CITY OF OAKLAND

Privacy Advisory Commission

February 2, 2023
5:00 PM
Teleconference
Meeting Agenda

***Commission Members**: **District 1 Representative**: Reem Suleiman, **District 2 Representative**: Chloe Brown, **District 3 Representative**: Brian Hofer, Chair, **District 4 Representative**: Lou Katz, Vice Chair **District 5 Representative**: Omar De La Cruz, **District 6 Representative**: Gina Tomlinson, **District 7 Representative**: Robert Oliver, **Council At-Large Representative**: Henry Gage III **Mayoral Representative**: Jessica Leavitt*

Pursuant to California Government Code section 54953(e), Oakland Privacy Advisory Commission Board Members/Commissioners, as well as City staff, will participate via phone/video conference, and no physical teleconference locations are required.

TO OBSERVE:
Please click the link below to join the webinar:
https://us02web.zoom.us/j/85817209915
Or iPhone one-tap:
US: +16699009128, 85817209915# or +13462487799, 85817209915#
Or Telephone:
Dial (for higher quality, dial a number based on your current location):
US: +1 669 900 9128 or +1 346 248 7799 or +1 253 215 8782 or +1 646 558 8656
Webinar ID: 858 1720 9915
International numbers available: https://us02web.zoom.us/u/kDUn0z2rP

TO COMMENT:
1) To comment by Zoom video conference, you will be prompted to use the "Raise Your Hand" button to request to speak when Public Comment is being taken on the eligible Agenda item. You will then be unmuted, during your turn, and allowed to make public comments. After the allotted time, you will then be re-muted.

2) To comment by phone, you will be prompted to "Raise Your Hand" by pressing "* 9" to request to speak when Public Comment is being taken on the eligible Agenda Item. You will then be unmuted, during your turn, and allowed to make public comments. After the allotted time, you will then be re-muted.

ADDITIONAL INSTRUCTIONS:
1) Instructions on how to join a meeting by video conference is available at: https://support.zoom.us/hc/en-us/articles/201362193%20-%20Joining-a-Meeting#
2) Instructions on how to join a meeting by phone are available at: https://support.zoom.us/hc/en-us/articles/201362663%20Joining-a-meeting-by-phone
3) Instructions on how to "Raise Your Hand" is available at: https://support.zoom.us/hc/en-us/articles/205566129-Raising-your-hand-In-a-webinar

Privacy Advisory Commission

February 2, 2023
5:00 PM
Teleconference
Meeting Agenda

---

1. Call to Order, determination of quorum

2. Adopt a Renewal Resolution regarding AB 361 establishing certain findings justifying the ongoing need for virtual meetings

3. Open Forum/Public Comment

4. Surveillance Technology Ordinance – OFD MACRO – Julota software (case management)
    a. Review and take possible action on the proposed Use Policy and draft Impact Report

City of Oakland Fire Department

Surveillance Technology Use Policy for Julota Software

Used by the Oakland Fire Department MACRO Program

A. Purpose:

The purpose of this case management platform is for the Oakland Fire Department MACRO Program to track service referrals and outcomes for individuals and families engaged in MACRO services and receive local service referrals from a MACRO EMT or MACRO Community Intervention Specialist. Typically, the local service referrals include local organizations that provide individualized care that ranges from behavioral health, food assistance, housing support, substance abuse, justice involvement, or any combination of the aforementioned.

The case management platform will be used by specific and limited MACRO staff to track engagement, milestones, and outcomes for individual clients as well as attendance, duration, and feedback of local services. Limited, leadership staff within the MACRO Program will use the system to ensure quality of local services and to improve on the quality of local service referrals to community members in need. The list of local service providers includes many players at the state, county, and municipal level as well as public-private partnerships and local non-government organizations. This group of providers also can fluctuate based on resources, creating a need for a program such as the OFD MACRO Program to maintain reliability of referrals to Oaklanders in need without compromising staff resources. The Julota case management platform allows the MACRO Program a simple, secure, and effective communication across the continuum of care while managing a fluctuating rolodex of community partners.

The MACRO Program will use the Julota case management platform to monitor aggregate service referrals, data capture of each incident, quality of service referral programs, and outcome data, to track the program deliverables as specified by various grant funds and stakeholder interest. The Julota platform will also be used to provide quality improvement of services, identify challenges with program referrals and programmatic gaps that require remediation. The MACRO Program's staff will use the system to gain and store consent of information documents, communicate with other providers such as case managers, and provide the best blend of resources based on individual needs and experiences as informed by the Julota platform aggregating essential information. Finally, service delivery and outcomes data will be available for program evaluation and delivery of program efficacy to local stakeholders such as the MACRO Advisory Board, Oakland City Council, Oakland Mayor, surrounding municipalities, and, of course, the Oakland community.

B. Authorized Use:

All data will be accessed on a need-to-know and right-to-know basis, meaning that individuals will only be able to access information within the data management system that is essential to their job function. Categories of data management system usage are described below.

- **Service delivery:** Direct service staff and supervision staff will use the Julota data management system to track information on client contacts, referrals, and other aspects of service delivery. The system will track tasks related to service delivery and present summarized data on clients served though dashboards that are helpful to staff who are directly responsible for service delivery to clients.

- **Internal evaluation:** OFD MACRO leadership staff and Program Analyst will use data from the system to ensure that the MACRO Program is serving the correct target population, that services are being delivered as expected, that referral sources are current, and quality of referral is upheld, and that summarized service delivery data are available to a range of external stakeholders, including councilmembers, advisory board members, grantors, and the public.

- **External evaluation:** Data from the Julota system will be used to evaluate the effectiveness of the MACRO Program, including services and referrals delivered by the MACRO Responders. Evaluation will be conducted by the MACRO Program Analyst, who will only use the data from the Julota platform to evaluate efficacy of the MACRO Program. The data used from the Julota platform will be discreet, omit personally identifiable information (PII), and will be used to address the population served as a whole. The MACRO Program Analyst and leadership staff will seek and receive Institutional Review Board (IRB) approval prior to commencing any research activities. Once IRB approval is obtained, evaluators will only have access to Personally Identifiable Information (PII) of individuals who sign a consent form agreeing to have their data used for evaluation. These consent forms will be kept on file and can be accessed for audit or review purposes. For clients who do not sign a consent form, data from the Julota system will only be provided without PII or in aggregate form.

C. Data Collection:

The Julota platform will receive data from MACRO Responder who enter it directly into the case management platform and through interfaces with other data systems, 911 Dispatch (Oakland Police and Oakland Fire Dispatch), ESO (Electronic Health Records for Emergency Services), and CHR (Community Health Records, maintained by Alameda County Care Connect).

The sources of this data can also be found on the *Impact Policy Report for the Julota Software* under *F. Data Types and Sources*. Data to be collected will include basic demographics, past 911 calls or visits to Emergency Department for treatment/care,

summary of work with the MACRO program, including brief information about referrals to community-based services to address identified needs. This is further outlined in the following two tables.

Prior to enrollment in services, individuals will complete consent forms pertaining to general storage of their information in the Julota data management system. Direct service staff will then enter in data provided by participants or related to participant interactions with the staff member into the data management system in accordance with the signed consent forms. The staff will use 'Toughbook' computer devices, also used by Emergency Response personnel, which is secured and provided private MACRO server connectivity sourced from the MACRO vehicles.

Table 1 presents an overview of service delivery and outcome data that will be collected through the data management system. **Table 2** provides an overview of the Julota system use pertaining data analysis, data visualization, and data management.

Table 1. Service delivery and outcome data collected through the Julota data management system.

Category	Service delivery and outcome data
Individual service delivery	▪ Date, method, and result of outreach attempts ▪ Client name and contact information ▪ Client demographic information (e.g. age, race, gender, education, language spoken at home) ▪ Client's current education, employment, and housing information ▪ Risk and protective factor assessment results ▪ Program referral, intake, and exit information ▪ Individual flags to identify unique features of clients ▪ Information about important people (contact information and affiliation for family members, spouses, close friends, probation or parole officer, etc.) ▪ Date, duration, and method of all communication involving client (including communication *about* client with important person or other service provider) ▪ Date, location, type, and duration of all activities involving client ▪ Date, amount, and purpose of financial incentives received ▪ Client outcomes (e.g. obtained GED, completed probation) ▪ Case plan goals, actions, start dates, and completion dates ▪ Date and status of referrals made to other service providers
Group services	▪ Date, location, and duration of service ▪ Name of Local Service Referral, duration of program utilized, provider notes on individual, and communication between service referral and ▪ Number of staff members present ▪ Other metrics based on event (e.g. number of meals distributed)

Category	Service delivery and outcome data
First Responder Partners Interaction	▪ Date, time, and name of emergency response units responding to the individual ▪ Individual name and demographics ▪ Incident type (e.g. wellness check, business entrance obstruction)

Table 2. Data management system use pertaining data analysis, data visualization, and data management.

Category	Functionality requirement
Data analysis and visualization	▪ Download raw data in Excel files and CSV files and customize file downloads to specify fields included, date ranges, etc. ▪ Within the data management system, display easy-to-understand graphs and charts of service or contract data that are relevant to each individual staff member ▪ Customize and generate reports that yield performance measures or deliverables
Data management	▪ Display or hide specific data fields based on staff credentials ▪ Flag and prompt a correction for missing or incomplete data ▪ Retain historical data entries (e.g. prior service referrals) ▪ Store consent forms, sign-in sheets, and other scanned documents ▪ Provide mobile database access that allows staff to easily record data in the field ▪ Provide a high level of privacy security that complies with the Health Insurance Portability and Accountability Act (HIPAA), Confidentiality of Substance Use Disorder Patient Records (42 CFR Part 2), and Criminal Justice Information Services (CJIS). ▪ Issue reminders for MACRO staff regarding upcoming tasks or clients ▪ Identify and merge duplicate client records ▪ Allow for staff to communicate with local service referrals securely and safely regarding a client's program interaction.

