	Contact Number
Abhineet Raj Development Operations Manager	Work	888-678-5735 x754
	Mobile	909-541-3447
	Home	
	Email Address	Abhineet.Raj@mPulseMobile.com
	Alternative Email	

Name, Title	Contact Option	Contact Number
Kunal Agrawal Development Manager	Work	888-678-5735 x720
	Mobile	803-397-2107
	Home	
	Email Address	kunal.agrawal@mPulseMobile.com
	Alternative Email	

Name, Title	Contact Option	Contact Number
Tony Askar Development Manager	Work	888-678-5735 x736
	Mobile	818-486-5179
	Home	
	Email Address	Tony@mPulseMobile.com
	Alternative Email	

Name, Title	Contact Option	Contact Number
Jeff Martinez Compliance & Security Manager	Work	888-678-5735 x719
	Mobile	925-325-4521
	Home	
	Email Address	Jeff.Martinez@mPulseMobile.com
	Alternative Email	

External – Key Client and Notification Contacts

Account Managers and Client Success Manager for each client will reach out to their respective key contacts as per the SLA and BAA requirements.

5. Plan Overview

Plan Updating

It is necessary for the Disaster Recovery Plan updating process to be properly structured and controlled. Whenever changes are made to the plan they are to be fully tested and appropriate amendments should be made to the training materials. This will involve the use of formalized change control procedures under the control of the IT Director.

Plan Documentation Storage

Copies of this Plan and hard copies will be stored in secure locations to be defined by the company. Each member of senior management, Disaster Recovery Team will be issued a document link and a hard copy of this plan to be filed at home. A master protected copy will be stored on specific resources established for this purpose.

Backup Strategy

Key Business	Back Up Strategy
IT Operations	All operations are in the cloud and therefore recovery can occur from any location
Email	In the cloud

Finance	Work from remote safe location using cloud-based services
Sales Marketing	Work from remote safe location using cloud-based services
Account	Work from remote safe location using cloud-based services
Human	Work from remote safe location using cloud-based services
Application & Platform	Pilot-On Failover location (See Details Below)
Data Backup	Fully replicated failover location (See Details Below)
Hardware & Server Infrastructure ere	AWS See SOC 2 (available by signed NDA) And SOC 3 (https://d0.awsstatic.com/whitepapers/compliance/soc3_amazon_web_services.pdf)

We maintain a pilot-on application and infrastructure environment with for our platform services. When code is deployed to the main production environment, it is also migrated to the failover site. All current production code and deployments (including any OS, access, and infrastructure patches) shall be deployed to the failover site application servers on the next business day (generally Wednesday). Services can be started in the event of a failover.

Data Backup & Realtime Replication

Our Master Postgres Databases are replicated to a failover Passive Slave within an alternate region. This ensures that data has a geographic failover with near instant data recovery. Backups in our public cloud are taken of Postgres daily. We retain 30 days of database (Postgres) backup data. These database backups are copied to a private S3 bucket in different geographic region and are stored on an encrypted file system (using AES256 encryption).

Risk Management

There are many potential disruptive threats, which can occur at any time and affect the normal business process. We have considered a wide range of potential threats and the results of our deliberations are included in this section. Each potential environmental disaster or emergency situation has been examined. The focus here is on the level of business disruption, which could arise from each type of disaster.

Potential disasters have been assessed as follows:

Potential Disaster	Probability Rating	Impact Rating	Risk Mitigation Strategy
Storms, Flood, & Fire	4	4	**Deemed adequately mitigated by AWS Controls**

Act of Terrorism	**3**	**4**	**Deemed adequately mitigated by AWS Controls**
Act of Sabotage	**3**	**4**	**Deemed adequately mitigated by AWS Controls**
Major Earthquake or Similar natural disaster	**2**	**1**	**Deemed adequately mitigated by AWS Controls**
Loss of Communications Network Services	**3**	**5**	**Remote location access available**

Probability: 1=Very High, 5=Very Low Impact: 1=Total destruction, 5=Minor annoyance

6. Emergency Response

Alert, escalation and plan invocation

a. Plan Triggering Events

Key trigger issues at headquarters that would lead to activation of the DRP are:

- Major disaster at our primary data center
- Temporary or permanent loss access to several staff member due to a physical disaster (natural or man-made)

b. Assembly Points

Where the premises need to be evacuated, the DRP invocation plan identifies two evacuation assembly points:

- Primary – Far end of main parking lot;
- Alternate – Parking lot of company across the street

c. Activation of Emergency Response Team

When an incident occurs the Emergency Response Team (ERT) must be activated. The ERT will then decide the extent to which the DRP must be invoked. All employees must be issued a Quick Reference card containing ERT contact details to be used in the event of a disaster. Responsibilities of the ERT are to:

- Respond immediately to a potential disaster and call emergency services;
- Assess the extent of the disaster and its impact on the business, data center, etc.;
- Decide which elements of the DR Plan should be activated;
- Establish and manage disaster recovery team to maintain vital services and return to normal operation;
- Ensure employees are notified and allocate responsibilities and activities as required.

Disaster Recovery Team

The team will be contacted and assembled by the ERT. The team's responsibilities include:

- Establish facilities for an emergency level of service within 2.0 business hours;
- Restore key services within 4.0 business hours of the incident;
- Recover to business as usual within 8.0 to 24.0 hours after the incident;
- Coordinate activities with disaster recovery team, first responders, etc.
- Report to the emergency response team.

Emergency Alert, Escalation and Disaster Recovery Plan Activation

This policy and procedure has been established to ensure that in the event of a disaster or crisis, personnel will have a clear understanding of who should be contacted. Procedures have been addressed to ensure that communications can be quickly established while activating disaster recovery.

The Disaster Recovery Plan will rely principally on key members of management and staff who will provide the technical and management skills necessary to achieve a smooth technology and business recovery. Suppliers of critical goods and services will continue to support recovery of business operations as the company returns to normal operating mode.

a. Emergency Alert

The person discovering the incident calls a member of the Emergency Response Team in the order listed:

Emergency Response Team

1. Jeffrey Martinez, Compliance and Security Manager
2. Chris Nicholson, CEO
3. Ram Prayaga, CTO
4. Brian Chudleigh, CFO

If not available try:
Tony Askar, Development Manager
Kunal Agrawal, Engineering Manager
Abhineet Raj, Development Operations Manager
Paige Mantel, Chief Marketing Officer
Karen Fischer, Director of Account Management
Mike Vogt, Sales Director

The Emergency Response Team (ERT) is responsible for activating the Disaster Recovery Plan for disasters identified in this plan, as well as in the event of any other occurrence that affects the company's capability to perform normally.

