HIPAA Security Rule Overview

Marc D. Goldstone, Esq.
Hoagland, Longo, Moran, Dunst & Doukas, LLP
40 Paterson Street, P.O. Box 480
New Brunswick, NJ 08903
732-545-4717
732-545-4579 (FAX)
MGoldstone@Hoaglandlongo.com
www.healthlawnj.com
www.hipaasurvivalkit.com

Presentation Overview

- ✓ Audience Demographics
  - Novice (Can find the disk drive and put a disk in when prompted by Windows)

  - User (Can Install Windows Drivers for a new disk drive)

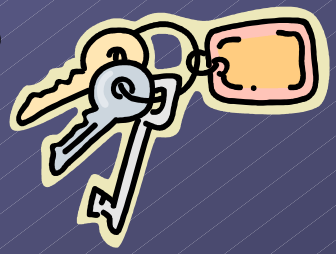
  - Techno-Geek (Who needs Windows? LINUX is where the action is!)

- ✓ HIPAA Security Rule Overview
- ✓ What's Coming Next?

Why do we need to know about information security? That's what I.T. folks are for.

- HIPAA's Privacy and Security Rules place a substantial burden on healthcare providers, health insurance plans, and healthcare clearinghouses (covered entities, or CEs.), regarding the private medical information that they maintain.
- The Security Rule applies to all "electronic protected health information" (E-PHI) maintained by CEs
- If you are a healthcare provider who bills electronically (or sends any of the standard transactions electronically, as most do, and as Medicare has REQUIRED if you have more than 10 FTEs after October of 2003), you are a CE AND you have E-PHI that you must keep secure in compliance with the Security Rule.

HIPAA is HIPAA, Right? Privacy vs. Security



- ***What*** to protect: The HIPAA Statute (and later additions contained in the *Privacy Rule)* identify the organizations that are covered entities, and the elements of health information that must be protected by a CE. Additionally, the Privacy Rule sets forth the only acceptable means of disclosing and using such protected information. The Privacy Rule applies to **ANY AND ALL** forms of protected health information (PHI).

- ***How*** to protect it: In contrast, the *Security Rule* only establishes minimum standards for the security of the information that the Privacy Rule sets out to protect. The Security Rule ONLY applies to information received, created, stored, maintained, or transmitted in ANY ELECTRONIC media or format (E-PHI). The Security Rule is an apparent attempt to drive "Best Practices" in information security for CE's; the Security Rule standards are flexible.

What Does the Security Rule Require?

- CEs must "[m]aintain reasonable and appropriate safeguards to ensure the integrity and confidentiality of the protected health information and to protect against reasonably anticipated threats or hazards to the security and integrity of the information, use or disclosure of this information."
- If only it were as simple as not forgetting to lock the door…

What That Means "In English"

- Covered Entities must:
  - Use their best efforts (or at least document that they gave it a really valiant try) …
  - to apply the best safeguards (or at least an affordable method that provides reasonably strong protection) …
  - to prevent the unauthorized modification or alteration of electronic form PHI (E-PHI) in their possession, and …
  - protect E-PHI from those who do not have a right to possess or view it, and …
  - protect E-PHI from computer viruses, worms, hackers, packet sniffers, disgruntled employees, etc., and also …
  - protect E-PHI from hazards such as lightning, floods, fire, etc.
- I said it would be "in English";
  I didn't say it would be brief.

Is There A Roadmap?

- The Security Rule permits each entity to review their own internal strengths and weaknesses, and then implement appropriate and reasonable action to comply with the Rule's requirements.
- The Security Rule does NOT dictate what method, means, software, hardware, etc., must be utilized.
- The Security Rule DOES require that CEs maintain detailed records of compliance.
- Thus, each CE sows the seeds of their own success or failure regarding the Security Rule, and, more disconcertingly, CE's must provide the "smoking gun" proving their failure to comply with the Security Rule to the Government, if asked!

Implementation Standards

- The Security Rule's individual compliance points are referred to as "SPECIFICATIONS."
- There are approximately 40 such specifications that CE's must address (there are a handful that, for several reasons, are either repetitive or are likely to apply to a very small subset of covered entities).

