HIPAA Technical Training

CIBHS Small Counties Training
January 29, 2016

Training content accurate as of 1/28/2016 and will not reflect any regulation changes that are published after that date.
Copyright © by Xpio Health. All rights reserved.
- Progress through the slides at your own pace by either selecting the Next button at the bottom of the form or other buttons as instructed.

- Be sure to take your exam at the end of class!

How to Navigate the Class
- HIPAA Security Rules
- Security Responsibilities for IT Managers
- Encryption
- Computer and Laptop Security
- Strategies for Compliance

Covered in this session
Every organization must:
- Conduct a Security Risk Analysis
- Implement updated HIPAA documentation included P&P, BA agreements and Notice of Privacy Protection (NPP)
- Complete and document HIPAA training

Half of all data breaches now occur in healthcare
Attacks by hackers on healthcare providers have increased more than 100% since 2010
Most valuable data with the least protections
- Set rules for how PHI must be protected.
- Effective in 2005, located in 45 CFR Part 160 and Part 164; subparts A and C
- Privacy vs. Security
- Concerns the Confidentiality, Integrity and Availability (CIA) of ePHI
- The Rule is made up of Administrative, Physical and Technical Safeguards
- Safeguards are divided into Standards and Implementation Specifications; required or addressable

**Required or Addressable?**
- Specifications are set up as either
- Addressable does not mean optional
- Addressable allows more flexibility, but you must document why specification does not apply or your alternative method of satisfying

**The Security Rule**

- Approximately 50% of the rules are Administrative
- Focus is on the technology measures
- Primary goal is to create a “culture of compliance” that is realized through proper P&Ps, training and sanctions for failing to follow the rules
Requirements we designed to be scalable from the very largest of health plans to the very smallest of private practices.

The Security rule requires an evaluation of what security measures are in place, an accurate and complete risk analysis and the gap items mitigated.
The First and most important requirement of the Security Rule

Includes the process of identifying the potential security risks and determining the probability of occurrence and magnitude of risks

**Two parts:**
- Risk Assessment that includes a detailed list of questions based on ONC/OCR/NIST guidelines
- IT Infrastructure Assessment

---

**Top 10 Myths of a Security Risk Analysis**
- The security risk analysis is optional for small providers
- Simply installing a certified EHRs fulfills the SRA
- My EHR vendor took care of everything
- I have to outsource the SRA
- A checklist will suffice for the SRA
- There is a specific SRA method I must follow
- My SRA only needs to look at my EHR
- I only need to do an SRA once
- Before I attest for an EHR incentive program I must fully mitigate all risks
- Each year I have to completely redo my SRA

---

https://www.healthit.gov/providers-professionals/top-10-myths-security-risk-analysis

http://www.hhs.gov/hipaa/for-professionals/index.html

---

**The Security Risk Analysis**
• Security Management Process Standards
  • Risk Analysis (R)
  • Risk Management (R)
  • Sanction Policy (R)
  • Information System Activity Review (R)
• Assigned Security Responsibility (R)
• Workforce Security-access control
  • Authorization and/or Supervision (A)
  • Workforce Clearance Procedure (A)
  • Termination Procedures (A)
• Information Access Management
  • Isolating Health Care Clearinghouse Functions (R)
  • Access Authorization (A)
  • Access Establishment and Modification (A)

Administrative Safeguards; establishes the foundation for a security program
Security Awareness and Training
- Security Reminders (A)
- Protection from Malicious Software (A)
- Log-in Monitoring (A)
- Password Management (A)

Security Incident Procedures (R)
- Evaluation (R)
- BA Agreements (R)

Contingency Plan
- Data Back up Plan (R)
- Disaster Recovery Plan (R)
- ER Mode Operation Plan (R)
- Testing and Revision Procedure (A)
- Applications and Data Criticality Analysis (A)

Administrative Safeguards (continued)
https://www.law.cornell.edu/cfr/text/45/164.308
- **Facility Access Controls**
  - Contingency Operations (A)
  - Facility Security Plan (A)
  - Access Control and Validation Procedures (A)
  - Maintenance Records (A)
- **Workstation Use**
- **Workstation Security**