One of the tasks during the early stages of the emergency is to notify the Disaster Recovery

Team (DRT) that an emergency has occurred. The notification will request DRT members to assemble at the site of the problem and will involve sufficient information to have this request effectively communicated. The Business Recovery Team (BRT) will consist of senior representatives from the main business departments. The BRT Leader will be a senior member of the company's management team, and will be responsible for taking overall charge of the process and ensuring that the company returns to normal working operations as early as possible.

b. Disaster Recovery Procedures for Management

Members of the management team will keep a hard copy of the names and contact numbers of each employee in their departments and is also contained in the employee contact list. In addition, management team members will have a hard copy of the company's disaster recovery and business continuity plans on file in their homes in the event that the headquarters building is inaccessible, unusable, or destroyed.

c. Contact with Employees

Managers will serve as the focal points for their departments, while designated employees will call other employees to discuss the crisis/disaster and the company's immediate plans. Employees who cannot reach staff on their call list are advised to call the staff member's emergency contact to relay information on the disaster.

d. Backup Staff

If a manager or staff member designated to contact other staff members is unavailable or incapacitated, the designated backup staff member will perform notification duties.

e. Recorded Messages / Updates

For the latest information on the disaster and the organization's response, staff members will receive SMS messages from HR and the ERT with information - included in messages will be data on the nature of the disaster, assembly sites, and updates on work resumption.

f. Alternate Recovery Facilities / Hot Site

Given the availability of all resources online, staff members are recommended to operate from a safe location that provides adequate access to our online resources. In the case of workstation destruction, alternative computers may be available during the recovery process.

g. Personnel and Family Notification

If the incident has resulted in a situation, which would cause concern to an employee's immediate family such as hospitalization of injured persons, it will be necessary to notify their immediate family members quickly. All emergency contact information should be available within our HR management system.

7. IT Systems

Failure of a single application server

All instances are automatically monitored and any failure of a server results in an alert. The monitoring system alerts (via SMS) the system admin and NOC of this failure. However, since the entire infrastructure is designed as N+1 the infrastructure tolerates any single point of failure. In the event of a single server failure our load balancer will automatically seek another active and responsive server. The failing server will be restored offline and re-introduced into the load balancer when the issue has been resolved.

Recovery of Database failure

In the event of a failure, a DB master failure alert is sent via SMS and Email to the System Admin and NOC. Upon such notification, the System Admin will immediately work on restoring the database using the following process:

- Escalate the local failover slave to be the new master
- Modify the settings to look for the new will failover to one of the slaves and the slave is escalated to be the new master.

Catastrophic Failure Recovery

Upon evaluation and approval by CTO or CEO, the IT recovery from a catastrophic failure will take place. This consists of the following actions:

- Client IT Emergency contacts are informed that all services will be switched over to a failover
- DNS entries will be rerouted to temporary unavailable notification endpoints
  - apps.mpulsemobile.com -> apps.mpulsemobile.com/servicenotavailable
  - engage.mpulsemobile.com -> engage.mpulsemobile.com/servicenotavailable
  - ms-api.mpulsemobile.com -> ms-api.mpulsemobile.com/servicenotavailable
  - www.mpulsemobile.com -> www.mpulsemobile.com/servicenotavailable
  - All solutions' services will likewise have their equivalent unavailable notification page
- All external web requests for the following web services are rerouted to the following:
  - This endpoint informs all requests that we are currently unavailable
  - API requests will receive a 500 error in order to inform the client system of a failure. Since authentication is likely unavailable, the service will provide this response to all requestors regardless of authorization
- Promote the geographic database slave to DR master
  - This is performed by the System Admin with oversight of the IT DRT Lead and ERT
  - Shutdown of all services on Primary Postgres DBs
  - Update configuration settings to the new failover

- Promote the geographic Redis slave to DR Master
  - This is performed by the System Admin with oversight of the IT DRT Lead and ERT o Shutdown of all services on Primary Redis Cache/DBs
  - Update configuration settings to the new failover
- Aggregator is informed of traffic from our failover bind
- External data sources will have additional IT proxy changes
- All services are started on the pilot environment
  - Celery – restart services within local celery queues
  - RabbitMQ
  - Crontab
  - Webservers (NGINX, Apache and Tornado)
- DNS changes are applied to reflect new proxy location
- Clients reminded that callback sources must be whitelisted if not already
- Additional services are provisioned as needed to restore full capacity.
- New alternate region selected and a slave deployed to new alternate region
- Full smoke test is performed by QA to ensure all key services are back and functional
- ERT and DRT is informed of the failover and IT functionality has been successfully restored in a reduced capacity.
- Additional capacity requirements might suggest that new application servers can be added to the load balancer as needed.

Emergency Access

Emergency Access shall only be used when normal processes are insufficient.

8. Media

Media Contact

Assigned staff will coordinate with the media, working according to guidelines that have been previously approved and issued for dealing with post-disaster communications.

Media Strategies

1. Avoiding adverse publicity
2. Take advantage of opportunities for useful publicity
3. Have answers to the following basic questions:

a. What happened?
b. How did it happen?
c. What are you going to do about it?

Media Team

- Paige Mantel, Chief Marketing Officer

- Josh Ades, Marketing Program Manager
- Chris Nicholson, CEO

Rules for Dealing with Media

Only the media team is permitted direct contact with the media; anyone else contacted should refer callers or in- person media representatives to the media team.

9. Financial and Legal Issues

Financial Assessment

The emergency response team shall prepare an initial assessment of the impact of the incident on the financial affairs of the company. The assessment should include:

- Loss of financial documents
- Loss of revenue
- Theft of check books, credit cards, etc.

Financial Requirements

The immediate financial needs of the company must be addressed. These can include:

- Cash flow position
- Temporary borrowing capability
- Upcoming payments for taxes, payroll taxes, Social Security, etc.
- Availability of company credit cards to pay for supplies and services required post-disaster

Legal Actions

The company legal department and ERT will jointly review the aftermath of the incident and decide whether there may be legal actions resulting from the event; in particular, the possibility of claims by or against the company for regulatory violations, etc.

10. Disaster Recovery Plan Exercises

Disaster recovery plan exercises are an essential part of the plan development process. In a DRP exercise no one passes or fails; everyone who participates learns from exercises – what needs to be improved, and how the improvements can be implemented. Plan exercising ensures that emergency teams are familiar with their assignments and, more importantly, are confident in their capabilities.

