HIPAA Survival Guide

HITECH / HIPAA Best Practices
Securing PHI Basics

Topics

- Why secure PHI?
- Implications for the HIPAA Security Rule.
- Methods for securing PHI and corresponding Best Practices.

Why secure PHI?

Breach Notification

Section 13402(a) of the HITECH Act requires business associates and covered entities to report breaches of unsecured protected health information ("PHI").

What is unsecured PHI?

The term “unsecured PHI” means PHI that is ***not rendered unusable, unreadable, or indecipherable to unauthorized individuals*** through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111–5 on the HHS Web site.

What is secured PHI?

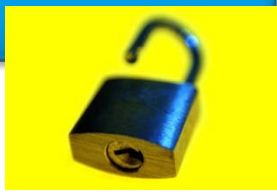
By contrast the term “secured PHI” means PHI that ***has been rendered unusable, unreadable, or indecipherable to unauthorized individuals*** by meeting the requirements of the technologies and methodologies provided in the Secretary’s guidance.

What is the bottom line?

If PHI is secured according to the Secretary's guidance then breach notification will ***never be triggered by definition***. Essentially, securing PHI according to the guidance provides the ultimate breach notification "safe harbor."

Security Rule Implications?

Security Rule Implications?

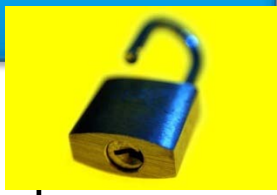


- The Security Rule ("SR") suggests but does ***NOT mandate*** the use of encryption and related technologies in order to secure PHI. *See* §164.312 (e) Technical safeguards.

- A covered entity or business associate ***may be in compliance with the Security Rule*** despite the fact that technologies recommended by the Secretary are not used.

- However, if the recommended technologies are not used then the PHI in question will be treated as "***unsecured*****"** and therefore breach notification may be triggered. *See* the Breach Notification Framework.

Security Rule Implications?



- The practical reality is that business associates and covered entities will likely have some PHI encrypted (e.g. where an EHR vendor provides it as part of their offering) while other PHI will remain in paper form or stored electronically but not encrypted.

- From a Security Rule compliance perspective, it is critical that the Required Risk Analysis capture where encryption and related technologies have been applied so as to facilitate a subsequent breach notification analysis. See §164.308 (a) (1) (Administrative safeguards).

Methods for securing PHI

PHI Data States

- The Secretary's guidance for securing PHI depends on the "state" the PHI is in.

- The following PHI data states have been identified:
  - PHI at Rest
  - PHI in Motion
  - PHI Disposed
  - PHI in Use

- The guidance refers to a number of National Institute of Standards and Technology ("NIST") guidelines for securing PHI in various states.

NIST Guidelines

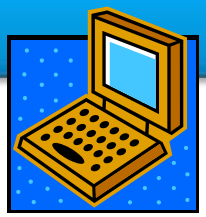
- NIST is ***responsible for developing standards and guidelines***, including minimum requirements, for providing adequate information security for all government agency operations and assets (except for national security systems).

- The Secretary's guidance is therefore ***based on a well vetted body of work*** that is suitable for business associates and covered entities because it is technically sound and widely used.

- The following NIST documents referenced in the guidance will be discussed: NIST Special Publication 800-111 (**PHI at Rest**); NIST Special Publication 800-52 (**PHI in Motion**); and NIST Special Publication 800-88 (**PHI Disposed**).

- Each NIST document contains ***references to other useful information*** (e.g. Federal Information Processing Standards or "FIPS") that provide more detailed treatment of various topics.

NIST Publication 800-111



- This is the NIST document that pertains to **PHI at Rest**.

- **PHI at Rest** is best thought of as PHI that is “stored” in end user devices (e.g. desktops, laptops, etc.), in file and database servers, in consumer devices (e.g. personal digital assistance, smart phones, etc.) and in removable storage media (e.g., USB flash drives, memory cards, external hard drives, writeable CDs and DVDs).

- **PHI at Rest** represents the “lion’s share” of the PHI that requires protection. It also represents the most significant challenge in terms of cost and operational complexity, especially because of the explosion in consumer devices and removable storage media.

- Assume that not all **PHI at Rest** will be encrypted as required anytime in the foreseeable future, and plan accordingly. For example, the amount of paper based PHI not subject to encryption will remain significant for many years to come. Further, even a substantial amount of electronically stored PHI may remain “unsecured” due to operational considerations.

PHI at Rest Challenges

- Experienced information security program managers, system administrators, and others who are responsible for selecting, deploying, managing, and maintaining storage encryption technologies are required.

- Encryption technologies must be centrally managed from an enterprise perspective to prevent, and/or respond to, technical challenges faced by clinical, administrative, and other staff as they perform their job responsibilities.

