Privacy and Security: Creating a Culture of Compliance from Purchase to Production

Catherine Gorman Klug RN, MSN
Corporate Director
Privacy and Data Security
Meridian Health

Agenda

- Evaluating potential purchases for compliance with applicable federal Privacy and Security Regulations
- Negotiating Contract Language that meets current requirements and sets the groundwork for continued compliance
- Implementing Customer Service Procedures that meet requirements without alienating customers
- “Deputizing” Users to monitor compliance

Patients Rights To Privacy and Security

- Rights are guaranteed and protected by multiple regulations and regulating bodies
- JCAHO, CMS and State Laws all have standards that require certain measures be put in place
- HIPAA as well as other Federal Laws have strict requirements

HIPAA:

- Focuses on the rights of individuals to control the uses & disclosures of their protected health information
- This includes but is not limited to the paper chart, the electronic chart, ancillary tests and results and all financial information
- Requirements are not new to healthcare but we have been lax in upholding the standards especially in areas not usually considered to be part of the “Medical Record”

Why Is HIPAA Different?

- It is a federal law, designed to establish a minimum floor for policies and procedures to protect patients
- Applies to not only information that is normally considered “clinical” information
- Covers any & all information gathered during a healthcare encounter
- The regulations apply to written, electronic and spoken information (including photos and X-Rays)
- It requires sanctions for violations

HIPAA is “Patient-Centric”

- Patients are granted certain rights
- They are Knowledgeable about these rights
- And they expect compliance!

Advances in Technology

- Medical Technology has made significant advances in recent years
- The advances have allowed people to lead longer and healthier lives
- They have also increased privacy and security risks

Points to Consider

- Less distinction between medical records, medical devices and technology
- Biomedical systems benefiting from advances in technology-many are mini EHRs
- Increase in use of technology has resulted in an increase of systems, devices and records not under the direct control of Information Technology, HIM or Privacy and Security Professionals

Examples of Information Systems

- PACS Systems
- Electronic Fetal Monitoring
- CT Scanners
- Electronic Medical Records
- Registry Data Bases
- Web Based Data Repositories
- EKG Systems

And all of these can create, store and transmit PHI!

Failure to Put Safeguards in place can lead to :

- Privacy and security breaches including inappropriate access or disclosure of information
- Malfunction of Patient Care Systems
- Loss of Patient Care Data
- Patient Injury
- Sanctions

The Result:

A greater proliferation, reliance and decentralization of Technology and Patient Information than ever before in History!

And it will only continue to escalate in geometric proportions.

The Good News

- Advances in the use of technology have improved patient and business outcomes
- Have made information more readily available for providers, even from remote locations
- Decreased TAT for billing and remittance

The Biggest Challenges

- Defining, Meeting and Maintaining standards for the Protection of the Information
- Produced, Stored and Transmitted by these Systems

Additional Challenges

- Devices and Other Medical Information Systems operate on a wide range of platforms
- Technology is often older and not designed with consideration of security and privacy needs
- Traditionally purchased and maintained at the department level
- “System Owners” are often not technically savvy or up to speed on Privacy and Security Issues

Vulnerabilities

- Privacy and Security Staff may not even be aware that these systems exist
- Potential exists for harm to the technology Infrastructure
- System Owners are likely unaware of controls that need to be put in place

Remember…

The vast majority of the owners of these systems are clinicians whose interpretation of Patient Confidentiality is a world away from that of a Privacy Professional-Namely Us!!!

But……It isn't the end of the world!

With careful planning and controls you can

- get control of the systems you currently have in place and those on your doorstep
- educate your users and vendors about your expectations

How do we tackle this?

- Know the key constituents that need to be involved:
- Materials Management or Purchasing Staff
- Legal/Risk
- Information Technology and Biomedical
- Privacy Officer
- Security Officer
- HIM

Convene the Group and Set forth their charge:

- Determine baseline system requirements
- Review of Applicable laws and regulatory requirements (HIPAA, JCAHO, FDA, OSHA, etc)
- Develop contract language that must be included, including BAA
- Develop a Process to review requests
- Process for addressing legacy systems

Lessons Learned…

- Be up front about your requirements
- Develop a minimum set of criterion that must be met prior to the purchase
- Consider developing a “Project Packet” for users that guides them through the requirements
- Be detailed-guide them to your requirements-

Contracts

- Detail exactly what your expectations are in the contract
- Do not rely solely on the Business Associate Agreement
- Ask for and review documentation to support features

Set the Ground Rules and Stick to Them

- Require the completed packet be submitted with a contract, drawings, etc for all new system purchases
- Get as much detail as you can
- Encourage your users to enlist the help of their vendors
- Apply this requirement to ALL new purchases, leases, grants, etc

Remember…

The vast majority of the owners of these systems are clinicians whose interpretation of Patient Confidentiality is a world away from that of a Privacy Professional-Namely Us!!!

Baseline System Requirements Should Address

- Access Control
- Physical Security
- Software Updates and Virus Protection
- System Backups
- Logging and Auditing

Access Control
Users

- User Access-unique I.D.s
- Ability to change passwords
- Role Based Access
- Auto Log Out
- Lock Out after failed attempts

Access Control: Support

- Will the vendor access the system remotely?
- What vehicle do they generally employ to do so?
- Is data encrypted?
- How do they address terminated users?
- What Privacy and Security Measures do they have in place?

Software Updates and Virus Protection

- Does the vendor allow application of virus protection software?
- How do they handle Operating system patches?
- What is their TAT for analyzing and approving new patches and updates?
- Does the application of patches void the warranty?
- What is their position on auditing scans for Compliance? Must this be done when the system is not live?

Evaluating the Requests

- Designate someone to screen all packets against your baseline standards (a checklist works well here)
- Distribute any outliers to the subject matter expect of that area
- Develop deal breakers and areas of compromise
- If the product is not compliant but there is a business case to support its purchase document the rationale and any measures you can put in place to mitigate risk

Next Steps….

- If you haven't already done so conduct an enterprise wide risk assessment
- Send out and require a response for all departments
- Do Not Assume that you are aware of everything that is out there
- Develop an inventory of all networked and stand alone devices and systems that create, store or transmit PHI in any form

The Results are In…

- After reviewing Security and Privacy features they have in place develop a mechanism to contact your high risk ones immediately
- These are those systems that have no user I.D.s, no back ups, no timeouts and no audit trails

Do a Screening-First

- Utilize your new Product Evaluation tool to identify the Systems putting you at the greatest risk
- Utilize a more in-depth tool to evaluate these
- Remember to review Policies on the Designated Record Set and Record Retention Requirements

Be Careful What you Wish For…

- Likely you will find an abundance of systems that have little or no security features
- You'll find a handful that have minimal available features, but they aren't "turned on"
- But, there will be a few that have the features you are looking for, but no one knew about them!

Knowledge=Compliance

- Educate your users
- Bring them up to speed on what your expectations are and what is at stake
- Encourage them to work with their vendors

Education Needs

- Assigning user I.D.s and passwords
- Removing deleted users
- Monitoring and applying operating system patches and service packs
- Storage of Information
- Back-up Procedures
- System Administrator Responsibilities

Drizzle..don’t drown!

- Old habits will die hard…
  - Provide and guide the owners of these systems with basic information in small doses
  - Make sure you have policies and procedures that they can understand

Remember…

The vast majority of the owners of these systems are clinicians whose interpretation of Patient Confidentiality is a world away from that of a Privacy Professional-Namely Us!!!