InfoSafe Shredding
Mobile Document Destruction
"Protecting Your Privacy"
402-891-2688

"Protecting Your Privacy"
InfoSafe Shredding
Mobile Document Destruction
(402) 891-2688
www.infosafeshredding.com

FAQ on InfoSafe Shredding Services: Frequently Asked Questions on InfoSafe Shredding
Information And Video on One Time Cleanouts: Cleanouts and Purges

What does it mean to be “HIPAA Compliant”?

Article and information from True Vault author Trey Swann 10/30/13

This article is not a definitive list of what is required for HIPAA compliance. A Privacy Officer should be assigned to review each rule in its entirety. This article is intended to point you in the right direction with a more specific slant toward Document Destruction

If you have determined that you are handling protected health information (PHI) and that you need to be HIPAA compliant. Covered Entities and their Business Associates need to protect the privacy and security of protected health information (PHI).

There are 4 rules that you will need to explore:

1. HIPAA Privacy Rule
2. HIPAA Security Rule
3. HIPAA Enforcement Rule
4. HIPAA Breach Notification Rule

You need to follow the HIPAA Privacy Rule and the HIPAA Security Rule. And you need to provide notification following a breach of unsecured PHI (the Breach Notification Rule).

HIPAA Privacy Rule

The HIPAA Privacy Rule establishes national standards to protect individuals’ medical records and other personal health information and applies to health plans, healthcare 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.

Business Associates are directly liable for uses and disclosures of PHI that are not covered under their Business Associate Agreement (BAA) or the HIPAA Privacy Rule.

The Privacy Rule requires Business Associates to do the following:

1. Do not allow any impermissible uses or disclosures of PHI.
2. Provide breach notification to the Covered Entity.
3. Provide either the individual or the Covered Entity access to PHI.
4. Disclose PHI to the Secretary of HHS, if compelled to do so.
5. Provide an accounting of disclosures.
6. Comply with the requirements of the HIPAA Security Rule.

HHS, Privacy Rule:

http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html

HIPAA Security Rule

The HIPAA Security Rule requires appropriate Administrative, Physical, and Technical Safeguards to ensure the confidentiality, integrity, and security of protected health information (PHI).

The Security Rule is made up of 3 parts.

1. Technical Safeguards
2. Physical Safeguards
3. Administrative Safeguards

All 3 parts include implementation specifications. Some implementation specifications are “required” and others are “addressable.” Required implementation specifications must be implemented. Addressable implementation specifications must be implemented if it is reasonable and appropriate to do so; your choice must be documented.

An addressable implementation specification is not optional. When in doubt, you should just implement the addressable implementation specifications.

Technical Safeguards

The Technical Safeguards focus on the technology that protects PHI and controls access to it. The standards of the Security Rule do not require you to use specific technologies. The Security standards were designed to be "technology neutral.”

There are 5 standards listed under the Technical Safeguards section.

1. Access Control
2. Audit Controls
3. Integrity
4. Authentication
5. Transmission Security

Security Standards: Technical Safeguards

HHS offers insight into the Security Rule and assistance with the implementation of the security standards.

HHS: http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf

Physical Safeguards

Physical Safeguards are a set of rules and guidelines that focus on the physical access to PHI.

There are 4 standards in the Physical Safeguards section.

1. Facility Access Controls
2. Workstation Use
3. Workstation Security
4. Device and Media Controls

Security Standards: Physical Safeguards

HHS: http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/physsafeguards.pdf

Administrative Safeguards

The Administrative Safeguards are a collection of policies and procedures that govern the conduct of the workforce, and the security measures put in place to protect ePHI.

The administrative components are really important when implementing a HIPAA compliance program; you are required to assign a privacy officer, complete a risk assessment annually, implement employee training, review policies and procedures, and execute Business Associate Agreements (BAAs) with all partners who handle protected health information (PHI).

There are 9 standards under the Administrative Safeguards section.

