CITY OF OAKLAND

Privacy Advisory Commission

November 3, 2022
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

November 3, 2022
5:00 PM
Teleconference

Meeting Agenda

1. Call to Order, determination of quorum

2. Open Forum/Public Comment

3. Federal Task Force Transparency Ordinance – OPD – Drug Enforcement Agency (DEA), US Marshals Services (USMS), Alcohol Tobacco Firearms (ATF)
    a. Review and take possible action on the proposed memoranda of understanding (MOU) (Attachments 1-3

4. Surveillance Technology Ordinance – OFD - Mobile Assistance Community Responders of Oakland (MACRO)
    a. Review and take possible action on the proposed use policy and impact statement for review and approval to enter into a contract with Julota software from Touchphrase Development, LLC
    (Attachments 4-10)

MEMORANDUM OF UNDERSTANDING

BETWEEN

THE BUREAU OF ALCOHOL, TOBACCO, FIREARMS AND EXPLOSIVES (ATF),

AND

THE OAKLAND POLICE DEPARTMENT (OPD)

This Memorandum of Understanding ("MOU") is entered into by and between the Bureau of Alcohol, Tobacco, Firearms and Explosives ("ATF") and Oakland Police Department ("participating agency") as it relates to the Oakland Crime Gun Enforcement Team (herein referred to as the "Task Force").

BACKGROUND

The Oakland Crime Gun Enforcement Team ("CGET") is primarily tasked with combatting violent crime in the counties of Alameda and Contra Costa by conducting both state and federal investigations with partner agencies targeting those involved in shootings, armed robberies, homicides, and armed narcotics trafficking.

AUTHORITIES

The authority to investigate and enforce offenses under provisions of this MOU are found at 28 U.S.C. § 599A , 28 C.F.R. §§ 0.130, 0.131, and 18 U.S.C. § 3051.

PURPOSE

The Task Force will perform the activities and duties described below:

a. Investigate violent offenders using crime gun intelligence
b. Investigate firearms related violent crime
c. Investigate firearms trafficking
d. Gather and report intelligence data gathered through the National Integrated Ballistic Information Network ("NIBIN")
e. Conduct undercover operations where appropriate and engage in other traditional methods of investigation in order that the Task Force's activities will result in effective prosecution before the courts of the United States and the State of California.

MEASUREMENT OF SUCCESS

The success of Task Force's investigative initiatives will be measured by the reduction of violent crime within the Area of Responsibility (AOR). These measurements would include, but is not

limited to, tracking the successful criminal prosecutions of shooters and their sources of crime guns (federal and state), NIBIN leads, firearm recoveries, firearm traces, and sharing crime gun intelligence (CGI).

PHYSICAL LOCATION

Officers/agents assigned to this Task Force by their employer shall be referred to as task force officers (TFOs). TFOs will be assigned to the ATF Oakland Field Office and will be located at 1301 Clay Street #670S, Oakland, CA 94612.

SUPERVISION AND CONTROL

The day-to-day supervision and administrative control of TFOs will be the mutual responsibility of the participants, with the ATF Special Agent in Charge or his/her designee having operational control over all operations related to this Task Force.

Each TFO shall remain subject to their respective agencies' policies, and shall report to their respective agencies regarding matters unrelated to this agreement/task force. With regard to matters related to the Task Force, TFOs will be subject to Federal law and Department of Justice (DOJ) and ATF orders, regulations and policy, including those related to standards of conduct, sexual harassment, equal opportunity issues and Federal disclosure laws.

Failure to comply with this paragraph could result in a TFO's dismissal from the Task Force.

PERSONNEL, RESOURCES AND SUPERVISION

To accomplish the objectives of the Task Force, ATF will assign 5 Special Agents to the Task Force. ATF will also, subject to the availability of funds, provide necessary funds and equipment to support the activities of the ATF Special Agents and officers assigned to the Task Force. This support may include: office space, office supplies, travel funds, funds for the purchase of evidence and information, investigative equipment, training, and other support items.

Each participating agency agrees to make available to their assigned task members any equipment ordinarily assigned for use by that agency. In the event ATF supplies equipment (which may include vehicles, weapons or radios), TFOs must abide by any applicable ATF property orders or policy, and may be required to enter into a separate agreement for their use.

To accomplish the objectives of the Task Force, the OPD agrees to detail up to 3 fulltime TFOs to the Task Force for a period of not less than two (2) years.

All TFOs shall qualify with their respective firearms by complying with ATF's Firearms and Weapons Policy.

SECURITY CLEARANCES

All TFOs will undergo a security clearance and background investigation, and ATF shall bear the costs associated with those investigations. TFOs must not be the subject of any ongoing investigation by their department or any other law enforcement agency, and past behavior or punishment, disciplinary, punitive or otherwise, may disqualify one from eligibility to join the Task Force. ATF has final authority as to the suitability of TFOs for inclusion on the Task Force.

DEPUTATIONS

ATF, as the sponsoring Federal law enforcement agency, may request at its sole discretion that the participating agency's TFOs be deputized by the U.S. Marshals Service to extend their jurisdiction, to include applying for and executing Federal search and arrest warrants, and requesting and executing Federal grand jury subpoenas for records and evidence involving violations of Federal laws. Such requests will be made on an individual basis as determined by ATF.

A TFO will not be granted Department of Justice legal representation if named as a defendant in a private-capacity lawsuit alleging constitutional violations unless all deputation paperwork has been completed prior to the event(s) at issue in the lawsuit.

The participating agencies agree that any Federal authority that may be conferred by a deputation is limited to activities supervised by ATF and will terminate when this MOU is terminated or when the deputized TFOs leave the Task Force, or at the discretion of ATF.

ASSIGNMENTS, REPORTS AND INFORMATION SHARING

An ATF supervisor or designee will be empowered with designated oversight for investigative and personnel matters related to the Task Force and will be responsible for opening, monitoring, directing and closing Task Force investigations in accordance with ATF policy and the applicable United States Attorney General's Guidelines.

Assignments will be based on, but not limited to, experience, training and performance, in addition to the discretion of the ATF supervisor.

All investigative reports will be prepared utilizing ATF's investigative case management system, (N-Force) utilizing ATF case report numbers. The participating agency will share investigative reports, findings, intelligence, etc., in furtherance of the mission of this agreement, to the fullest extent allowed by law. For the purposes of uniformity, there will be no duplication of reports, but rather a single report prepared by a designated individual which can be duplicated as necessary. Every effort should be made to document investigative activity on ATF Reports of Investigation (ROI), unless otherwise agreed to by ATF and the participating agency(ies). This section does not preclude the necessity of individual TFOs to complete forms required by their employing agency.

Information will be freely shared among the TFOs and ATF personnel with the understanding that all investigative information will be kept strictly confidential and will only be used in furtherance of criminal investigations. No information gathered during the course of the Task Force, to include informal communications between TFOs and ATF personnel, may be disseminated to any third party, non-task force member by any task force member without the express permission of the ATF Special Agent in Charge or his/her designee.

Any public requests for access to the records or any disclosures of information obtained by task force members during Task Force investigations will be handled in accordance with applicable statutes, regulations, and policies pursuant to the Freedom of Information Act and the Privacy Act and other applicable federal and/or state statutes and regulations.

