
# Advanced Strategies for Auditing HIPAA Compliance

Catherine M. Gorman-Klug RN, MSN
Corporate Director, Privacy and Data Security
December 2007

# Auditing

- Can be thought of the systematic, objective examination of processes, policies and activities that have been put in place to ensure compliance with regulatory or accreditation requirement
- At its best it is a collaborative effort of information exchange and mutually developed corrective action plans
- At it’s worst, it can be intimidating, appear as a dictatorship and thus create more problems then it solves

# Auditing as Risk Management

- The process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level
- Affords Covered Entities the opportunity to identify and remedy potential areas of non compliance before an incident occurs
- If a complaint is received will demonstrate good faith effort and due diligence in monitoring ongoing compliance

MERIDIAN HEALTH

# Auditing as an Educational Tool

- Rounding Audits can present opportunities for refreshers on varied topics
- Reignites staff awareness of need for compliance
- Opportunity to highlight and share creative approaches with other departments

MERIDIAN HEALTH

# “Perpetual Auditing”

- Ensuring Compliance with Privacy and Security regulations should be no different than ensuring readiness for any audit or survey!
- It must be
  - Ongoing
  - Embraced by the Operational Staff
  - Creative
  - Collaborative

MERIDIAN HEALTH

# Capitalize on Other Initiatives and Processes

- Ensure that a Privacy and Security Compliance Checklist is “snuck” into the ongoing JCAHO rounds
- Include an Assessment of Privacy and Security Features for all new purchases, agreements or other transactions that include PHI
- If your organization develops a system wide Risk Assessment ensure that Privacy and Security Compliance is included therein
- Include these initiatives on the system wide audit plans so they are reviewed at a Board Level

MERIDIAN HEALTH

# Don't *"HIPAA-tize"* Yourself into Compliance Complacency

- FDA
- GLB
- HIPAA
- S-OX
- PCI
- President's Task Force on Identity Theft

*All* have requirements for the protection of the privacy and security of an individual's information

# “Poly-Regulatoryism”

- The condition whereby you are afflicted with compliance of a multitude of regulation
- Chronic Disease State
- Will have frequent exacerbations
- Can cause a varied array of physical, emotional and financial symptoms

MERIDIAN HEALTH

# The “Ultimate” Audit

Familiarize yourself and the IT Technical and Security Staff with the components of the OIG Technical Security Audit

Conduct a Mock Audit of your Compliance

Develop a Checklist for what Privacy Issues you would audit if *you* were the OIG

# “Outside the Box” Auditing

- Data Loss Prevention
- Minimum Necessary
- Access Control
- Remote Users

MERIDIAN HEALTH

# Data Loss Prevention

Can loosely be defined as:

processes designed to prevent and detect the unauthorized transmission of data to those unauthorized to have access

Can occur maliciously or inadvertently

MERIDIAN HEALTH

# Data Loss Prevention

- Potential Risks:
  - Release of PHI performed that is not in accordance with federal and state laws
  - If standard procedures are circumvented there is an inability to demonstrate to whom the information was released and for what purpose
  - Potential for release to individuals to whom the patient has restricted access or release
  - Loss of proprietary information

MERIDIAN HEALTH

# The Myriad of Vectors of Loss

- Faxing to Erroneous Locations
- USB Drives
- Misdirected Emails
- Internet Postings including Blogs
- Remote Users
- Mobile Workforce
- Web-Based Email

MERIDIAN HEALTH

# Audit Strategies to Mitigate The Risk

- Review of Policies on the transmission of confidential information
- Review Technical Safeguards in place to prevent unauthorized transmission of confidential information
- Review processes in place to protect confidential data in transit
- Review Audit Logs of Transmission

MERIDIAN HEALTH

# Specifically Inquire:

- Are USB drives able to be used on devices that contain PHI?
- If so, how are the user rights to do so controlled?
- Is there an audit log in place to monitor such activity?
- How is the burning of CDs, DVDs controlled and Audited?
- Are mechanisms in place to provide HIM with a list of all such activity to adhere to ROI regulations?

MERIDIAN HEALTH

# Specifically Inquire:

- What mechanisms are in place to monitor FTP transactions?  What about interfaces? What about Internet postings?
- Is there the ability to control who has the ability to print PHI?
- How is this enforced with remote users?
- Is email traffic monitored for the transmission of PHI?
- Is there the ability to “white list” certain staff members who are permitted to email PHI and “blacklist” those who aren’t?

