Section I – Data Management Policies and Procedures

Overview

The MyMedicalShopper platform is built on components from service providers who are SOC2 Type II compliant and MyMedicalShopper has initiated the SOC2 Type II compliance process internally. MMS Analytics expects full SOC2 Type II compliance to be certified after one year of controls monitoring, currently Q4 of 2018.

All data in-flight and at-rest is encrypted, credentials and sensitive information are encrypted at the application and database layers, and strict access controls are enforced for MMS Analytics personnel, partners, and customers. Access control logs, server logs, and network logs are all captured and maintained for standard compliance intervals.

Encryption

MyMedicalShopper Application

All data sent to and from the MyMedicalShopper application, either to clients or between the application server and the database is encrypted using HTTPS and TLS.

Amazon WEB Services (AWS)

All data stored within AWS is encrypted, this includes:

1. EC2
2. SFTP Server(s)
3. MySQL (Amazon Aurora)
4. MongoDB (mLab)
5. S3

All data in flight within AWS is encrypted using HTTPS, TLS, and SSH.

Local Data

Apple FireVault is used to encrypt data on all laptops.

HTTPS, TLS, and SSH are used for all data transfers.

AWS Key Management Service (KMS)

MMS Analytics uses the AWS KMS to create and control the encryption keys use to encrypt data.

Data Destruction Controls

Amazon WEB Services (AWS)

The MyMedicalShopper application runs in AWS and is therefore subject to AWS Data Privacy and data destruction upon service/system decommissioning.

All data stored in AWS is erased within 30 days of it not being needed within the MyMedicalShopper and data analytics applications. At present we maintain all data for 3 years (and some data sets longer for historical analysis) before it is destroyed, unless otherwise specified by a data use agreement.

Physical Storage

Any data not in AWS that is stored in local systems/physical storage is subject to data wiping (via at least 3 overwrites) and physical destruction before media disposal.

System Access Controls

Critical Infrastructure

Multi-factor authentication (MFA) and administrative roles are used when accessing all critical infrastructure. This infrastructure includes, but is not limited to:

- AWS
- Meteor Galaxy
- mLab

MyMedicalShopper Application

The MyMedicalShopper application presents an administrative interface to MMS Analytics Administrators. This interface is secured using MFA and is provided to a very limited subset of MMS Analytics employees.

Physical Access Controls

Amazon WEB Services (AWS)

All infrastructure is located in AWS, see AWS Security Whitepaper (https://aws.amazon.com/whitepapers/overview-of-security-processes/) for details on AWS physical security.

Corporate Headquarters

Secure facility with proximity card access and visitor sign in and sign out. Multiple offices overlook the entryway.

Protected data on physical systems (i.e. thumb drives) is encrypted, password protected, and stored in physical fire safe(s) when not in use.

Section 2 – Physical Possession and Storage of Data Files

1. **Who will have the main responsibility for organizing, storing, and archiving the data? Please provide the name(s) and job title(s).**
   Jason Jeffords, CTO

2. **Describe how your organization will maintain an inventory of Initiative data files and manage physical access to them for the duration of the project.**
   All raw data and derivative works will be collected within a single schema. As you will read in other sections, data access is limited to three research team members. Technical and physical safeguards, including private keys, closely held passwords, IP address restrictions, a locked safe (containing the storage media on which the data is transmitted to us), and more are used to manage access.

3. **Describe how your organization binds all members (i.e., organizations, individual staff) to specific privacy and security rules in using Initiative data files. This includes confidentiality agreements and non-disclosure agreements.**
   All employees of MMS Analytics sign Non-Disclosure agreements. An example of the form document is attached to this application. Specifically, the agreement states "Confidential Information" also includes any information described above which the Company has obtained from a third party and which such party treats as proprietary or confidential information." in paragraph 1(a).

4. **Provide details about how your organization will notify the Arkansas Center for Health Improvement (ACHI) of any project staffing changes.**
   All research team members listed in this application will be active until the Company sends a notice to the ACHI to the contrary. Were a new member to join the team, the Company will notify the ACHI and substantiate the new member's qualifications for working with claims data as well as their security proficiency. If written approval is required for a new member to join the research team, such approval will be sought before allowing the new member to access the data.

5. **Describe your organization's training programs that are used to educate staff on how to protect Initiative data files.**
   There are no staff training programs as all three research team members are highly experienced experts in their field and senior employees, two of which have worked for the company for substantially all of its history, two of which are officers, and one of which co-founded the company. They are fully aware of all provisions of the Security Policy (in Section I of this document) and other security best practices not explicitly enumerated therein.

6. **Explain the infrastructure (facilities, hardware, software, and other) that will access the Initiative data files.**
   Data will be stored in a SQL database hosted by Amazon Web Services (AWS). All data in-flight and at-rest is encrypted. Research team personnel all use Apple MacBook Pro computers as workstations and access the data through MySQL Workbench for Mac as well as Terminal. Employee workstation operating systems and applications are updated to the newest releases regularly.

7. **Describe the policies and procedures regarding access to Initiative data files.**
   Technical and physical safeguards, including private keys, closely held passwords, IP address restrictions, a locked safe (containing the storage media on which the data is transmitted to us), and more are used to manage access. Administrative safeguards restrict access to Initiative data to just three senior employees.

8. **Explain your organization's system or process to track the status and roles of the project team.**
   Our process to track the status of members of the research team is given in question four of this section. Given that there are currently only three individuals with access to the data all of whom work from the same office daily, there is no need for a formal process to define the roles and responsibilities of each member. In general, Jason Jeffords is tasked with all items related to data storage and security and usually lends his expertise in data analysis to aid in problem solving. Evan Young is the lead researcher and is solely responsible for the content published for consumption by users and the methodology/algorithms underlying such content. Matt Robinson is the web and mobile app developer and he works with Evan Young to deliver a great user experience with the data at our disposal.

9. **Describe your organization's physical and technical safeguards used to protect Initiative data files, including actions taken to physically secure data files and safeguards to limit access to Initiative data and analytical extracts among the project team.**
   In addition to the details discussed in the Security Policies document, access to the database containing APCD data requires a private key stored on only the three workstations belonging to members of the research team. The database is only accessible from our office and each team member's home, as identified by the IP address. All research team members are granted the same level of access. Further details are given throughout this document, especially in questions two and seven of this section.

Section III – Data Sharing, Electronic Transmission, Distribution

1. **Describe your organization's policies and procedures regarding the sharing, transmission, and distribution of Initiative data files.**

As you will read in other sections, data access is limited to three research team members. Technical and physical safeguards, including private keys, closely held passwords, IP address restrictions, a locked safe (containing the storage media on which the data is transmitted to us), and more are used to manage access. Once the Initiative data is uploaded to the AWS Aurora instance, it is accessed directly by each research team member. Derivative works are also kept on the server, which any research team member can access without copying the data to their local machine or receiving data in an unsecure way from another research team member.

2. **If your organization employs a data tracking system, please describe.**
   Data tracking system is somewhat ambiguous. If components of such a system are not touched upon in other sections, please provide more context, and we will be able to provide a more comprehensive answer.

3. **Describe the policies and procedures your organization has developed for the physical removal, transport, and transmission of Initiative data files.**
   ACHI data will be hosted on a separate encrypted server instance hosted by Amazon Web Services. When the time comes to destroy the data, we will "secure shred" all of the data, and then delete the instance, at which point Amazon will completely wipe the drive. No extracts of the raw database will ever be taken from the server, either as a printed or electronic document, so data destruction procedures will be limited to the hosting server.

4. **Explain how your organization will tailor and restrict data access privileges based on an individual's role on the project team.**
   There is no technical barrier in place to prevent any of the three named members of the team from accessing any portion of the data, as they are all granted the highest levels of access to the database. Administrative and physical safeguards do restrict access to a very limited number of privileged, senior employees and without access to one of these privileged employee's computers, stored in a locked office, access would be impossible. No privileges are granted to non-research team employees.

5. **Explain the use of technical safeguards for data access (which may include password protocols, log-on/log-off protocols, session time out protocols, and encryption for data in motion and data at rest).**
   Data is encrypted at-motion and at-rest. Employee workstations automatically log out after no more than 15 minutes of inactivity. Passwords must meet stringent standards for complexity, which we do not share for security reasons. The database can only be accessed from our office in Portsmouth, NH and each of the research team member's homes. Each research team member has a private key stored on their workstation required to make a connection with the database. The AWS hosting instance itself can be turned off and even wiped from Amazon's admin portal, which requires a separate password.

6. **Are additional organizations involved in analyzing the data files provided by ACHI?**
   No.

   If so, please indicate how these organizations' analysts will access the data files:

   ___ VPN connection
   ___ Travel to physical location of data files at requesting organization
   ___ Request that a copy of the data files be housed at second location
   ___ Other:

7. **If an additional copy of the data will be housed in a separate location, please describe how the data will be transferred to this location.**
   Data will be transmitted to an AWS instance upon receipt and then the original storage medium will be placed in a locked safe to which only the three research team members know the code (unless data is sent to an SFTP folder, of course). Data will be uploaded via SFTP.

Section IV – Data Reporting and Publication

1. **Who will have the main responsibility for notifying ACHI of any suspected incidents wherein the security and privacy of the Initiative Data may have been compromised?**
   Jason Jeffords, CTO

2. **Please describe and identify your organization's policies and procedures for responding to potential breaches in the security and privacy of the Initiative Data.**
   a. Breach of Protected Health Information. MMS shall report, following discovery and without unreasonable delay, any "Breach" of "Protected Health Information," as these terms are defined in 45 C.F.R. § 164.402, or other data in the Company's possession which is covered by a Data Use Agreement. MMS shall make an initial report to Data Owner not more than ten (10) business days after MMS learns of the Breach. MMS shall cooperate with Data Owner in investigating the Breach and in meeting all obligations under the Breach Notification Rule and any other security breach notification law.

   b. Security Incidents. MMS shall report to Data Owner any successful (a) unauthorized Access, Use, Disclosure, modification, or destruction of Protected Health Information or (b) unauthorized interference with system operations in MMS's Information System, of which MMS becomes aware. MMS shall make the report available to Data Owner not more than ten (10) business days after MMS learns of such incident.

3. **Explain how your organization's data management plans are reviewed and approved.**
   MMS Analytics is currently in the midst of the Assurance and Testing phase of a SOC2 audit. All policies are procedures are under constant review for improvement opportunities based on our experience under the policy. Regarding policies related to

data management, revisions and approval of such policies are made under the direction of our CTO, Jason Jeffords.

4. **Explain whether and how your organization’s data management plans are updated during the Data Use Agreement (DUA) period.**
   When changes are made they are communicated to employees, as applicable to their work. If the ACHI would like to be copied on such changes as they apply to Initiative data, we can accommodate that request.

5. **Please attest to the ACHI cell suppression policy of not publishing or presenting tables with cell sizes with less than 11 observations to anyone who is not an authorized user of the Data.**
   MMS Analytics has a cell suppression policy matching the CMS standard of at least 11 records.

Evan Young **I agree.**

Section V – Completion of Research Tasks and Data Destruction

ACHI data will be hosted on a separate encrypted server instance hosted by Amazon Web Services. When the time comes to destroy the data, we will “secure shred” all of the data, and then delete the instance, at which point Amazon will completely wipe the drive. No extracts of the raw database will ever be taken from the server, either as a printed or electronic document, so data destruction procedures will be limited to the hosting server.