---

- **Device and Media Controls**
  - Media Disposal (R)
  - Media Re-use (R)
  - Media Accountability (A)
  - Data Backup and Storage (A)

---

**Physical Safeguards-to protect systems and buildings**

https://www.law.cornell.edu/cfr/text/45/164.310
- **Access Control**
  - Unique User ID (R)
  - Emergency Access Procedures (R)
  - Automatic Logoff (A)
  - Encryption and Decryption (A)
- **Audit Controls** (R)
- **Integrity** (A)

---

**Technical Safeguards** - the technology and P&Ps to use that protect ePHI

[https://www.law.cornell.edu/cfr/text/45/164.312](https://www.law.cornell.edu/cfr/text/45/164.312)

---

- **Person or Entity Authentication** (R)
- **Transmission Security**
  - Integrity Controls (A)
  - Encryption (A)
Business Associates are now fully responsible for following HIPAA regulations

Make a list of your current contracts that have exposure to PHI
- Some examples: Server support, network support, risk analysis vendor, copy or fax machines that save data to a hard drive

What’s included in a BAA?
- Include contract language
- Clearly define what is expected based on the most current 45 CFR regulations
- Protect your PHI and your reputation
- Process for regular audits
THIS HIPAA BUSINESS ASSOCIATE AGREEMENT (the "Agreement") is entered into effective [date] (the “Effective Date”), by and between XXXX ("Business Associate") and <<organization>> (the "Covered Entity").

Business associate and covered entity have a business relationship (the “Relationship” or the “Agreement”) in which business associate may perform functions or activities on behalf of covered entity involving the use and/or disclosure of protected health information received from, or created or received by, business associate on behalf of covered entity. Therefore, if business associate is functioning as a business associate to covered entity, business associate agrees to the following terms and conditions set forth in this HIPAA Business Associate Agreement.

Definitions

Catch-all definition:

The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

Specific definitions:

(a) Business Associate. “Business Associate” shall generally have the same meaning as the term “business associate” at 45 CFR 160.103, and in reference to the party to this agreement, shall mean [Insert Name of Business Associate].
- Encryption is considered Addressable, but by no means should be ignored
- If data on a server, fixed device or mobile device is encrypted, you are not obligated to report a loss as a breach
- We’ll discuss in the following slides
Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals

Protected health information (PHI) is rendered unusable, unreadable, or indecipherable to unauthorized individuals if one or more of the following applies:

1. Electronic PHI has been encrypted as specified in the HIPAA Security Rule by “the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key” (45 CFR 164.304 definition of encryption) and such confidential process or key that might enable decryption has not been breached. To avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt. The encryption processes identified below have been tested by the National Institute of Standards and Technology (NIST) and judged to meet this standard.

   ○ Valid encryption processes for data at rest are consistent with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices.¹

   ○ Valid encryption processes for data in motion are those which comply, as appropriate, with NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs, or others which are Federal Information Processing Standards (FIPS) 140-2 validated.
About FileVault

- You can use FileVault full disk encryption (FileVault 2) to help prevent access to documents and other data stored on your startup disk.

- FileVault uses XTS-AES 128 encryption. To use this feature, you need OS X Lion or later, and a working [OS X Recovery](#) volume on your startup disk.
Turn on FileVault

When you first set up your Mac, you might be asked if you want to turn on FileVault. You can check to see if FileVault is turned on in the Security & Privacy pane of System Preferences.

FileVault secures the data on your disk by encrypting its contents automatically.

**WARNING:** You will need your login password or a recovery key to access your data. A recovery key is automatically generated as part of this setup. If you forget both your password and recovery key, the data will be lost.

FileVault is turned off for the disk “Macintosh HD”.

