Overview

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.

Protected Health Information (PHI) is securely handled with entities external to TALON as outlined by SOP: Sending/Receiving PHI External to TALON.

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. **Postgress (Amazon Redshift)**
4. **MongoDB (Atlas)**
5. **S3**
6. **ClickHouse (ClickHouse Cloud)**

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 used 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. 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

All internal User Access to critical infrastructure and MyMedicalShopper databases is reviewed quarterly at a minimum for accuracy and appropriateness for a given users roles and responsibilities. Review results and any issues are reported to the Information Security Officer and Compliance Officer. Evidence is captured in quarterly review tickets.

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 (MeteorJS as a Service running within AWS)**

- MongoDB Atlas (MongoDB as a Service running within AWS)

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 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. Visitor entry requires the use of a doorbell, and after-hours entryway activity is monitored by video surveillance.

Protected data on physical systems (i.e. thumb drives) is encrypted, password protected, and stored in a physical fire safe(s) when not in use. NOTE: no application data is stored in this way.

Training

All TALON employees must complete and pass a Cyber and Information Security Training course upon employment. From then on, all employees are required to take and pass the training course annually to reinforce and be aware of any changes to standard Cyber and Information Security procedures and knowledge.