Successful DR plans launch into action smoothly and effectively when they are needed. This will only happen if everyone with a role to play in the plan has rehearsed the role one or more times. The plan should also be validated by simulating the circumstances within which it has to work and seeing what happens.

11. Application and Enforcement

This document is part of the company's comprehensive set of policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

This policy will be enforced by the IT Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

Any questions about this Policy should be sent via e-mail to Compliance@mpulsemobile.com

12. Revision History

Revision	Name	Date
1.0 – Initial	Ram Prayaga	6/7/2016
2.0 – Significant addition of non-IT related activities to support a disaster recovery.	Ram Prayaga	8/5/2016
2.1 – Update layout, and contacts list	Simon Leung	7/21/2017
2.2 – Updated cover page to include signature and effective date. Removed old contacts.	Simon Leung	12/28/2017
2.3 – Updated contacts.	Simon Leung	4/24/2018
2.4 – Updated contacts, and associated titles. Added Engage URL to Catastrophic Failure Recovery section.	Simon Leung	8/15/2018

13. Appendix – Suggested Forms

Damage Assessment Form

Key Business Process Affected	Description Of Problem	Extent Of Damage

Management of DR Activities Form

- During the disaster recovery process all activities will be determined using a standard structure;
- Where practical, this plan will need to be updated on a regular basis throughout the disaster recovery period;
- All actions that occur during this phase will need to be recorded.

Activity Name:
Reference Number:
Brief Description:

Commencement Date/Time	Completion Date/Time	Resources Involved	In Charge

Disaster Recovery Event Recording Form

- All key events that occur during the disaster recovery phase must be recorded.
- An event log shall be maintained by the disaster recovery team leader.
- This event log should be started at the commencement of the emergency and a copy of the log passed on to the business recovery team once the initial dangers have been controlled.
- The following event log should be completed by the disaster recovery team leader to record all key events during disaster recovery, until such time as responsibility is handed over to the business recovery team.

Description of Disaster:
Commencement Date:
Date/Time DR Team Mobilized:

Activities Undertaken by DR Team	Date and Time	Outcome	Follow-On Action Required

Disaster Recovery Team's Work Completed: <Date>
Event Log Passed to Business Recovery Team: <Date>

Disaster Recovery Activity Report Form

- On completion of the initial disaster recovery response the DRT leader should prepare a report on the activities undertaken.
- The report should contain information on the emergency, who was notified and when, action taken by members of the DRT together with outcomes arising from those actions.
- The report will also contain an assessment of the impact to normal business operations.
- The report should be given to business recovery team leader, with a copy to senior management, as appropriate.
- A disaster recovery report will be prepared by the DRT leader on completion of the initial disaster recovery response.
- In addition to the business recovery team leader, the report will be distributed to senior management

The report will include:

- A description of the emergency or incident
- Those people notified of the emergency (including dates)
- Action taken by members of the DRT
- Outcomes arising from actions taken
- An assessment of the impact to normal business operations
- Assessment of the effectiveness of the BCP
- Lessons learned

Mobilizing the Disaster Recovery Team Form

- Following an emergency requiring recovery of technology infrastructure assets, the disaster recovery team should be notified of the situation and placed on standby.
- The format shown below can be used for recording the activation of the DR team once the work of the damage assessment and emergency response teams has been completed.

Description of Emergency:
Date Occurred:
Date of Work of Disaster Recovery Team Completed:

Name of Team Member	Contact Details	Contacted On (Time/Date)	By Whom	Response	Start Date Required
Relevant Comments (e.g. Specific Instructions Issued)					

Mobilizing the Business Recovery Team Form

- Following an emergency requiring activation of the disaster recovery team, the business recovery team should be notified of the situation and placed on standby.
- The format shown below will be used for recording the activation of the business recovery team once the work of the disaster recovery team has been completed.

Description of Emergency:
Date Occurred:
Date Work of Business Recovery Team Completed:

Name of Team Member	Contact Details	Contacted On (Time / Date)	By Whom	Response	Start Date Required
Relevant Comments (e.g., Specific Instructions Issued)					

Monitoring Business Recovery Task Progress Form

- The progress of technology and business recovery tasks must be closely monitored during this period of time.
- Since difficulties experienced by one group could significantly affect other dependent tasks it is important to ensure that each task is adequately resourced and that the efforts required to restore normal business operations have not been underestimated.

Note: A priority sequence must be identified although, where possible, activities will be carried out simultaneously.

Recovery Tasks (*Order of Priority*)	Person(s) Responsible	Completion Date		Milestones Identified	Other Relevant Information
		Estimated	Actual		
1.					
2.					
3.					
4.					
5.					
6.					
7.					

Preparing the Business Recovery Report Form

- On completion of business recovery activities the BRT leader should prepare a report on the activities undertaken and completed.
- The report should contain information on the disruptive event, who was notified and when, action taken by members of the BRT together with outcomes arising from those actions.
- The report will also contain an assessment of the impact to normal business operations.
- The report should be distributed to senior management, as appropriate.

The contents of the report shall include:

- A description of the incident
- People notified of the emergency (including dates)
- Action taken by the business recovery team
- Outcomes arising from actions taken
- An assessment of the impact to normal business operations
- Problems identified
- Suggestions for enhancing the disaster recovery and/or business continuity plan
- Lessons learned

Communications Form

- It is very important during the disaster recovery and business recovery activities that all affected persons and organizations are kept properly informed.
- The information given to all parties must be accurate and timely.
- In particular, any estimate of the timing to return to normal working operations should be announced with care.
- It is also very important that only authorized personnel deal with media queries.

Groups of Persons or Organizations Affected by Disruption	Persons Selected To Coordinate Communications to Affected Persons / Organizations		
	Name	Position	Contact Details
Customers			
Management & Staff			
Suppliers			
Media			
Stakeholders			
Others			

Returning Recovered Business Operations to Business Unit Leadership

- Once normal business operations have been restored it will be necessary to return the responsibility for specific operations to the appropriate business unit leader.
- This process should be formalized in order to ensure that all parties understand the change in overall responsibility, and the transition to business-as-usual.
- It is likely that during the recovery process, overall responsibility may have been assigned to the business recovery process lead.
- It is assumed that business unit management will be fully involved throughout the recovery, but in order for the recovery process to be fully effective, overall responsibility during the recovery period should probably be with a business recovery process team.

Business Process/Function Recovery Completion Form

The following transition form should be completed and signed by the business recovery team leader and the responsible business unit leader, for each process recovered.

A separate form should be used for each recovered business process.

