HIPAA Safeguard Training Curriculum
for Privacy and Security Officials:
A Simplified Approach

by
Edward D. Jones III
CEO, Cornichon Healthcare Select, LLC
March 10, 2016

Presented In HIPAA Integrity Webinar sponsored by WEDI
Today’s Focus (1/3)

- *HIPAA Integrity* Safeguard Training Curriculum
  - Covers HIPAA Privacy Administrative Requirements, HIPAA Security, and HITECH Act Breach Notification Training.
  - Designed for Covered Entity and Business Associate Privacy and Security Officials to Train Their Workforce Members.
  - Included with, Linked to, and Utilizes *HIPAA Integrity* Risk Analysis and Safeguard Policies and Procedures Compliance Text and Video Tools.
  - Provides Only Essential Concepts in a Simplified Format that Lead to Effecting Change in Workforce “Awareness and Understanding” of Safeguards and to Creating a More Secure Working Environment.
    » Safeguard Training Helps Your Workforce Avoid Costly Mistakes.
  - *HIPAA Integrity* Makes Available at an Optional Nominal Charge per Workforce Member a T/F and MC Questionnaire to Test and Document Workforce Member Safeguard “Awareness and Understanding”.
  - Curriculum Presented in Five (5) Lessons that can be Taught in a Single Seminar or in Sessions Over Several Staff Meetings.
• Today’s Focus (2/3)
  • Privacy, Security, Breach Notification Safeguard Training is Critical because...
    – Trained workforce members have a common interest in supporting and reinforcing each other in safeguarding protected health information (PHI) from unauthorized use, disclosure, or access.
    – The probability of a costly breach is less when each trained workforce member in a covered entity or business associate has the same “awareness and understanding” of safeguard policies and procedures.
    – Federal HIPAA Privacy and Security and HITECH Act Breach Notification Rules require such training of all workforce members (including management).
    – Cyber Security Insurers increasingly are requiring evidence of risk mitigation analysis, policies & procedures, and workforce member training.
      » Commercial general liability (CGL) policies no longer cover HIPAA/HITECH Act breaches, effective May 1, 2014, under Insurance Services Office (ISO) policy exclusions in most states.
• Today’s Focus (3/3)
  • “The most difficult part of implementing information protection is people. Security is ultimately a ‘people problem,’ not a technology issue.... People do not always understand the value of the healthcare data they access, but healthcare organizations can remedy this issue by educating and training the people who collect, use, store, and share that information. In doing this, healthcare IT can ensure that employees are aware of the value of their data, and therefore more inclined to take the extra steps to protect that data and ensure adversaries are not able to intercept it.... Training is crucial.” [emphasis added]

Today’s Agenda (1/2)

- Curriculum Scope
  - Lesson 1 (Safeguard Training Landscape)
    - HIPAA and HITECH Act Legislation
    - Enabling Regulations
    - Safeguard Compliance
      - Mission
      - Evidence (High Level)
      - Why Invest in Safeguard Compliance?
    - Safeguard Failures
      - Incidence
      - Costs
    - Enforcement
      - Principles
      - Compliance Reviews
    - Safeguard Training Regulations
      - Privacy and Breach Notification
      - Security

- Legend
  - FR means Federal Register (www.federalregister.gov)
• Today’s Agenda (2/2)
  • Lesson 2 (Foundational Principles and Definitions)
    – 3 Foundational Safeguard Principles
    – 14 Critical Safeguard Definitions
  • Introduction to Lessons 3-5
  • Lesson 3 (HIPAA Privacy Rule Administrative Requirements)
    – HIPAA Privacy Rule Administrative Requirements
  • Lesson 4 (HIPAA Security Rule)
    – HIPAA Security Rule
      » Administrative Safeguards
      » Physical Safeguards
      » Technical Safeguards
  • Lesson 5 (HITECH Act Breach Notification Rule)
    – HITECH Act Breach Notification Rule
Lesson 1 (HIPAA and HITECH Act Legislation)

  - Title II: Administrative Simplification (Privacy and Security).