D. Data Access:

The OFD MACRO Program will take special care to ensure that data are only accessed on a need to know and right to know basis, meaning that individuals will only be able to access information within the data management system that is essential to their job function. The Julota platform allows administrators to restrict access to client records and individual fields within client records for individual staff members based on their pre-determined access requirements. For example, a MACRO Community Intervention Specialist will only have access to service delivery records for his or her clients; the Community Intervention Specialist will not have access to service delivery records for clients being served by other Emergency Response Programs. Additionally, Community

Intervention Specialist will only have access to data records pertaining to services the client is receiving from the Community Intervention Specialist directly; the Community Intervention Specialist will not be able to view records from other service providers that are delivering services to the same client.

Only MACRO Program leadership (currently four staff members) will have access to all data across providers (including individual-level client data) to allow for quality assurance reviews and technical assistance. All other administrative staff within the MACRO Program will only have access to aggregate service delivery data to observe overall trends and progress towards meeting stakeholder and grant deliverables. Unauthorized use of the system by any staff person with any level of access will lead to disciplinary action that may include retraining, suspension, or termination

E. Data Protection:

Julota data is backed up and AES-256 encrypted daily and stored off-site in 3 different geographic locations for redundancy and for at least 3 years up to 10 years where required by law. Data can only be accessed by Users governed by the Oakland Fire Department that must log in through a Multi-Factor Authentication process. Julota does not support access to the platform unless such access satisfies industry standard practices of Multi-Factor Authentication. Oakland Fire Department's Julota Administrator will be responsible for granting and revoking access to data. Julota maintains a full audit trail of all activity in the system. This audit trail will be available to Oakland by request.

F. Data Retention:

Julota maintains records per the SaaS agreement (included as attachment) signed by the City of Oakland and all necessary laws and regulations associated with Health Insurance Portability and Accountability Act (HIPAA), Confidentiality of Substance Use Disorder Patient Records (42 CFR Part 2), and Criminal Justice Information Services (CJIS). Data retention requirements can be configured to meet the needs of the City of Oakland within and respective of those laws and regulations. The Julota software retains data in compliance with state and federal requirements. Data is retained for the duration of the 1-year contract for the purpose of an Annual Impact Report as expected by Oakland City Council as stated in Resolution 88553 and for monthly and annual performance measure reporting requirements for a federal grant from the Substance Abuse and Mental Health Services Administration (SAMHSA) under the U.S. Department of Health and Human Services.

G. Public Access:

Information inside of Julota is not accessible by the public unless granted authorization to access by the Oakland Fire Department or if given information via an authorized user. There will be absolutely no public access to the raw data in this system. As with any government record, a member of the public may submit a Public Records Act Request,

but only aggregated data with no PII would be released subject to any applicable federal, state, and local privacy and/or confidentiality laws.

Aggregated data from this system (e.g. how many individuals were served in a specific strategy during a specific time period) will be available in periodic impact reports which are also made available on the in tables, charts, or dashboards in public reports or MACRO's public website.

H. Third Party Data Sharing:

Julota will be administered by the MACRO team and staff of the Oakland Fire Department. Primary users will be the MACRO team members. Oakland Fire Department will be responsible for granting user access and setting appropriate permissions for access to data in Julota.

No other city departments will have access to this data and no third party has been contracted to evaluate this data. The MACRO Program will use the data in this system for evaluation purposes to examine the efficacy of the MACRO Program. If external parties are involved for evaluation purposes, these parties will only have access to the aggregate level or individual level data for individuals who sign a consent form allowing their data to be shared with a third-party evaluator. For clients who do not sign a consent form, data from the data management system will only be provided to a third-party evaluator without individual identifiers or in aggregate form.

I. Training:

MACRO Program leadership and MACRO Responders will attend one 3-hour training sessions for the Julota platform, which will review the Julota system's user interface and review tips and tricks for training end users. In addition, MACRO staff will be required to attend annual HIPAA training to understand the sensitivity of the PII that would be entered or received in the Julota platform. Furthermore, all MACRO leadership and responders have attended trainings on the platforms that provide data that will populate into the Julota program. This includes CHR, 911 Dispatch information, and ESO.

Touchphrase Development, LLC will provide technical assistance, a phone number for trouble-shooting, and other supportive services for the Julota software. This is further outlined in the *TouchPhrase HIPAA Security Rule Policies and Procedures*. This will include trainings specific to need and use of specific interactions with clients, ongoing one-on-one training, support, and technical assistance. All trainings will specify appropriate usage of the system pertaining to data privacy and consequences of inappropriate system usage, which could include termination cessation of partnership with the local service provider and, with respect to City employees, discipline up to and including termination.

J. Auditing and Oversight:

The MACRO Program leadership staff will be responsible for ensuring that the Surveillance Use Policy is followed by internal staff and staff from partner organizations. All actions in the system (add, edit, delete, view, etc.) are accessible through audit log reporting built into the system for administrator monitoring. Any indication of inappropriate system usage will be thoroughly investigated by MACRO leadership staff in consult with the City Attorney's Office. Inappropriate system usage could result in termination cessation of partnership with the local service provider and, with respect to City employees, discipline up to and including termination.

K. Maintenance:

Maintenance and security management of the architecture of the Julota system is the responsibility of Julota and part of the contractual obligations assigned through the Software as a Service (SaaS) agreement. Touchphrase Development, LLC's security mechanisms and procedures comply with HIPAA amendment and are audited by Touchphrase Development's HIPAA Security Official or senior member of the IT team. That external individual will be responsible for overseeing compliance of Touchphrase Development policies and procedures by reviewing records of information system activity for inappropriate use on an "need to know" and "right to know" basis to ensure no inappropriate access is taking place within our systems which house the electronic protected health information. A written account of audits is kept on within Touchphrase Development's Access Monitoring Log as needed indicating when the audit was done, what was audited, and who conducted the audit. This can be referenced in the *TouchPhrase HIPAA Security Rule Policies and Procedures*. All City of Oakland MACRO Program staff will sign a non-disclosure agreement in addition to secure PII.

City of Oakland

Surveillance Impact Report for Julota;

Used by the Oakland Fire Department MACRO Program

A. Description:

The Julota platform is an interoperability case management platform that allows different data systems to connect around individuals. It provides teams with a comprehensive historical record of the individual with data from multiple sources, to determine the best care needed, and allows teams to receive proactive updates as individuals are engaging community organizations across the continuum of care.

The Oakland Fire Department MACRO (Mobile Assistance Community Responders of Oakland) Program will be using the platform to collect and share data on the individuals identified and served through 911 dispatch, community requests, and self-dispatched incidents from the MACRO Responder crews. They will address non-violent law enforcement calls better suited for community resources to provide a more compassionate care first response model for community members in dire need. The purpose of the MACRO Program is to ultimately reduce responses by police and reduce arrests, reduce negative interactions between Black, Indigenous, and People of Color (BIPOC) and the Oakland Police, and increase access to community-based services for impacted individuals and families.

B. Purpose:

The purpose of this case management platform is for the Oakland Fire Department MACRO Program to track service referrals and outcomes for individuals and families engaged in MACRO services and receive local service referrals from a MACRO EMT or MACRO Community Intervention Specialist. Typically, the local service referrals include local organizations that provide individualized care that ranges from behavioral health, food assistance, housing support, substance abuse, justice involvement, or any combination of the aforementioned.

The case management platform will be used by specific and limited MACRO staff to track engagement, milestones, and outcomes for individual clients as well as attendance, duration, and feedback of local services. Limited, leadership staff within the MACRO Program will use the system to ensure quality of local services and to improve on the quality of local service referrals to community members in need. The list of local service providers includes many players at the state, county, and municipal level as well as public-private partnerships and local non-government organizations. This group of providers also can fluctuate based on resources, creating a need for a program such as the OFD MACRO Program to maintain reliability of referrals to Oaklanders in need without compromising staff resources. The Julota case management platform allows the MACRO Program a simple, secure, and effective communication across the continuum of care while managing a fluctuating rolodex of community partners.

The MACRO Program will use the Julota case management platform to monitor aggregate service referrals, data capture of each incident, quality of service referral programs, and outcome data, to track the program deliverables as specified by various grant funds and stakeholder interest. The Julota platform will also be used to provide quality improvement of services, identify challenges with program referrals and programmatic gaps that require remediation. The MACRO Program's staff will use the system to gain and store consent of information documents, communicate with other providers such as case managers, and provide the best blend of resources based on individual needs and experiences as informed by the Julota platform aggregating essential information. Finally, service delivery and outcomes data will be available for program evaluation and delivery of program efficacy to local stakeholders such as the MACRO Advisory Board, Oakland City Council, Oakland Mayor, surrounding municipalities, and, of course, the Oakland community.

C. Location:

Julota is a cloud-based system that will be used for data collection and reporting. No software is installed locally. The system is accessed through a unique URL for Oakland Fire Department. Julota is a software program under the company, Touchphrase Development, LLC, which is based in Colorado Springs, Colorado, 80907.

The MACRO Program will be utilizing the Julota platform when entering data on each incident that occurred earlier in the day, either on secure devices within authorized MACRO vehicles on private servers or in MACRO facility headquarters, with encrypted and protected devices. The MACRO vehicles will only operate within Oakland city limits.

D. Impact:

The aggregation of demographic, service delivery, and outcome data on individual clients receiving services through the MACRO Program in a single data management system poses the following potential risks:

- Data breach: A staff member could accidentally or purposefully download and share client data with unauthorized users, compromising client privacy. Alternatively, a third party could hack into the data management system to access records without authorization.
- Subpoena or public data request: The MACRO Program could be required by law to release individual client records to an outside agency, compromising client privacy.

