collaborate

Your Organization, Collaborate, and HIPAA

(and common sense best practices for security and maintaining confidentiality of sensitive data)

Updated 02/01/2018

This document is not a replacement for professional legal advice. It’s a primer. The Client Responsibilities section is “for your reference”, but you will want to follow up with your own legal, security, and IT resources for confirmation and elaboration. These are not requirements by Network Ninja of Client, but requirements of Client per HIPAA (“Health Insurance Portability and Accountability Act”).

The objective of HIPAA is to protect the privacy and security of Protected health information (PHI) by limiting access to those authorized persons that need it, and restricting the allowed uses and disclosures of PHI. Those charged with the security of PHI must identify areas where that PHI is potentially at risk, reduce those risks, and have a plan in place that can be executed in the event of a breach.

“The HIPAA Privacy Rule establishes national standards to protect individuals’ medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.” - HHS.gov

Client Responsibilities

Keeping in mind that Client is responsible for their own business practices, and will manage who accesses Collaborate, and how, the below is a summary of items for which the Client is responsible.

Risk Analysis

Client should perform a risk analysis, and document the results. The intent is to identify any and all ways PHI could be at risk of being used or accessed in an unauthorized manner. This includes, but is not isolated to, a review of technology practices.

Risk Management

After risks are identified, safeguards should be implemented to reduce those risks. Some of these safeguards involve Collaborate, some don’t. See below, under “Collaborate-specifics” as to how Collaborate can assist in managing your risk.

User Management and Policy Training

Unrelated to Network Ninja, Collaborate, or software in general, HIPAA requires Client perform regular risk assessments, develop and implement a risk management policy, train employees in regard to security and how it relates to PHI, and develop contingency plans in the event of an outage. Your resulting security policy should cover such things as:

Access Management

Client is responsible for policies relating to user workstations and any other devices that will access Collaborate. Under no circumstances are individual accounts to be shared by multiple users.

Password Management

- Use your risk analysis to determine a password policy that will work for your organization. Examples include:
  - Do not physically write down passwords unless they are stored behind lock and key.
  - Do not use the same username and password combination to access any other sites.
  - Do not use easily guessable passwords.
  - Do not issue incremental or universal passwords for your organization.

Malware Avoidance (Viruses, Trojans, Ransomware, etc.)

Client is responsible for having procedures in place to guard against, detect, and rectify malware and computer viruses. Client will be sole source of uploaded pre-existing files, and has sole responsibility for ensuring said files are not corrupted.

Encryption and Storage

Absolutely no PHI should be sent via email unless encrypted - if unsure, assume it is unsafe.
Absolutely no client-owned PHI should be stored on personal computers, mobile devices, or other hardware.

Sanctions for Rule Breakers

In the event that client staff fails to comply with client standards, as they relate to HIPAA, action must be taken by client, and that action must be documented.

Contingency Plan for “Emergency Mode” (in the event of a complete outage)

In the event of a disaster, Internet, workstations, or even power, may not be reliable. Client should put in place a contingency plan for such a disaster. Paper copies of all forms is a good first step. After recovery, paper copies can be entered into Collaborate and shredded. PDFs of forms, stored locally, can help in the event of an Internet or server outage.

Collaborate-specifics

To help Client develop its HIPAA security policies, below is a (mostly) non-technical summary detailing how Collaborate helps you manage confidential information, including PHI.

Encryption

- Everything from your browser to Collaborate is encrypted using TLS 1.2 / SHA 256. TLS is essentially the successor to SSL.
- Everything on the server itself is stored on encrypted volumes, based on the industry standard AES-256.
- Backups also encrypted using AES-256.
- Any and all administration is done over SSH, it's an encrypted tunnel, which either uses AES-128 or AES-256.

Limiting who has access to what

Users

Each user has a unique username and password. Accounts are designed to be used by a single user, and not shared.

Passwords

Previous NIST guidelines suggest:

1) Forcing "strong passwords" that are not realistically memorizable.
2) Forcing users to reset passwords periodically.

Newer studies suggest both of these are potentially counterproductive. 2017 NIST password guidelines suggest memorizable passwords that are hard to guess, forbidding easily guessable passwords, and only forcing reset of password if a breach has been identified.

Network Ninja suggests using randomly generated passwords, and a password manager, and never using the same username & password combination for more than one resource.

Collaborate can be configured to work with client's password policy, the fundamentals of which should be based on the findings of their risk analysis.

Access Control Lists

IP Filtering can be enabled in Security Settings to limit what IP addresses are allowed to access your Collaborate instance. IPs can also be blacklisted. Traffic can be further restricted by Role. For example, "Administrators can only access our Collaborate instance from [this specific IP address].".

Role-Based Access

Client has ability to create Roles and isolate specific data access to those Roles. In production, client is responsible for ensuring the Roles in place meet the requirements identified during their risk analysis.

Login Monitoring & Security Events

Collaborate has built-in account and event monitoring to be used by client. Thresholds can be set for the following:

- Multiple security issues for the same IP address
- Attempts to perform unauthorized database activity
- Multiple login attempts for the same user account
- Multiple login attempts for the same IP address
- Multiple logins for the same user account from different IP Addresses

Limit Physical Access / Facility Access

These are reasonable standards for client to employ, as well, but this section is dedicated to Network Ninja's strategies.

Workstation Use Standards and Security

Username and password required to use, automatic logout, access both stage and production instances via encrypted means only, and encrypted filesystems.

Disposal of Data / Hardware

Client PHI is not co-mingled with other unrelated client data - each instance is segregated. The instance itself and the backups can be destroyed at clients request.

Backups and Storage

Backups are stored on disk, each backup contains only 1 client instance, and all backups are encrypted. Backups can be purged, and are not stored under any circumstances for more than 10 years, unless specifically requested.

Physical Access to Servers

Collaborate instances are hosted on AWS EC2. Their physical and operational security processes can be explored here. Physical access to hardware is strictly limited.

Data Integrity and Logging

- Cases cannot be deleted, but instead are made invalid.
- Creation and changes to data are logged, and admin-accessible, down to the form field, with time stamps - who did what, when.
- Locking of Clinical and Medical forms, so they can no longer be edited or deleted.

Automatic Logoff

- Automatic logoff/logout after 30, 60, or 90 minute increments (duration configurable, at client request) - 60 is typical.
- Logout redirect allowing automatic clearing of screen data at logoff time.
- When a user logs in after automatic logoff, they are brought back to their previous form.

Security Scanning and Automated Testing

All Collaborate instances are regularly scanned for both local and remote vulnerabilities, and patched in accordance to severity.

Security Incident Response

Breach Notification

In the event Network Ninja becomes aware of a security breach, client will be notified per industry standards and Business Associate Agreement (BAA) requirements.

Mitigation

Primary priority if a breach is discovered is mitigation.