- Health Information Technology for Economic and and Clinical Health (HITECH) Act, enacted February 17, 2009, as part of the American Recovery and Reinvestment Act (Public Law 111-5).
  » Subtitle D (Privacy) of Title XIII of Division A (Breach Notification).
• Lesson 1 (Enabling Regulations) (1/2)
  • Privacy
  • Security
  • Breach Notification
    – Breach Notification for Unsecured Protected Health Information: Interim Final Rule. 74 FR 42740-42770, August 24, 2009. Compliance for covered entities and business associates: September 23, 2009 (effective date for reporting breaches of PHI occurring on or after that date, with enforcement commencing for breaches occurring on or after February 22, 2010).
• Lesson 1 (Enabling Regulations)  

  • Modifications Final Rule

  • Each of these enabling regulations is accessible at: [http://www.hhs.gov/hipaa/for-professionals/index.html](http://www.hhs.gov/hipaa/for-professionals/index.html) or [http://www.ecfr.gov/cgi-bin/text-idx?SID=d7016c224c7c49489e98a2394c19b404&mc=true&tpl=/ecfrbrowse/Title45/45CsubchapC.tpl](http://www.ecfr.gov/cgi-bin/text-idx?SID=d7016c224c7c49489e98a2394c19b404&mc=true&tpl=/ecfrbrowse/Title45/45CsubchapC.tpl).
• Lesson 1 (Safeguard Compliance)  
  (1/2)

  • Mission for Covered Entities and Business Associates
    – Securing *protected health information* (PHI) so that it is not impermissibly accessed, disclosed, or used by unauthorized persons or processes.

  • Evidence (High Level)
    – Designating Privacy and Security Officials to **manage safeguard efforts and ensure ongoing vigilance**.
    – Conducting and periodically reviewing and updating an **analysis of risks** (threats and vulnerabilities) pertaining to PHI.
    – Identifying risk mitigation strategies and shaping safeguard **policies and procedures** based on risk analysis findings.
    – Training workforce members on “awareness and understanding” of safeguard **policies and procedures**.
    – Having in place and applying **sanctions** for safeguard violations.
    – **Documenting** all safeguard activities, actions, and assessments.

  – **Policy**
    • “a definite course or method of action selected from among alternatives and in light of given conditions to guide and determine present and future decisions.”
    • “a high level overall plan embracing the general goals and acceptable procedures especially of a government body.”

  – **Procedure**
    • “a series of steps followed in a regular definite order.”

  – **Note.** HIPAA and HITECH Act Safeguard Rules require policies and procedures to be in writing, which can be in electronic form, and be accessible to all covered entity and business associate workforce members.
• Lesson 1 (Safeguard Compliance) (2/2)

• Why Invest in Safeguard Compliance?

  – Evidence readily available in the event of a compliance audit or an investigation pertaining to a privacy breach, security incident, or complaint investigation.
  
  – Avoidance of significant federal financial penalties for a determination of noncompliance (e.g., audit) or evidence of a safeguard violation (e.g., investigation).
    » Up to $50,000 per violation and $1.5 million/calendar year for repeat of the same violation.
  
  – Increasing requirement by cyber security insurers of documentation in support of issuance or renewal of cyber security coverage.
    » “Recent breaches such as the massive attack on health insurer Anthem Inc. [78.8 million individuals affected] have caused underwriters to intensify their scrutiny of cyber risks.” Business Insurance, May 17, 2015.
    
    » Cyber security insurers will be increasing concerned with re-emergent costly threats, such as the recent ransomware threat at Hollywood, CA Presbyterian Medical Center.
• Lesson 1 (Safeguard Failures) (1/2)
  • Incidence (2011-2012)
    – OCR received 710 reports (breaches of 500 or more individuals) affecting a total of \( \approx 22.5 \) million individuals.
    – OCR received 77,240 reports (breaches of less than 500 individuals) affecting a total of 378,740 individuals.
  • Incidence (2015)
    – There have been 1,470 major breaches reported to OCR since September 2009, of which 11% were due to hacking, affecting 115.6 million individuals’ medical records. Of those records hacked, 97% occurred in 2015. Four of the five largest healthcare data breaches occurred in 2015. Data are from “Cybersecurity rising as health IT concern,” *Modern Healthcare*, February 29, 2016, p.33.
Lesson 1 (Safeguard Failures) (2/2)

Costs

- “The average cost paid for each lost or stolen record containing sensitive and confidential information increased from $145 in 2014 to $154 in this year’s study.”
- “If a healthcare organization has a breach, the average cost could be as high as $363.”
- Costs include remediating the harm, notification of breach to affected individuals, and lost business.
  - Ponemon Institute 2015 Annual Survey (sponsored by IBM), available at:
Lesson 1 (Safeguard Enforcement) (1/2)

Principles

– Covered entities and business associates retain the burden of proof under HHS compliance enforcement actions and must submit written records to HHS in an audit or investigation.

– Cooperation. HHS will seek cooperation of covered entities and business associates in obtaining compliance with Administrative Simplification provisions.