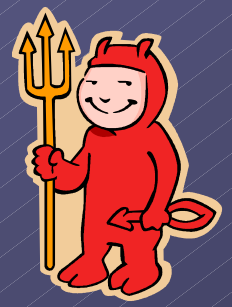
Categories

- The Standards are categorized in three groups; ADMINISTRATIVE, PHYSICAL and TECHNICAL, and collectively these groups are known as SAFEGUARDS.
  - Administrative Safeguard-9 Standards
  - Physical Safeguard-4 Standards
  - Technical Safeguard-5 standards
- The 40 implementation “specifications” exist within these standards

“Shall Do” or “May Do”?

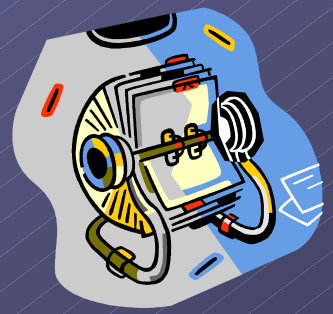
- The Rule establishes that each Specification is either *REQUIRED* or *ADDRESSABLE.*
- There are 20 required Specifications and 21 addressable Specifications.
- Required Specifications are, well… required. Gotta comply.
- Addressable Specifications are those that are not likely to be an issue with every covered entity, but must be addressed if one or more apply to a CE’s particular circumstances.
- It’s a little like Purgatory-your Security Rule compliance plan can place you between Security “heaven” and “hell”.

Is there a "Get out of Purgatory Free Card" available?



- CEs can implement ***Addressable Specifications*** in one of three ways:
  1. If a CE could reasonably and appropriately apply the Specification in its current business environment, then ***the CE must implement the specification.***
  2. If a CE cannot reasonably meet the Specification, but could implement an alternative measure accomplishing the same goal, then ***the CE must implement the alternative.*** The CE must document the rationale for utilizing alternative measures.
  3. Finally, if, after an assessment, the CE determines that the particular Specification is simply not applicable (neither reasonable nor appropriate) to it, ***then no action need be taken***. Again, the CE must ***document*** the rationale for determining that the Specification is not applicable to it.
- ***Documentation is KEY***; if you don't have the "back up" available when the Government comes calling, they reserve the right to assume you didn't intend to comply with the Security Rule!

Addressability-An Example



- Password Management is an addressable Specification.
  - A large integrated health system with hospitals, SNFs and medical groups in 4 states, and thousands of employees may require a code key (i.e, SecureID, etc.) that utilizes random numbers issued via satellite every 30 seconds to assure that all access is properly authenticated and that passwords remain safe
  - A medium sized physician practice may require only an operating system level (i.e., “Windows Log-On”) password management plan that requires the user to select a new password every two weeks (be careful; this one is easy to defeat by the employees!)
  - A solo practitioner with a support staff of one may not need password management at all (but lock the doors when the office is closed!)
- Now, on to the Individual Specifications …

Administrative Safeguards: Security Management

The first Standard is “Security Management process”. CE’s must implement policies and procedures to *attempt* to prevent, detect, contain, and correct security violations.

- ✓ Specification-Risk Analysis (Mandatory): A CE must conduct a thorough assessment of the potential risks and vulnerabilities to the security of the protected health information.
  - This is simply a baseline security audit. It may be helpful to model the analysis on a compliance baseline audit. Keep records of the audit methods and results.
- ✓ Specification (“Spec”)-Risk Management (Mandatory): A CE must implement a policy to maintain security measures sufficient to reduce risks and vulnerabilities.
  - If you find a security problem, or a high (unreasonable) risk, you must address it and document what you did. Think TQM. This is the “catch-all” standard.

Security Management-Con't

- Spec-Sanction Policy (Mandatory): CE's must implement a "Sanction Policy", to take corrective actions against employees who fail to comply with the CE's security policies and procedures. Corrective actions and sanctions should be graduated according to the severity of the breach. Additionally, other factors such as intent, malice, prior offenses, and the ultimate effect of the breach should all be considered as well. (Basically, the punishment should fit the crime.)
  - Write down what will happen to your staff if they violate your policies. The penalty for a security breach should be more severe than the penalty for showing up to work 6 minutes late.

- Spec-Information System Activity Review (Mandatory): CE's must establish a policy that requires regular reviews of the records of system activities to assure prolonged security. This includes such reviews as audit logs, access reports, tracking failed password attempts, and security incident reports and trends.
  - It's not enough to draft compliance documents; a CE must operate an "effective" Security plan (and maintain the ***documentation*** to prove it).