Name Of Business Process	
Completion Date of Work Provided by Business Recovery Team	
Date of Transition Back to Business Unit Management *(If different than completion date)*	

I confirm that the work of the business recovery team has been completed in accordance with the disaster recovery plan for the above process, and that normal business operations have been effectively restored.

Business Recovery Team Leader Name: ______________________

Signature: ______________________

Date: ______________

(Any relevant comments by the BRT leader in connection with the return of this business process should be made here.)

I confirm that above business process is now acceptable for normal working conditions.

Name: ______________________

Title: ______________________

Signature: ______________________

Date: ______________

Q

Exhibit Q

mPulse Mobile Patch Management Policy v1.1

mPulse Mobile

Patch Management Policy

This policy outlines the baseline behaviors required to ensure that employees, contractors and related constituents who use company resources for business do so in a safe, secure manner. It is designed to protect private and confidential data through creation, use, transmission and destruction. As a signed document, it is an addition to the library of acceptable use policies on file within Human Resources that allow employee behaviors to protect confidentiality of data.

Effective Date:	9/10/2018
Document Owner:	Ram Prayaga
Signature:	
Version:	1.1
Version Date Revision / Description Author:	8/17/2018 / Simon Leung

1. PURPOSE 3
2. SCOPE 3
3. POLICY 3
4. PROCEDURES 4
4.1 IDENTIFY NEWLY DISCOVERED VULNERABILITIES AND SECURITY PATCHES 4
4.2 PRIORITIZE PATCH APPLICATION 4
4.3 VERIFY PATCH INSTALLATION 4
4.4 PATCH APPROVAL PROCESS 5
4.5 AUDITING AND MONITORING 5
4.6 COMMUNICATION 5
5. COMPLIANCE AND SANCTIONS 5
6. APPLICABILITY AND ENFORCEMENT 5
7. REVISION HISTORY 6

1. Purpose

The mPulse Mobile Patch Management Policy has been formulated with the following goals in mind:

- Ensure security, reliability and privacy of mPulse Mobile 's systems, networks and data, and the networks, systems and data of others.
- Protect mPulse Mobile's systems, networks and data from harm and interference.
- Ensure that mPulse Mobile, its employees and other users of its facilities comply with the law and avoid legal liability.
- Encourage the responsible use of resources, and discourage practices which degrade the usability of network resources or cause harm to resources or individuals.
- Maintain mPulse Mobile's reputation as a responsible organization.
- Access to online content via the network may be restricted in accordance with our policies and federal regulations.

2. Scope

This policy provides guidelines for permissible and impermissible actions regarding company information systems. This policy applies not only to mPulse Mobile's systems and networks, but to activities mPulse Mobile conducts on client systems and networks. This policy applies to any user of mPulse Mobile's systems, including, but not limited to, employees, interns, contractors, consultants and temporaries (referred to in this policy as "users").

Patches are released:

- To fix faults in an applications or operating systems. Patches are also released to correct performance or functionality problems.
- To alter functionality or to address a new security threat.
- To change or modify the software configuration to make it less susceptible to attacks and therefore more secure.

3. Policy

The patch management process establishes a manual and automated companywide system for all IT systems, devices and appliances, regardless of operating system or platform. This will consist of clearly assigned specific responsibilities for the System Administrator(s) or other authorized personnel. All authorized personnel are trained in system administration to include patch management techniques. Patch management will be used in conjunction with the normal vulnerability scanning efforts. The IT department will certify that system patches have been applied using the quarterly vulnerability scanning.

Patches will be tested on non-production systems prior to installation on all production systems. In addition, the IT department will maintain an organizational hardware and software inventory and an electronic database of information on patches required and deployed on the systems or applications for the purposes of proper internal controls.

Policy Exception Requirements - Exceptions to policy will be considered only in terms of implementation timeframes.

4. Procedures

Managing servers in the third party hosted facility is a shared responsibility between mPulse Mobile and the third party company. mPulse Mobile works with the third party facility to designate requirements for patch management.

4.1 Identify Newly Discovered Vulnerabilities and Security Patches

mPulse Mobile development team is responsible for proactively monitoring security sources for vulnerabilities and patches that correspond to the software within the organizational hardware and software inventory.

When a vulnerability has no satisfactory patch, the development team will present alternative risk mitigation approaches to development management and support the management decision by testing, documenting, and coordinating implementation with the appropriate system or network administrators.

4.2 Prioritize Patch Application

The development department prioritizes the set of known patches and provides advice on the criticality of each patch. The development department will document the critical vulnerabilities each quarter and production servers will be patched. Two weeks prior to patching in the production environment, patched will be tested in a sandbox environment. Post patch implement, tests for the validity of the patch are done within 1 week. Critical patches will be applied within 30 days.

Patches will be tested in a test environment before being implemented in the production environment.

4.3 Verify Patch Installation

Quarterly network and host vulnerability scanning are scheduled to identify systems that are vulnerable. Whenever possible, patch management vulnerability scanning and configuration management should be tightly integrated. When a new vulnerability is announced that is deemed critical, or after any significant change in the network, the IT department will scan the network for systems that may be vulnerable within 30 calendar days.

4.4 Patch Approval Process

It is the responsibility of application owners to identify any problem(s) with a patch(s) and to notify the mPulse Mobile development of the problem(s). It is also the responsibility of application owners to resolve this incompatibility with the application's maker. If the maker cannot resolve the incompatibility, the risk incurred by not patching the computer(s) in question are weighed against the risk of not running the application.

4.5 Auditing and Monitoring

- Post-patch audit scans must occur within 1 week after release of a critical security patch.
- Regular or pre-patch network-wide audit scans are performed at least quarterly.

4.6 Communication

The patch cycle will be communicated to all system and administrators and business unit owners 3 business days prior to deployment. Any downtime will be communicated.

5. Compliance and Sanctions

All users are expected to comply with this policy and other mPulse Mobile policies. Anyone found in violation of this policy, may be subject to disciplinary action up to and including termination and criminal and civil prosecution.

All users are required and expected to report any information concerning violations or suspected violations of this policy to mPulse Mobile.

6. Applicability and Enforcement

This document is part of the company's comprehensive set of policies. Other policies may apply to the topics covered in this document and as such, the applicable policies should be reviewed as needed.

This policy will be enforced by the IT Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

Any questions about this Policy should be sent via e-mail to Compliance@mpulsemobile.com

7. Revision History

Revision	Name	Date
1.0 – Initial	Simon Leung	7/20/2017
1.1 – Update cover page to include effective date and signature field. Correct reference to mPulse Mobile development team.	Simon Leung	8/17/2018

Exhibit R

mPulse Mobile Security Awareness and Training Policy v1.2

mPulse Mobile

Security Awareness & Training Policy

This policy outlines the baseline behaviors required to ensure that employees, contractors and related constituents who use company resources for business do so in a safe, secure manner. It is designed to protect private and confidential data through creation, use, transmission and destruction. As a signed document, it is an addition to the library of acceptable use policies on file within Human Resources that allow employee behaviors to protect confidentiality of data.