– Assistance. HHS, as part of its enforcement activities, may provide technical assistance to covered entities and business associates to help them comply voluntarily.

– Resolution Agreement and Corrective Action Plan if determination of willful neglect-not corrected as result of compliance audit or investigation related to a complaint or a breach. Examples at: http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html.
• Lesson 1 (Safeguard Enforcement)   (2/2)

• Compliance Reviews
  – HHS will conduct a compliance review to determine if a covered entity or business associate is complying with Administrative Simplification provisions if there is preliminary evidence indicating a potential violation due to willful neglect.
    » HHS Office for Civil Rights (OCR) has enforcement authority for HIPAA Privacy and Security Rules, and HITECH Act Breach Notification Rule.
  – HHS may conduct a compliance review to determine if a covered entity or business associate is complying with Administrative Simplification provisions in any other circumstance.
  – A covered entity or business associate must permit access to HHS during normal business hours to review records pertaining to compliance, or at any time and without notice if there is evidence of exigent circumstances.
  – HHS expected to begin desk audit compliance reviews later this month.
• **Lesson 1 (Safeguard Training Regulations)** (1/5)

• **Privacy and Breach Notification** (1/3)

  **Applicability.** Where provided, the standards, requirements, and implementation specifications adopted under [the Privacy Rule] apply to a business associate with respect to the protected health information of a covered entity. 45 CFR 164.500(c)

  **Standard: Training.** A covered entity [and business associate] must train all members of its workforce on the policies and procedures with respect to protected health information required by the [Privacy and Breach Notification Rules], as necessary and appropriate for the members of the workforce to carry out their functions....

  45 CFR 164.530(b)(1)
• Lesson 1 (Safeguard Training Regulations ) (2/5)
  • Privacy and Breach Notification (2/3)

**Implementation specifications: Training.**

(i) A covered entity [and business associate] must provide training that meets the requirements of paragraph (b)(1) of this section, as follows:

(A) To each member of the covered entity's [or business associate’s] workforce...
(B) Thereafter, to each new member of the workforce within a reasonable period of time after the person joins the covered entity's [or business associate’s] workforce; and
(C) To each member of the covered entity's [or business associate’s] workforce whose functions are affected by a material change in the policies or procedures required by the [Privacy or Breach Notification Rules], within a reasonable period of time after the material change becomes effective in accordance with the [Privacy Rule Policies and Procedures Administrative Requirement].

(ii) A covered entity must document that the training as described in paragraph (b)(2)(i) of this section has been provided, as required by the [Privacy Rule Documentation Administrative Requirement].

45 CFR 164.530(b)(2)
• Lesson 1 (Safeguard Training Regulations) (3/5)
  • Privacy and Breach Notification (3/3)

“We emphasize the importance of ensuring that all workforce members are appropriately trained and knowledgeable about what constitutes a breach and on the policies and procedures for reporting, analyzing, and documenting a possible breach of unsecured protected health information.”

78 FR 5658
Lesson 1 (Safeguard Training Regulations) (4/5)

Security (1/2)

- The HIPAA Security Rule Administrative Safeguard training objective is “to prevent, detect, contain, and correct security violations” pertaining to unauthorized access, disclosure, or use of electronic protected health information. 68 FR 8377

- Applicability. A covered entity or business associate must comply with the applicable standards, implementation specifications, and requirements of [the Security Rule] with respect to electronic protected health information of a covered entity. 45 CFR 164.302
• Lesson 1 (Safeguard Training Regulations ) (5/5)

• Security (2/2)

Standard: Security awareness and training.
(i) Implement a security awareness and training program for all members of its workforce (including management).

Implementation specifications.
(ii) Implement:

(B) Protection from malicious software (Addressable). Procedures for guarding against, detecting, and reporting malicious software.
(D) Password management (Addressable). Procedures for creating, changing, and safeguarding passwords.

45 CFR 164.308(a)(5)
• Lesson 2 (Foundational Safeguard Principles) (1/3)
  • Safeguards are rules and actions that fulfill the following three foundational properties of protecting an individual’s healthcare data or information:

    – **Confidentiality** is the property that data or information is not made available or disclosed to unauthorized persons or processes.
    – **Integrity** is the property that data or information have not been altered or destroyed in an unauthorized manner.
    – **Availability** is the property that data or information is accessible and useable upon demand by an authorized person.
• Lesson 2 (Foundational Safeguard Principles) (2/3)
  - *Confidentiality, Integrity, and Availability* are principles pertaining to Security Standards for the Protection of Electronic Protected Health Information—the Security Rule at 45 CFR 164.304.
  - These principles also are the foundation for rules and responsibilities of workforce members under the HIPAA Privacy Rule and HITECH Act Breach Notification Rule for safeguarding protected health information (PHI) when we broaden the definition of PHI and its identifiers to include information in hard copy and conveyed orally.
Lesson 2 (Foundational Safeguard Principles) (3/3)

- Know these overarching safeguard principles about **protected health information**...
  - **Confidentiality**: Unavailable to unauthorized users.
  - **Availability**: Accessible to authorized users.
  - **Integrity**: Not altered or destroyed without authorization.