- Commercial solutions are available but may be cost prohibitive for all but the largest business associates and covered entities.

- Implementation of encryption technologies may have hidden costs reflected in increased staff training and redefined workflows.

PHI at Rest Best Practices

- **Adopt an 80/20 Rule**: develop a strategy for securing 80% of your PHI at Rest through the use of encryption functionality provided by commercial vendors that you are already doing business with (e.g. EHR vendors).

- **Mitigate Through Polices and Procedures**: reduce your exposure to potential PHI at Rest data breaches by implementing policies and procedures that limit the amount of PHI contained in end user devices and removable storage media to those that are deemed absolutely necessary.

- **Build Organizational Awareness**: develop a training program that stresses the importance of reducing the propagation of unsecured PHI and that encourages the prompt reporting of any unsecured PHI on devices the have been lost or stolen.

NIST Publication 800-52

- This is the NIST document that pertains to **PHI in Motion**.

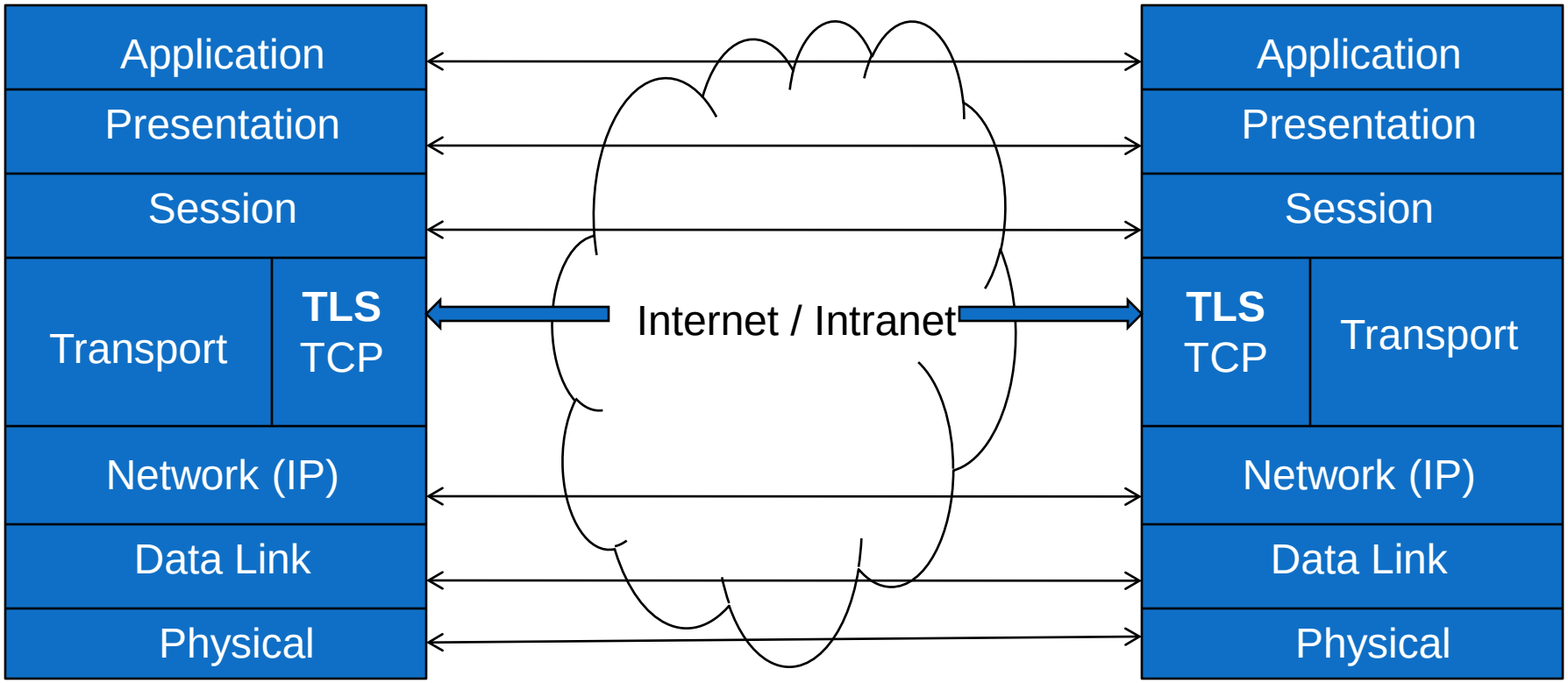
- **PHI in Motion** is best thought of as PHI that is “moving across the wire” either between applications that are communicating over the Internet or between applications communicating within the organization’s Intranet.

