Syntermed Live™
HIPAA Compliance
&
Security Overview

Syntermed Live™ is an online platform that manages electronic Protected Health Information (ePHI[1]), including but not limited to, medical image data sets, patient identifiers, patient contact information and physician generated reports in a way that balances the stringent security required by HIPAA with the speed and reliability our customers have come to expect. Syntermed's core application suite is built on top of the Syntermed Live™ platform, allowing medical professionals to securely access their data from anywhere in the world. This document will outline the infrastructural and application specific configuration and security measures Syntermed employs to ensure the safety of its customers' data.

I. HIPAA Compliance

The Syntermed Live application conforms to the general HIPAA Compliance statement used company wide at Syntermed, internally referred to as the **Syntermed HIPAA Security Policies and Procedures** document. Any and all employee interaction with the Syntermed Live application is performed in accordance with the **Syntermed HIPAA Security Policies and Procedures** document, including training on the proper use of ePHI[1], passwords, hardware and media security, privacy and termination.

Additionally, Syntermed commonly enters into a Business Associate Agreement (BAA) with its customers that ensures that all parties involved in the use and/or disclosure of ePHI[1] comply with current HIPAA regulations.

II. Security Overview

i. Infrastructure

The Syntermed Live™ server infrastructure leverages any and all available technologies to balance the needs of our customers while maximizing both security and performance. For security reasons, many specific details as to the configuration and management of Syntermed Live are considered proprietary.

ii. Physical Security / Hardware Maintenance

Physical access to the hardware that comprises the Syntermed Live^{TM} infrastructure is strictly prohibited.

iii. Network Security

The server(s) that host the Syntermed Live^{TM} infrastructure are protected by multiple distinct layers of network security. Each server has its own software based firewall which denies all incoming traffic by default. Each server is secured using a secondary Intrusion Prevention System (IPS) again denying all incoming traffic by default. Finally, all servers exist on an isolated, internal network where Network Address Translation (NAT) is used to ensure that only specific ports are publicly available.

Network traffic is only allowed to pass through these firewalls on the ports necessary to use or administer the system(s). These ports are configured only by Syntermed technical personnel. Additionally, all traffic incoming and outgoing is monitored for abnormalities. Any traffic identified as being “of malicious intent” or “out of range” will trigger automatic notifications to Syntermed.

iv. Operating System

Syntermed Live^{TM} employs a vast array of server(s) each adhering to the following strict security rules.

Authentication / Access

Server(s) can only be accessed remotely over secure/encrypted channels originating from predetermined locations. Access to server(s) is restricted to the highest tier of technical employees within Syntermed. Every server is protected by individual software firewalls and all ports are blocked by default unless required.

Redundancy
All servers employ storage mechanisms which include some form of real time redundancy.

Audit Logs
The standard OS Event Logs are monitored daily. Security logs audit all login attempts to the OS, both failed and successful.

Monitoring
All servers are monitored both internally (disk space and stress, event log warnings and errors) and externally (uptime and availability, network activity) for health and security purposes.

Patching / Update(s)
All servers are up to date with patches and security updates within 90 days of release. A patch or security update may be tested and applied earlier if a serious threat has been assessed.

Anti-Virus
All servers run real-time anti-virus protection software. Definition updates are performed multiple times per day.

v. Encryption

All application data transferred to/from the Syntermed Live^{TM} server(s) is encrypted "in-flight". The data is required to travel over a secure channel using SSL (Secure Sockets Layer) encryption, the standard for secure Internet network connections.

All application data (including backup data sets) that exist within the Syntermed Live system(s) are stored in an encrypted state while "at-rest" using standard AES algorithms with a minimum key length of 256 bits.

vi. Application

Data stored within the Syntermed Live application is restricted as follows:

Access
Access to data contained in the Syntermed Live™ system is only available via two methods; direct connection through an Internet browser and via Syntermed's desktop software, the Master Control Program (MCP). Both access methods require a secure Internet connection (industry standard SSL over port 443).

Authentication
When accessing data, valid credentials in the form of a username and password combination must be supplied. The Syntermed Live™ system employs a one-way hashing system for password storage; therefore passwords are never stored in a human readable format.

The password is configured by the user and must conform to a very high level of complexity. A minimum length of 7 alphanumeric characters which must include at least one character, at least one number, at least one symbol. In the rare event that a password must be reset by Syntermed, the user will be required to change the password at the next login to the system.

Password expiration and reuse guidelines are <u>not</u> enforced by Syntermed. This is because these requirements vary so greatly from site to site and can affect workflow in negative ways if implemented incorrectly. Syntermed relies on the customer to implement and enforce all policies related to password expiration and reuse.

MCP

When accessing data through MCP, in addition to the user's credentials, the application must first be registered with the Syntermed Live^{TM} system by Syntermed personnel in the form of a machine key encrypted license. Additional security is negotiated based on information in the license before data can be accessed.