- Any question by a workforce member as to authorization pertaining to these principles should be referred immediately to the Security Official.
• Lesson 2 (Critical Safeguard Definitions)
  • Know these 14 definitions...
    – Workforce
    – Person
    – Covered entity
    – Business associate
    – Use
    – Disclosure
    – Access
    – Health information
    – Individually identifiable health information
    – Protected health information
    – Designated record set
    – De-identification of protected health information
    – Requirements for de-identification of PHI (18 identifiers)
    – Unsecured protected health information
  • Will discuss those in red today!
• Lesson 2 (Critical Safeguard Definitions)

• **Workforce** means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate. 45 CFR 160.103

• **Person** means a natural person, trust or estate, partnership, corporation, professional association or corporation, or other entity, public or private. 45 CFR 160.103
Lesson 2 (Critical Safeguard Definitions)

- **Protected health information** means individually identifiable health information:
  
  (1) Except as provided in paragraph (2) of this definition, that is:
  
  (i) Transmitted by electronic media;
  
  (ii) Maintained in electronic media; or
  
  (iii) Transmitted or maintained in any other form or medium.

  (2) Protected health information excludes individually identifiable health information:

  (i) In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;

  (ii) In [certain student treatment] records described at 20 U.S.C. 1232g(a)(4)(B)(iv);

  (iii) In employment records held by a covered entity in its role as employer; and

  (iv) Regarding a person who has been deceased for more than 50 years.

45 CFR 160.103
Lesson 2 (Critical Safeguard Definitions)

Designated record set means:

1. A group of records maintained by or for a covered entity that is:
   i. The medical records and billing records about individuals maintained by or for a covered health care provider;
   ii. The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
   iii. Used, in whole or in part, by or for the covered entity to make decisions about individuals.

2. For purposes of this paragraph, the term record means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity. 45 CFR 164.501
Lesson 2 (Critical Safeguard Definitions)

Requirements for de-identification of protected health information.

(1/3)

A covered entity may determine that health information is not individually identifiable health information only if the following [18] identifiers of the individual or of relatives, employers, or household members of the individual, are removed:

(A) Names;
(B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:
   (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
   (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
(C) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
Lesson 2 (Critical Safeguard Definitions)

Requirements for de-identification of protected health information (2/3)

(D) Telephone numbers;
(E) Fax numbers;
(F) Electronic mail addresses;
(G) Social security numbers;
(H) Medical record numbers;
(I) Health plan beneficiary numbers;
(J) Account numbers;
(K) Certificate/license numbers;
(L) Vehicle identifiers and serial numbers, including license plate numbers;
(M) Device identifiers and serial numbers;
(N) Web Universal Resource Locators (URLs);
(O) Internet Protocol (IP) address numbers;
(P) Biometric identifiers, including finger and voice prints;
(Q) Full face photographic images and any comparable images; and
(R) Any other unique identifying number, characteristic, or code, except as permitted.

45 CFR 164.514(b)
• Lesson 2 (Critical Safeguard Definitions)

Requirements for de-identification of protected health information
(3/3)

Any of the 18 identifiers required for de-identification of protected health information can pinpoint the identity of an individual associated with healthcare information in a designated record set (medical record) at a healthcare provider, at a health plan (insurance file), or in the custody of a healthcare clearinghouse or business associate working on behalf of a covered entity.
Lesson 2 (Critical Safeguard Definitions)

- **Unsecured protected health information** means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of [the HITECH Act]. 45 CFR 164.402

- **Note.** Appropriate encryption for *data at rest* and *data in motion* is based on National Institute of Standards and Technology (NIST) specifications in sections 1(i) and 1(ii), respectively, in *Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals* at: [http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html](http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html).
  - Encryption under the NIST specifications provides a “safe harbor” for breach notification if ePHI is “secure” and not accessible to unauthorized persons.
• Lesson 2 (Summary)

