Intro to HIPAA and how it relates to docSTAR

Disclaimer

This document is provided by docSTAR to our partners and customers in an attempt to answer some of the questions and clear up some of the mystery of HIPAA. The information provided herein is only intended to be a general summary of the subject matter. While every effort has been made to provide accurate information, no guaranty or warranty, express or implied, is made about the accuracy, currency, completeness or adequacy of the information provided, and no liability is assumed for any errors or omissions with respect to that information. The information is intended for educational purposes only and is not legal advice and should not be used as a substitute for legal or other professional advice. Each person and/or business should consult with counsel, as appropriate, concerning the applicability of this information to the particulars of their situation.

Summary

Some people may be under the mistaken impression that HIPAA compliance can be solved solely with technology. On the contrary, HIPAA compliance is primarily an organizational issue, over 70% of it being operational in nature. This means that in order to be compliant, the entire organization needs to be HIPAA compliant. Technology can help an organization get there, but it is only a small part of the solution. In fact it is impossible for any technology vendor to claim that their product is HIPAA compliant. The best a technology vendor can do is to design their products to make it easier for the customer to achieve HIPAA compliance.

Toward that end, docSTAR has been enhanced for use within a HIPAA compliant organization.

Introduction

The issue of HIPAA is something that has been troubling industries for several years now. Companies know that there is this new set of regulations that they need to adhere to, but there is much confusion about the specifics of these regulations. As a result many organizations don't know what they need to do, if anything, to achieve compliance. This whitepaper will attempt to answer questions that you might have about HIPAA and how it relates to document imaging.

The Health Insurance and Portability Act of 1996 (HIPAA) was passed as federal law on August 21, 1996. It contained the following general objectives:
- Guarantee health insurance portability
- Reduce healthcare fraud and abuse
- Guarantee the security and privacy of health information
- Introduce standards for the administration of health information to increase the efficiency of health care organizations

HIPAA was originally created primarily to make it easier for employees to move from one job to another without fear of losing health coverage. Most of HIPAA revolves around these considerations, however many other provisions were added to the law that deal with the other three areas listed above.

Although the law was passed several years ago, as of this writing, not all of its rules have been finalized. Since the law is not yet complete, organizations have some time to get up to speed with the new regulations. Additionally, the law will not be enforced until two years after all the rules have been written and finalized. This is important for the obvious reason that it is impossible to be in compliance with a law that has not yet been fully defined. With this in mind, we can discuss what we do know about HIPAA.

Administrative Simplification
HIPAA contains a large subset of rules called "Administrative Simplification." It is in here that we find the rules that are applicable to our needs. The rules are defined in three separate sections:
- Standards for Electronic Transactions
- Standards for Privacy of Individually Identifiable Health Information
- Security and Electronic Signature Standards

Of these rules, the first two have been finalized but do not really affect us, as they apply mostly to procedural issues surrounding health care organizations. The third rule is of the most interest to us, but has been languishing since 1998 and has not been finalized. As a result, the best information we have is from the proposed rule as published in the Federal Register on August 12, 1998. Details on these regulations can be found at http://aspe.hhs.gov/admnsimp/

Specifics of Security Standard (not yet finalized)
The following tables contain the items that are required for compliance with HIPAA. Items of interest to document imaging applications are in bold. After each table it is noted what, if any, items relate to docSTAR.

ADMINISTRATIVE PROCEDURES TO GUARD DATA INTEGRITY, CONFIDENTIALITY, AND AVAILABILITY	
REQUIREMENT:	IMPLEMENTATION:
Certification	
Chain of trust partner agreement	
Contingency plan (all listed implementation features must be	Applications and data criticality analysis. **Data backup plan.**

implemented).	**Disaster recovery plan.** Emergency mode operation plan. Testing and revision.
Formal mechanism for processing records.	
Information access control (all listed implementation features must be implemented).	**Access authorization.** **Access establishment.** **Access modification.**
Internal audit	
Personnel security (all listed implementation features must be implemented).	Assure supervision of maintenance personnel by authorized, knowledgeable person. **Maintenance of record of access authorizations.** Operating, and in some cases, maintenance personnel have proper access authorization. Personnel clearance procedure. Personnel security policy/procedure. System users, including maintenance personnel, trained in security.
Security configuration mgmt. (all listed implementation features must be implemented).	Documentation. Hardware/software installation & maintenance review and testing for security features. Inventory. Security Testing. **Virus checking.**
Security incident procedures (all listed implementation features must be implemented).	Report procedures. Response procedures.
Security management process (all listed implementation features must be implemented).	Risk analysis. Risk management. Sanction policy. Security policy.
Termination procedures (all listed implementation features must be implemented).	Combination locks changed. **Removal from access lists.** **Removal of user account(s).** Turn in keys, token or cards that allow access.
Training (all listed implementation features must be implemented)	Awareness training for all personnel (including mgmt). Periodic security reminders. User education concerning virus protection.

	User education in importance of monitoring log in success/failure, and how to report discrepancies. User education in password management.