- The technology that NIST recommends for securing **PHI in Motion** is Transport Layer Security (“TLS”). TLS is a protocol created to provide authentication, confidentiality and data integrity between two communicating applications.

- TLS protects **PHI in Motion** at the transport layer of the ISO seven-layer communications model (also known as the seven-layer stack) and thereby allows two applications communicating PHI across the wire to secure communications without the need for intermediaries to participate.

- The TLS protocol specifications use cryptographic mechanisms to implement the security services that establish and maintain a secure TCP/IP connection. The secure connection prevents eavesdropping, tampering, or message forgery and thereby protects **PHI in Motion** from unauthorized use.

The ISO Communications Stack



TLS protects PHI in Motion across the wire

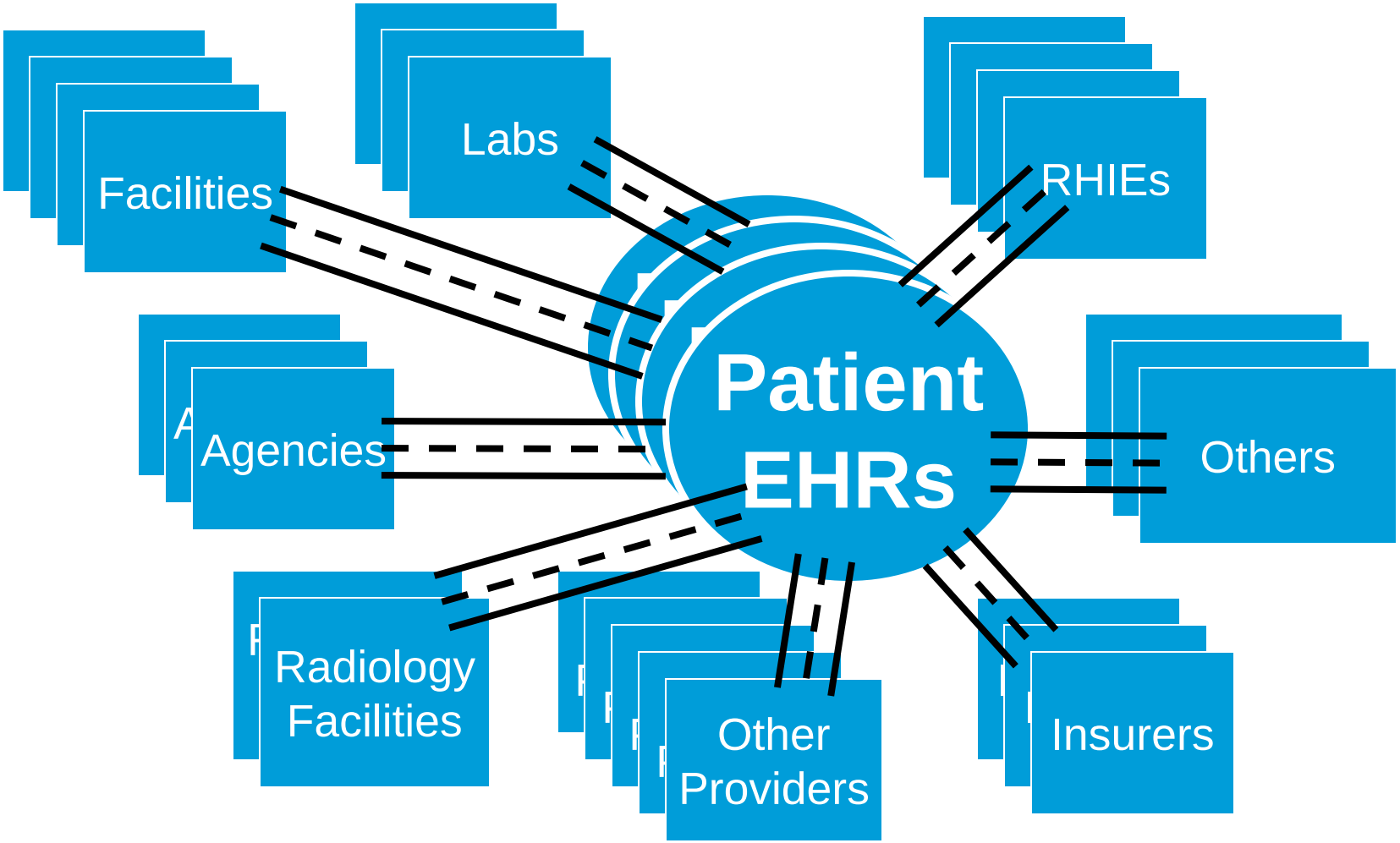
PHI in Motion Challenges

- You will need to identify all the “compliance touch points” wherein PHI is communicated, especially into and outside of the organization by way of the Internet.