Know with certainty and understand the 3 foundational principles and 14 critical definitions for safeguarding protected health information.
• Introduction to Lessons 3-5
  • HIPAA Safeguard Compliance Landscape
    – HIPAA Privacy Rule
    – HIPAA Security Rule
      » Administrative Safeguards—29
        • Business Associate Agreement—2
      » Physical Safeguards—14
      » Technical Safeguards—14
      » Compliance Protocols—3
    – HITECH Act Breach Notification Rule—18
  • 92 safeguard written policies and procedures required.
    – *HIPAA Integrity* has written all of them, ready to be tailored by findings from a covered entity or business associate’s risk analysis.
    – Workforce members are required to have access to a covered entity or business associate’s policies and procedures. 45 CFR 164.316(b)(2)(ii)
<table>
<thead>
<tr>
<th>HIPAA Integrity Privacy Rule Codes</th>
<th>Privacy Rule Administrative Requirements Standards</th>
<th>Privacy Rule Administrative Requirements Implementation Specifications</th>
<th>Exhibits: HIPAA Integrity Privacy Rule Administrative Requirements Forms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Rule (PR) Administrative Requirements (AR)</td>
<td>Introduction to Administrative Requirements</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PR AR 0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PR AR 1.1</td>
<td>Personnel Designations</td>
<td>Personnel Designations</td>
<td></td>
</tr>
<tr>
<td>PR AR 2.1</td>
<td>Training</td>
<td>Training</td>
<td>Privacy Safeguard Training for Workforce Members Log</td>
</tr>
<tr>
<td>PR AR 3.1</td>
<td>Safeguards</td>
<td>Safeguards</td>
<td></td>
</tr>
<tr>
<td>PR AR 4.1</td>
<td>Complaints to the Covered Entity</td>
<td>Documentation of Complaints</td>
<td>Privacy Safeguard Complaint Log</td>
</tr>
<tr>
<td>PR AR 5.1</td>
<td>Sanctions</td>
<td>Documentation</td>
<td></td>
</tr>
<tr>
<td>PR AR 6.1</td>
<td>Mitigation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PR AR 7.1</td>
<td>Refraining from Intimidating or Retaliatory Acts</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PR AR 8.1</td>
<td>Waiver of Rights</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PR AR 9.1</td>
<td>Policies and Procedures</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PR AR 9.2.1</td>
<td>Changes to Policies and Procedures</td>
<td>Changes in Law</td>
<td></td>
</tr>
<tr>
<td>PR AR 9.2.2</td>
<td></td>
<td>Changes to Privacy Practices Stated in the Notice</td>
<td></td>
</tr>
<tr>
<td>PR AR 9.2.3</td>
<td></td>
<td>Changes to Other Policies or Procedures</td>
<td></td>
</tr>
<tr>
<td>PR AR 10.1</td>
<td>Documentation</td>
<td>Retention Period</td>
<td></td>
</tr>
<tr>
<td>PR AR 11.1</td>
<td>Group Health Plans</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Lesson 3 (Privacy Rule Administrative Requirements)

- Know these Administrative Requirements, paying particular attention to...
  - (d) Standard: Complaints to the covered entity
  - (e) Standard: Sanctions
  - (g) Standard: Refraining from intimidating or retaliatory acts
  - (h) Standard: Waiver of rights

- A workforce member with any concern pertaining to these four standards should take his or her concern to the Privacy Official immediately.

- Where provided, the standards, requirements, and implementation specifications adopted under [Privacy Rule Administrative Requirements] apply to a business associate with respect to [use and disclosure privacy provisions specified in the business associate agreement or contract] with regard to the protected health information of a covered entity. 45 CFR 164.500(c)
Lesson 4 (Security Rule)