Click the lock to prevent further changes.
# Macintosh HD:

<table>
<thead>
<tr>
<th>Available:</th>
<th>56.07 GB (56,069,779,456 bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capacity:</td>
<td>499.05 GB (499,054,952,448 bytes)</td>
</tr>
<tr>
<td>Mount Point:</td>
<td>/</td>
</tr>
<tr>
<td>File System:</td>
<td>Journaled HFS+</td>
</tr>
<tr>
<td>Writable:</td>
<td>Yes</td>
</tr>
<tr>
<td>Ignore Ownership:</td>
<td>No</td>
</tr>
<tr>
<td>BSD Name:</td>
<td>disk1</td>
</tr>
<tr>
<td>Volume UUID:</td>
<td>0E2C3B3F-B7DE-38C0-99A8-EC99661CE09C</td>
</tr>
</tbody>
</table>

**Logical Volume:**

| Revertible: | Yes (unlock and decryption required) |
| Encrypted:  | Yes                                 |
| Encryption Type: | AES-XTS |
| Locked:     | No                                  |
| LV UUID:    | C6C6ADBC-890B-4C84-9CF7-D4CE717B2269 |

**Logical Volume Group:**

<table>
<thead>
<tr>
<th>Name:</th>
<th>Macintosh HD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size:</td>
<td>499.42 GB (499,417,919,488 bytes)</td>
</tr>
<tr>
<td>Free Space:</td>
<td>10.5 MB (10,530,816 bytes)</td>
</tr>
<tr>
<td>LVG UUID:</td>
<td>951BEAB5-AEF9-4B64-A933-76770136AF9F</td>
</tr>
</tbody>
</table>

**Physical Volumes:**

**disk0s2:**

<table>
<thead>
<tr>
<th>Device Name:</th>
<th>APPLE SSD SM0512F</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media Name:</td>
<td>APPLE SSD SM0512F Media</td>
</tr>
<tr>
<td>Size:</td>
<td>499.42 GB (499,417,919,488 bytes)</td>
</tr>
<tr>
<td>Medium Type:</td>
<td>SSD</td>
</tr>
<tr>
<td>Protocol:</td>
<td>PCI</td>
</tr>
<tr>
<td>Internal:</td>
<td>Yes</td>
</tr>
<tr>
<td>Partition Map Type:</td>
<td>GPT (GUID Partition Table)</td>
</tr>
<tr>
<td>Status:</td>
<td>Online</td>
</tr>
<tr>
<td>S.M.A.R.T. Status:</td>
<td>Verified</td>
</tr>
<tr>
<td>PV UUID:</td>
<td>C7AA0EDB-8CC7-4817-9933-6C256F60537C</td>
</tr>
</tbody>
</table>
- Windows 7 Enterprise or Ultimate/Windows 8 Professional / Windows 10 Professional required
- Bit Locker integrated encryption
- TPM Module Admin may be required – BIOS
- And / or you may need to modify group policy
If you have a lot of devices, you may need to use an enterprise encryption management solution. Either way, the time, date, and mechanism the device was encrypted, screen shots, retention of keys, and lock down of local user ability to override encryption settings and then time date positive (legally defensible) upload (for CIBHS we use our Xpio Health ShareFile solution) to ensure device encryption in advance of loss can be proven.
- Included in the modifications to the HITECH Act in 2013
- If you render PHI unusable, unreadable, or indecipherable to unauthorized persons through the use of technology then there is no reportable breach in the event a device is lost or stolen.
- There is also a Safe Harbor method for de-identifying PHI covered in the HIPAA Privacy Rule 164.514 (b)(2). There are specific rules about how to de-identify the data that must be followed to meet the safe harbor requirements.
IT needs policies and procedures related to Workstation configuration that included detailed documentation of all configs.

All configurations should be periodically reviewed and validated.

- Can be completed by using a utility such as MS Baseline Security Analyzer (BMSA) or remotely using a scanner like Nessus.

- Group and Local Policies
- Registry settings
- Patches

**Workforce Training**
- Acceptable Use
- Unattended Workstations
- Passwords
- Use of Mobile Devices
- Media Disposal
- Incident/Breach Reporting
- Complete a Security Risk Analysis
- Evaluate all P&Ps for current regulation compliance
- Confirm your Contingency Plan is complete and you have a test plan for routine testing
- Evaluate your Physical Security and make necessary improvements
- Review the BAA in each contract that has access to PHI and update as needed
- Schedule staff training on security items, acceptable use
- Create the “Culture of Compliance”

**Compliance Strategies**
- You have completed the HIPAA 303-Technical Training
- Celebrate your successes!
- Reach out to Cheri Silveira at cheri@xpiohealth.com or Rikki Addis at raddis@cibhs.org

- Don’t forget to take the exam! Refer to the “How to Register” document for instructions