- You will need to have access to experienced Internet security specialists that can help you setup, and periodically ensure, that the TLS version is up to date and “patched” with respect to the latest threats. Unfortunately, TLS is ***not the kind of technology that you simply set and forget***.

- TLS requires server-side “certificates” which is yet another technical component that must be managed over time—a level of complexity and sophistication that many small business associates and covered entities may find burdensome.

PHI “Touch Points”



PHI in Motion Best Practices

- **Secure Portals**: if you provide an Internet portal to patients, covered entities, business associates, employees, agencies, heath information exchanges, and/or others, where PHI is made available over the Internet, then TLS should be implemented.

- **Leverage Business Relationships**: for outbound PHI traffic insist that the party you are communicating with has implemented TLS on their web servers. At a minimum, you should inquire as to what secured communications features are in place.

- **Build Organizational Awareness**: ensure that your inventory of PHI communication touch points stay updated as you add a host of potentially new communications partners as envisioned by the HITECH Act (e.g. health information exchanges, regional health information organizations, etc.).

NIST Publication 800-88

- This is the NIST document that pertains to **PHI Disposed** or “sanitized.”

- When storage media are transferred, become obsolete, or are no longer usable or required by an information system containing PHI, it is important to ensure that residual magnetic, optical, electrical, or other representation of PHI that has been deleted (assuming that it has) is ***not easily recoverable*.**

- Sanitization refers to the general process of removing data from storage media, such that there is reasonable assurance that ***PHI may not be easily retrieved and reconstructed***.

- Covered entities and business associates ***must sanitize information system digital media containing PHI*** using approved equipment, techniques, and procedures prior to its release outside of the organization or if made available for alternative uses internally

- Covered entities and business associates must ***track documents and sanitization and destruction actions*** and periodically tests PHI sanitization equipment/procedures to ensure correct performance.

Media Types

- **Hard Copy**: media is comprised of physical representations of ***PHI such as: paper printouts, printer, and facsimile ribbons, drums, and platens*** are all examples of hard copy media. These types of media are often the most uncontrolled. PHI tossed into the recycle bins and trash containers exposes a significant vulnerability to “dumpster divers”, and overcurious employees, risking accidental disclosures. The Secretary has stated that ***redaction is not a proper method for destroying paper based PHI***.

- **Electronic (or Soft Copy):** PHI that is stored as bits and bytes contained in hard drives, random access memory (RAM), read-only memory (ROM), disks, memory devices, phones, mobile computing devices, networking equipment, and many other types. Electronic PHI is ***PHI at Rest*** when stored in various devices. Soft copy PHI ***must be disposed according to the Secretary’s guidance***.

Sanitization Methods

Method	Description
Clearing	Clearing is a method that ***protects the confidentiality of PHI against a robust keyboard attack.*** Simple deletion of items would not suffice for clearing. Clearing must not allow information to be retrieved by data, disk, or file recovery utilities. Clearing uses “overwrite” technology to remove all traces of PHI ***preventing most (but not all) unauthorized uses***.
Purging	Purging is a sanitization method that ***protects the confidentiality of PHI against a laboratory attack***. A laboratory attack involves a threat with the resources and knowledge to use nonstandard systems to conduct PHI recovery attempts on a device outside its normal operating environment. ***Degaussing is an example of a technology that can be use for purging***.
Destroying	***Destruction of PHI is the ultimate form of sanitization***. After PHI is destroyed, it cannot be reused as originally intended. Physical destruction can be accomplished using a variety of methods, including ***disintegration, incineration, pulverizing, shredding, and melting*** depending on the media.

PHI Disposed Challenges

- The primary challenge with respect to disposing of PHI according to the guidance is to have ***adequate training and processes*** in place to ensure that proper disposal of PHI is not overlooked during day-to-day operations.

- You will also have to ***purchase the tools and other equipment*** required to adequately dispose of PHI as well as providing training regarding proper use .

- There are many types of office equipment (e.g. copiers and faxes) that retain images of PHI and are almost never disposed of properly. You will need to build a ***complete list of equipment that may contain PHI*** that must be disposed of according to the guidance at its end of life.

PHI Disposed Best Practices

- **Get the Stupid Stuff Right**: shred or incinerate all paper based PHI so as to eliminate any potential for reconstruction.

- **Use Clearing Technologies for Electronic Media**: the Clearing method should be adequate for most electronic PHI unless special and unique circumstances exists that would indicate a need for Purging.

- **Build Organizational Awareness**: ensure that training with respect to PHI disposal accounts for all equipment that may contain “lurking PHI” and that staff is aware of PHI disposal requirements. You should also have a named individual that is responsible for PHI disposal and articulate a well defined process for equipment that is at end-of-life.