- The HIPAA Security Rule comprises Administrative, Physical, and Technical Safeguards.
- Covered entities and business associates—contractors and subcontractors are required to implement all provisions of the HIPAA Security Rule, having choice of security measures (inputs) as long as protections (outputs) are attained.
- The Security Rule is scalable and flexible, taking into consideration size and structure of business, costs of security measures, and probability and criticality of potential risks (threats and vulnerabilities), and is technology neutral with one exception: choice of encryption.
- Key provisions of the Security Rule are implemented through policies and procedures based on defined standards and implementation specifications and from findings from a written risk analysis periodically updated.
  - Foundation for the three types of safeguards—Administrative, Physical, and Technical—policies and procedures related to them, and safeguard training.
  - All safeguard policies and procedures and actions related to them must be documented, with documentation retained for 6 years from last action.
<table>
<thead>
<tr>
<th>HIPAA Safeguard</th>
<th>Security Rule</th>
<th>Security Rule</th>
<th>Exhibit: HIPAA Safeguard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Rule (SR) Administrative Safeguards (AS) 45 CFR 164.308(a)</td>
<td>Introduction to Administrative Safeguard Standards</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SR AS 0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SR AS 1.0</td>
<td>Security Management Process</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SR AS 1.1</td>
<td>Risk Analysis (R)</td>
<td>HIPAA Safeguard Risk Analysis Template</td>
<td></td>
</tr>
<tr>
<td>SR AS 1.2</td>
<td>Risk Management (R)</td>
<td>Risk Analysis Report Log</td>
<td></td>
</tr>
<tr>
<td>SR AS 1.3</td>
<td>Sanction Policy (R)</td>
<td>Workforce Member Sanctions Policy Acknowledgement</td>
<td></td>
</tr>
<tr>
<td>SR AS 1.4</td>
<td>Information System Activity Review (R)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SR AS 2.0</td>
<td>Assigned Security Responsibility</td>
<td>Security Safeguard Complaint Log</td>
<td></td>
</tr>
<tr>
<td>SR AS 3.0</td>
<td>Workforce Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SR AS 3.1</td>
<td>Authorization and/or Supervision (A)</td>
<td>1. Workforce Member Authorization Acknowledgement; 2. Stationary Hardware Assignment and Encryption Log</td>
<td></td>
</tr>
<tr>
<td>SR AS 3.2</td>
<td>Workforce Clearance Procedure (A)</td>
<td>Workforce Member Background Check Log</td>
<td></td>
</tr>
<tr>
<td>SR AS 3.3</td>
<td>Termination Procedures (A)</td>
<td>1. Workforce Member Exit Checklist; 2. Workforce Member Exit Interview Acknowledgement</td>
<td></td>
</tr>
<tr>
<td>SR AS 4.0</td>
<td>Information Access Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SR AS 4.1</td>
<td>Isolating Health Care Clearinghouse Functions (R)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SR AS 4.2</td>
<td>Access Authorization (A)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SR AS 4.3</td>
<td>Access Establishment and Modification (A)</td>
<td>1. Workforce Member Right of Access Authorization Modification Acknowledgement; 2. Workforce Member Right of Access Authorization Modification Log</td>
<td></td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>---------------------------------------------------</td>
<td>-----------------------------------------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>SR AS 5.0</td>
<td>Security Awareness and Training</td>
<td>Security Awareness and Training Specifications</td>
<td>Security Awareness and Training Forms</td>
</tr>
<tr>
<td>SR AS 5.1</td>
<td>Security Reminders (A)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SR AS 5.2</td>
<td>Protection from Malicious Software (A)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SR AS 5.3</td>
<td>Log-in Monitoring (A)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SR AS 5.4</td>
<td>Password Management (A)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SR AS 6.0</td>
<td>Security Incident Procedures</td>
<td>Response and Reporting (R)</td>
<td>Security Incident Report Forms</td>
</tr>
<tr>
<td>SR AS 6.1</td>
<td>Contingency Plan</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SR AS 7.1</td>
<td>Data Backup Plan (R)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SR AS 7.2</td>
<td>Disaster Recovery Plan (R)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SR AS 7.3</td>
<td>Emergency Mode Operation Plan (R)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SR AS 7.4</td>
<td>Testing and Revision Procedures (A)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SR AS 7.5</td>
<td>Applications and Data Criticality Analysis (A)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SR AS 8.0</td>
<td>Evaluation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SR BA 0</td>
<td>Written Contract or Other Arrangement</td>
<td></td>
<td>Business Associate Agreement Status Tracking Log</td>
</tr>
<tr>
<td>SR BA 1.0</td>
<td>Introduction to Requirements for Business Associate Contracts or Other Arrangements for Contractors and Subcontractors</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SR PS 0</td>
<td>Facility Access Controls</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SR PS 1.0</td>
<td>Contingency Operations (A)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SR PS 1.1</td>
<td>Facility Security Plan (A)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SR PS 1.2</td>
<td>Access Control and Validation Procedures (A)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SR PS 1.4</td>
<td>Maintenance Records (A)</td>
<td></td>
<td>Maintenance Records Log</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>--------------------------------------------------</td>
<td>-------------------------------------------------</td>
<td>-----------------------------------------</td>
</tr>
<tr>
<td>SR PS 2.0</td>
<td>Workstation Use</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SR PS 3.0</td>
<td>Workstation Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SR PS 4.0</td>
<td>Device and Media Controls</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SR PS 4.1</td>
<td>Disposal (R)</td>
<td>Log for Disposal of Hard Copy and Electronic Media Containing Protected Health Information (PHI)</td>
<td></td>
</tr>
<tr>
<td>SR PS 4.2</td>
<td>Media Re-use (R)</td>
<td>Log for Removal of Electronic Protected Health Information on Electronic Media Before Re-use</td>
<td></td>
</tr>
<tr>
<td>SR PS 4.3</td>
<td>Accountability (A)</td>
<td>1. Log of Movements of Stationary Information Systems and Electronic Media; 2. Log of Use of Portable Electronic Media Outside of the Facility: Assignment and Encryption</td>
<td></td>
</tr>
<tr>
<td>SR PS 4.4</td>
<td>Data Backup and Storage (A)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Rule (SR) Technical Safeguards (TS) 45 CFR 164.312</td>
<td>Introduction to Technical Safeguard Standards</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SR TS 0</td>
<td>Access Control</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SR TS 1.1</td>
<td>Unique User Identification (R)</td>
<td>Emergency Access Log</td>
<td></td>
</tr>
<tr>
<td>SR TS 1.2</td>
<td>Emergency Access Procedure (R)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SR TS 1.3</td>
<td>Automatic Log-off (A)</td>
<td>Data at Rest Encryption Log</td>
<td></td>
</tr>
<tr>
<td>SR TS 1.4</td>
<td>Encryption and Decryption (Data at Rest) (A)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SR TS 2.0</td>
<td>Audit Controls</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SR TS 3.0</td>
<td>Integrity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SR TS 3.1</td>
<td>Mechanism to Authenticate Electronic Protected Health Information (A)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SR TS 4.0</td>
<td>Person or Entity Authentication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SR TS 5.0</td>
<td>Transmission Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SR TS 5.1</td>
<td>Integrity Controls (A)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SR TS 5.2</td>
<td>Encryption (Data in Motion) (A)</td>
<td>Data in Motion Encryption Log</td>
<td></td>
</tr>
</tbody>
</table>
### HIPAA Safeguard Security Rule Codes