MCP has the ability store credentials to allow for automatic login at startup. If this option is enabled, the password is stored locally in an encrypted state. *Syntermed recommends that this feature should only be used if the computer MCP is installed on is secured in other ways that are enforced by the customer.*

MCP caches data accessed via Syntermed Live for use on the local computer in a non-encrypted state. MCP can be configured to store this data in either a "per computer" or "per user" setting as is dictated by the workflow of the site. MCP can be configured to automatically clear the cache upon application exit. *Syntermed recommends that MCP is configured to store data in a secure, encrypted location on any system that may leave the hospital network.*

Web Browser

No data accessed using a web browser is cached locally and all web sessions automatically expire after 15 minutes of inactivity.

Access Control

Access to data contained in the Syntermed Live™ system is managed according to Access Control Lists (ACLs). By default, only members of an ACL have access to the data contained within. Access to data outside of an ACL is explicitly denied. All data access attempts are audited.

All administrative actions related to the management of ACLs, including customer records, licenses and user account credentials are available only to employees of Syntermed, Inc. All actions related to the management of customer ACLs are performed at the request of the customer and in accordance with the Syntermed Security Authorization Policy[2].

For the purposes of administrative maintenance and/or troubleshooting, Syntermed employees may need to access a customer's ePHI[1]. Syntermed will only access a customer's data under the strict HIPAA guidelines set forth in 45 C.F.R. Section 164.501.

Data Access Layer (DAL)

Direct access to data stored in the Syntermed Live™ system is restricted locally. Application access to the database(s) is regulated through a Data Access Layer (DAL) which performs all actions related to Access Control and Audit Logging.

Audit Logging

All read and write access to the Syntermed Live^{TM} system is logged for security purposes. Each log entry includes, but is not limited to, the timestamp, IP address, credentials, license ID (if applicable), ID of data to be accessed, action to be performed, status and result.

vii. Backups / Disaster Recovery / Contingency Plan

All data stored within the Syntermed Live infrastructure is backed up regularly and replicated to multiple locations including some that may be off-site. Backup operation schedules and data retention durations will vary based on data type and circumstance. All backup data sets are stored in an encrypted state and transmitted (if applicable) over an encrypted channel.

Syntermed maintains multiple tiers of Disaster Recovery and Contingency Plans. These documents set forth a course of action that is maintained for emergency response, backup operations, and post-disaster recovery. The purpose of these plans are to ensure availability of critical resources and facilitate the continuity of operations in an emergency. The plans include procedures for performing backups, preparing critical facilities that can be used to facilitate continuity of critical operations in the event of an emergency and recovering from a disaster.

Syntermed maintains detailed Disaster Recovery and Contingency Plans on file that are updated and reviewed bi-annually at a minimum. The details of these documents contain sensitive information that may be a breach of security to divulge to a customer, therefore they are kept as an INTERNAL ONLY documents.

viii. Hardware Retirement, Replacement and Disposal

Over time, the hardware used at Syntermed must be retired, abandoned or replaced. This hardware can be anything from office printers and laptop computers to production level servers and network attached storage (NAS) devices. Whether the hardware is retired due to failure, upgrade or it has simply reached “end-of-life”, Syntermed will attempt to recycle everything possible both internal and external to the company.

If a piece of hardware has any sort of storage capability (e.g. hard drive, flash, etc...) that may have contained ePHI[1] or any other data that is protected by the HIPAA guidelines, it cannot be recycled outside of Syntermed without adhering to the following internal policies.

If being reused internally, the storage hardware must be formatted, partitioned and “Low Level” or “Level 2” formatted, meaning that all data on the disk is overwritten. Additionally, commercially available, off-the-shelf software may be used to sanitize the device in accordance with the highest available standards[3].

If being recycled or disposed of outside of Syntermed, any storage devices will be removed and either recycled internally (following the above procedure for sanitation) or destroyed. *No storage device that may have contained ePHI[1] as described above will ever leave Syntermed in working order.*

ix. Data Retention

Syntermed systems will maintain all ePHI[1] in perpetuity for the duration in which it is contractually bound.

Throughout the contract period, all ePHI[1] will be secured as described in this document. In the event of contract termination with Syntermed, any and all ePHI[1] retained in the Syntermed system may be disposed of immediately. However, data is typically retained for a minimum period of 180 days from the date of contract termination. During this time, read-only access can be supplied to the customer which will allow for retrieval of ePHI[1] from the Syntermed systems. Syntermed reserves the right to charge for additional assistance in retrieval of ePHI[1].

x. Maintenance and Logging

All Syntermed Live system(s) will undergo standard maintenance tasks as well as troubleshooting and repairs for problems that may arise over time. No matter what type of task is performed on a system that is a part of the Syntermed Live application infrastructure, it is logged by the employee performing the task and filed internally.

Appendix A: References

[1] Health Information Privacy - http://www.hhs.gov/ocr/privacy

[2] The Syntermed Security Authorization Policy is a part of the Master Services Agreement (MSA).

[3] Department of Defense standard 5220.22-M - http://www.usaid.gov/policy/ads/500/d522022m.pdf