HIPAA Overview

Version 1.2

Contents

Introduction

At Canvas we take security seriously. With the 2.2 release of Canvas, we have extended our basic security and infrastructure to allow Canvas to be used as a HIPAA compliant tool capable of safely storing patient information. The specific areas of Canvas that have been improved are centered around:

1. Increased usage of encryption above and beyond what was already being utilized by Canvas
2. Incorporation of auto-log-off and session time out features to prevent information leaks due to lost or unsecured devices
3. Disabling of auto-email features to prevent accidental disclosure of sensitive information
4. Increased usage of logging and checksums to validate that data has not been manipulated

These improvements are spread across the entire Canvas infrastructure. The following sections break down security features by components within the Canvas infrastructure.

Canvas Server Infrastructure

Physical Components

The Canvas server infrastructure is hosted in a secure facility with the appropriate physical authorization and authentication protocols in place to be HIPAA compliant. In addition, the facility processes old hardware in a proper manner to guarantee that no information can be read off of old disk drives or memory. Before Canvas decommissions a disk used within the Canvas server environment, it is correctly sanitized and cleaned of data before being decommissioned.

Software Components

Canvas servers reside behind a complete firewall solution, with all access defaulting to deny incoming traffic. Only the minimum necessary protocols and traffic are allowed access to the Canvas servers. Any changes to the firewall configuration require access to the necessary protected X.509 certificate in addition to a private key, which provides an extra layer of security to prevent unauthorized access or modification of Canvas firewall rules.

Administrative access to Canvas servers is limited to a select few Canvas personnel, with access only being available via encrypted shell (SSH). In addition, all remote file transfers needed for administration of Canvas servers is also done via encrypted means (SCP).

Canvas Software

The server-side Canvas software incorporates a number of features to keep Protected Health Information (PHI) secure. All PHI is encrypted using the industry accepted AES encryption algorithm before being written to any permanent data storage. All backups and replication of the Canvas data

store are also encrypted in the same manner. All remote web browser access to areas of the Canvas website which may display PHI, in addition to any authorization information, are required to be accessed via 256-bit encrypted TLS version 1.0 (Hypertext Transfer Protocol Secure) .

In addition to encryption, the server-side infrastructure uses logging and checksums to allow for PHI data to be verified as un-altered at any point in time. Canvas has also increased logging to track what users and administrators accessed PHI at what time, from what remote IP address and using what medium (HTML, PDF, CSV, WebService). In addition, Canvas logs all authentication and authorization functions, such as logging-in, logging-out and changing passwords.

Since no valid method exists for encrypting e-mail communication in a secure and widely adopted manner, Canvas disables all in-application e-mail capabilities for accounts specified as being HIPAA compliant. Even though the HIPAA specification is ambiguous in allowing e-mail correspondence, the Canvas team decided that the risk outweighs any potential benefits when it comes to e-mail communication and PHI.

Another security measure undertaken by the server side components of Canvas, is the shortening of user-idle time for accounts marked as being HIPAA compliant, before the user is logged out of the Canvas website. In addition, the “remember password” feature is disabled for HIPAA compliant accounts.

Canvas Client Infrastructure

The Canvas client application has been developed for a number of different runtime environments and operating systems. Regardless of the environment, the Canvas client has been improved to guarantee that PHI is kept secure using a number of features and functional changes.

All data stored by the Canvas client, whether it is data read from the Canvas server or data entered by a user, is encrypted using an encryption algorithm recognized as industry approved before being stored to disk. The encryption algorithms utilized vary by device. The current algorithms are:

Client	Algorithm
.NET	RC4
BB	AES 256
iOS	AES 256
Android	AES 128

All communication with the Canvas server infrastructure is always secured by 256-bit SSL, which cannot be disabled by a user of the Canvas client.

In addition to encryption on the Canvas client, additional security constraints have been put into place when accessing accounts that have been marked as being HIPAA compliant. A user-idle timeout has been implemented which will limit the amount of time the Canvas application can remain idle before the user is logged out. The user is also no longer allowed to save their password on the device when accessing HIPAA compliant accounts. These features were put in place to prevent unauthorized data access in case a mobile device is lost or a terminal is left unlocked in a non-secured location.

Summary

The Canvas team takes security and privacy seriously. The already existing Canvas features and functionality provided a high level of security for our users. By implementing the discussed additional security and functional features and conforming to HIPAA requirements, we are confident that all PHI stored by Canvas is safe and secure for our end users.