Effective Date:	7/25/2018
Document Owner:	Ram Prayaga
Signature:	
Version:	1.2
Version Date Revision / Description Author:	7/21/2018 / Simon Leung

1. PURPOSE 3
2. SCOPE 3
3. DEFINITIONS 3
4. POLICY 4
5. COMPLIANCE AND SANCTIONS 6
6. APPLICABILITY AND ENFORCEMENT 6
7. REVISION HISTORY 6

1. Purpose

The mPulse Mobile Security Awareness & Training Policy has been formulated with the following goals in mind:

- Ensure security, reliability and privacy of mPulse Mobile's systems, networks and data, and the networks, systems and data of others.
- Protect mPulse Mobile's systems, networks and data from harm and interference.
- Ensure that mPulse Mobile, its employees, and other users of its facilities comply with the law and avoid legal liability.
- Encourage the responsible use of resources, and discourage practices which degrade the usability of network resources, or cause harm to resources or individuals.
- Maintain mPulse Mobile's reputation as a responsible organization.
- Access to online content via the network may be restricted in accordance with our policies and federal regulations.

2. Scope

This policy provides guidelines for permissible and impermissible actions regarding company information systems. This policy applies not only to mPulse Mobile's systems and networks, but to activities mPulse Mobile conducts on client systems and networks. This policy applies to any user of mPulse Mobile's systems, including, but not limited to, employees, interns, contractors, consultants, and temporaries (referred to in this policy as "users").

For the purposes of this document, the term incident is considered to be any adverse event that threatens the confidentiality, integrity, accessibility, or ability to audit company information resources. Information resources belonging to customers are expressly included in this definition, and covered by this policy.

These events include but are not limited to:

- Attempts (either failed or successful) to gain unauthorized access to a system or its data.
- Unwanted disruption or denial of service.
- Unauthorized use of a system for the transmission, processing, or storage of data.
- Changes to system hardware, firmware, or software characteristics without the company's knowledge, instruction or consent.
- Attempts to cause failures in infrastructure or services.

3. Definitions

<u>mPulse Mobile Information Systems:</u> mPulse Mobile repositories and conduits of electronic data, including servers and devices.

mPulse Mobile Workforce: All full- and part-time employees of mPulse Mobile, and all persons engaged (director or indirectly and whether paid or not) to perform services for mPulse Mobile under the direct control of mPulse Mobile, including mPulse Mobile contractors and their subcontractors, and excluding individuals whose conduct is not under the direct control of mPulse Mobile.

Electronic Protected Health Information or e-PHI: Individually identifiable health information, as further described in the HIPAA Regulations, that is transmitted over, or maintained in, any Electronic Media.

e-PHI Systems: All mPulse Mobile Information Systems that contain or provide access to e-PHI.

HIPAA Regulations: Rules and standards for safeguarding the privacy and security of individually identifiable health information that are codified at 45 CFR Part 164, Subparts A, C, and E.

HIPAA Security Regulations: Rules and standards for safeguarding e-PHI that are codified at 45 CFR Part 164, Subparts C.

4. Policy

General Policy

mPulse Mobile Workforce are required to complete training on policies and procedures regarding awareness of physical safeguards and risks of malicious threats and accidental errors and omissions involved with PHI, access to e-PHI, and e-PHI Systems.

mPulse Mobile Workforce are held accountable for their failure to comply with this policy and any related procedures. Sanctions for non-compliance with this policy and any related procedures many include disciplinary action, up to and including termination.

HIPAA Security Training

mPulse Mobile requires all new and current mPulse Mobile Workforce to attend training appropriate for mPulse Mobile Workforce access to e-PHI and e-PHI Systems. mPulse Mobile logs and tracks mPulse Mobile Workforce HIPAA security training. Periodically, but at a minimum bi-annually, mPulse Mobile evaluates the effectiveness of its security training.

The security training includes: training on the mPulse Mobile password policy; password management procedures; use of screen savers; security incident reportings; automatic logoff for inactivity; and logon security.

Security Reminders

mPulse Mobile disseminates information, updates, and reminders to mPulse Mobile Workforce as needed, including, but not limited to, the following:

- Corporate policies, security policies, and revisions to e-PHI policies and procedures;
- Information security controls and processes;
- Warnings on risks to mPulse Mobile information assets, e-PHI, and e-PHI Systems;
- Security best practices;
- Legal and business responsibilities for information security, including e-PHI security;
- New security controls;
- Changes to significant security controls;
- New threats or risks to mPulse Mobile;
- Changes to HIPAA Privacy and HIPAA Security Regulations; and
- Other regulatory update relating to security.

Protection from Malicious Software Training

mPulse Mobile trains mPulse Mobile Workforce on additional protections maintained by mPulse Mobile, including anti-virus protection, malicious file attachments, anti-malware protection, SPAM and unsolicited email, and social engineering, and provides ongoing training on suspected malicious file attachments.

Log-in Monitoring Training

mPulse Mobile's security training addresses procedures for monitoring log-in attempts and reporting discrepancies as set forth in the mPulse Mobile Access Terms and Conditions.

Password Management Training

mPulse Mobile's security training addresses password management procedures as set forth in the mPulse Mobile's Access Terms and Conditions.

Training Documentation

Security training documentation is maintained by mPulse Mobile and includes the time, date, place, and content of each training session, as well as the names of mPulse Mobile Workforce who attended each training session. mPulse Mobile maintains such documentation in accordance with the Record Retention Policy and makes it available for inspection by regulatory authorities, as appropriate.

mPulse Mobile Workforce Responsibilities

mPulse Mobile Workforce are required to complete all required security training before accessing, or attempting to access, e-PHI or e-PHI Systems.

5. Compliance and Sanctions

All users are expected to comply with this policy and other mPulse Mobile policies. Anyone found in violation of this policy, may be subject to disciplinary action up to and including termination and criminal and civil prosecution.

All users are required and expected to report any information concerning violations or suspected violations of this policy to mPulse Mobile.