Administrative Safeguards: Assigned Security Responsibility

- ✓ Spec-Assigned Security Responsibility (Mandatory): Since there are no Specifications listed under this Standard, the Standard is in and of itself the Specification.
  - Have a policy in place to ensure the appointment of an appropriately qualified and trained Security Officer, and make sure that someone actually get appointed.
  - Tip-There are dozens of certifications in the I.T. world; do some "due diligence" to be sure that the Security Officer has the experience and qualifications to do the job, no matter how much "alphabet soup" he or she lays claim to.

Administrative Safeguards: Workforce Security

- Spec-A CE is required to implement policies and procedures to ensure that all members of the work force who require access to “electronic PHI” are granted such access, and that access to such E-PHI is restricted from those members of the workforce that do not require such access.
  - Each employee must be “cleared” by the CE to a) be present in an area where access to E-PHI is available, and b) each employee working in an E-PHI area must be subject to progressive levels of supervision (who watches the watchers?).

Workforce Security-Con't.

- Spec-Workforce Clearance Procedure: Each CE must have a policy to determine whether an employee should have physical access to E-PHI systems while "on the job."
  - Tip: this can be implemented within a "job-class" structure, rather than on an individual employee-by-employee basis.
- Spec-Termination Procedure: If you fire an employee, cut off their access to E-PHI **before or at the moment of termination**; if they change jobs, make sure that they still need the level of access they were granted at their prior assignment, or change their access.

Administrative Safeguards: Information Access Management

- Spec-Access Authorization: A CE must establish procedures to ensure that employees who are "cleared" are further "authorized" for access to E-PHI.
  - Pre-employment "background checks" cannot be the basis for granting access to E-PHI; the "clearance" to be *present* in areas where E-PHI access is available cannot automatically be the basis for a grant of *access* to E-PHI (although, practically, that may end up being the case). E-PHI should only be available to those employees who NEED the access to do their jobs.
- Spec-Access Modification: Once an employee is authorized to have access to E-PHI, the CE must respond appropriately to changes in job title and/or responsibilities, modifying or revoking access.
- Spec-Isolating Healthcare Clearinghouse Function: (Only applicable if the CE functions as a Healthcare Clearinghouse in a hybrid organization)

Administrative Safeguards: Security Awareness and Training

CE's must implement a security awareness/training program for all members of the workforce.

- ✓ Spec-Security Reminders (Mandatory): The CE must have a policy regularly to remind each member of the workforce of the CE's security policies.
  - Tip-obtain each employee's signature to prove that they received the periodic written reminder. Security post-test results are excellent documentation.
- ✓ Spec-Protection from Malicious Software (Mandatory): Each CE must establish procedures to protect their systems from malicious software.
  - 3 words: Anti Virus Program.

Security Awareness and Training-Con't

- Spec-Log-in Monitoring: Each CE must establish procedures to monitor log-on attempts.
  - Check who is "knocking" at the door of your E-PHI vault.

- Spec-Password Management: Each CE must establish procedures to manage the selection, and periodic revision of access passwords.
  - Make sure that people pick passwords that are hard to guess, and that the users change them periodically! A CE's password policy should reflect the security requirements of their organization, should be clearly documented, and should include a defined procedure for changing and safeguarding passwords.
  - TIP- require a minimum of 8 characters, including a combination of alphabetic and numeric characters (much harder for "password sniffer" programs to break than all "letter" passwords.)

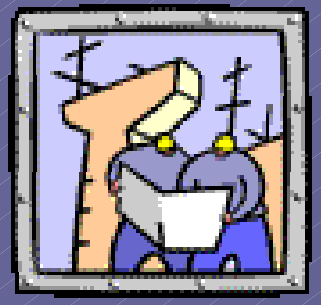
Administrative Safeguards: Security Incident Procedures

- ✓ Spec-Response and Reporting: A CE must implement procedures for responding to security incidents and for reporting the results of such response investigations.
  - In English: 2 Words-Internal Investigation. Simply knowing that a breach or attempted breach occurred is not enough. Just as with Medicare compliance, a CE must plan to investigate each incident, implement changes designed to mitigate the problems discovered by the investigation, and fully disclose the fact and results of the investigation to the CE's highest management levels.
  - Tip: The HIPAA Security Rule implies that ALL improper attempts (successful and unsuccessful) to access e-systems are "security incidents," period! (including "Pings"). There is controversy over what a "security incident" is, and whether DHHS has defined it appropriately. DHHS has acknowledged this and said it is working on clarifying the Rule's definition.