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SR CP 0</td>
<td>Policies and Procedures</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SR CP 1.0</td>
<td>Documentation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SR CP 2.0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SR CP 2.1</td>
<td></td>
<td>Time Limit (R)</td>
<td></td>
</tr>
<tr>
<td>SR CP 2.2</td>
<td></td>
<td>Availability (R)</td>
<td></td>
</tr>
<tr>
<td>SR CP 2.3</td>
<td></td>
<td>Updates (R)</td>
<td></td>
</tr>
</tbody>
</table>
Lesson 4 (Security Rule)

- **HIPAA Integrity** recommends that the covered entity or business associate Security Official provide an electronic copy of the *tailored* Security Rule policies and procedures to each workforce member for reading prior to the training seminar or staff meeting session for Lesson 4.

- The Security Official should describe at a high level the intent of each policy/procedure combination in securing protected health information and ask for any questions to ensure that there is an understanding of the safeguards.

- *The Security Official should emphasize that a workforce member who discovers or becomes aware of a security incident should report it immediately to the Security Official.*

- The Security Official should highlight access and use authorizations specified in each workforce member’s job description *and* the sanctions for non-compliance.

- The Security Official should maintain a safeguard training attendance log that is included with the **HIPAA Integrity** policies and procedures.
Lesson 5 (Breach Notification Rule)

What is a breach?

-Breach is the acquisition, access, use, or disclosure of protected health information in a manner not permitted under [the Privacy Rule] which compromises the security or privacy of the protected health information.

-This definition is abbreviated as there are exclusions and exigent circumstances. The complete definition can be accessed at 45 CFR 164.402 on the CFR Website: www.ecfr.gov.
• Lesson 5 (Breach Notification Rule)
  • If there is evidence of a breach, there are required reporting requirements unless there is a determination of a “low probability” of an “impermissible use or disclosure” of unsecured protected health information.
  • Determination of “low probability” is based on conducting a risk analysis that includes focusing on four required factors.
  • A covered entity or business associate may proceed with notification in the absence of conducting such a risk analysis.
  • There is a “safe harbor” in the event of a breach if the protected health information were secured through appropriate encryption described in the Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals, accessible at: http://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html.
Lesson 5 (Breach Notification Rule) (1/2)