In a situation where individual data were released to a law enforcement agency, it is possible that the data could be used to support law enforcement claims regarding an individual being involved in violent activity due to the individual's enrollment in violence prevention or intervention services.

In a situation where individual data were released to a landlord or commercial party, it is possible that the data could be used to obstruct the client's ability to gain housing access due to discrimination based on the client's private information being used against an application for housing, for example.

To reduce the potential damage of the misuse of a client's aggregation of demographic, service, and outcome data, the MACRO program addresses these risks by authorizing narrow use of the Julota platform to a need to know and right to know basis and a reduced retention of client data.

E. Mitigations:

The OFD MSD will take special care to ensure that data are only accessed on a need to know and right to know basis, meaning that individuals will only be able to access information within the data management system that is essential to their job function. Julota allows administrators to restrict access to client records and individual fields within client records for individual staff members based on their pre-determined access requirements. Only MACRO staff with strict access will have access to data across providers to allow for quality assurance reviews and technical assistance.

To prevent against data breaches, either intentional or unintentional, the MACRO team leadership will extensively train all staff within the MACRO Program who will have access to Julota in proper usage of the system prior to granting access. For more information on this training, please see the *TouchPhrase HIPAA Security Rule Policies and Procedures.*

In situations when the OFD receives a subpoena or public data request pertaining to data in the Julota system, the OFD Program Analyst or other OFD MACRO Program staff will first consult with the City Attorney's Office regarding the OFD's obligation to provide the requested data. If the City Attorney's Office confirms that data must be provided, the OFD will work closely with the City Attorney's Office to redact all Personally Identifiable Information (PII) to maintain client privacy. Additionally, clients will be notified in advance of their data being shared in these very rare, unanticipated circumstances.

Hacking attempts will be prevented through strict data security measures that are discussed further under *Data Security*.

Data will be retained for up to 1 year after an individual completes their interaction the with the OFD MACRO Program. Once the 1-year period has ended, all data on a given individual will be deleted from the Julota system.

F. Data Types and Sources:

Table 1 presents an overview of the type of data that can be collected on an individual with the Julota platform and the source of that information.

Table 1.

Data Type	Data Source
Some Personally Identifiable Information	Survey Conducted by MACRO Responder
Demographics	Survey Conducted by MACRO Responder
History of 911 calls and Emergency Department visits	Community Health Records – Alameda County Care Connect
Vitals, labs, and weights	Survey Conducted by MACRO Responder
Medications used	Survey Conducted by MACRO Responder, Community Health Records – Alameda County Care Connect
Referrals made to community organizations	Community Health Records – Alameda County Care Connect
Referrals to MACRO and the source of referrals	911 Oakland Fire Dispatch, Oakland Police Dispatch
Dates and times of contacts by the MACRO staff	MACRO Survey Records
Participant and staff survey information Identified or suspected needs to address Mental Health, Substance Use, or co-occurring issues	Community Health Records – Alameda County Care Connect

G. Data Security:

The Julota platform will be administered by specified MACRO staff. Primary users will be the MACRO team members. The MACRO Program leadership staff will have responsibility and control to grant narrow user access and set appropriate permissions for access to client data in Julota on a need to know and right to know basis.

Access will be governed by the MACRO Program leadership staff and primarily be granted only to specific members of the MACRO team. MACRO Programmatic staff will have administrative accounts on the Julota platform designated by MACRO Program leadership staff. MACRO Program leadership staff will determine, in consultation with Julota platform support staff, what roles and permissions are necessary for the layers of access needed to ensure data integrity, security, and retention.

Julota data is backed up and AES-256 encrypted daily and stored off-site in 3 different geographic locations for redundancy and for at least 3 years up to 10 years where it is required by law. Data can only be accessed by users governed by the MACRO Program leadership staff that must log in through a Multi-Factor Authentication process. Julota does not support access to the platform unless such access satisfies industry standard

practices of Multi-Factor Authentication. The MACRO Program's singular Julota Administrator will be responsible for granting and revoking access to data.

Julota maintains a full audit trail of all activity in the system. This audit trail will be available to the Oakland Fire Department MACRO Program leadership by request to Touchphrase Development, LLC.

H. Fiscal Cost:

The fiscal cost of Julota will be approximately $48,000 and it will be sourced from the General Funds granted to the MACRO program by Oakland City Council in September 2021 under Resolution 88553. If the MACRO Program is approved to continue past its Pilot period or the MACRO program concludes a year of working with the Julota program, there is an opportunity to renew the contract for another year if the Julota platform is considered successful, useful, secure, and effective. The cost of the Julota platform would then cost an additional $48,000.

I. Third Party Dependence:

All data collected will be stored in Julota and be managed by the SaaS agreement executed with the City of Oakland. This can be further understood in the contract document Schedule E – Project Consultant Team Listing which verifies no subconsultants under the Touchphrase Development contract with the MACRO Program.

J. Alternatives:

The only comparable alternative on the market for this kind of program is FirstWatch, although that software does not bridge social entities in the continuum of care.

Without the Julota program altogether, the MACRO Responders would be forced to input information manually which would lead to longer wait times for community members seeking to interact with the MACRO Program, potentially fewer community members receiving time and attention from the MACRO teams, more intake forms that do not exchange vital information that could save community members time and resources, more forms would take the MACRO teams out of the field which again would lead to fewer community members receiving care, and a potential for less data collection compliance. Multiple intake forms would create more opportunities for human error as the crews input information from their calls at the end of every shift.

K. Track Record:

The Julota platform is used by many other Alternative Emergency Response Programs (AERP) across the United States, with like-minded missions with the MACRO Program. Those 58 other communities include, but are not limited to: Colorado Springs, Colorado; El Paso, Texas; San Juan Island, Puerto Rico; Chesapeake, Virginia; Denton, Texas; Buncombe County, North Carolina; Chatham County, Georgia; Durham County EMS,

North Carolina; Seattle and King Counties Public Health, Washington; Pittsburgh, Pennsylvania; and Tulsa, Oklahoma.

The Julota Platform has also received positive testimonials from other EMS leaders, who have had positive implementation of the product for their needs. They are included below.

“The county gave us six months to develop the MIH program. Like most EMS, our data systems were incident-based, but with MIH we needed to keep track of who we saw, how many times and what we saw them for. We also needed to be able to share that information. Julota has worked hard to create a data- sharing program that works for us. They have created bridges with other software vendors that serve different parts of the healthcare system. One software that is focused on hospital emergency visits and Julota receives data from that source, so we are alerted to when one of the patients we serve has gone to the emergency room. Another software collects data for 911/EMS, and Julota gets data from that source. It also integrates EHR data from hospitals,” stated Data Yost, Chief Operating Officer of Northwest Medical in Kirkland, Washington.

“Peace Island Medical Center has embraced the Community Health Needs Assessment process as a means of realizing our mission. Our mission includes building a strong healthy community by engaging with our community partners to identify disparities and to prioritize community health needs. Julota provides our community a common information exchange that flows us to track coordination of referrals to address social and economic health needs for our patients outside the hospital walls. Healthier communities enable all of us to rise to a batter life. Julota is an important community connects technology that will assist us in creating a better future for our community,” shared Beth Williams-Gieger, Director of Administrative Services for Peace Island Medical Center of Friday Harbor, Washington.

HIPAA –SECURITY RULE
POLICIES AND PROCEDURES

Policies and Procedures for the:

18 Standards and 44 Implementation Specifications of the HIPAA Security Rule

Touchphrase Development, LLC
1755 Telstar Dr., Suite 300
Colorado Springs, CO 80907

Brian L Tuttle, CHP, CPHIT, CBRA, CHA, CISSP, CCNA

Personal and Confidential

Revision 1: August 2016

Table of Contents

HIPAA Security Rule: Administrative Safeguards

Standard: Assigned Security Responsibility

Implementation Specification: *Assigned Security Responsibility*

Assigned Security Responsibility		
Safeguard: Administrative	**Federal Register**	**Required/Addressable**
Assigned Security Responsibility	68 Federal Register 8377 45 CFR 164.308 (a)(1)(ii)(A)	Required

Requirement: Identify the security official who is responsible for developing and implementing the policies and procedures required by the Security Rule for the protection of electronic health information.

Policy: Our business will designate a security official to be the go to person who will have overall responsibility to protect the confidentiality, integrity, and availability of protected health information and to guide our business through compliance activities and meet relevant standards and regulations.

Procedures: We have designated Michael Schaedel to be our HIPAA security official. Our Security Official is the go-to for any compliance questions or issues, including:

- Developing and implementing security policies and procedures in accordance with the HIPAA Security Rule and all other applicable laws;
- Providing leadership and assume accountability for compliance with the HIPAA Policies and Procedures related to security;
- Coordinating risk assessment and risk management activities to ensure ongoing identification of threats to the confidentiality, integrity and availability of PHI and selection of appropriate safeguards to manage and reduce risks;
- Ensuring that operations comply with policies and procedures related to security and that security policies, procedures, and practices are revised as needed;
- Reviewing and investigating all security incidents and ensuring that response and reporting procedures are followed and that harm caused by security incidents is mitigated to the extent practicable;
- Cooperating with oversight agencies in any investigations of security violations;

- Developing and conducting training on and fostering awareness of security policies and procedures to ensure that all members of the workforce, including management, receive adequate and appropriate security training;
- Ensuring that all documentation required by the HIPAA Security Rule is created and maintained for six years from the date it was created or was last in effect, whichever is later;
- Serving as an internal and external liaison and resource with outside entities (including business associates, technology vendors, trustees, and other parties) to ensure that security practices are implemented, consistent and coordinated.

HIPAA Security Rule: Administrative Safeguards

Standard: Security Management Process

Implementation Specification: *Risk Analysis/Assessment*

Risk Analysis/Assessment		
Safeguard: Administrative	**Federal Register**	**Required/Addressable**
Security management process	68 Federal Register 8377 45 CFR 164.308 (a)(1)(ii)(A)	Required

Requirement: Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.

Policy: We conducted a third party risk assessment on August 22nd, 2016 to review our HIPAA policies.

We will reassess at least every year or whenever a new regulation affecting the business requires compliance.

We will conduct a third party external or an internal HIPAA audit every year to ensure our business is taking reasonable and appropriate actions regarding the security of electronic protected health information.

Procedure: We analyzed our weaknesses in business workflow and procedures, and consulted the risk analysis reports, audit comments, security requirements, and results of security assessment prior to completing our policies and procedures.

We identified any history of attacks, including those caused by natural disasters, disgruntled employees, water damage, electrical outages, viruses, HIPAA concerns, and current controls in place. Our findings are included in our risk assessment report completed on August 22nd, 2016 by outsourced consultant Brian L Tuttle with over 13 years of experience in health IT and HIPAA compliance.

We rated the likelihood of each risk, including potential contingencies and potential issues, on a scale of 1 to 5, with 1 being least likely and 5 being highly likely, and developed steps to mitigate the future likelihood of any potential risk.

**These policies and procedures were developed as a result of the risks we discovered in our risk analysis and the need to control and mitigate those risks and ensure all implementation specifications are addressed.

HIPAA Security Rule: Administrative Safeguards

Standard: Security Management Process

Implementation Specification: *Sanction Policy*

Sanction Policy		
Safeguard: Administrative	**Federal Register**	**Required/Addressable**
Security management process	68 Federal Register 8377 45 CFR 164.308 (a)(1)(ii)(C)	Required

Requirement: Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.

Policy: Our business has implemented a sanction policy to safeguard confidential health information in oral, written, and electronic forms. Workforce members are responsible for complying with our HIPAA Security policies and procedures as well as information contained within the confidentiality agreement. Failure to do so may result in disciplinary action, up to and including termination of employment.

Procedures: All workforce members including contracted employees will receive training on our policies and procedures prior to adoption of new policies or modification of existing policies.

As part of new employee orientation, all new workforce members are trained for HIPAA, required to sign our employee handbook, confidentiality agreement and abide by these written policies.

Sanctions: Any wrongful disclosure of private health information will lead to **immediate** termination of employee or breach of business associate agreement for our contractors.

If an employee wrongfully discloses private health information inadvertently, a warning will be issued. These measures are consistent with what is contained within our confidentiality agreement and employee handbook.

Any contractors working on our behalf are beholden to the bylaws contained within HIPAA as a “business associate”.

HIPAA Security Rule: Administrative Safeguards

Standard: Security Management Process

Implementation Specification: *Information System Activity Review*

Information System Activity Review		
Safeguard: Administrative	**Federal Register**	**Required/Addressable**
Security management process	68 Federal Register 8377 45 CFR 164.308 (a)(1)(ii)(D)	Required

Requirement: Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

Policy: Where applicable our business will safeguard electronic protected health information and regularly review records of information activity, such as audit trails, system logs, access reports, and security incident tracking reports, for inappropriate use. Our business does not accept unauthorized snooping or peeking into any medical records, regardless of their public or private status.

We will impose sanctions on any workforce member who violates this policy.

Procedure: Our HIPAA Security Official or member of the IT team will be responsible for overseeing compliance of our policies and procedures by reviewing records of information system activity for inappropriate use on an "as needed" basis to ensure no inappropriate access is taking place within our cloud based software which houses protected health information.

As needed a written account of audits is kept on within our *Access Monitoring Log* indicating when the audit was done, what was audited, and who conducted the audit.

Any of our staff members or contractors privy to private health information (or sensitive data) are subject to system use auditing to ensure access to patient information is appropriate.

HIPAA Security Rule: Administrative Safeguards

Standard: Workforce Security

Implementation Specification: *Authorization and/or Supervision*

Authorization and/or Supervision		
Safeguard: Administrative	**Federal Register**	**Required/Addressable**
Workforce security	68 Federal Register 8377 45 CFR 164.308 (a)(3)(ii)(A)	Addressable

Requirement: Implement policies and procedures to ensure that all workforce members have appropriate access to confidential health information and to prevent those workforce members who do not have access from obtaining it.

Policy: Users are only granted the minimum necessary access to perform job function. This applies both to paper based private health information (PHI) access and electronic private health information access (ePHI) our clients maintain.

Procedure: Our staff and contractors are only granted access to private health information based on the "minimum necessary" principle.

"Minimum necessary" means that our Security Official or IT management only grants access to staff or contractors for the specific areas within the database needed to perform job function.

Considering our business operates as a software development group, all of our developers and support need full access into the systems to perform job function.

However, staff member and contractor access is only granted with final approval of the HIPAA Security Official and user access can be monitored via auditing capabilities within the databases.

When accessing customer systems in a support role, our staff members are only granted access with permission of the customer and shadow the customer to assist the customer's need.

HIPAA Security Rule: Administrative Safeguards

Standard: Workforce Security

Implementation Specification: *Workforce Clearance Procedure*

Workforce Clearance Procedures		
Safeguard: Administrative	**Federal Register**	**Required/Addressable**
Workforce security	68 Federal Register 8377 45 CFR 164.308 (a)(3)(ii)(B)	Addressable

Requirement: Determine that the access of a workforce member to confidential health information is appropriate.

Policy: At the security official's discretion or management, a background check will be authorized for any new employees or contractors.

Procedures: Our business analyzes job responsibilities of each workforce member or contractor on an individual basis.

As part of our hiring procedures, we will:

- Require a written application for employment and conduct a criminal background check for any staff member privy to protected health information
- Require proof of citizenship or resident alien status
- Confirm prior employment history
- Request professional/personal references and contact those references
- Confirm educational history and practicing credentials
- Confirm application statements, as appropriate.

Our business also will require that workforce members provide:

- Federal and state tax withholding - Social Security number -any change in immigration status if not a US citizen.

HIPAA Security Rule: Administrative Safeguards

Standard: Workforce Security

Implementation Specification: *Termination Procedures*

Termination Procedures		
Safeguard: Administrative	**Federal Register**	**Required/Addressable**
Workforce security	68 Federal Register 8377 45 CFR 164.308 (a)(3)(ii)(C)	Addressable

Requirement: Terminate access to confidential health information when the employment of a workforce member ends or as required by determinations made as part of our workforce clearance procedures.

Policy: It is our company policy to make every effort to preserve the relationship between employee and employer. We also acknowledge that there may be voluntary and involuntary reasons for termination of employment. Regardless of the cause, the employee's access to confidential health information will cease within **2 hours** of termination.

Procedures: We analyzed job responsibilities of workforce members and contractors. We incorporated those responsibilities into job descriptions prior to issuing a clearance for work on client systems. In the event those clearances change through termination of employment or contract, the following will occur:

- We will explain that authorization for access to electronic protected health information has changed and the user ID and password have been terminated
- We will follow the steps within our *termination checklist*
- Workforce member will be reminded of our sanction policy for a security incidents resulting from an unauthorized workforce member attempting to gain access to client protected health information, and of the potential criminal and civil penalties for a privacy breach or unauthorized disclosure of protected health information (even after employment ends).

HIPAA Security Rule: Administrative Safeguards

Standard: Information Access Management

Implementation Specification: *Isolating Clearinghouse Functions*

Information Access Management		
Safeguard: Administrative	**Federal Register**	**Required/Addressable**
Isolating Healthcare Clearinghouse Functions	68 Federal Register 8377 45 CFR 164.308 (a)(4)(ii)	Required
Requirement: Isolate Clearinghouse Functions Touchphrase does not function as a clearinghouse in any way		

HIPAA Security Rule: Administrative Safeguards

Standard: Information Access Management

Implementation Specification: *Access Authorization*

Access Authorization		
Safeguard: **Administrative**	**Federal Register**	**Required/Addressable**
Information access management	68 Federal Register 8377 45 CFR 164.308 (a)(4)(ii)(B)	Required

Requirement: Authorize access to confidential health information consistent with your privacy rule.

Policy: Each workforce member is responsible for complying with our policies and procedures for accessing workstations, transactions, programs, processes, and other mechanisms used in the practice. Outside vendors who require access must be subject to the business associate agreement, with an obligation to comply with the Security Rule, as provided for in the HITECH Act provisions of the American Recovery and Reinvestment Act of 2009, signed into law by President Obama on February 17, 2009 and the provisions within the HIPAA Omnibus Rule of 2013.

Procedure: When accessing customer systems in a support role, our staff members are only granted access with permission of the customer and shadow the customer to assist the customer's need.

All access to our internal systems containing private health information is granted by the HIPAA Security Official or member of the IT staff and based upon the minimum necessary standard. "Minimum necessary" means that our Security Official only grants access to staff or contractors for the specific areas within the database needed to perform job function. Considering our business operates as a software development group, all of our developers and support need full access into the systems to perform job function.

However, staff member and contractor access is only granted with final approval of the HIPAA Security Official and user access can be monitored via the auditing capabilities within the databases.

HIPAA Security Rule: Administrative Safeguards

Standard: Information Access Management

Implementation Specification: *Access Establishment and Modification*

Establish and Modify Access		
Safeguard: **Administrative**	**Federal Register**	**Required/Addressable**
Information access management	68 Federal Register 8377 45 CFR 164.308 (a)(4)(ii)(C)	Addressable
Requirement: Implement policies and procedures for how the workforce will be granted access (via workstation, transaction, program, or other mechanism). **Policy:** Only persons authorized to modify electronic protected health information may do so. **Procedure:** Each workforce member or contractor is granted the minimum amount of information necessary to complete assigned tasks. "Minimum necessary" means that our Security Official or senior member of the IT staff only grant access to staff or contractors for the specific areas within the database needed to perform job function. Our HIPAA Security Official or senior member of the IT staff reviews and modifies user access "as needed" or as part of our termination checklist to ensure there are no unauthorized users within our system. Based upon risk, all access from staff members, contractors, and customers into the backend of the system for development requires a password of at least 8 characters (and complex). "Complex" meaning a number, symbol, and capital letter must be used. *See BYOD policy for personal devices.*		

HIPAA Security Rule: Administrative Safeguards

Standard: Security Awareness and Training

Implementation Specification: *Security Reminders*

Security Awareness and Training		
Safeguard: Administrative	**Federal Register**	**Required/Addressable**
Security awareness and training	68 Federal Register 8377 45 CFR 164.308 (a)(5)(i)	Addressable

Requirement: Implement a security awareness and training program for all members of the workforce (including management).

Policy: Securing our clients' protected health information is more than a policy; it is a primary responsibility of each workforce member who works for us.

Each workforce member and contractor is responsible for complying with these policies and procedures.

To demonstrate our commitment to security we provide a HIPAA security awareness course once per year and upon employment.

Procedure: Upon employment each workforce member must sign off on our employee handbook and our confidentiality agreement which covers HIPAA Security and sanctions. Contractors must also sign off on our confidentiality agreement and our business associate agreement which clearly outlines the responsibilities of business associates to properly secure protected health information.

Staff members are also trained upon hire on the specific support systems used to assist clients with technical issues using our software.

HIPAA training will be conducted upon hire and on an annual basis using any of the following methods (which will be signed off by staff member and contractors):

- Outsourced onsite training
- Seminars
- Web based training, or
- In house training

Any training provided reinforces the individual responsibility aspect of securing protected health information.

HIPAA Security Rule: Administrative Safeguards

Standard: Security Awareness and Training

Implementation Specification: *Protection from Malicious Software*

Protection from Malicious Software		
Safeguard: Administrative	**Federal Register**	**Required/Addressable**
Security awareness and training	68 Federal Register 8377 45 CFR 164.308 (a)(5)(ii)(B)	Addressable

Requirement: Develop procedures for protecting our assets and confidential health information against malicious software.

Policy: We will guard against, detect, and report malicious software, including software that has not yet compromised the system but is suspect.

This includes firewalls, virus protection software, and other measures to protect the confidentiality, integrity, and availability of protected health information.

Procedure: Our system is hosted within an offsite cloud based service which provides enterprise level firewalls as well as intrusion detection to secure our server which resides at the offsite location.

Each workstation or laptop contains anti-virus which is updated and we use Apple products due to the higher levels of inherent security versus Microsoft Windows Operating Systems.

Based on risk, “free” versions of anti-virus are not to be used only robust enterprise level anti-virus (this applies to Microsoft operating systems due to higher risks).

The above also applies to any machines used by contractors to access private health information on behalf of our business.

Workforce members will report immediately any detected virus to the security official.

All staff members are required to sign our Cryptology policy and BYOD policy which outlines the requirements for personal devices used to access, transmit, or maintain electronic protected health information.

HIPAA Security Rule: Administrative Safeguards

Standard: Security Awareness and Training

Implementation Specification: *Login Monitoring*

Login Monitoring		
Safeguard: **Administrative**	**Federal Register**	**Required/Addressable**
Security awareness and training	68 Federal Register 8377 45 CFR 164.308 (a)(5)(ii)(C)	Addressable
Requirement: Protect your assets and confidential health information by monitoring login attempts and reporting discrepancies. **Policy:** Our system containing private health information will monitor failed login attempts. **Procedure:** Any user logging into our system is proactively monitored by our system logging capability and the system will lock out user after no more than 10 failed login attempts for both customer and staff access.		

HIPAA Security Rule: Administrative Safeguards

Standard: Security Awareness and Training

Implementation Specification: *Password Management*

Password Management		
Safeguard: **Administrative**	**Federal Register**	**Required/Addressable**
Security awareness and training	68 Federal Register 8377 45 CFR 164.308 (a)(5)(ii)(D)	Addressable

Requirement: Protect our assets and confidential health information by creating, changing, and safeguarding passwords.

Policy: Our business will create, change, and safeguard user IDs and passwords.

Procedures: Our alpha-numeric passwords will be compatible with those designed by our systems containing private health information (PHI).

Passwords will not relate to the user's personal identity, nor will two members of our staff have the same password.

Each workforce member and contractor is responsible for providing protection against loss or disclosure of any passwords in his or her possession. For example, passwords may not be posted on monitors or under keyboards or disclosed to other workforce members.

Passwords that are forgotten will not be reissued, but rather replaced.

Passwords for staff members may be initially assigned by the HIPAA security official or senior member of the IT staff but must be user selected upon first login.

User logins into the cloud based system containing private health information are monitored proactively by the logging abilities of the system.

Passwords will be revoked immediately when a workforce member or contractor leaves employment.

Users are required to report any compromise of their password to the security official.

Passwords are not to be shared with other workforce members.

Based upon risk, all internal access from staff members and contractors into the backend of the system for development require two factor authentication.

For staff accessing the any systems which access transmit or maintain electronic protected health information (EPHI) a password of at least 8 characters (and complex) is used which is changed every 180 days as a forced system setting.

For customer access into the system a password of at least 8 character (and complex) is also required, customer has ability to change their password voluntarily.

Both front end access and back end access into our system require an SMS token – this provides our system with multi-factor authentication to enhance security at the login level.

“Complex” meaning a number, symbol, and capital letter must be used.

See BYOD policy for personal devices.

HIPAA Security Rule: Administrative Safeguards

Standard: Security Incident Procedures

Implementation Specification: *Response and Reporting*

Security Incident Reporting		
Safeguard: Administrative	**Federal Register**	**Required/Addressable**
Security awareness and training	68 Federal Register 8377 45 CFR 164.308 (a)(6)(ii)	Required

Requirement: Implement policies and procedures to address security incidents.

Policy: We will manage and mitigate the effects of suspected and known security incidents in the business.

Procedures: Our workforce members are responsible for reporting security incidents to the security official as soon as they are recognized. Failure to report such incidents may result in sanctions, as appropriate.

Upon notification of a security incident, the security official will contact the IT department which will attempt to contain the incident and minimize damage to the business systems and data. This is a low risk as no private health information is kept on our local machines, machines are only conduits to access the remote system.

Nonetheless, the security official shall document in a security incident report, the security incident and actions taken to minimize damage to the business computers.

The security official shall maintain a current written security incident log.

The security official shall determine the extent of reporting, including to outside authorities as appropriate, based on business and legal considerations, and in response to HITECH Act breach notification requirements.

The security official will review security safeguard procedures following any security incident, make appropriate changes to minimize recurrence of such incidents, discuss changes with workforce members, and include these actions in the security incident report.

The Breach Notification Policy is also included within this booklet on page 49.

HIPAA Security Rule: Administrative Safeguards

Standard: Contingency Plan

Implementation Specification: *Data Backup Plan*

Data Backup Plan		
Safeguard: **Administrative**	**Federal Register**	**Required/Addressable**
Contingency plan	68 Federal Register 8377 45 CFR 164.308 (a)(7)(ii)(A)	Required
Requirement: Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information. **Policy:** We will ensure our business has the ability to access private health information in the event normal access procedures are down. **Procedure:** Our data hosted within our offsite datacenter is backed up daily and per service level agreement by our cloud based vendor. The Aptible database (which hosts our application) is backed up daily by the vendor to both east coast and west coast of USA for redundancy and disaster recovery All backups go through data integrity checksums and will proactively notify the internal IT department if a failure occurs. Cloud vendor policies on data backup can be ascertained upon request and are contractually bound per service level agreement.		

HIPAA Security Rule: Administrative Safeguards

Standard: Contingency Plan

Implementation Specification: *Disaster Recovery Plan (Contingency Plan)*

Contingency Plan		
Safeguard: **Administrative**	**Federal Register**	**Required/Addressable**
Contingency plan	68 Federal Register 8377 45 CFR 164.308 (a)(7)(ii)	Required

Requirement: Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence, such as fire, vandalism, system failure, or natural disaster, that damage systems containing electronic protected health information.

Policy: Our business will respond to emergencies that may impair the business's computer systems and electronic protected health information.

Procedures: A simple internet connection is all that is needed to securely access the cloud based systems containing our private health information in a secure encrypted manner from the perspective of our customer on the front end as well as our developers on the backend.

The order of importance for our system is clearly understood by our internal IT staff.

Order of importance is:

1. DNS for IP address resolution
2. Internet Service Provider (must be up)
3. Gateway must be active
4. Application server hosting the system
5. Database server hosting the database

HIPAA Security Rule: Administrative Safeguards

Standard: Contingency Plan

Implementation Specification: *Emergency Mode Operation Plan*

Emergency Mode Operation Plan		
Safeguard: Administrative	**Federal Register**	**Required/Addressable**
Contingency plan	68 Federal Register 8377 45 CFR 164.308 (a)(7)(ii)(C)	Required
Requirement: Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in the emergency mode. **Low Risk:** This is not a risk for our business. Accessing our systems containing private health information can only be done in a secure encrypted fashion or from physical onsite login at the datacenter regardless if in emergency mode or not. There is no other way to access our system which maintains the electronic protected health information unless via encrypted channels both from front end as well as back end		

HIPAA Security Rule: Administrative Safeguards

Standard: Contingency Plan

Implementation Specification: *Testing and Revision Procedure*

Testing and Revision		
Safeguard: Administrative	**Federal Register**	**Required/Addressable**
Contingency plan	68 Federal Register 8377 45 CFR 164.308 (a)(7)(ii)(D)	Addressable

Requirement: Implement procedures for periodic testing and revision of contingency plans.

Policy: Our business will ensure data integrity is maintained by testing the database

Procedure: Daily backups are confirmed for success or fail through data integrity checksums and a notification is proactively sent to the IT department in the event of a failure.

A simple internet connection is all that is needed to securely access the cloud based systems containing our private health information in a secure encrypted manner from the perspective of our customer on the front end as well as our developers on the backend.

Our cloud vendor policies on testing and revision can be ascertained upon request, the vendor is contractually beholden to our service level agreement.

HIPAA Security Rule: Administrative Safeguards

Standard: Contingency Plan

Implementation Specification: *Applications and Data Criticality Analysis*

Applications, Data Criticality Analysis		
Safeguard: Administrative	**Federal Register**	**Required/Addressable**
Contingency plan	68 Federal Register 8377 45 CFR 164.308 (a)(7)(ii)(E)	Addressable

Requirements: Assess relative criticality of specific applications and data in support of other contingency plan components.

Policy: We have determined the applications and data that are most critical for operation of the business and have prioritized that to be internet access.

Procedures: Our business clearly understands the priorities in terms of data criticality.

An internet connection is all that our business requires to access our electronic medical records system (which contains electronic private health information) in a secure encrypted fashion.

As previously stated within our *Disaster Recovery Plan* policy on page 23, the order of importance for our system is clearly understood by our internal IT staff.

Order of importance is:

1. DNS for IP address resolution
2. Internet Service Provider (must be up)
3. Gateway must be active
4. Application server hosting the system
5. Database server hosting the database

HIPAA Security Rule: Administrative Safeguards

Standard: Evaluation

Implementation Specification: *Evaluation*

Evaluation		
Safeguard: Administrative	**Federal Register**	**Required/Addressable**
Evaluation	68 Federal Register 8377 45 CFR 164.308 (a)(8)	Required

Requirement: Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently in response to environmental or operational changes affecting the security of electronic protected health information that establishes the extent to which an entity's security policies and procedures meet the requirements of security standards for the protection of electronic protected health information.

Policy: We will re-evaluate, through internal and external audits, all of our security policies and procedures at least every year to determine whether the risks can be reduced or efforts should be increased and new tasks assigned to a workforce member to manage.

Procedures: Our security official will:

- Utilize in-house auditing or outsourced audit services for a full "bird's eye view" of our business.
- Evaluate risks at least every year and whenever the business determines that risks or changes in its operating environment warrant review.

This will apply to IT as well as HIPAA.

HIPAA Security Rule: Administrative Safeguards

Standard: Business Associate Agreement

Implementation Specification: *Business Associate Agreement*

Business Associate Agreements		
Safeguard: Administrative	**Federal Register**	**Required/Addressable**
Evaluation	68 Federal Register 8377 45 CFR 164.308 (b)(1)	Required

Requirement: In accordance with general rules of the security standards, a covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf. This is permissible only if the covered entity obtains satisfactory assurances that the business associate will appropriately safeguard such information in accordance with the standard for business associate contracts or other arrangements under organizational requirements.

Policy: Our business associates may create, receive, maintain, or transmit electronic protected health information on our behalf only if the business obtains satisfactory assurances that the business associate will appropriately safeguard protected health information in accordance with the standard for business associate contracts.

Procedures: In accordance with our policies and procedures, any entity deemed a business associate will be required to sign our business associates agreement accepting liability for any breach of ePHI or PHI.

Our contractors are not only required to sign our business associates agreement but also sign off on our confidentiality/non-disclosure agreement.

Our HIPAA Security Official takes ownership of getting the agreements signed and saved digitally.

HIPAA Security Rule: Physical Safeguards

Standard: Facility Access Controls

Implementation Specification: *Contingency Operations*

Contingency Operations		
Physical Safeguard Standard	**Federal Register**	**Required or Addressable**
Facility access controls	68 *Federal Register* 8378 45 CFR 164.310(a)(2)(i)	Addressable
Requirement: Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data. **Low Risk:** This is not a risk for our business. Accessing our systems containing private health information can only be done in a secure encrypted fashion or from physical onsite login at the datacenter regardless if in emergency mode or not. There is no other way to access our system which maintains the electronic protected health information unless via encrypted channels both from front end as well as back end. In terms of physical access to the building, it is clearly understood which individuals need access, not deemed a risk due to the fact almost all of the protected health information within our organization is cloud based.		

HIPAA Security Rule: Physical Safeguards

Standard: Facility Access Controls

Implementation Specification: *Facility Security Plan*

Facility Security Plan		
Physical Safeguard Standard	**Federal Register**	**Required or Addressable**
Facility access controls	68 *Federal Register* 8378 45 CFR 164.310(a)(2)(ii)	Addressable
Requirement: Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft. **Policy:** We will safeguard its facility and systems equipment from unauthorized physical tampering, and theft. **Procedures:** There is no electronic protected health information (EPHI) in any form at any physical location of the business. Our business does not have a "store front" at this point – completely cloud based. EPHI resides only within the secure offsite datacenter per the sound policies of the datacenter and the vendor policies on physical security can be ascertained upon request. All portable devices used by the business (including BYOD) are encrypted using whole disk encryption as well as file level encryption, this is to protect the information in the event of theft or loss of portable devices.		

HIPAA Security Rule: Physical Safeguards

Standard: Facility Access Controls

Implementation Specification: *Access Control and Validation Procedures*

Access Control and Validation Procedures		
Physical Safeguard Standard	**Federal Register**	**Required or Addressable**
Facility access controls	68 *Federal Register* 8378 45 CFR 164.310(a)(2)(iii)	Addressable

Requirement: Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control and control of access to software programs for testing and revision.

Policy: We will control and validate a person's access to our facility based on that person's role or function.

Procedures: As stated within our *Facility Security Plan* policy on page 30, this is low risk for us based on the way the business functions.

There is no electronic protected health information (EPHI) in any form at any physical location of the business.

Our business does not have a "store front" at this point – completely cloud based.

EPHI resides only within the secure offsite datacenter per the sound policies of the datacenter and the vendor policies on physical security can be ascertained upon request.

All portable devices used by the business (including BYOD) are encrypted using whole disk encryption as well as file level encryption, this is to protect the information in the event of theft or loss of portable devices.

HIPAA Security Rule: Physical Safeguards

Standard: Facility Access Controls

Implementation Specification: *Maintenance Records*

Maintenance Records		
Physical Safeguard Standard	**Federal Register**	**Required or Addressable**
Facility access controls	68 *Federal Register* 8378 45 CFR 164.310(a)(2)(iv)	Addressable
Requirement: Implement policies and procedures to document repairs and modifications to the physical components of a facility, which are related to security (e.g. hardware, walls, doors, and locks). **Not a risk:** Considering private health information resides in an offsite data center this is not deemed a risk to wrongful disclosure of private health information.		

HIPAA Security Rule: Physical Safeguards

Standard: Workstation Use

Implementation Specification: *Workstation Use*

Workstation Use		
Physical Safeguard Standard	**Federal Register**	**Required or Addressable**
Workstation use	68 *Federal Register* 8378 45 CFR 164.310(b)(2)	Required

Requirement: Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation that can access electronic protected health information.

Policy: We have specified appropriate functions to be performed on each workstation in the facility or outside the facility, the manner in which they are to be used.

Procedures:

- Our security official or internal IT department shall be responsible for establishing and implementing workstation use procedures and physical access controls to servers which maintain protected health information
- We shall comply with any software license agreements.
- Our business requires enterprise level antivirus and other protective software tools on each workstation and server.

**Machines are only to be used as needed for work purposes, no social media or any other sort of inappropriate web browsing is permitted while accessing clients' systems containing private health information.

All staff are required to sign the employee handbook which clearly outlines acceptable use, in addition all staff members must sign the Cryptology, BYOD and Telework policy as it relates to personal devices and teleworking.

HIPAA Security Rule: Physical Safeguards

Standard: Workstation Security

Implementation Specification: *Workstation Security*

Workstation Security		
Physical Safeguard Standard	**Federal Register**	**Required or Addressable**
Workstation security	68 *Federal Register* 8378 45 CFR 164.310(c)	Required

Requirement: Implement physical safeguards for all workstations that access electronic protected health information to restrict access to authorized users.

Policy: We make sure that all workstations that access sensitive information are secure, restricting access to authorized users. Workforce members of our business are responsible for complying with our workstation security policy and related procedures.

Procedures: Our security official and IT manager:

- Shall be responsible for and ensure access if appropriate for business associates

In addition:

- Enforces that workforce members shall not display written passwords on or near workstations, desktop surfaces, or in drawers, and shall not share passwords with other workforce members in the business.
- Shall take measures to shield electronic protected health information from unauthorized individuals.

Based on risk our system auto locks or drops to a password protected screen saver in no more than 30 minutes of idle time as a required local system policy

See BYOD policy for personally owned devices.

HIPAA Security Rule: Physical Safeguards

Standard: Devices and Media Controls

Implementation Specification: *Disposal*

Disposal		
Physical Safeguard Standard	**Federal Register**	**Required or Addressable**
Device and media controls	68 *Federal Register* 8378 45 CFR 164.310(2)(i)	Required

Requirement: Implement policies and procedures to address the final disposal of electronic protected health information and the hardware or electronic media on which it is stored.

Policy: We will delete or erase any electronic protected health information prior to final disposal of hardware or electronic media on which it is stored. Workforce members of our business are responsible for complying with our disposal policy and related procedures.