Administrative Safeguards: Contingency Plan

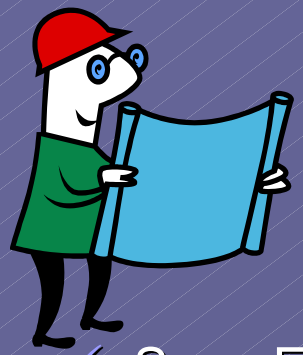
Each CE must implement a set of procedures in order to respond to any emergency or other occurrence that damages any system(s) that contain E-PHI.

- ✓ Spec-Data Backup Plan (Mandatory): This Specification requires that each CE implement procedures for the creation and maintenance of retrievable exact copies of any original files lost.
  - Make up-to-date backup copies of E-PHI. Further, each CE should have some means of creating and maintaining these “exact” copies at an off-site location. If a disaster damages the data at one location, the other set of data should remain safe.



Contingency Plan-Con't.

- Disaster Recovery Plan: Each CE must develop a set of procedures to restore any lost, damaged, or corrupt data, utilizing a backup set. Since this Specification relies upon the Data Backup Plan, failure to comply is likely to result in a sanction for violating both Specifications.
  - In English: Know how to get access to your backup data. If someone makes backups and takes them offsite each night, make sure to know how to get hold of that person (or their alternate) in case you need the backups to restore your data.
  - Tip-It's very easy to get carried away with redundancy; balance the cost of the proposed backup system with the risk of the loss and the immediacy of the need for the data.



Contingency Plan-Con't.

- Spec-Emergency Mode Operation Plan (Mandatory): A CE must develop backup procedures concerning emergencies, when usual policies and procedures for the protection of E-PHI can not be utilized.
  - Tell your staff what to do if your systems go down.
- Spec-Testing and Revision Procedure: Each CE must develop a plan to periodically test their electronic security systems, and to remediate any test failures.
  - Think of this Specification as a "fire drill" for your emergency mode operations plan.
- Spec-Applications and Data Criticality Analysis: A CE must review all E-PHI access programs in use. Additionally, any data stored by the applications should be assessed to determine if a data set is critical to operations. The CE must implement a procedure to readily restore any critical application or data set prior to the restoration of less critical information.
  - Tip: determine which of your software programs are critical to the security and access of E-PHI. Make sure that you have a plan to and are able to restore these applications (and their associated data files) in a timely manner, if they fail. Don't plan to restore the Kazaa or Limewire client before you restore your critical apps.

Physical Safeguards: Facility Access Controls

CE's must establish of a set of policies and procedures to assure that those employees with authorization can access electronic protected health information, while restricting the access of those without the necessary authorization.

- ✓ Spec-Contingency Operations (Mandatory): A CE must establish procedures for authorized personnel to gain physical access to all workstations or hardware containing or accessing E-PHI, at all times that the CEs business operates
  - If the administration office is open 9A-5P. but the patient care divisions see patients 7A-7P, and the E.D. is open 24/7, then there must be a plan in place to allow emergency access to the hardware that contains E-PHI 24/7. Giving the right people in the IT department master keys generally meets this specification.
- ✓ Spec-Facility Security Plan (Mandatory): The Specification requires policies and procedures to limit physical access to areas where E-PHI can be accessed
  - Lock doors; set alarms; install appropriate security systems, and use the security systems in place as they are designed to be used. If there is a need for human vigilance, security patrols or remote video access may be appropriate.

Facility Access Controls-Con't.

- Access Controls and Validation Procedures: A CE must implement a means of controlling and validating an individual's access to facilities where E-PHI may be accessed, based on the individual's role or function.
  - Think "Minimum Necessary" access to E-PHI. In general, the procedures used by a CE to determine the minimum necessary access to PHI for each employee (or class thereof) can be applied to E-PHI, as well. Simply put, everyone gaining intended or unintended access to E-PHI information should be authorized to access it. For example, an outside vendor on-site to fix a broken printer (not ordinarily considered a HIPAA "business associate") should not be given unrestricted access to the CE's E-PHI systems, nor should he or she be able to access E-PHI across the CE's network.
- Maintenance Records: A CE must document the state of the physical E-PHI security mechanisms in place, and the maintenance plan and actual damage, failures and repairs that have occurred to the physical mechanisms.
  - In English: Know what's locked and what's not. If a lock breaks, fix it and keep a record. If a breach occurs and you determine that a non-lockable door should now be locked, plan to install the lock, install it, and keep a record of the plan and the installation. It's just that simple.

Physical Safeguards: Workstation Use/Security

- Each CE must establish procedures for determining which workstations will be utilized for accessing E-PHI health information, and then restrict all other workstations from gaining access to E-PHI.
  - Think “overkill.” In addition to making sure that each employee knows the CE’s security policies, and is only granted password access to E-PHI if they have a “need to know”, each computer itself should only be capable of the access to E-PHI that the user of that computer needs.
- The physical location of the computers that access E-PHI must be secure.
  - Don’t leave your E-PHI workstations unattended/unsupervised, or accessible to unauthorized personnel. Some CEs may have to install separate “PHI” and non “PHI” workstations to comply.
  - TIP: This is a SIGNIFICANT change from the way that network architecture has evolved in the past 25 years. Network architecture is designed to REDUCE the number of computers and resources needed by SHARING the resources, not to increase the number required by SEGREGATING them. The technical folks will likely be VERY resistant to implement this Specification.

Physical Safeguards: Device and Media Controls

E-PHI is maintained on memory "Media". A CE must have memory media policies regarding:

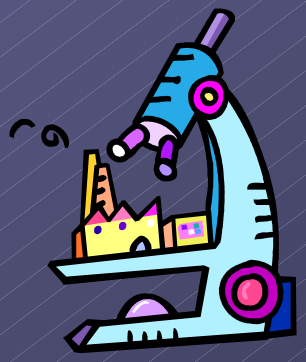
- ✓ Spec-Media Disposal (Mandatory): A CE must implement procedures to assure that E-PHI does not remain on discarded computers or components
  - **One word-Sledgehammer. Really. Physical destruction is good.**
- ✓ Spec-Media Re-Use (Mandatory): A CE must establish a procedure to "scrub" E-PHI from media when the media is to be re-issued or decommissioned.
  - **Simply deleting data/formatting a hard drive DOES NOT render the E-PHI on that device unrecoverable; it's just harder to access. Before the media is reused, the CE must have a procedure to "shred" or otherwise eradicate the data on it.**
- ✓ Spec-Accountability: A CE must document and track the movements of any hardware or electronic media that contains or access electronic protected health information. The documentation should also include the identity of the employee(s) responsible for the movement.
  - **It's 11:00. Do you know where your E-PHI is?**
- ✓ Spec-Data Backup and Storage: A CE must implement procedures to make current and accurate backup copies of E-PHI data.
  - **Someone or something has to regularly and accurately make backup copies of a CE's PHI, and store them in a safe place, readily accessible to a CE's authorized personnel … especially if hardware will be physically moved or relocated**

Technical Safeguards: Access Control

A CE must implement a means of appropriately granting or denying access to electronic protected health information.

- ✓ **Spec-Unique User Identification (Mandatory): A CE must implement procedures to uniquely identify each user of systems that contain or can access E-PHI.**
  - Make sure each authorized user has a unique log-in identification and password (know WHO is knocking, AND be sure that they are allowed in).
- ✓ **Spec-Emergency Access Procedures (Mandatory): A CE must implement procedures so that E-PHI can be accessed in an emergency.**
  - The IT staff must maintain an off-hours on-call schedule, and the CE's employees must know how to contact the on-call techs. The "human element" is indispensable; if a CE relies on redundant mechanical systems, and all systems fail, without the availability of "live" assistance to gain access to E-PHI, a Security Rule violation will probably result.
- ✓ **Spec-Automatic Logoff: CE's should have a procedure to implement automatic logoff on workstations that have access to E-PHI.**
  - Password Protected Screen Saver. This is not a required Specification, but there is no reason not to implement it. (every version of Windows since Windows 95 has this option available.) When someone walks away from their workstation, after a predetermined period of time, the computer should lock, requiring entry of a password to prevent unauthorized access to E-PHI.
- ✓ Spec-Encryption and Decryption: CEs should have a procedure to encrypt E-PHI.
  - Have the ability to use a code so that your E-PHI will be unintelligible to anyone who views it without authorization.

Technical Safeguards: Audit Controls



- Spec-A CE must implement hardware, software, or procedural mechanisms that record and examine the activity in computer systems that contain or access E-PHI.
  - Know who is entering your computer systems and what they are looking at, and keep records of this access and use.
  - TIP: This functionality is built into most modern operating systems (such as Windows), but usually must be manually enabled by the system administrator before it is effective.

Technical Safeguards: Integrity

Spec-A CE must implement policies and procedures to protect E-PHI from improper alteration or destruction.

- ✓ There must be a safeguard against unauthorized data alteration or destruction (i.e., “hacking”).
  - TIP-It isn’t enough to know that someone has “gotten in”; you must also be made aware if someone has changed any of your E-PHI (i.e., changed a 1.7 Potassium level to 7.1 [the difference between “dead” and “alive”, basically])

Technical Safeguards: Person or Entity Authentication

- Spec-A CE must implement procedures to verify that a person or entity seeking access to electronic protected health information is actually that person or entity.
  - Two Forms of I.D., please. This Specification is the reason that most CE's will need, at a minimum, unique user I.D.'s AND unique passwords.
  - TIP-An additional layer of assurance can be gained by restricting entry into the network based on the location from which the user seeks access. After all, someone surfing the 'net at the Beijing Starbucks probably doesn't need access to most CE's systems.

Technical Safeguards: Transmission Security

A CE must implement technical security measures to guard against unauthorized access to E-PHI that is being transmitted over an electronic communications network, such as the Internet.

- ✓ Spec-Integrity Controls: A CE must implement security measures to ensure that *electronically transmitted* E-PHI is not improperly modified without detection, and/or that electronic protected health information is not disposed of without authorization.
  - E-mailed E-PHI should arrive in the same form as it was electronically sent, and no one should have seen it during or after the transmission but the intended recipient.
- ✓ Spec-Encryption: A CE should implement a a means of encrypting electronic protected health information whenever deemed appropriate – such as when being transmitted over an insecure network.
  - The Internet is the world's BIGGEST AND MOST INSECURE network. Any time E-PHI is to be transported across the Internet, the transmission should be protected in some fashion.
  - **Tip: Unless a transmission is encrypted, it isn't secure. Secure transport mechanisms automatically encrypt the data for the user; Insecure transport mechanism can become more secure if the data to be sent is encrypted by the user before sending. The Internet doesn't have a roof or walls-ALL TCP/IP transmissions are subject to "packet sniffing."**

We're from the Government and we're here to help …

- The industry may now submit security questions to the ASKHIPAA mailbox at askhipaa@cms.hhs.gov
- *"The questions will become part of the FAQ under construction...."*
- So far, HHS hasn't been spectacularly helpful with HIPAA technical security issues, but that may change.

The Next Big Things

- Patch Management-when a vendor releases "fixes" for software, how does a CE manage the process of authenticating and installing the "patches."
- Social Engineering Training-how to prevent "bad actors" from conning the workforce into performing a seemingly innocent act that puts network security at risk (i.e., "Phishing").
- E-mail Fraud Prevention-how to ensure that the CE's systems aren't unwittingly used in part of an e-mail fraud scheme.

Other Resources

- The HIPAA Security Rule Survival Kit
  http://www.hipaasurvivalkit.com
- SANS Top 20 Internet Access Threats
  http://www.sans.org/top20/
- Mistakes People Make that Lead to Security Breaches:
  http://www.sans.org/resources/mistakes.php
- NIST Federal I.S. Standards FAQ:
  http://csrc.nist.gov/fasp/FAQ.html
- Firewall FAQ:
  http://www.interhack.net/pubs/fwfaq/
- CERT Coordination Center:
  http://www.cert.org/nav/other_sources.html
- Security Focus-good discussion of IS Security Issues
  http://www.securityfocus.com

Any Questions?

- Thanks for your kind attention!
- Follow-up questions/inquiries to:
  - MGoldstone@HoaglandLongo.com
  - Telephone: 732-545-4717
  - Fax: 732-545-4579