- Data Backup Plan - docSTAR has a mechanism for backup of database and image files
- Disaster Recovery - docSTAR has an ability to rebuild its database from archived files in the event of a serious database failure
- Access Authorization/Establishment/Modification - docSTAR has a robust security mechanism for establishing and modifying user access to documents
- Internal Audit - The standard suggests companies audit logins, file accesses, security incidents, etc. docSTAR has mechanisms for auditing all types of document access. In docSTAR, the auditing capabilities were enhanced to include modifications of user rights, logons, logoffs, and failed logon attempts
- Maintenance of record of access authorizations - In docSTAR, (including later versions), the auditing capabilities were enhanced to include modifications of user rights, logons, logoffs, and failed logon attempts
- Virus Checking - Virus checking of critical systems is a good idea and docSTAR has approved the use of certain versions of Norton AntiVirus on docSTAR Host systems.
- Removal from access lists/Removal of user accounts - docSTAR has a mechanism for removing user accounts

PHYSICAL SAFEGUARDS TO GUARD DATA INTEGRITY, CONFIDENTIALITY, AND AVAILABILITY	
REQUIREMENT:	IMPLEMENTATION:
Assigned security responsibility	
Media controls (all listed implementation features must be implemented).	Access control. Accountability (tracking mechanism). Data backup. Data storage. Disposal.
Physical access controls (limited access) (all listed implementation features must be implemented).	Disaster recovery. Emergency mode operation. Equipment control (into and out of site). Facility security plan. Procedures for verifying access authorizations prior to physical access. Maintenance records. Need-to-know procedures for personnel access. Sign-in for visitors and escort, if appropriate. Testing and revision.
Policy/guideline on work station use	

Secure work station location	
Security awareness training	

None of these items relate to document imaging applications, so there is nothing of interest to us here.

TECHNICAL SECURITY SERVICES TO GUARD DATA INTEGRITY, CONFIDENTIALITY, AND AVAILABILITY	
REQUIREMENT:	**IMPLEMENTATION:**
Access control (The following implementation feature must be implemented: Procedure for emergency access. In addition, at least one of the following three implementation features must be implemented: Context-based access, Role-based access, User-based access. **The use of Encryption is optional**).	Context-based access. **Encryption.** Procedure for emergency access. Role-based access. **User-based access.**
Audit controls	
Authorization control (At least one of the listed implementation features must be implemented).	Role-based access. **User-based access**.
Data Authentication	
Entity authentication (The following implementation features must be implemented: Automatic logoff, Unique user identification. In addition, at least one of the other listed implementation features must be implemented).	**Automatic logoff**. Biometric. **Password.** PIN. Telephone callback. Token. **Unique user identification.**

- Encryption - This is optional, so there is nothing for us to be concerned with here
- User-Based Access - docSTAR has a robust security mechanism for establishing and modifying user access to documents with docSTAR Access Management module
- Audit Controls - docSTAR has mechanisms for auditing all types of document access with docSTAR Audit Trail module

  Data Authentication - docSTAR incorporates sophisticated Authentidate technology to ensure that documents have not been tampered with

- Data Authentication - Additional security is added with the United States Postal Service Electronic Postmark™(USPS EPM™) which is applied daily to provide trusted, third party verification for ultimate document integrity.

- Automatic Logoff - docSTAR has a mechanism for automatically logging off users that are idle for too long
- Password - docSTAR utilizes a password authentication mechanism
- Unique User Identification - docSTAR's security system provides for assigning each user a unique ID.
  In addition, docSTAR has a mechanism for importing users directly from a Windows domain server.

TECHNICAL SECURITY MECHANISMS TO GUARD AGAINST UNAUTHORIZED ACCESS TO DATA THAT IS TRANSMITTED OVER A COMMUNICATIONS NETWORK	
REQUIREMENT:	**IMPLEMENTATION:**
Communications/network controls (If communications or networking is employed, the following implementation features must be implemented: Integrity controls, Message authentication. In addition, one of the following implementation features must be implemented: Access controls, Encryption. In addition, if using a network, the following four implementation features must be implemented: Alarm, Audit trail, Entity authentication, Event reporting).	**Access controls.** **Alarm.** **Audit trail.** **Encryption.** **Entity authentication.** **Event reporting.** **Integrity controls.** **Message authentication.**

Since these items only apply to data transmitted across a network, they are mostly outside then realm of document imaging. In general, the security of the packets on a network is the responsibility of the network administrator. One exception to this would be if a client were to connect to a docSTAR host via NetConnect. In this case, use of SSL with NetConnect would be a requirement to be in compliance.

Another area that this could apply to is docSTAR's Send To capability. If Send To is used to get documents outside of docSTAR, these documents would no longer be inside docSTAR's secure environment. For this reason use of Send To in certain environments might not be considered compliant. In docSTAR, any or all of the Send To features can be disabled system-wide.

ELECTRONIC SIGNATURE	
REQUIREMENT:	**IMPLEMENTATION:**
Digital signature (If digital signature is employed, the following three implementation features must be implemented: Message integrity, Non-	Ability to add attributes. Continuity of signature capability. Countersignatures. Independent verifiability.

repudiation, User authentication. Other implementation features are optional.)	Interoperability. Message integrity. Multiple Signatures. Non-repudiation. Transportability. User authentication.

Electronic Signatures are not required for HIPAA compliance and are not currently implemented in docSTAR.

Conclusion
Understanding HIPAA can be a daunting task. This is largely because of the complexity of the legislation. Fortunately for a document imaging vendor, the majority of the effort in achieving and maintaining HIPAA compliance is administrative in nature for an organization that maintains health information. The technology used to store the health information is only a small part of the whole HIPAA equation.

Some organizations that need to be HIPAA compliant will appoint people within their organization to be in charge of the privacy and security aspects of the HIPAA regulations. These people will become intimately familiar with all the rules (once they are final,) and will be the ones responsible for ensuring that their organization is compliant.

Other organizations will opt to outsource these positions. There are already several companies offering HIPAA analysis and auditing services. Whatever route these organizations take, they can be sure that docSTAR will be helping them on their quest for HIPAA compliance.