Procedures: HIPAA Security Official or internal IT department dispose of any old business owned media using physical destruction or by logically wiping the drive using a utility if the drive is to be reused or resold.

All machines are maintained within secured areas prior to destruction or logical wiping.

See separate BYOD policy for personally owned devices

HIPAA Security Rule: Physical Safeguards

Standard: Devices and Media Controls

Implementation Specification: *Media Re-Use*

Media Reuse		
Physical Safeguard Standard	**Federal Register**	**Required or Addressable**
Device and media controls	68 *Federal Register* 8378 45 CFR 164.310(2)(ii)	Required

Requirement: Implement procedures for removal of electronic protected health information from electronic media before the media are made available for reuse.

Policy: We will delete any electronic protected health information on electronic media although no media containing electronic protected health information (EPHI) resides at the facility.

Procedure: This is a relatively low risk as our business rarely reuses or hands down machines.

If this is ever done our IT department ensures that the device has the appropriate applications installed and that there is not any electronic protected health information (EPHI) on the device.

In addition, the device is encrypted using whole disk encryption if maintaining, accessing, or storing EPHI.

See separate BYOD policy for personally owned devices

HIPAA Security Rule: Physical Safeguards

Standard: Devices and Media Controls

Implementation Specification: *Accountability*

Accountability		
Physical Safeguard Standard	**Federal Register**	**Required or Addressable**
Device and media controls	68 *Federal Register* 8378 45 CFR 164.310(2)(iii)	Addressable
Requirement: Maintain a record of the movements of hardware and electronic media and any person responsible therefore. **No Risk:** Very low risk, each staff member is assigned one machine per user and the staff members are responsible for physical security of the portable machines. To ensure no electronic protected health information (EPHI) is wrongfully disclosed due to theft or loss of device, we force all portable tablets and laptops to be encrypted if accessing, transmitting, or storing EPHI. Staff members who use personal devices are beholden to our BYOD and Cryptology policy. *See separate BYOD policy which all staff members are required to sign.*		

HIPAA Security Rule: Physical Safeguards

Standard: Devices and Media Controls

Implementation Specification: *Data Backup and Storage*

Data Backup and Storage		
Physical Safeguard Standard	**Federal Register**	**Required or Addressable**
Device and media controls	68 *Federal Register* 8378 45 CFR 164.310(2)(iv)	Addressable
Requirement: Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment. **Policy:** Our business ensures that data backups are available in the event they are needed due to a physically mishap with a server **Procedure:** As stated within our Data Backup Plan policy on page 21, our data hosted within our offsite datacenter is backed up daily and per service level agreement by our cloud based vendor. The Aptible database (which hosts our application) is backed up daily by the vendor to both east coast and west coast of USA for redundancy and disaster recovery All backups go through data integrity checksums and will proactively notify the internal IT department if a failure occurs. Cloud vendor policies on data backup can be ascertained upon request and are contractually bound per service level agreement.		

HIPAA Security Rule: Technical Safeguards

Standard: Access Control

Implementation Specification: *Unique User Identification*

Unique User Identification		
Technical Safeguard Standard	**Federal Register**	**Required or Addressable**
Access control	68 *Federal Register* 8378 45 CFR 164.312(a)(1)	Required

Requirement: Assign a unique name and/or number for identifying and tracking user identity.

Policy: Workforce members shall not share or otherwise disclose user IDs or passwords with any other individuals except for the three employees of the business.

Procedures: All internal staff and customers are assigned a unique user ID into any systems containing or accessing electronic protected health information (EPHI).

Customer user ID's are selected by the customer per their preference.

Internal user ID's are manually assigned by the IT department, all user ID's are unique and specific to the user.

Passwords are not shared within the organization. This is forbidden for all internal staff and specifically covered within training and via the employee handbook.

See separate BYOD policy which all staff members are required to sign.

HIPAA Security Rule: Technical Safeguards

Standard: Access Control

Implementation Specification: *Emergency Access Procedure*

Emergency Access Procedure		
Technical Safeguard Standard	**Federal Register**	**Required or Addressable**
Access control	68 *Federal Register* 8378 45 CFR 164.312(a)(ii)	Required
Requirement: Establish and implement, as needed, procedures for obtaining necessary electronic protected health information during an emergency. **Low Risk:** This is not a risk for our business. Accessing our systems containing private health information can only be done in a secure encrypted fashion or from physical onsite login at the datacenter regardless if in emergency mode or not. There is no other way to access our system which maintains the electronic protected health information unless via encrypted channels both from front end customer access as well as back end developer access.		

HIPAA Security Rule: Technical Safeguards

Standard: Access Control

Implementation Specification: *Automatic Logoff*

Automatic Logoff		
Technical Safeguard Standard	**Federal Register**	**Required or Addressable**
Access control	68 *Federal Register* 8378 45 CFR 164.312(a)(iii)	Addressable

Requirement: Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

Policy: Our security official shall make sure that automatic logoff procedures are in place on all systems and devices that provide access to sensitive information, including desktops, laptops, tablets, and handheld devices.

Procedures: Workforce members may frequently leave their workstations without time to completely log off the computer system.

The solution is to activate a password-protected screensaver or auto lock that locks a workstation or portable laptop and prevents unauthorized users from viewing or accessing sensitive information but that does not log the user off the system.

On the user's return to the machine, it is only necessary to reenter the password to gain access as before.

Password protected screen saver or auto lock is set to no more than 10 minutes for all machines accessing private health information, this is a forced local machine policy within the organization.

See BYOD policy for personal devices.

HIPAA Security Rule: Technical Safeguards

Standard: Access Control

Implementation Specification: *Encryption and Decryption*

Encryption and Decryption		
Technical Safeguard Standard	**Federal Register**	**Required or Addressable**
Access control	68 *Federal Register* 8378 45 CFR 164.312(a)(iv)	Addressable

Requirement: Implement a mechanism to encrypt and decrypt electronic protected health information.

Policy: Our business will ensure that any electronic data being transmitted or physically taken offsite are to be secured.

Procedure: We ensure any data transmissions of private health information are secure by:

- Accessing our electronic protected health information (EPHI) system which is located within our offsite datacenter can only be done via secured encrypted channels regardless if accessing from the front end or the back end
- We ensure our electronic private health information database is physically secured at rest within our offsite datacenter behind multiple levels of physical and technological security
- Our database maintaining the EPHI is encrypted at rest on a Linux server inside the physically secured offsite datacenter
- Our database which houses the application is encrypted at rest behind firewall with intrusion detection
- No private health information is ever emailed unless informational (i.e. *please login to system*)
- No EPHI is ever transmitted or locally maintained on any portable devices unless encrypted using whole disk encryption or file level encryption – see *Cryptology Policy*

HIPAA Security Rule: Technical Safeguards

Standard: Audit Controls

Implementation Specification: *Audit Controls*

Audit Controls		
Technical Safeguard Standard	**Federal Register**	**Required or Addressable**
Audit controls	68 *Federal Register* 8378 45 CFR 164.312(b)	Required

Requirement: Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

Policy: Our security official must make sure that workforce members are in compliance with our technical safeguards pertaining to use of electronic systems and networks and access to and protection of electronic protected health information (ePHI).

Compliance means that use and access conform to the scope of each workforce member's responsibilities. The business shall take appropriate actions to correct inappropriate use or accessibility issues or incidents. The security official must make sure that all existing and newly acquired software which is owned by the business and contains private health information has auditing capability, and that the auditing function is enabled.

Procedure: As stated within our Information System Activity Review policy, our HIPAA Security Official or senior member of the IT team will be responsible for overseeing compliance of our policies and procedures by reviewing records of information system activity for inappropriate use on an "as needed" basis to ensure no inappropriate access is taking place within our systems which house the electronic protected health information (EPHI)

As needed a written account of audits is kept on within our *Access Monitoring Log* indicating when the audit was done, what was audited, and who conducted the audit.

Any of our staff members or contractors privy to private health information (or sensitive data) are subject to system use auditing to ensure access to patient information is appropriate.

System auditing is covered within any staff training given, and all staff members are aware of sanctions involving inappropriate access or snooping.

HIPAA Security Rule: Technical Safeguards

Standard: Integrity

Implementation Specification: *Integrity*

Integrity		
Technical Safeguard Standard	**Federal Register**	**Required or Addressable**
Integrity	68 *Federal Register* 8378 45 CFR 164.312(c)(1)	Required

Requirement: Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

Policy: We will ensure data is protected and secured.

Procedure: Our security official or senior IT staff member will ensure that our electronic health records system maintains mechanisms that authenticate the integrity of confidential health information.

This is done by:

- encrypted access/data transmissions,
- encryption of portable tablets and laptops (if maintaining EPHI),
- unique user logins,
- use of the minimum necessary standard,
- system auditing,
- high levels of physical security,
- Encrypted application database at rest on secured Linux server,
- end user tracking mechanisms,
- adequate staff training prior to accessing or entering live data into systems,
- and a strong multi-tiered password policy

HIPAA Security Rule: Technical Safeguards

Standard: Integrity

Implementation Specification: *Mechanisms to authenticate ePHI*

Mechanism to Authenticate Electronic Protected Health Information		
Technical Safeguard Standard	**Federal Register**	**Required or Addressable**
Integrity	68 *Federal Register* 8378 45 CFR 164.312(c)(2)	Addressable

Requirement: Implement electronic controls to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

Policy: Our business will ensure that private health information data be protected to a reasonable and appropriate extent. No private health information is ever to be sent or accessed by our business in a non-secure fashion.

Procedure: Based on risk, there are several areas where information may be damaged or altered, primarily due to human error, data input, or insufficient training. As a result, our organization will ensure that each user has access to system training to the extent needed to maintain the highest level of integrity.

