HIPAA Security

Grace Upleger
3-7-05

HIPAA

Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Administration Simplification
- Facets and respective compliance dates:
  - Privacy – 4-14-03
  - Transactions and Code Sets – 10-16-03
  - Identifiers – Various (next is 5-23-07)
  - Security – 4-20-05

Security

HIPAA Security Regulation’s Goal: To adopt national standards for safeguards to protect the confidentiality, integrity, and availability of Electronic Protected Health Information (EPHI).

EPHI includes all individually identifiable health information related to our patients or research subjects that is created, maintained, or transmitted electronically by VUMC.
Issues in the HIPAA team scope

- Business Associate Agreements
- Encryption
- Email correspondence
- IT Procurement initiatives
- Physical security for systems that contain EPHI
- Role-based access in systems that contain EPHI
- Audit trails and monitoring log-ins
- Mobile device requirements
- Maximum Data Center requirements
- Disaster Recovery/Data Backup requirements
- Being able to recover from backup to time of downtime
- Etc....

What exactly does HIPAA say? Some required pieces that will affect you:

- Risk analysis & Risk management
- Security awareness and training
- Password management
- Sanctions
- Security Incidents

Access policy & Sanctions policy in draft
Information System Activity Review policy in draft

Sanctions policy - draft

<table>
<thead>
<tr>
<th>Level (1 to 4)</th>
<th>Offences</th>
<th>Minor Disciplinary Corrective Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1: Carelessness</td>
<td>Failure to properly sign off a terminal or secure a computer</td>
<td>VERBAL WARNING</td>
</tr>
<tr>
<td></td>
<td>Leaving medical records or a copy of patient health information (PHI) or other confidential information in a non-secure area</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Entering a file that includes PHI or other confidential information to the wrong person</td>
<td></td>
</tr>
</tbody>
</table>

VERBAL WARNING
<table>
<thead>
<tr>
<th>Level (1-4 levels)</th>
<th>Principles</th>
<th>Minimum Disciplinary / Corrective Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>2: Ngentive Act:</td>
<td>Failure to account for disclosures outside of treatment, payment, and operations within the VUMC Disclosure Tracking system. Failure to take reasonable precautions to prevent incidental disclosures of highly sensitive patient health information. Sending protected health information through unsecured email.</td>
<td>WRITTEN PERFORMANCE COUNSELING</td>
</tr>
<tr>
<td>Not following procedure</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Level (1-4 levels)</th>
<th>Principles</th>
<th>Minimum Disciplinary / Corrective Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>3: Purposeful Act: Curiosity or Concern</td>
<td>Sharing an ID/password with another coworker or encouraging another coworker to share an ID/password. Accessing or connecting to VUMC information systems (i.e., computers, servers, routers, switches) without authorization. Accessing and reviewing the record of a public personality or any other patient record out of concern or curiosity without authorization.</td>
<td>Final performance improvement counseling</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Level (1-4 levels)</th>
<th>Principles</th>
<th>Minimum Disciplinary / Corrective Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>4: Purposeful Act: Blatant Misuse</td>
<td>Accessing or allowing access to patient health information (PHI) without having a legitimate reason, and disclosures or abuse of the patient health information (PHI) for personal gain or malicious intent. Accessing a patient record for non-information in a personal relationship. Compiling a mailing list for personal use or to be sold</td>
<td>INITIATE TERMINATION</td>
</tr>
</tbody>
</table>
Email *draft policy*

Email traversing the network from an internal Vanderbilt source to outside the network is insecure (like a postcard).

We need to protect our EPHI.

**Solutions:**
- Use MHAV for communicating with patients or referring physicians
- Use encrypted portals or other mechanisms

*In draft Communications Policy*

---

**Device and media controls**

- **Disposal**
- **Media re-use**
- **Accountability**

Device and Media Controls Policy in draft

---

**Draft Communications Policy**

To protect Vanderbilt University Medical Center (VUMC) electronic restricted data in transit and in storage on any computing device or media, such as workstations, laptops, PDA’s, floppy disks, and flash drives.

Username and password is the minimum requirement for unique user identification for all devices, including hand held devices, if possible.

Also required: anti-virus software; password protected screen savers; automatic logoffs.
Other policies in draft

- Business Associate Agreements
- Transcription
- Maximum Data Center (MDC)
  - Data that is considered primary source, needing high availability or highly confidential data will be recommended to be placed in a MDC
  - Standards have been developed, such as fire suppression, visitor control, raised floor, etc....

Information Systems Activity Review (draft policy)

- Review system level reports regularly that depict user activity
  - Audit Trails – 1 year for inquiries; 5 years for modifications
  - Log-In monitoring (user ID’s)
- Requesting plans on how/when departments will implement

Business Continuity Pieces of HIPAA

- Standard: Contingency plan
- Data backup plan (Required)
- Disaster recovery plan (Required)
- Emergency mode operation plan (Required)
- Testing and revision procedures (Addressable)

Business Continuity policy finalized - 2004
What Can You Do to Assist the HIPAA Team?

- Answer questionnaires
- Respond to gap analysis, if needed
- Attend educational sessions
- Complete HIPAA training

The HIPAA Task Ahead

- Ensure compliance or plans in place by April 2005
- Contact 800+ departmental groups to identify systems and verify System Owners
- Ensure all information, even “under the desk” and “closet” servers and systems appears in assessment
- Gather – Review – Recommend
- