HIPAA Compliance

Purpose:

This document will outline the measures taken to meet the HIPAA Security Standards and Technical Safeguards as given in 45 CFR Part 160 and Part 164 Subparts A and C commonly known as the Security Rule. This document also explains how PIMSY addressed the various security requirements levied in the ONC-ATCB Certification procedures.

Forward on HIPAA Security Rule

The following is a quote from article 4 Security Standards: Technical Safeguards, *"…the Security Rule is based on the fundamental concepts of flexibility, scalability and technology neutrality. Therefore, no specific requirements for types of technology to implement are identified. The Rule allows a covered entity to use any security measures that allows it reasonably and appropriately to implement the standards and implementation specifications. A covered entity must determine which security measures and specific technologies are reasonable and appropriate for implementation in its organization."* This statement rests the responsibility on the provider to ensure that appropriate provisions are made to comply with the standards laid out in the HIPAA documentation, but does not specify the means in which they are applied.

Access Control § 164.312(a)(1)

The Security Rule defines Access Control in § 164.304 as *"the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource. (This definition applies to "access" as used in this subpart, not as used in subpart E of this part [the HIPAA Privacy Rule])."*

PIMSY complies with this standard in the following ways:

- All users have a Unique Identifier
- An auto locking mechanism is in place which restricts access to the application when users leave their workstation
- All User Passwords are encrypted
- PIMSY requires all users to be assigned a profile which is a list of rules that define what actions (view, create, modify and delete) a user can perform on data in the application.
- Multiple layers of authentication are required by the application
    - Login to PIMSY Application
    - Separate database login used by web service

- The data and the application are both stored off sight in a secure facility. In the event of a natural or manmade disaster the PIMSY application is designed to be accessible and secure from any computer (using windows OS) that has an internet connection.
- A Hardware firewall is in place to guard against unauthorized access to the hosting server.
- The number of Open Ports is strictly limited to ensure a very small surface area. The Database Port is not open. Remote access is limited via IP address. There are only a hand full of people that have access to the production environment.

Audit Control § 164.312(b)

The Audit Controls Standard requires the following of a covered entity but has no implementation specifications. *"Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information."*

PIMSY complies with this standard by providing the following:

- Key forms in the application contain non-editable fields that state who created the record and when it was created and who last edited the record and when.
- The auditing module in PIMSY allows administrators to flag key areas of the system to audit. Inserts, modification and deletes can all be audited on any area of the application. When auditing is flagged a complete audit trail is recorded in the database. The audit trail includes the time the change was made, who made the change, the previous value, the new value and finally what operation was performed.

Integrity § 164.312(c)(1)

The Integrity Standard requires the covered Entity to: *"Implement policies and procedures to protect electronic protected health information from improper alteration or destruction."*

PIMSY complies with the standard in the following ways.

- Integrity Constraints (Primary and Foreign Key Relationships) are placed on all data stored in the database that prevent the corruption data.
- Procedures and Triggers are implemented in the database to ensure data integrity.
- A Hardware firewall is in place to guard against unauthorized access to the hosting server.
- PIMSY is a closed/compiled system which means that sql injection attacks cannot be utilized to access or corrupt data.

Person or Entity Authentication § 164.312(d)

This standard requires the covered entity do the following: *"Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed."*

PIMSY complies with the standard in the following way.

- PIMSY requires a unique login and unique password for all users entering the application.
- Passwords cannot be cached on workstation which prevents unauthorized logins.

Transmission Security § 164.312(e)

This standard requires the covered entity do the following: *"Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network."*

PIMSY complies with this standard in the following ways.

- PIMSY utilizes Secure Socket Layer (SSL) technologies in all its communications to and from the hosted web service.
  - http://www.webopedia.com/TERM/S/SSL.html
- In addition to the above SSL technology PIMSY utilizes additional encryption methods for a high percentage of its transmissions. (Advanced Encryption Standard AES AKA Rijndael
  - http://en.wikipedia.org/wiki/Advanced_Encryption_Standard)
- A unique and encrypted security key is sent with and required by all transmissions. This key is unique to each provider using the PIMSY application and prevents any unauthorized communications with the web service.

Physical Safeguards § 164.310

The Security Rule defines physical safeguards as *"physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion."*

For workstation security see the provider's SOP for workstation security.

The PIMSY Database and web service are hosted with Immedion, a 3rd party hosting company. Immedion does not have the necessary passwords to access any information stored on the SMIS server(s). The physical safeguards implemented by Immedion are listed below. (http://www.immedion.com/colocation/colocation)

State-of-the-Art Facilities

Immedion's data centers are custom designed with multiple levels of security, diesel generators, redundant uninterruptible power supply systems, pre-action dry-pipe and FM-200 fire suppression systems, and redundant precision air conditioning systems. Immedion guarantees its customers, whether a one-person IT shop or a multi-national corporation, the highest levels of support, uptime, and data security.

Immedion is SSAE 16, SOC 1 Type II compliant

Security

- Multiple levels of physical security including biometrics, prox card with PIN, locked cabinets and cages, and video surveillance

Power

- Redundant, uninterruptible power including multiple UPS and diesel generator systems backing up redundant transformers with multiple substation feeds

Environment

- Redundant Liebert precision computer room air conditioners to maintain optimal temperature and humidity

Connectivity

- Immedion's Network is one of the most robust in the southeast. Multiple Internet and fiber optic connectivity options: AT&T, Level (3), Charter Business, tw telecom, PalmettoNet, Time Warner Cable, ERC, Spirit Communications, SC Gov and PSPN

Fully Monitored

- Staffed 24x7x365 by Immedion's Network Operations Center (NOC) technicians to continually monitor data center security, environmental conditions, and technical infrastructure to provide around the clock assistance. 24x7x365 customer access without call ahead or prior appointment.

Disaster Recovery and Contingency Operations (A) - *§ 164.310(a)(2)(i)*

- The PIMSY Data is backup up and encrypted 3 separate times on daily basis (See Disaster Recovery Plan)
- Multiple backups for each system are stored over several days
- A single backup of each system is taken on the first of every month and stored for 6 months
- Backups are stored across multiple servers and locations

- Roll over procedures are in place on alternate servers to ensure minimal disruption in the event of a failure.

Development and Release Processes

- PIMSY has an extensive framework that is built around Security
- All new development is built upon this framework which utilizes the previously mentioned security profiles. Each screen, feature and function is integrated into the security profile framework which allows our clients total control over a user's actions.
- MS Team Foundation Server is utilized in the development process on both the UI and the Database to ensure code conflicts do not occur and or are resolved effectively.
- Development is held and Maintained in a secure Microsoft Azure Environment.
- Each release goes through an extensive set of Quality Assurance Measures.
    - Code reviews are performed.
    - Use cases are performed.
    - Regression testing is performed.
    - Each new screen/feature goes through a 15+ point inspection by a minimum of 3 different QA professionals.
    - Testing is logged in a tracking system and nothing is released until it has passed the 3 different inspections.
    - Testing Failures are sent back through the process until the feature is passed by all 3 inspectors.
    - Each release is tested on multiple MS OS environments.
    - All changes to the system are logged and reviewable several weeks prior to the release via version reports.
    - Prerelease trainings and webinars are given to ensure our clients are educated on any upcoming changes.
    - Releases are cut from a single secure environment.
    - Prerelease backups of each system are performed.
    - Platinum Clients are given a release date option.

Meaningful Use Certification

PIMSY is Meaningful Use Certified, which means that it has undergone rigorous security testing, required by the federal government, to qualify for this elevated standard. PIMSY's testing was facilitated by the Drummond Group (www.drummondgroup.com). For more information about what functionality was tested and to what degree, refer to the government overview at www.cms.gov or contact us for details.

Below are explanations of how PIMSY handled(s) the various security elements required in the ONC-ATCB certification process.

Privacy and Security

170.302.o – Access control

Users are assigned a Profile. That profile determines what access they have to various parts of the system.

170.302.p – Emergency access

When a user takes emergency access their profile is changed to the emergency access profile until they log out of that session. They will then be able to log into the system and have access to areas and patients they would not normally have. This is a temporary status that ends when they log off of the session.

170.302.q – Automatic log-off

After a certain period of time of inactivity PIMSY will lock itself. A password is then required to get back into the system.

170.302.r – Audit log

Actions are audited via the database and are presented to the user in an Audit grid. The data elements are capturing the user id, patient id, time stamp and action taken. The Audit Log can be filtered and sorted.

170.302.s – Integrity

PIMSY uses MD 5 as the Hashing Algorithm on specified documents, and used a third party secure email vendor to send the message digest and the test data to our tester.

170.302.u – Encryption

The encryption algorithm used in PIMSY is AES256 (Rijndael).

170.302.v – Encryption when exchanging electronic health information

A 3rd party secure email application was used during the certification process.

Closing

The PIMSY application takes all precautions to meet and exceed the standards and requirements expressed in the HIPAA documentation.