MERIDIAN HEALTH

# A Word about Web Based E-Mail….

- Often used by individuals who have legitimate access to information in the performance of illegal activities
- Will bypass protections in place for encrypting or otherwise protecting data-thus increasing the risk
- Is not monitored by all Data Loss Prevention Solutions

MERIDIAN HEALTH

# Minimum Necessary

- Also known as the rule of “Least Privilege”
- Should not just be applied to users of Clinical Applications
- Standard needs to be enforced across the enterprise
- Local and Remote Users

MERIDIAN HEALTH

# Areas to Investigate

- How is access assigned to Technical Staff?
- Are those individuals who are assigned to maintain the servers and other hardware also granted access tot the application level?
- If so, is this necessary to perform service?
- Is it audited?
- Can the same functions be accomplished by only granting access to “test” patients?

MERIDIAN HEALTH

# Areas to Investigate

- Are all members of a technical team given access “just in case” they may need to do repairs?
- Is it the practice to grant all Executives access to all systems by virtue of their position?
- Who has access to read email transmissions, as these may contain PHI?

MERIDIAN HEALTH

# Areas to Investigate

- How is the amount of access that is minimally necessary determined and defined?
- What process is in place to re-evaluate access when an individual changes positions within the Corporation?
- Do users who have dual roles (i.e. Nurses who serve as Clinical Instructors in Nursing Programs) required to use different access levels?

# Access Control

- Control is the operative word
- Essential for ensuring that minimum necessary standards are met, exceptions are documented, terminated users are removed in a timely manner, ongoing monitoring and auditing of access
- Must represent more than the creation of user accounts

MERIDIAN HEALTH

# Areas to Review

- What processes are in place for authorizing access to systems?
- Are these processes consistent across the enterprise?
- Are there different standards and processes for systems controlled by IT and those outside the purview of IT?
- How are exceptions tot the standard access levels requested and approved?

MERIDIAN HEALTH

# Areas to Review

- How are temporary employees granted access?  What authorization is required?
- How are students given access?  How is the life of their access determined?
- How is access granted to vendors?
- What processes are in place for emergency access? What is the time period that access granted via emergency access is valid?

MERIDIAN HEALTH

# Areas to Review

- What processes are in place for Physician Office Staff?
- What contractual requirements are in place to ensure compliance with policies including notification of new and removed users?
- Are there safeguards. i.e. Access Control processes in place to conduct period evaluations of validity of access needs?

# Terminating Users

- How is Access Control notified of users no longer employed or needing access?
- How are “departmental system” managers notified?
- What is the turn around time for access termination? How is this monitored?
- Are there different processes for Voluntary and Involuntary terminations?

# Terminating Users

What are the mechanisms in place for notification of termination for the following:

- Vendors
- Temporary Users
- Students
- Physician Office Staff

MERIDIAN HEALTH

# Remote Users

- Considered to be an area of great risk
- All individuals who access information remotely, by any means, including via the Internet (webmail), Extranet accounts, through the use of PDAs, and by the use of portable media should be considered remote users
- Unwise to not consider members of your own workforce as remote users

MERIDIAN HEALTH

# Definition to Consider

- **Portable Device:**
- 
- Media and devices which are or could potentially be removed from the organization's facilities or control. Such devices include but are not limited to PDAs, phones, smart phones,  laptops, hard drives; backup media, USB flash drives and any other data storage item which may contain "Confidential Information" as defined above.

- Includes all devices as defined above, which contain XYZ Confidential Information or EPHI even if **not** issued or owned by XYZ

# Evaluating the Risk

- What policies are in place defining remote access and the associated requirements?
- What processes are in place for granting users remote access?
- What policies and training mechanisms are in place for these users?
- Do you require encryption of information transmitted and stored on portable media?
- Are controls in place for devices not owned by your enterprise but which house your PHI?

MERIDIAN HEALTH

# Evaluating the Risk

- Is a listing of all Remote Users maintained? How is it updated? How is access controlled?
- Are users of systems outside the purview of IT included in this list?
- Are BAAs in place with all non-workforce members who access PHI remotely?
- How is remote activity logged?
- Are safeguards or policies in place to prevent users from saving passwords on remote devices such as those found at kiosks?

MERIDIAN HEALTH

# Proceeding With Audit Findings

- It will be impossible to mitigate all areas of risk
- Do not try and implement Corrective Actions that will jeopardize patient care
- Document acceptable risk exceptions and follow processes for Risk Acceptance

MERIDIAN HEALTH

# Remember…

The vast majority of the owners and users of these systems are individuals whose main occupation and focus and therefore knowledge of the requirements are worlds away from that of a Privacy/Security Professional- Namely Us!!!