INVESTIGATIVE METHODS

The parties agree to utilize Federal standards pertaining to evidence handling and electronic surveillance activities to the greatest extent possible. However, in situations where state or local laws are more restrictive than comparable Federal law, investigative methods employed by state and local law enforcement agencies shall conform to those requirements, pending a decision as to a venue for prosecution.

The use of other investigative methods (search warrants, interceptions of oral communications, etc.) and reporting procedures in connection therewith will be consistent with the policy and procedures of ATF. All Task Force operations will be conducted and reviewed in accordance with applicable ATF and Department of Justice policy and guidelines.

None of the parties to this MOU will knowingly seek investigations under this MOU that would cause a conflict with any ongoing investigation of an agency not party to this MOU. It is incumbent upon each participating agency to notify its personnel regarding the Task Force's areas of concern and jurisdiction. All law enforcement actions will be coordinated and cooperatively carried out by all parties to this MOU.

INFORMANTS

ATF guidelines and policy regarding the operation of informants and cooperating witnesses will apply to all informants and cooperating witnesses directed by TFOs.

Informants developed by TFOs may be registered as informants of their respective agencies for administrative purposes and handling. The policies and procedures of the participating agency with regard to handling informants will apply to all informants that the participating agency registers. In addition, it will be incumbent upon the registering participating agency to maintain a file with respect to the performance of all informants or witnesses it registers. All information obtained from an informant and relevant to matters within the jurisdiction of this MOU will be shared with all parties to this MOU. The registering agency will pay all reasonable and necessary informant expenses for each informant that a participating agency registers.

DECONFLICTION

Each participating agency agrees that the de-confliction process requires the sharing of certain operational information with the Task Force, which, if disclosed to unauthorized persons, could endanger law enforcement personnel and the public. As a result of this concern, each participating agency agrees to adopt security measures set forth herein:

a. Each participating agency will assign primary and secondary points of contact.
b. Each participating agency agrees to keep its points of contact list updated.

The points of contact for this Task Force are:

ATF: The assigned ATF Assistant Special Agent in Charge/ASAC (primary) and the assigned ATF Resident Agent in Charge/RAC of the Oakland/CGET FO (secondary)

Participating Agency: Oakland PD Sgt. Steve Valle (primary) and Oakland PD Sgt. Seth Neri (secondary)

EVIDENCE

Evidence will be maintained by the lead agency having jurisdiction in the court system intended for prosecution. Evidence generated from investigations initiated by a TFO or ATF special agent intended for Federal prosecution will be placed in the ATF designated vault, using the procedures found in ATF orders.

All firearms seized by a TFO will be submitted for fingerprint analysis, DNA and/or for National Integrated Ballistic Information Network (NIBIN) examination as appropriate. Once all analyses are completed, all firearms seized under Federal law shall be placed into the ATF designated vault for proper storage. All firearms information/descriptions taken into ATF custody must be submitted to ATF's National Tracing Center.

JURISDICTION/PROSECUTIONS

Cases will be reviewed by the ATF Special Agent in Charge or his/her designee in consultation with the participating agency and the United States Attorney's Office and appropriate State's attorney offices, to determine whether cases will be referred for prosecution to the U.S. Attorney's Office or to the relevant State's attorney's office. This determination will be based upon which level of prosecution will best serve the interests of justice and the greatest overall benefit to the public. Any question that arises pertaining to prosecution will be resolved through discussion among the investigative agencies and prosecuting entities having an interest in the matter.

In the event that a state or local matter is developed that is outside the jurisdiction of ATF or it is decided that a case will be prosecuted on the state or local level, ATF will provide all relevant

information to state and local authorities, subject to Federal law. Whether to continue investigation of state and local crimes is at the sole discretion of the state or local participating agency.

USE OF FORCE

All fulltime TFOs will comply with ATF and the Department of Justice's (DOJ's) Use of Force orders and policies. TFOs must be briefed on ATF's and DOJ's Use of Force policy by an ATF official, and will be provided with a copy of such policy.

BODY WORN CAMERAS AND TASK FORCE OFFICERS

In accordance with DOJ policy, dated October 29, 2020, Body Worn Cameras (BWCs) may be worn by TFOs operating on a Federal Task Force when their parent agency mandates their use by personnel assigned to the task force. In such cases, the parent agency must formally request to participate in the TFO BWC program and, upon approval, shall comply with all DOJ and ATF policies, and the required procedures, documentation, and reporting while participating on the task force. This provision is only in effect when an Addendum to Task Force Agreements Pertaining to Body Worn Cameras is signed by the participating agency.

MEDIA

Media relations will be handled by ATF and the U.S. Attorney's Office's public information officers in coordination with each participating agency. Information for press releases will be reviewed and mutually agreed upon by all participating agencies, who will take part in press conferences. Assigned personnel will be informed not to give statements to the media concerning any ongoing investigation or prosecution under this MOU without the concurrence of the other participants and, when appropriate, the relevant prosecutor's office.

All personnel from the participating agencies shall strictly adhere to the requirements of Title 26, United States Code, § 6103. Disclosure of tax return information and tax information acquired during the course of investigations involving National Firearms Act (NFA) firearms as defined in 26 U.S.C., Chapter 53 shall not be made except as provided by law.

SALARY/OVERTIME COMPENSATION

During the period of the MOU, participating agencies will provide for the salary and employment benefits of their respective employees. All participating agencies will retain control over their employees' work hours, including the approval of overtime.

ATF may have funds available to reimburse overtime to the State and Local TFO's agency, subject to the guidelines of the Department of Justice Asset Forfeiture Fund. This funding would be available under the terms of a memorandum of agreement (MOA) established pursuant to the provisions of 28 U.S.C. section 524. The participating agency agrees to abide by the applicable Federal law and policy with regard to the payment of overtime from the Department of Justice Asset Forfeiture Fund. The participating agency must be recognized under State law as a law

enforcement agency and their officers/ troopers/investigators as sworn law enforcement officers. If required or requested, the participating agency shall be responsible for demonstrating to the Department of Justice that its personnel are law enforcement officers for the purpose of overtime payment from the Department of Justice Asset Forfeiture Fund. **This MOU is not a funding document.**

In accordance with these provisions and any MOA on asset forfeiture, the ATF Special Agent in Charge or designee shall be responsible for certifying reimbursement requests for overtime expenses incurred as a result of this agreement.

AUDIT INFORMATION

Operations under this MOU are subject to audit by ATF, the Department of Justice's Office of the Inspector General, the Government Accountability Office, and other Government-designated auditors. Participating agencies agree to permit such audits and to maintain all records relating to Department of Justice Asset Forfeiture Fund payments for expenses either incurred during the course of this Task Force or for a period of not less than three (3) years and, if an audit is being conducted, until such time that the audit is officially completed, whichever is greater.

FORFEITURES/SEIZURES

All assets seized for administrative forfeiture will be seized and forfeited in compliance with the rules and regulations set forth by the U.S. Department of Justice Asset Forfeiture guidelines. When the size or composition of the item(s) seized make it impossible for ATF to store it, any of the participating agencies having the storage facilities to handle the seized property agree to store the property at no charge and to maintain the property in the same condition as when it was first taken into custody. The agency storing said seized property agrees not to dispose of the property until authorized to do so by ATF.

The MOU provides that proceeds from forfeitures will be shared, with sharing percentages based upon the U.S. Department of Justice Asset Forfeiture policies on equitable sharing of assets, such as determining the level of involvement by each participating agency. Task Force assets seized through administrative forfeiture will be distributed in equitable amounts based upon the number of full-time persons committed by each participating agency. Should it become impossible to separate the assets into equal shares, it will be the responsibility of all the participating agencies to come to an equitable decision. If this process fails and an impasse results, ATF will become the final arbitrator of the distributive shares for the participating agencies

DISPUTE RESOLUTION

In cases of overlapping jurisdiction, the participating agencies agree to work in concert to achieve the Task Force's goals and objectives. The parties to this MOU agree to attempt to resolve any disputes regarding jurisdiction, case assignments and workload at the lowest level possible.

LIABILITY

ATF acknowledges that the United States is liable for the wrongful or negligent acts or omissions of its officers and employees, including TFOs, while on duty and acting within the scope of their federal employment, to the extent permitted by the Federal Tort Claims Act.

Claims against the United States for injury or loss of property, personal injury, or death arising or resulting from the negligent or wrongful act or omission of any Federal employee while acting within the scope of his or her office or employment are governed by the Federal Tort Claims Act, 28 U.S.C. sections 1346(b), 2672-2680 (unless the claim arises from a violation of the Constitution of the United States, or a violation of a statute of the United States under which other recovery is authorized).

Except as otherwise provided, the parties agree to be solely responsible for the negligent or wrongful acts or omissions of their respective employees and will not seek financial contributions from the other for such acts or omissions. Legal representation by the United States is determined by the United States Department of Justice on a case-by-case basis. ATF cannot guarantee the United States will provide legal representation to any State or local law enforcement officer.

Liability for any negligent or willful acts of any agent or officer undertaken outside the terms of this MOU will be the sole responsibility of the respective agent or officer and agency involved.

DURATION

This MOU is effective with the signatures of all parties and terminates at the close of business on December 31, 2023.

This MOU supersedes previously signed MOUs and shall remain in effect until the aforementioned expiration date or until it is terminated in writing (to include electronic mail and facsimile), whichever comes first. All participating agencies agree that no agency shall withdraw from the Task Force without providing ninety (90) days written notice to other participating agencies. If any participating agency withdraws from the Task Force prior to its termination, the remaining participating agencies shall determine the distributive share of assets for the withdrawing agency, in accordance with Department of Justice guidelines and directives.

The MOU shall be deemed terminated at the time all participating agencies withdraw and ATF elects not to replace such members, or in the event ATF unilaterally terminates the MOU upon 90 days written notice to all the remaining participating agencies.

MODIFICATIONS

This agreement may be modified at any time by written consent of all participating agencies. Modifications shall have no force and effect unless such modifications are reduced to writing and signed by an authorized representative of each participating agency.

SIGNATURES

_____/_____	_____/_____
LeRonne Armstrong Date	Patrick Gorman Date
Chief of Police	Special Agent in Charge, ATF
Oakland Police Department	San Francisco Field Division

FISCAL YEAR 2023

PROGRAM - FUNDED STATE AND LOCAL TASK FORCE AGREEMENT BETWEEN OAKLAND POLICE DEPARTMENT (CA0010900) AND DEA TASK FORCE GROUP (OAKLAND)

This agreement is made this 1st day of October, 2022, between the United States Department of Justice, Drug Enforcement Administration (hereinafter "DEA"), and the Oakland Police Department - ORI# CA0010900 (hereinafter "OPD"). The DEA is authorized to enter into this cooperative agreement concerning the use and abuse of controlled substances under the provisions of 21 USC § 873.

WHEREAS there is evidence that trafficking in narcotics and dangerous drugs exists in the Greater East Bay Area of California and that such illegal activity has a substantial and detrimental effect on the health and general welfare of the people of Alameda, Contra Costa, and Solano Counties, the parties hereto agree to the following:

1 The Task Force Group (Oakland) Task Force will perform the activities and duties described below:

   a. disrupt the illicit drug traffic in the Oakland area by immobilizing targeted violators and trafficking organizations;

   b. gather and report intelligence data relating to trafficking in narcotics and dangerous drugs; and

   c. conduct undercover operations where appropriate and engage in other traditional methods of investigation in order that the Task Force's activities will result in effective prosecution before the courts of the United States and the State of California.

2 To accomplish the objectives of the Task Force Group (Oakland) Task Force, the parent agency agrees to detail one (1) experienced officers to the Task Force Group (Oakland) Task Force for a period of not less than two years. During this period of assignment, the parent agency officers will be under the direct supervision and control of DEA supervisory personnel assigned to the Task Force.

3 The parent agency officers assigned to the Task Force shall adhere to DEA policies and procedures. Failure to adhere to DEA policies and procedures shall be grounds for dismissal from the Task Force.

4 The parent agency officers assigned to the Task Force shall be deputized as Task Force Officers of DEA pursuant to 21 USC § 878.

5 To accomplish the objectives of the Task Force Group (Oakland) Task Force, DEA will assign eight (8) Special Agents to the Task Force. The parent agency agrees to provide and maintain a vehicle for use for each of its assigned Task Force Officers-. DEA will also, subject to the availability of annually appropriated funds or any continuing

resolution thereof, provide necessary funds and equipment to support the activities of the DEA Special Agents and parent agency officers assigned to the Task Force. This support will include: office space, office supplies, travel funds, funds for the purchase of evidence and information, investigative equipment, training, and other support items.

6 During the period of assignment to the Task Force Group (Oakland) Task Force, the parent agency will remain responsible for establishing the salary and benefits, including overtime, of the officers assigned to the Task Force, and for making all payments due them. DEA will, subject to availability of funds, reimburse the parent agency for overtime payments. Annual overtime for each state and local law enforcement officer is capped at the equivalent to 25% of the salary of a GS-12, step 1, of the general pay scale for the rest of the United States. Reimbursement for all types of qualified expenses shall be contingent upon availability of funds and submission of a proper request for reimbursement which shall be submitted monthly or quarterly on a fiscal year basis, and which provides the names of investigators who incurred overtime for DEA during invoiced period, the number of overtime hours incurred, the hourly regular and overtime rates in effect for each investigator, and the total cost for the invoiced period. The parent agency will bill overtime as it is performed and no later than 60 days after the end of each quarter in which the overtime is performed. . ***Note: Task Force Officer's overtime "shall not include any costs for benefits, such as retirement, FICA, and other expenses."***

7 In no event will the parent agency charge any indirect cost rate to DEA for the administration or implementation of this agreement.

8 The parent agency shall maintain on a current basis complete and accurate records and accounts of all obligations and expenditures of funds under this agreement in accordance with generally accepted accounting principles and instructions provided by DEA to facilitate on-site inspection and auditing of such records and accounts.

9 The parent agency shall permit and have readily available for examination and auditing by DEA, the United States Department of Justice, the Comptroller General of the United States, and any of their duly authorized agents and representatives, any and all records, documents, accounts, invoices, receipts or expenditures relating to this agreement. The parent agency shall maintain all such reports and records until all audits and examinations are completed and resolved, or for a period of six (6) years after termination of this agreement, whichever is later.

10 The parent agency shall comply with Title VI of the Civil Rights Act of 1964, Section 504 of the Rehabilitation Act of 1973, the Age Discrimination Act of 1975, as amended, and all requirements imposed by or pursuant to the regulations of the United States Department of Justice implementing those laws, 28 C.F.R. Part 42, Subparts C, F, G, H and I.

11 The parent agency agrees that an authorized officer or employee will execute and return to DEA the attached OJP Form 4061/6, Certification Regarding Lobbying; Debarment, Suspension and Other Responsibility Matters; and Drug-Free Workplace Requirements.

The parent agency acknowledges that this agreement will not take effect and no Federal funds will be awarded to the parent agency by DEA until the completed certification is received.

12 When issuing statements, press releases, requests for proposals, bid solicitations, and other documents describing projects or programs funded in whole or in part with Federal money, the parent agency shall clearly state: (1) the percentage of the total cost of the program or project which will be financed with Federal money and (2) the dollar amount of Federal funds for the project or program.

13 The term of this agreement shall be effective from the date in paragraph number one until December 31, 2023. This agreement may be terminated by either party on thirty days' advance written notice. DEA's support to the Task force, including reimbursement of overtime, is subject to the availability of funds on a fiscal year basis (October 1 through September 30 of the next year). Billing for all outstanding obligations must be received by DEA within 60 days of the end of the fiscal year or within 60 days of the date of termination of this agreement. DEA will be responsible only for obligations incurred by parent agency during the term of this agreement on a fiscal year basis, subject to the availability of funds.

For the Drug Enforcement Administration:

Bob P. Beris
Name

Date

Acting Special Agent in Charge (SAC)
Title

For the Oakland Police Department
(CA0010900)

Name

Date

Title

United States Marshals Service

Fugitive Task Force

Memorandum of Understanding

For Non-Federal Agencies

Rev. 01/2022

PARTIES AND AUTHORITY:

This Memorandum of Understanding is entered into by the [Agency] and the United States Marshals Service (USMS) pursuant to 28 U.S.C. § 566(e)(1)(B). As set forth in the Presidential Threat Protection Act of 2000, codified at 34 U.S.C. 41503, and directed by the Attorney General, the USMS has been granted authority to direct and coordinate permanent Regional Fugitive Task Forces consisting of federal, state, and local law enforcement authorities for the purpose of locating and apprehending fugitives. The authority of the USMS to investigate fugitive matters as directed by the Attorney General is set forth in 28 USC § 566. The Director's authority to direct and supervise all activities of the USMS is set forth in 28 USC § 561(g) and 28 CFR 0.111. The authority of United States Marshals and Deputy U.S. Marshals, "in executing the laws of the United States within a State . . . [to] exercise the same powers which a sheriff of the State may exercise in executing the laws thereof" is set forth in 28 USC § 564. Additional authority is derived from 18 USC § 3053 and Office of Investigative Agency Policies Resolutions 2 & 15. *See also* Memorandum for Howard M. Shapiro, General Counsel, Federal Bureau of Investigation concerning the "Authority to Pursue Non-Federal Fugitives," issued by the U.S. Department of Justice (DOJ), Office of Legal Counsel, dated February 21, 1995; Memorandum concerning the "Authority to Pursue Non-Federal Fugitives," issued by the USMS Office of General Counsel, dated May, 1, 1995; 42 U.S.C. § 16941(a)("The Attorney General shall use the resources of Federal law enforcement, including the United States Marshals Service, to assist jurisdictions in locating and apprehending sex offenders who violate sex offender registration requirements."). Additional authority is derived from the Attorney General's Memorandum, Implementation of National Anti-Violent Crime Initiative (March 1, 1994); Attorney General's Memorandum, Policy on Fugitive Apprehension in FBI and DEA Cases (dated August 11, 1988); Memorandum of Understanding between the Drug Enforcement Administration and the United States Marshals Service (dated September 28, 2018, or as hereafter amended); and Federal Rules of Criminal Procedure 41 – Search and Seizure.

MISSION: The primary mission of the task force is to investigate and arrest, as part of joint law enforcement operations, persons who have active warrants for their arrest. The intent of the joint effort is to investigate and apprehend federal, local, state, tribal, and territorial fugitives, thereby improving public safety and reducing violent crime. Each participating agency agrees to refer cases for which they hold the primary warrant for the subject to the RFTF (Regional Fugitive Task Force) or VOTF (Violent Offender Task Force) for adoption and investigation. Cases will be adopted by the RFTF/VOTF at the discretion of the RFTF/VOTF Chief Inspector/Chief Deputy. Targeted crimes will primarily include violent crimes against persons, weapons offenses, felony drug offenses, failure to register as a sex offender, and crimes committed by

subjects who have a criminal history involving violent crimes, felony drug offenses, and/or weapons offenses. Upon receipt of a written request, the RFTF/VOTF may also adopt non-participating law enforcement agencies in investigating, locating, and arresting their fugitives. Task force personnel will be assigned federal and adopted fugitive cases for investigation. Investigative teams will consist of personnel from different agencies whenever possible. Participating agencies retain responsibility for the cases they refer to the RFTF/VOTF. Federal fugitive cases referred to the task force for investigation by any participating agency will be entered into the National Crime Information Center (NCIC) by the USMS or originating agency, as appropriate. State, local, tribal, or territorial fugitive cases will be entered into NCIC (and other applicable state or local lookout systems) as appropriate by the concerned agency.

SUPERVISION: The RFTF/VOTF may consist of law enforcement and administrative personnel from federal, state, local, tribal, and territorial law enforcement agencies. Agency personnel must be approved by the RFTF/VOTF Chief Inspector/Chief Deputy prior to assignment to the RFTF/VOTF. Agency personnel may be removed at any time at the discretion of the RFTF/VOTF Chief Inspector/Chief Deputy. Direction and coordination of the RFTF/VOTF shall be the responsibility of the RFTF/VOTF Chief Inspector/Chief Deputy. Administrative matters which are internal to the participating agencies remain the responsibility of the respective agencies. Furthermore, each agency retains responsibility for the conduct of its personnel. A Task Force Advisory Committee, consisting of representatives of participating agencies and USMS RFTF/VOTF personnel, may be established at the discretion of the RFTF/VOTF Chief Inspector/Chief Deputy and will meet and confer as necessary to review and address issues concerning operational matters within the RFTF/VOTF.

PERSONNEL: In accordance with Homeland Security Presidential Directive 12, personnel assigned to the task force are required to undergo background investigations to be provided unescorted access to USMS offices, records, and computer systems. The USMS shall bear the costs associated with those investigations. Non-USMS law enforcement officers assigned to the task force will be deputized as Special Deputy U.S. Marshals.

REIMBURSEMENT: If the Marshals Service receives Asset Forfeiture funding for either 1) overtime incurred by state, local, tribal, or territorial investigators who provide full time support to USMS RFTF/VOTF joint law enforcement task forces; or 2) travel, training, purchase or lease of police vehicles, fuel, supplies or equipment for state, local, tribal, or territorial investigators in direct support of state, local, tribal or territorial investigators, the USMS shall, pending availability of funds, reimburse your organization for expenses incurred, depending on which category of funding is provided. Reimbursement of overtime work shall be consistent with the Fair Labor Standards Act. Annual overtime for each state or local law enforcement officer is capped the equivalent 25% of a GS-1811-12 Step 1, of the general pay scale for the Rest of United States. Reimbursement for all types of qualified expenses shall be contingent upon availability of funds and the submission of a proper request for reimbursement which shall be submitted quarterly on a fiscal year basis, and which provides the names of the investigators who incurred overtime for the RFTF/VOTF during the quarter; the number of overtime hours incurred, the hourly regular and overtime rates in effect for each investigator, and the total quarterly cost. The request for reimbursement must be submitted to the RFTF/VOTF Chief

Inspector/Chief Deputy, who will review the request for reimbursement, stamp and sign indication that services were received and that the request for reimbursement is approved for payment. Supporting documentation must accompany requests for reimbursement for equipment, supplies, training, fuel, and vehicle leases.
Reimbursement for other types of qualified expenses (i.e., investigative or travel) shall be contingent upon availability of funds and the submission of a proper request for reimbursement. Task force personnel may incur investigative expenses or may be required to travel outside of the jurisdiction to which they are normally assigned in furtherance of task force operations. State, local, tribal, or territorial task force officers (TFOs) traveling on official business at the direction of the USMS shall be reimbursed directly by the USMS for their authorized travel expenses in accordance with applicable USMS policy, federal laws, rules, and regulations. The request for reimbursement must be submitted to the RFTF/VOTF Chief Inspector/Chief Deputy, or IOD program Chief (i.e., SOIB or OCAG), and must include appropriate supporting documentation.

VEHICLES: Pending the availability of asset forfeiture funding, the USMS may acquire vehicles to be utilized by state, local, tribal, or territorial investigators assigned to the RFTF/VOTF. Vehicles provided by the USMS remain in the control of the USMS and must be used solely in support of RFTF/VOTF operations. The vehicles must be available for exclusive use of the TFOs assigned to the RFTF/VOTF by the undersigned participant agency for the duration of the agency's participation on the task force. If the agency is no longer a participating member of the RFTF/VOTF, any USMS vehicle provided to the agency for use by TFO(s) must be returned to the USMS. Operators of USMS-provided vehicles must adhere to USMS policy regarding the use of government owned vehicles. Any violation of the USMS vehicle policy may result in the vehicle being repossessed by the USMS and the operator and/or agency forfeiting the opportunity to utilize a USMS-provided vehicle in the future. Vehicles provided to state, local, tribal, or territorial investigators may be subject to additional regulations or restrictions pursuant to USMS lease agreements. Replacement or removal of any vehicle provided by the USMS will be at the discretion of the USMS and/or subject to lease agreement terms.

EQUIPMENT: Pending the availability of Asset Forfeiture funding, the USMS may purchase equipment for state, local, tribal, or territorial investigators assigned to the RFTF/VOTF. Equipment purchased by the USMS using Asset Forfeiture funding must be used solely in support of RFTF/VOTF operations. The equipment must be available for exclusive use of the TFOs assigned to the RFTF/VOTF by the undersigned participant agency for the duration of the agency's participation on the task force. If the agency is no longer a participating member of the RFTF/VOTF, any equipment purchased with Asset Forfeiture and provided to TFOs from the agency may be retained by the agency. Equipment provided by the USMS that is not purchased using Asset Forfeiture funding remains the property of the USMS and will be issued to state, local, tribal, or territorial investigators for exclusive use in support of the RFTF/VOTF. If the investigator or agency is no longer a participating member of the RFTF/VOTF, any equipment issued that was not purchased with Asset Forfeiture funding will be returned to the USMS.

BODY-WORN CAMERAS AND TASK FORCE OFFICERS: As per USMS Policy, Body Worn Cameras (BWC) may be worn by TFOs operating on a USMS Task Force when their parent agency mandates their use by personnel assigned to the task force. A partner agency must

formally request to participate in the TFO BWC program and, upon approval, comply with all USMS policies, procedures, documentation, and reporting during their participation. The USMS will inform all partner agencies of which other partner agencies, if any, have been authorized to have their TFOs wear BWCs on the Task Force. Accordingly, all partner agencies should be aware that TFOs may be participating in the TFO BWC program and may be operating with BWCs on USMS task force operations in their agency's jurisdiction. TFOs whose parent agency is not approved for participation in the TFO BWC program are not allowed to deploy with BWCs on USMS missions. As of September 2021, DOJ law enforcement components are implementing BWC into their agency missions. Accordingly, all partner agencies should be aware that USMS and other DOJ law enforcement personnel may be operating with BWCs on USMS task force operations.

RECORDS, REPORTS, AND TESTIMONY: After the RFTF/VOTF has adopted a warrant, all investigative reports, evidence, and other materials generated, seized or collected by the RFTF/VOTF, relating to the fugitive investigation, shall be material within the custody and control of the RFTF/VOTF. Physical evidence, such as drugs, firearms, counterfeit credit cards, and related items may be released to the appropriate prosecuting agency. Records and information obtained during the RFTF/VOTF fugitive investigation are ordinarily not evidence and may not be released unless authorized by the Office of General Counsel (OGC). A participating agency may retain copies of RFTF/VOTF investigative reports, and other documents or materials, but they may be released only upon approval of the USMS (OGC), in consultation with the local U.S. Attorney's Office, if and as applicable. If an applicable state law mandates the release of records or reports pertaining to RFTF/VOTF activities, those documents may only be released after coordination with USMS OGC.

All investigative reporting will be prepared in compliance with existing USMS policy and procedures utilizing USMS case management systems. Every effort should be made to document investigative activities on USMS forms, such as USM-11s and USM- 210s. Reports should never contain information related to sensitive USMS programs that are deemed privileged and not subject to reporting. RFTF/VOTF records and documents, including reports on RFTF/VOTF activity prepared in cases assigned to TFOs, will be maintained in USMS electronic records and/or paper case files. Task force statistics will be maintained in the USMS case management systems. Statistics will be made available to any participating agency upon request. This section does not preclude the necessity of individual TFOs completing forms required by their employing agency. However, reports documenting task force related investigations or activities prepared by a TFO on their parent agency form, or authorized TFO BWC recordings during RFTF/VOTF operations, and any TFO's task force related email or text exchanges are deemed federal records under the control and purview of USMS, regardless of where these records are generated or kept. If an applicable state records law mandates the disclosure of task force records, the parent agency must coordinate with the USMS prior to any proposed disclosure. If information developed during a RFTF/VOTF investigation is included in such a form, the TFO's department will maintain the information as an agent of the RFTF/VOTF. Documents containing information that identifies, or tends to identify, a USMS confidential source, a USMS sensitive

program, or the use of sensitive equipment/techniques shall not be released outside of the USMS unless approved by the Office of General Counsel.

No information related to RFTF/VOTF activities may be disseminated at any time to any third party (including a non-task force law enforcement officer, other law enforcement agency, or prosecutor's office) by any task force member without the express permission of the RFTF/VOTF Chief Inspector/Chief Deputy or his/her designee, in consultation with USMS OGC where appropriate. This prohibition applies to formal and informal communications, as well as reports, memoranda, or other records compiled during the course of RFTF/VOTF operations. This prohibition also applies to information conveyed in the course of testimony. All requests for task-force related testimony requires compliance with the DOJ Touhy Regulations, 28 C.F.R. § 16.21, et seq. TFOs receiving requests to testify in federal or state court must notify the Office of General Counsel.

CONFIDENTIAL SOURCES / CONFIDENTIAL INFORMANTS: Pending the availability of funds, the USMS may provide funding for payment of Confidential Sources (CS) or Confidential Informants (CI). The use of CS/CIs, registration of CS/CIs and all payments to CS/CIs shall comply with USMS policy. USMS payment to an individual providing information or "tip" related to a USMS offered reward on an active fugitive case shall be accomplished by registering the individual or "tipster" through the established USMS CS payment process.

USE OF FORCE: All members of the RFTF/VOTF will comply with their agencies' guidelines concerning the use of firearms, deadly force, and less-than lethal devices, to include completing all necessary training and certification requirements. All members of the RFTF/VOTF will read and adhere to the DOJ Policy Statement on the Use of Less-Than-Lethal Devices, dated May 16, 2011, and their parent agencies will review the Policy Statement to assure that they approve. Copies of all applicable firearms, deadly force, and less-than-lethal policies shall be provided to the RFTF/VOTF Chief Inspector/Chief Deputy and each concerned TFO. In the event of a shooting involving task force personnel, the incident will be investigated by the appropriate agency(ies). Additionally, in the event of a shooting, the required reporting for the FBI National Use of Force Data Collection (NUOFDC) should be accomplished by the involved task force personnel's employing agency when the TFO is inside their primary/physical jurisdiction and by the USMS when the TFO is outside their employing agency's primary/physical jurisdiction. If the employing agency wishes to submit such NUOFDC entries regardless of the physical location of the event, that is allowed under this MOU with prior written notice to the USMS.

NEWS MEDIA: Media inquiries will be referred to the RFTF/VOTF Chief Inspector/Chief Deputy. A press release may be issued, and press conference held, upon agreement and through coordination with participant agencies' representatives. All press releases will exclusively make reference to the task force and participant agencies.

RELEASE OF LIABILITY: Each agency shall be responsible for the acts or omissions of its employees. Participating agencies or their employees shall not be considered as the agents of any other participating agency. Nothing herein waives, limits, or modifies any party's sovereign rights or immunities under applicable law.

EFFECTIVE DATE AND TERMINATION: This MOU is in effect once signed by all parties. Participating agencies may withdraw their participation after providing 30 days advanced written notice to the RFTF/VOTF Chief Inspector/Chief Deputy.

Task Force:

UNITED STATES MARSHAL:

Print Name:

Signature: Date:

CDUSM/RFTF COMMANDER (where applicable):

Print Name:

Signature: Date:

PARTNER AGENCY:

Name:

Location (City, State):

PARTNER AGENCY REPRESENTATIVE:

Print Name and Title:

Signature: Date:

ASSISTANT DIRECTOR, INVESTIGATIVE OPERATIONS DIVISION:

Print Name:

Signature: Date:

Julota®

Connecting Your Community

Oakland Fire Department's Mobile Assistance Community Responders of Oakland Proposal

We are excited to join with the Oakland Fire Department in their commitment toward improved outcomes and healthier citizens through the Mobile Assistance Community Responders of MACRO program has proven to strengthen the relationship with community partners, reduce negative outcomes from non-violent law enforcement calls, reduce expenses and strain for the city's emergency resources, while improving population outcomes. Thank you for considering Julota as the platform to launch this initiative. This document will provide our understanding of your program goals while outlining the scope and pricing necessary to meet them.

Our Understanding

The US Department of Justice's Bureau of Justice Statistics shows >50% of incarcerated persons have a mental behavioral health illness. Matt Zavadsky, President of NAEMT shares that 80% of all individuals who overuse the 911 emergency system have at least one diagnosable behavioral health disorder. We also understand 55% of US Healthcare dollars are spent on less than 5% of the population who are improperly using community resources. First responders are a community's front-line to meet these participants offering the greatest opportunity to reduce risk, lower costs, and increase health.

Following the successful CAHOOTS model, MACRO looks to utilize non-law enforcement mobile crisis intervention providing a mental health first for crisis involving mental illness, homelessness, and addiction. The specific goals are to reduce responses by police, resulting in fewer arrests and negative interactions, and increased access to community-based services and resources for impacted individuals and families, and most especially for Black, Indigenous, and People of Color.

Initially this will be a pilot response focused on East and West Oakland areas, as determined by City Council. Once the pilot is completed, a full evaluation will be conducted by OFD who will consider a plan for 24/7 deployment and full-city coverage.

Additionally, MACRO can mitigate emergency 911 calls better suited for community resources. The program is tasked to provide this service to the population and facilitate care coordination for patients throughout their continuum of care. Multiple partners, multiple patient records, and multiple individuals will typically be involved for each patient throughout this process.

Julota®

Connecting Your Community

The MACRO initiative is a unique program tailored for the OFD's East and West served communities. This initiative incorporates a model approaching clients to meet them exactly where they are, delivering the right resource to the right patient at the right time. The MACRO program is a unique initiative founded from a client-centric philosophy delivering community transparency. The innovative approach allows case managers to get the individual help while connecting them to basic needs and supports. It's our understanding that MACRO aligns with OFD's mission and goals for their community.

Overview

This proposal includes our MIH-CP/CORE module to support the MACRO program. We will be eliminating phone referrals while introducing accountability and closing the feedback loop. This includes: integrating with other data sources, enabling community resources to share information around clients, case management around clients, creating longitudinal records, and utilizing the alerts and notification setup.

Our implementation package covers:

- customization of the Julota platform to your workflows and program strategies
- migration of existing program data, from each program, into the Julota platform
- initial training
- additional platform customization required for reporting needs.

This solution is set up to be turn-key. Once you have signed a contract with us we will identify each hub's specific reporting needs and other software systems that are mission-critical to integrate prior to launch. Additionally, we will outline any full-level integrations necessary along with their associated costs. We will deliver a training environment that will mirror production, with a changeover to full production when ready.

I've included Julota Basic Support Service which includes access to the help desk, phone support M-F, 9 am - 5 pm MST for basic questions around platform use, three (3) hours per month per hub ongoing access to the individual who worked with each hub as their Implementation Specialist. Critical severity response will be within four (4) hours.

I also included a Julota Project Manager (PM) Consultant who will understand your immediate and long-term program goals, phased roll-out timelines, interfaces needed, and customization work necessary to ensure these pieces fit together and roll out seamlessly. The PM will not only offer experienced advice based on your programs' goals, but will also direct the Julota Implementation specialist on priorities as the PM will be aligned with your priorities.

Julota®

Connecting Your Community

I did not include Julota's white-glove Elite Support which includes a dedicated representative and phone line for each participating hub, help desk access, and 24-hour phone support for anyone within the hub's coverage area. For each participating hub Julota will add up to ten (10) community partners per year, four (4) hours of one-on-one training per month, one group training of up to two (2) hours. This level of support is highly recommended for programs who believe they will either add additional programs, enlarge their teams, will be highly involved within their community, or plan on growing their list of community partners throughout the year. Critical severity response will be within one (1) hour.

One-time Fees	Qty	Price Per	Total
Implementation Package per Hub	1	$6,100	$6,100
Workflow (Services) understanding and guidance	5	*Included*	*Included*
Modules per Hub	1	*Included*	*Included*
PDF Workflow Training Documents	1	*Included*	*Included*
Premium Launch Support (7 days)	1	*Included*	*Included*
Sixty (60) Minute Video Training Sessions	2	*Included*	*Included*
Custom Forms and Assessments (up to 30 fields)	1	*Included*	*Included*
Custom Report (up to 20 fields)	0	$1,800	$1,800
Onboarding Trusted Partners	0	$200	$0
Standard Dataset Migration	1	$1,800	$1,800
Interfaces one-way	1	$1,200	$1,200
Interfaces 2-directional	0	$2,400	$0
CJIS / SAMHSA 42 CFR Part 2 Workflow Validation	1	$6,000	$6,000
EMS Discount	1	(-$2,000)	(-$2,000)
Total One-time Fees			**$14,900**

Julota®

Connecting Your Community

Recurring Fees	Qty	Price Per	Total
Julota Platform License			$5,130
Includes basic reports and data extractions			
EMS Hubs	1	$3,000	$3,000
Hubs	0	$5,000	$0
Trusted Partner Organizations	0	$100	$0
Community Resource Organizations	25	$0	$0
Services	2	$350	$700
Interfaces one-way	1	$1,200	$1,200
Interfaces 2-directional	0	$1,200	$0
Monthly Actives converted into annual	600	$5	$3,000
Module - Client Notification	0	$1,200	$1,200
Module - Surveys	0	$900	$900
Module - Criminal History	0	$900	$0
Module - Enrollments	0	$900	$900
Module - Clinical	1	$900	$900
Module - SAMHSA 42 CFR Part 2	1	$4,800	$4,800
Module - CJIS	0	$4,800	$0
Custom Report (up to 20 fields)	0	$1,200	$1,200
Custom Report (21 to 40 fields)	0	$3,000	$0
Data Extraction			
Tableau Research and Analysis Reporting	0	$3,000	$0
Total Recurring Fees			**$22,930**

Julota Support Services	Qty	Price Per	Total
Julota Basic Support Service	1	$4,800	$4,800
Included for each Hub:			
Access to Implementation Specialists up to 3 hours per month	1	*Included*	*Included*
Help Desk access via web portal	1	*Included*	*Included*
Email access	1	*Included*	*Included*
Severity response for critical issues via hotline - 4 hours	1	*Included*	*Included*
**Post-implementation Development time charged $200/hour*			
Total One-time Fees			**$4,800**

Julota®

Connecting Your Community

Julota Project Manager Consultant	Qty	Price Per	Total
Julota Project Manager Consultant	1	$10,500	$10,500
Included for each Hub:			
Provide technical consulting	1	*Included*	*Included*
Provide business consulting	1	*Included*	*Included*
Provide product expertise	1	*Included*	*Included*
Produce and manage client-facing documentation	1	*Included*	*Included*
Direct Implementation to client goals and timelines	1	*Included*	*Included*
Total One-time Fees			**$10,500**

EMS Discount	Qty	Price Per	Total
EMS Discount	1	(-$7,000)	(-$7,000)
Total Discount			**(-$7,000)**

Grand Total Year One **$46,130**

City of Oakland

Mobile Assistance Community Responders of Oakland contracting Julota software from Touchphrase Development, LLC

Surveillance Technology Use Policy Guidelines

A. Purpose:

The purpose of the Julota software is to combine all the sources of data in one place and to create one form for the MACRO Responder‘s and Personal to use to populate however many data outputs are involved in information exchange agreements and partners to successfully accomplish the macro programs mission. The software would also protect HIPPA sensitive information of the service recipients that the macro program serves. This one oh wow an exchange of information between local service resource partners, the Macro program, And any other service provider partners to exchange information that is necessary to best serve the individuals and need. Furthermore, the purpose of using one software platform to combine multiple data sources used by county partners city programs and the like to reduce the burden on the service recipient to share vital information.

B. Authorized Use:

People who will be using the Julota software will have specific login credentials into the program. These logging credentials are controlled by the owners um the software program. Access will be determined by nature of the role and the need for information use. For example, if a macro vehicle comes upon an individual who is experiencing homelessness, and the individual expresses a desire to be transferred to housing shelter, with permission from the service recipient, the macro responders on the street well get identifiable information of the individual and share that with the MACRO community resource coordinator. The community resource coordinator will then use the Julota software to see if there’s any historical information provided by county partners like the Alameda county healthcare for the homeless team. Perhaps there’s information on that individual having had success at one homeless shelter over another. The Macro community resource coordinator would then use information amalgamated by the Julota program to choose the best resource for the service recipient in need and communicate that way with the Macro team on the street in as little time as possible. The Macro community resource coordinator could also communicate with that homeless shelter before directing the Macro team on the street to make the referral to make sure that that homeless shelter is open and available for intake before putting that community member through the hassle of moving. Ultimately this jalada software aims to reduce provider fatigue among individuals in need.

C. Data Collection:

The Julota software program can combine multiple data sources on the backend and present it in an easy-to-understand manner for community partners, Macro individuals, and anyone else who has permission and seeks the information in the program. These data sources include community health records which is a social health information exchange containing health and demographic information provided by various parties regarding individuals served by health care-related programs and other activities of HCSA and which HCSA wishes to use and/or disclose in connection with the organization and operation of those Programs.

Julota will also be pulling data using electronic software operations or ESL which will be pulling information from the fire of communications CAD dispatch system. This will use cat information to auto populate fields that have already contain information that had been collected by the 911 dispatcher. This reduces the possibility for error as the information is duplicated and not relied upon the individual entering the information to remember exactly as it was told to the 911 dispatcher initially. This also reduces the burden of data collection from the MACRO Responder when they are already asked to fulfill any other needs and provide top quality care to the service recipient. The macro program users and personnel such as the community resource coordinator and the Macro program manager may enter information directly into the Julota software for individuals based on the interactions and care that was provided from the Macro program personnel to the service recipient. The Macro program is also seeking a partnership with the housing and urban development med managed database HMIS. (Human management information system).

D. Data Access:

Individuals may only be able to gain access to information through permission from the program manager allowed by the login credentials from the software program. Movement through the software program can be tracked specific to user credentials. All Macro personnel will also undergo yearly HIPPA training To correctly identify and treat HIPPA sensitive information to protect the privacy of the service recipient. If there is a new individual on the Macro team who needs to be given access to the Julota program, the program manager or the program analyst would communicate with her point of contact on the Julota team to create credentials and to give them a specific level of access to information on the platform.

E. Data Protection:

There is no electronic protected health information (EPHI) in any form at any physical location of the business. Julota does not have a “store front” – information is stored 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 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.

No EPHI is ever transmitted or locally maintained on any portable devices unless encrypted using whole disk encryption or file level encryption. Julota security officials or senior IT staff member will ensure that our electronic health records system maintains mechanisms that authenticate the integrity of confidential health information, including encryption of portable tablets and laptops and encrypted access/data transmissions.

Julota 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.

F. Data Retention:

Touchphrase Development ensures that data backups are available in the event they are needed due to a physically mishap with a server. The data hosted within their offsite datacenter is backed up daily and per service level agreement by our cloud based vendor. The Aptible database (which hosts the Julota 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 Touchphrase Development IT department if a failure occurs. Touchphrase Development ensure the ability to access private health information in the event normal access procedures are down. Data hosted within its offsite datacenter is backed up daily and per service level agreement by our cloud-based vendor.

Public Access:

Currently, there is no plan in place for the information collected on the Julota platform to be made publicly available. The purpose of the Julota program is to have one software that can appropriately identify sensitive information and only give access to that information for necessary personnel and with the consent of the individual whose information it is. Other demographic information that is collected on the individuals being served as a whole undergoes review from partners in the city attorney’s office to redact identifiable Information before sharing it as a public records request.

G. Third Party Data Sharing:

Currently 1 two-way data agreement exists between the macro program and data partner which is Alameda healthcare for the homeless the conservators of the community health records database. Social Information Will be outputted from the Julota software back into the community health records database.

H. Training:

All MACRO personnel will undergo say three hour training to understand the user interface of the dilata software program. Additionally, as previously mentioned, all macro personnel will undergo a yearly HIPAA training. A Julota training partner will be provided from let's raise development LLC to provide the software specific training. The HIPAA training will be done electronically on the fire departments training platform, Target solutions.

I. Auditing and Oversight:

The following is an excerpt from Touchphrase Development's HIPPA Security Policy.

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.

J. Maintenance: The mechanisms and procedures to ensure that the security and integrity of the surveillance technology and collected information will be maintained.

Information will be maintained from the program analyst who will be pulling reports in addition to Touchphase Development back-end support that will be reviewing and maintaining the quality of information. The following is an excerpt from Touchphrase Development's HIPPA Security Policy.

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.

Mobile Assistance Community Responders of Oakland

Annual Surveillance Technology Impact Report - 9.64
OMC Impact Statement
October 28, 2022

Background

The Oakland Municipal Code (OMC) Chapter 9.64 regulates the City's use of surveillance technology. The statute requires the City to provide annual surveillance technology reports to the Privacy Advisory Commission (PAC) for continuing approval. The PAC will make a recommendation to City Council that either the technology usage should continue (the benefits outweigh the costs and civil liberties are safeguarded), the technology needs modifications to resolve concerns, or the technology usage should cease (OMC 9.64.040).

Required information to be included in an annual Surveillance Technology Impact Report (as per OMC 9.64.010.1):

A. Description

How was the surveillance technology used? Include the type and quantity of data gathered or analyzed by the technology

The purpose of the Julota software is to combine all the sources of data in one place and to create one form for the MACRO Responder's and Personnel to gather data on one form to successfully accomplish the MACRO Program's mission. MACRO Responders will submit information on the interaction with the service recipient recounting every incident that day by the end of every shift on the Julota platform. The Analyst will use Julota to pull reports with the Julota program protecting and redacting electronic protected health information (EPHI).

Finally, the Julota software will be used to measure a few indicators are difficult to effectively measure across disconnected databases. They include the MACRO program referrals efficacy and if the MACRO program effectively serves community members who require multiple contacts. The software allows for MACRO to identify these individuals while protecting and redacting electronic protected health information (EPHI).

B. Outside Entities

Whether and how often data acquired through the use of the surveillance technology was directly shared with outside entities? Include the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s):

The only two-way data sharing agreement will be with Alameda County's Community Health Records database. Electronic protected health information (EPHI) will be protected under the following guidelines.

HIPAA Security Rule: Technical Safeguards

Standard: Transmission Security

Implementation Specification: *Integrity Controls*

I. 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.		

a)

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.

C. Installation Objects

Where applicable, a breakdown of what physical objects the surveillance technology hardware was installed upon. Use general descriptive terms so as not to reveal the specific location of such hardware. For surveillance technology software, a breakdown of what data sources the surveillance technology was applied to:

The following policies are plans set in place by the software provider, Touchphrase Development LLC, on Security Procedures and Disaster Recovery Plans.

There is no electronic protected health information (EPHI) in any form at any physical location of the business. Julota does not have a "store front" – information is stored 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 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: Administrative Safeguards

Standard: Security Incident Procedures

Implementation Specification: *Response and Reporting*

II. 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. **a)** **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.

HIPAA Security Rule: Administrative Safeguards

Standard: Contingency Plan

Implementation Specification: *Data Backup Plan*

III. 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.

a)

Policy: We will ensure our business has the ability to access private health information in the event normal access procedures are down.

b)

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.

D. Location of usage

Where applicable, a breakdown of where the surveillance technology was deployed geographically, by each police area in the relevant year:

This does not apply, as the technology has not been acquired or therefore used yet.

E. Complaints and Concerns

A summary of community complaints or concerns about the surveillance technology, and an analysis of the technology's adopted use policy and whether it is adequate in protecting civil rights and civil liberties:
Note: The analysis shall also identify the race of each person that was subject to the technology's use. The Privacy Advisory Commission may waive this requirement if the probative value is outweighed administrative burdens and include writings on this determination in the annual report.

This does not apply, as the technology has not been acquired or used yet to solicit community complaints or concerns about the Julota program.

F. Internal Audits

The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response unless the release of such information is prohibited by law, including but not limited to confidential personnel file information:

No internal audits have been done at this time.

G. Data Breaches

Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response:

Please find the Data Breach Policy below.

IV. 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.

H. Results

Information, including crime statistics, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes:

The Julota software will be used to measure a few indicators that cannot be effectively measured using disconnected databases without the software. They are as follows:

- Measuring whether the MACRO program referrals are used effectively. The Julota program allows for unlimited partner credentials, to submit information to follow up on what happens after the MACRO program successfully achieves a referral with a partner resource organization. Did the individual fulfill the program to its entirety, did the individual walk away without engaging with the resource provider, or did the individual utilize the local resource to some measure in between? Information from the service provider will provide the MACRO program within depth information to measure its success, follow up, and to measure whether community partnerships yield results without expending precious time to follow up with the everchanging group of community resource partners.
- Does the MACRO program effectively serve community members who are frequent users of the Fire or Police Department services? The Julota program will protect the electronic protected health information (EPHI) while allowing us to monitor individuals throughout several contact points over multiple periods of time.

I. Public Records Act Requests

Statistics and information about public records act requests regarding the relevant subject surveillance technology, including response rates:

To date, there has been one Public Records Act Request regarding data collected by the MACRO program. The response rate was 2 weeks, and the information was reviewed with a point of contact with the City Attorney's office to redact electronic protected health information (EPHI) or identifiable information before sending the Public Records Act Request.

J. Annual Costs

Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year:

The annual cost for the Julota software is $48,000. The contract is for one year and would involve the City of Oakland to commit to another year before moving forward after one year has completed. This contract will be funded through the money allocated from the General Fund for the MACRO program.

K. Modification Requests

Any requested modifications to the Surveillance Use Policy and a detailed basis for the request.

The MACRO program has no modification requests to the Surveillance Use Policy. Thank you for your review.

Miscellaneous additional information:

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

Assigned Security Responsibility....4
Risk Analysis/Assessment....6
Sanction Policy....7
Information System Activity Review....8
Authorization and/or Supervision....9
Workforce Clearance Procedures....10
Termination Procedures....11
Information Access Management....12
Access Authorization....13
Establish and Modify Access....14
Security Awareness and Training....15
Protection from Malicious Software....16
Login Monitoring....17
Password Management....18
Security Incident Reporting....20
Data Backup Plan....21
Contingency Plan....22
Emergency Mode Operation Plan....23
Testing and Revision....24
Applications, Data Criticality Analysis....25
Evaluation....26
Business Associate Agreements....27
Contingency Operations....28
Facility Security Plan....29
Access Control and Validation Procedures....30
Maintenance Records....31
Workstation Use....32
Workstation Security....33
Disposal....34
Media Reuse....35

Accountability 36
Data Backup and Storage 37
Unique User Identification 38
Emergency Access Procedure 39
Automatic Logoff 40
Encryption and Decryption 41
Audit Controls 42
Integrity 44
Mechanism to Authenticate Electronic Protected Health Information 45
Person or Entity Authentication 46
Integrity Controls 47
Encryption 48
Breach Notification Policy 49
Breach Notification Template 52

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