<table>
<thead>
<tr>
<th>HIPAA Integrity Breach Notification Codes</th>
<th>Breach Notification Definition, Standards, and Requirements</th>
<th>Breach Notification Implementation Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table of Contents</td>
<td>Introduction and Breach Definition</td>
<td></td>
</tr>
<tr>
<td>Breach Notification Rule (BN) Notification (N) 45 CFR 164.400-.414</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BN N 0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BN N 1.0</td>
<td>Notification to Individuals</td>
<td></td>
</tr>
<tr>
<td>BN N 1.1</td>
<td>Timeliness of Notification</td>
<td></td>
</tr>
<tr>
<td>BN N 1.2.1</td>
<td>Content of Notification—Elements</td>
<td></td>
</tr>
<tr>
<td>BN N 1.2.2</td>
<td><strong>Content of Notification—Plain Language Requirement</strong></td>
<td></td>
</tr>
<tr>
<td>BN N 1.3.1</td>
<td>Methods of Individual Notification—Written Notice</td>
<td></td>
</tr>
<tr>
<td>BN N 1.3.2</td>
<td>Methods of Individual Notification—Substitute Notice</td>
<td></td>
</tr>
<tr>
<td>BN N 1.3.3</td>
<td>Methods of Individual Notification—Additional Notice in Urgent Situations</td>
<td></td>
</tr>
</tbody>
</table>
Lesson 5 (Breach Notification Rule) (2/2)

<table>
<thead>
<tr>
<th>HIPAA Safeguard Breach Notification Codes</th>
<th>Breach Notification Definition, Standards, and Requirements</th>
<th>Breach Notification Implementation Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>BN N 2.1</td>
<td>Notification to the Media</td>
<td></td>
</tr>
<tr>
<td>BN N 2.2</td>
<td></td>
<td>Timeliness of Notification to Media</td>
</tr>
<tr>
<td>BN N 2.3</td>
<td></td>
<td>Content of Notification to Media</td>
</tr>
<tr>
<td>BN N 3.1</td>
<td>Notification to the Secretary</td>
<td>Breaches Involving 500 or More Individuals</td>
</tr>
<tr>
<td>BN N 3.2</td>
<td></td>
<td>Breaches Involving Less Than 500 Individuals</td>
</tr>
<tr>
<td>BN N 4.1</td>
<td>Notification by a Business Associate</td>
<td></td>
</tr>
<tr>
<td>BN N 4.2</td>
<td></td>
<td>Timeliness of Notification</td>
</tr>
<tr>
<td>BN N 4.3</td>
<td></td>
<td>Content of Notification</td>
</tr>
<tr>
<td>BN N 5.1</td>
<td>Law Enforcement Delay Requirement</td>
<td></td>
</tr>
<tr>
<td>BN N 6.1</td>
<td>Administrative Requirements</td>
<td></td>
</tr>
<tr>
<td>BN N 6.2</td>
<td>Burden of Proof Requirement</td>
<td></td>
</tr>
</tbody>
</table>
Lesson 5 (Breach Notification Rule)

- A breach may be a privacy breach or a security incident.
- The Privacy and Security Official should emphasize in this lesson that a workforce member that is aware of or discovers a breach should contact each Official immediately and provide in writing information pertaining to the breach that is known.
- The Privacy or Security Official, as appropriate, should immediately assess the circumstances of the breach and strengthen defenses to avoid a recurrence.
- The Privacy or Security Official should access OCR’s Breach Notification Website at: [http://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html](http://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html), for information on timely reporting of the breach to affected individuals and to the Secretary of the Department of Health and Human Services (HHS).
• **Just to Recap before QUESTIONS... (1/2)**
  – Five Key Attributes for Achieving Safeguard Compliance
    • Designating Privacy and Security Officials
      – Can be same individual
    • Conducting a Written Risk Analysis
      – Reviewing and updating periodically
    • Implementing Safeguard Policies and Procedures
      – Compliant with standards and tailored to findings from Risk Analysis
      – Accessible to all workforce members.
    • **Training of Workforce Members on Safeguard Policies and Procedures**
      – Awareness and understanding of safeguards, with sanctions for violations.
    – **Maintaining Written Documentation of Safeguard Actions**
      – Written (can be electronic) and retained for 6 years from last action.
• **Just to Recap before QUESTIONS... (2/2)**

  – Most effectively taught by Privacy and Security Officials when risk analysis finished and policies and procedures tailored with risk analysis findings.

  – Most effectively learned when focus is on essential principles and definitions and workforce member directed to Privacy or Security Official when *any* question arises as to appropriate action.

  – Most effectively implemented when workforce members have immediate electronic access to in force policies and procedures.

  – Most likely to avoid privacy breach or security incident when workforce members participate together and mutually support each other in safeguard awareness training to manage threats and vulnerabilities as part of a risk mitigation strategy for sustaining the future of their businesses.