This is to be done using a mentoring program upon employment which is part of mandatory employee orientation.

Training is done specifically for the systems the staff member will be accessing and utilizing as part of their job function.

Additionally, access to systems containing electronic protected health information (ePHI) will be granted to users based upon the minimum necessary standard, which means users are only given the minimum amount of access needed to perform job function.

HIPAA Security Rule: Technical Safeguards

Standard: Person or Entity Authentication

Implementation Specification: *Person or Entity Authentication*

Person or Entity Authentication		
Technical Safeguard Standard	**Federal Register**	**Required or Addressable**
Person or entity authentication	68 *Federal Register* 8378 45 CFR 164.312(d)	Required

Requirement: Implement procedures to verify that a person or entity seeking access to electronic protected health information is the person or entity claimed.

Policy: All of our machines that access private health information or the server that stores private health information will be password protected.

Procedures: Any workforce member or other person requiring access to sensitive information must provide verification that they are the person accessing the system using an assigned user ID and password.

Systems we access must require proof of identity that it can authenticate in one of three ways (we chose the first):

- Something you know (e.g., user ID, mother's maiden name, personal ID number such as a national provider identifier, or password),
- Something you have (e.g., smart card, token, swipe card, or badge), or
- Something you are (e.g., biometric such as a finger image, voice scan, iris or retina scan).

HIPAA Security Rule: Technical Safeguards

Standard: Transmission Security

Implementation Specification: *Integrity Controls*

Integrity Controls		
Technical Safeguard Standard	**Federal Register**	**Required or Addressable**
Transmission security	68 *Federal Register* 8378 45 CFR 164.312(e)(2)(i)	Addressable

Requirement: Implement security measures to guard against unauthorized access to electronic protected health information over an electronic communications network; ensure that electronically transmitted protected health information is not improperly modified without detection until disposed of.

Policy: Very low risk for use but we ensure that sensitive data is protected.

Procedure: Our security official or member of the internal IT department will determine when, how, and if electronic protected health information will be shared over an electronic communications network.

Electronic protected health information will not be altered or destroyed in an unauthorized manner, that is, without knowledge or approval of our security official or internal IT department.

With assignment of user IDs, strong passwords, encrypted channels for transmitting any data containing private health information, encryption of portable devices, and audit trails of user activity where we can determine if any unauthorized changes to electronic protected health information have occurred and by whom.

We will apply appropriate sanctions to the workforce member or contractors that made unauthorized changes and remind workforce members of the need to maintain integrity of electronic protected health information.

HIPAA Security Rule: Technical Safeguards

Standard: Transmission Security

Implementation Specification: *Encryption*

Encryption		
Technical Safeguard Standard	**Federal Register**	**Required or Addressable**
Transmission security	68 *Federal Register* 8378 45 CFR 164.312(e)(2)(ii)	Addressable

Requirement: Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

Policy: Where reasonable we will ensure our business protects and encrypts private health information.

Procedure: We will ensure that any transmissions of electronic private health information (ePHI) be encrypted unless authorized to send in a non-encrypted manner.

This is done by use of secure encrypted remote access to and from our systems maintained within our offsite datacenter which contain electronic protected health information (EPHI), ensuring that no electronic protected health information ever is transmitted, stored, or physically taken offsite without encryption.

See *Cryptology Policy*

Breach Notification Policy

INTRODUCTION

A "breach" under the HIPAA Privacy Rule is an impermissible use or disclosure that compromises the security or privacy of unsecured protected health information (PHI) such that the use or disclosure poses a *significant* risk of financial, reputational, or other harm to the affected person(s). This does not include every impermissible use or disclosure.

UNSECURED PHI

Notification is required only if the breach involved "unsecured" protected health information. Unsecured protected health information (PHI) is PHI that has not been rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of the Department of Health and Human Services.

Acceptable methods of securing PHI include the following:

- Encryption of data at rest that meets the National Institute of Standards and Technology (NIST) Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices.*
- Encryption for data in motion that complies with the Federal Information Processing Standards.
- Storage media has been destroyed in one of the following ways:
    - Paper, film, or other hard copy that has been shredded or destroyed in such a way that it cannot be read or reconstructed.
    - Electronic media that has been cleared, purged, or destroyed according to NIST Publication 800-88, *Guidelines for Media Sanitization,* so that information cannot be retrieved.

The Breach Notification Rule allows three exceptions:

- An *unintentional* acquisition, access, or use of the PHI by a member of the workforce acting under the authority of a covered entity or a business associate.
- An inadvertent disclosure of PHI by a person authorized to access the information to another person authorized to access the information *at the same covered entity or business associate*.
- The covered entity or business associate has a good faith belief that the unauthorized individual who received the information was *unable to retain the information*.

POLICY

In compliance with the Breach Notification Rule, we will make every effort to prevent breaches and to notify affected individuals as soon as possible after we discover a breach of unsecured protected health information. Notifications will comply as much as possible with all requirements included in the Breach Notification regulations.

As part of our periodic HIPAA training, every member of our workforce will be reminded of the responsibility to report breaches or suspected breaches. Training may be an in-house presentation, web casts, and written communications.

When a staff member becomes aware of a breach, he or she must notify the Privacy/Security Officer, who is responsible for investigating the incident, documenting all findings, and initiating notification processes required if the incident meets the above definition. This obligation is included in our periodic HIPAA training.

Copies of all documentation and notices will be maintained.

Any member of our workforce found violating this or any other HIPAA violation will be dealt with according to our HIPAA policy. A team of staff members will review each violation and will determine the course of action to be taken. Discipline to be implemented will be based on the seriousness of the violation and the number of violations committed by the individual.

INDIVIDUAL NOTICE: When a breach is discovered, we will notify each affected individual by first-class mail, or, if the individual has agreed, by e-mail. This notification will be done as quickly as feasible, within a maximum of sixty (60) days after the discovery of the breach.

If we have insufficient contact information for fewer than ten (10) affected by the information, we will use alternative means for contacting them, such as a telephone call or written notification to an alternate address provided by the individual. If we have insufficient contact information for ten (10) or more affected individuals, we will:

- Post the notification on our web site, or
- Provide notification in major print or broadcast media where the affective individuals likely reside.

The notification, regardless of mechanism, will include the following information:

- A description of the breach
- A description of the types of information involved in the breach
- Steps the affected individuals should take to protect themselves from potential harm
- What the business is doing to investigate the breach, mitigate the harm, and prevent further breaches

- Contact information for the business

For notices posted via print or broadcast media or on our web site, we will include a toll-free number for individuals to use to contact the business to determine if their information was included in the breach.

MEDIA NOTICE: If more than five hundred (500) individuals were affected by the breach, we will notify each individual as described above and will also provide notification to prominent media outlets serving the area where our patients reside. This will be in the form of a press release and will be provided within sixty (60) days of the discovery of the breach. It will include the same information used in the individual notice.

NOTICE TO THE SECRETARY: In addition to notifying individuals and, where necessary, the media, this business will notify the Secretary of the Department of Health and Human Services. This includes breaches affecting fewer than five hundred (500) individuals and will be done electronically through the HHS web site, using the form provided. For a breach that affects more than five hundred (500) individuals, this notification will be done within sixty (60) days. If the breach affects fewer than five hundred (500) individuals, the report(s) will be done annually, no later than sixty (60) days after the end of the calendar year in which the breach(es) occurred.

The web site is http://transparency.cit.nih.gov/breach/index.cfm. The form is entitled "Notice to the Secretary of HHS of Breach of Unsecured Protected Information."

NOTIFICATION BY A BUSINESS ASSOCIATE: Our business associates are required to notify us if a breach of unsecured protected health information occurs at their business. This also must be done within sixty (60) days of discovery of the breach. They must provide a list of individuals affected and must provide information to allow us to notify our patients who have been affected. When we receive such information, we will immediately initiate our notification process based on the number of individuals affected. The notification will include information used for other notifications.

OTHER CONCERNS: In addition to recognized breaches, we understand that some uses or disclosures may be perceived by some individuals to constitute a "breach." The individual who is concerned should contact our Privacy Officer, who will explain to the individual that such uses and/or disclosures do not constitute a breach. The Privacy Officer may reference our HIPAA Manual or (preferably) the HIPAA standards.

Breach Notification Template

Business Name: Touchphrase Development, LLC

Business Address: 1755 Telstar Dr., Suite 300, Colorado Springs, CO 80907

A security breach occurred at our business on (date) _____. Our initial investigation suggested that your protected health information may have been compromised.

Type of breach:
__ Theft __Loss __ Improper disposal __ Unauthorized access
__ Hacking/IT incident __Unknown __Other: _____

Location of breached information:
__ Business Associate __ Laptop __ Desktop computer __E-mail
__ Network server __ Other portable electronic device
__ Electronic medical record __ Paper __ Other: _____

Type of information involved in the breach:
__ Demographic information __ Clinical Information
__ Financial information __Other: _____

How the breach occurred:

_____

_____.

Safeguards in place prior to the breach:
__ Firewalls __ Packet filtering __ Secure browser sessions
__ Strong authentication __ Encrypted wireless
__ Physical controls __ Logical access controls __Anti-virus software
__ Intrusion detection __ Biometrics

To further protect your PHI, we recommend that you send a copy of this notice to
__Your bank and credit card companies and national credit bureaus (if financial information was involved)
__ Insurance company (if clinical information was involved)
__ Your Internet service provider (if e-mail information was included)

This business is currently conducting a thorough review to mitigate the situation and to prevent further breaches. We will inform you immediately if we discover additional information of use to you in this situation.

You may contact our Security Officer: Michael Schaedel
By phone at: 719-360-3311