6. Applicability and Enforcement

This document is part of the company's comprehensive set of policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

This policy will be enforced by the IT Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

Any questions about this Policy should be sent via e-mail to Compliance@mpulsemobile.com

7. Revision History

Revision	Name	Date
1.0 – Initial	Ram Prayaga	12/15/2015
1.1 – Layout update	Simon Leung	7/20/2017
1.2 – Corrected reference to Access Terms and Conditions in Log In Monitoring Training and Password Management Training sections.	Simon Leung	7/21/2018

S

Exhibit S

mPulse Mobile Training Plan Template

Training Plan Template
& Planning Guide

V 1.0 – July 2017

mPulse™
mobile

Table of Contents

1 INTRODUCTION 3

2 PLANNING 3

3 AUDIENCE 3

4 CONTENT 4

5 LOGISTICS 4

6 MATERIALS 4

1 Introduction

mPulse Mobile training is tailored for each customer based on the roles, channels (SMS, email, etc.) and solution layer (communicate, engage, activate), project phase and size/scale of the implementation.

This document serves as a template and planning guide to ensure that effective training is designed and delivered to our customer.

2 Planning

The following information is gathered during the implementation phase of the project. Details are provided in each section.

- Audience
  - Who is being trained
  - Roles (List manager, IT, Call Center Representative, Analyst, etc.)
- Content
  - User Interface Training
    - Communication Console
    - Engagement Console
    - Custom Interfaces
  - Advanced Training
    - Data
    - API / Integrations
- Logistics
  - Number of sessions
  - Delivery mechanism (on site or remote)
  - Session Duration
  - Dates
- Materials
  - Guides, presentation, vidoes

3 Audience

Identify the target audiences for the training sessions. Specifically, roles and locations. The audience will drive the content and planning.

Name	**Role**	**Contact Info**	**Location / Time Zone**

4 Content

Content is identified by role (list manager, CSR, IT, etc.) component (communication console, engagement console, etc.) and topic (reporting, campaign management, etc.)

Advanced training can be provided for data owners, analysts and interface developers.

Role	**Component**	**Topic**

5 Logistics

Once the audience and content have been identified, a training plan will be developed, indicating the number of sessions, delivery mechanism, dates and times.

Session Topic	**Attendees**	**Date**	**Duration**	**Location**

6 Materials

As appropriate, training materials will be developed and delivered. They could include presentations, documentation, videos and recorded meetings.

Deliverable	**Description**	**Date**

T

Exhibit T

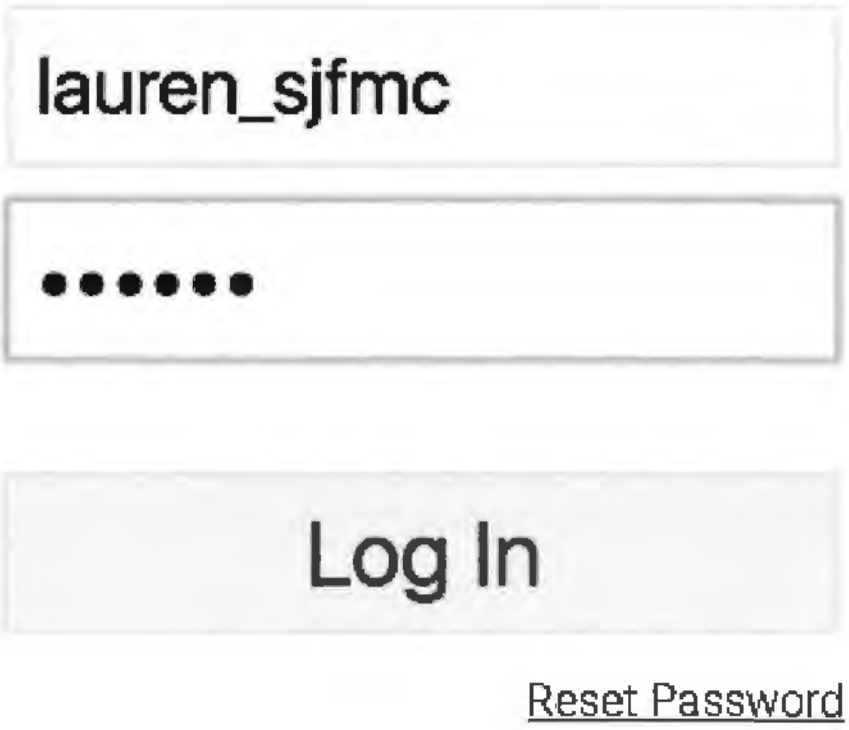
mPulse Mobile Example Training Material: SJFMC Member Engagement Console