1. Security Management Process
2. Assigned Security Responsibility
3. Workforce Security
4. Information Access Management
5. Security Awareness and Training
6. Security Incident Procedures
7. Contingency Plan
8. Evaluation
9. Business Associate Contracts and Other Arrangements

As with all the standards in this rule, compliance with the Administrative Safeguards standards will require an evaluation of the security controls already in place, an accurate and thorough risk analysis, and a series of documented solutions.

When you break down the 9 standards there are 18 things that you need to do.

1. Security Management Process - **Risk Analysis** (**required**): Perform and document a risk analysis to see where PHI is being used and stored in order to determine all the ways that HIPAA could be violated.
2. Security Management Process - **Risk Management** (**required**): Implement sufficient measures to reduce these risks to an appropriate level.
3. Security Management Process - **Sanction Policy** (required): Implement sanction policies for employees who fail to comply.
4. Security Management Process - **Information Systems Activity Reviews** (**required**): Regularly review system activity, logs, audit trails, etc.
5. Assigned Security Responsibility - **Officers** (**required**): Designate HIPAA Security and Privacy Officers.
6. Workforce Security - **Employee Oversight** (addressable): Implement procedures to authorize and supervise employees who work with PHI, and for granting and removing PHI access to employees. Ensure that an employee's access to PHI ends with termination of employment.
7. Information Access Management - **Multiple Organizations** (**required**): Ensure that PHI is not accessed by parent or partner organizations or subcontractors that are not authorized for access.
8. Information Access Management - **ePHI Access** (addressable): Implement procedures for granting access to ePHI that document access to ePHI or to services and systems that grant access to ePHI.
9. Security Awareness and Training - **Security Reminders** (addressable): Periodically send updates and reminders about security and privacy policies to employees.
10. Security Awareness and Training - **Protection Against Malware** (addressable): Have procedures for guarding against, detecting, and reporting malicious software.

11. Security Awareness and Training - **Login Monitoring** (addressable): Institute monitoring of logins to systems and reporting of discrepancies.
12. Security Awareness and Training - **Password Management** (addressable): Ensure that there are procedures for creating, changing, and protecting passwords.
13. Security Incident Procedures - **Response and Reporting** (**required**): Identify, document, and respond to security incidents.
14. Contingency Plan - **Contingency Plans** (**required**): Ensure that there are accessible backups of ePHI and that there are procedures for restore any lost data.
15. Contingency Plan - **Contingency Plans Updates and Analysis** (addressable): Have procedures for periodic testing and revision of contingency plans. Assess the relative criticality of specific applications and data in support of other contingency plan components.
16. Contingency Plan - **Emergency Mode** (**required**): Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode.
17. **Evaluations** (**required**): Perform periodic evaluations to see if any changes in your business or the law require changes to your HIPAA compliance procedures.
18. **Business Associate Agreements** (**required**): Have special contracts with business partners who will have access to your PHI in order to ensure that they will be compliant. Choose partners that have similar agreements with any of their partners to which they are also extending access.

Security Standards: Administrative Safeguards

HHS: http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards

HIPAA Enforcement Rule

The HIPAA Enforcement Rule spells out investigations, penalties, and procedures for hearings.

What's the penalty for a HIPAA violation?

HHS, Enforcement Rule:

http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/index.html

HIPAA Breach Notification Rule

The Breach Notification Rule requires most healthcare providers to notify patients when there is a breach of unsecured PHI. The Breach Notification Rule also requires the entities to promptly notify HHS if there is any breach of unsecured PHI, and notify the media and public if the breach affects more than 500 patients.

HHS, Breach Notification Rule:

http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html

Summary

HIPAA is really asking you to do 4 things:

1. Put safeguards in place to protect patient health information.
2. Reasonably limit uses and sharing to the minimum necessary to accomplish your intended purpose.
3. Have agreements in place with any service providers that perform covered functions or activities for you. These agreements (BAAs) are to ensure that these services providers (Business Associates) only use and disclose patient health information properly and safeguard it appropriately.

4. Have procedures in place to limit who can access patient health information, and implement a training program for you and your employees about how to protect your patient health information.