SJFMC
MEC Training Material

mPulse mobile

Log into the Mobile Engagement Console

URL: https://care.mpulsemobile.com/

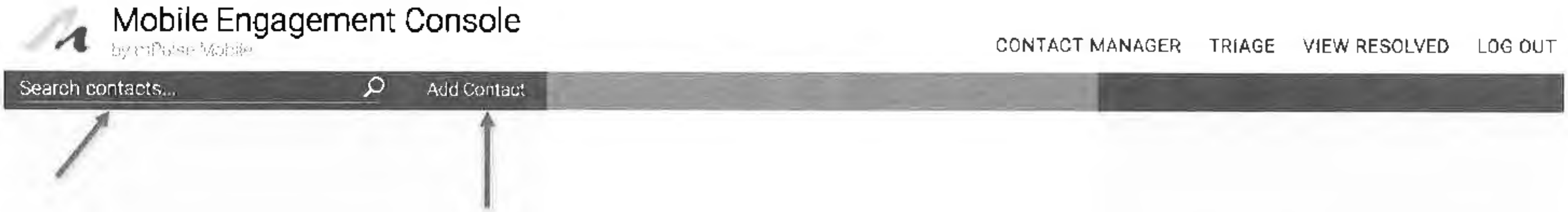


lauren_sjfmc

●●●●●●

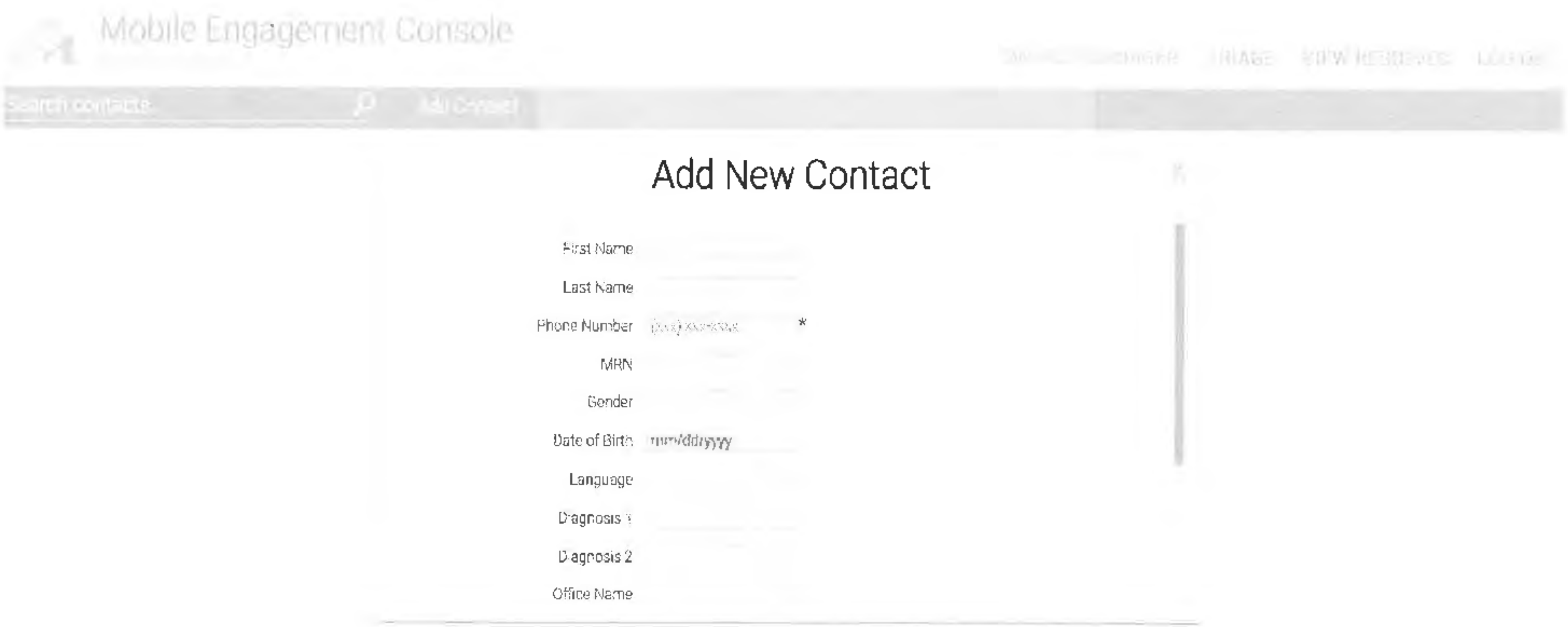
Contact Manager

This is the area you see right after logging into MEC. The search bar on the left can be used to search a member by mobile number, first name, last name, MRN, or email address. The 'Add Contact' button is for adding new members. A real-time query will be performed to verify the phone number is a valid mobile number.



Add New Contact

When adding a new contact, simply add the member's mobile number (which is a required field) and any other information you have, such as, name, care coordinator, office name, etc.

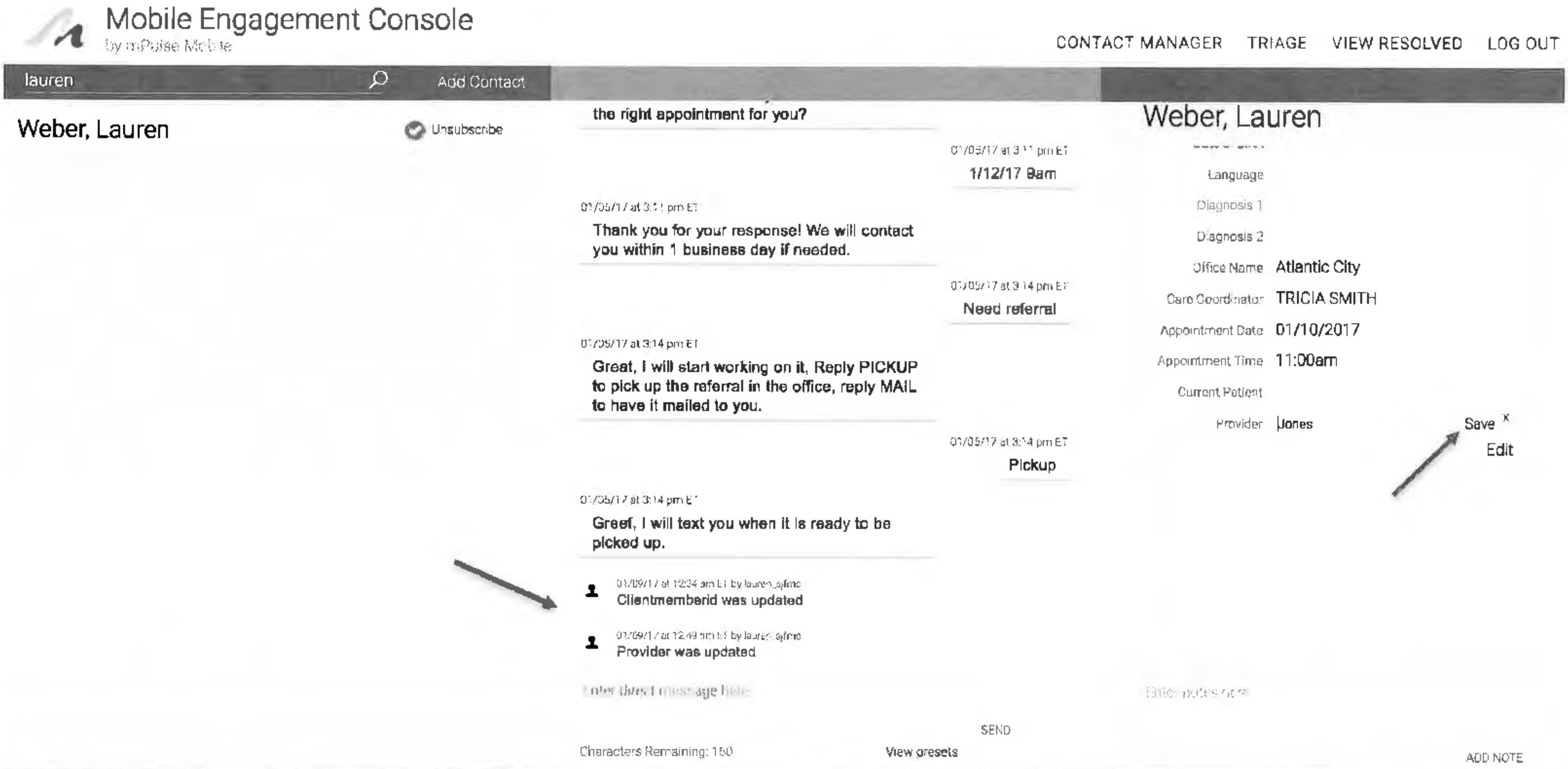


Add New Contact

First Name
Last Name
Phone Number (xxx) xxx-xxxx *
MRN
Gender
Date of Birth mm/dd/yyyy
Language
Diagnosis 1
Diagnosis 2
Office Name

Updating Member

To update a member's information, click on the 'Edit' button next to any of the fields on the right-hand side. Next click 'Save,' and the edit will then be displayed in the member's profile. Updates will also be reflected in the communication pane in the center.



Mobile Engagement Console
by mPulse Mobile

Weber, Lauren

the right appointment for you?

01/05/17 at 3:11 pm ET
1/12/17 9am

01/05/17 at 3:11 pm ET
Thank you for your response! We will contact you within 1 business day if needed.

01/05/17 at 3:14 pm ET
Need referral

01/05/17 at 3:14 pm ET
Great, I will start working on it, Reply PICKUP to pick up the referral in the office, reply MAIL to have it mailed to you.

01/05/17 at 3:14 pm ET
Pickup

01/05/17 at 3:14 pm ET
Greef, I will text you when it is ready to be picked up.

01/09/17 at 12:34 pm ET by lauren_sjfmc
Clientmemberid was updated

01/09/17 at 12:49 pm ET by lauren_sjfmc
Provider was updated

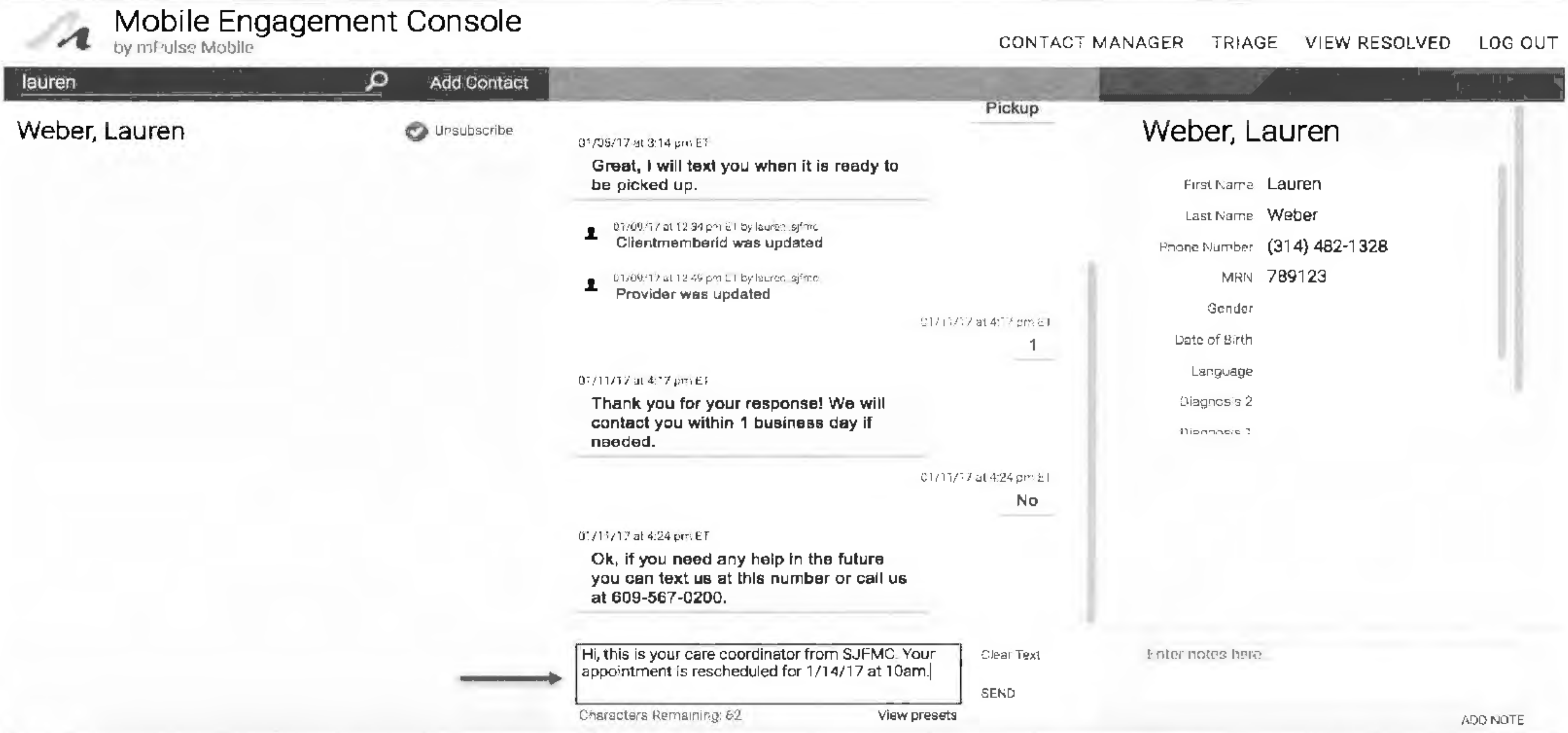
Enter direct message here

Weber, Lauren

Language	
Diagnosis 1	
Diagnosis 2	
Office Name	Atlantic City
Care Coordinator	TRICIA SMITH
Appointment Date	01/10/2017
Appointment Time	11:00am
Current Patient	
Provider	Jones

Direct Messaging a Member

You will have a list of preset messages to choose from when sending a message to a member. If none of the presets contain the message you want to send, you also have the option to send members a free-text message. Type a message up to 160 characters then click 'SEND.' You have a 10-second window to cancel the message, and it will not be sent.



Pickup

01/05/17 at 3:14 pm ET
Great, I will text you when it is ready to be picked up.

01/09/17 at 12:34 pm ET by lauren.sjfmc
Clientmemberid was updated

01/09/17 at 12:49 pm ET by lauren.sjfmc
Provider was updated

01/11/17 at 4:17 pm ET
1

01/11/17 at 4:17 pm ET
Thank you for your response! We will contact you within 1 business day if needed.

01/11/17 at 4:24 pm ET
No

01/11/17 at 4:24 pm ET
Ok, if you need any help in the future you can text us at this number or call us at 609-567-0200.

Hi, this is your care coordinator from SJFMC. Your appointment is rescheduled for 1/14/17 at 10am.

Characters Remaining: 62

Weber, Lauren

First Name	Lauren
Last Name	Weber
Phone Number	(314) 482-1328
MRN	789123
Gender	
Date of Birth	
Language	
Diagnosis 2	
Diagnosis 3	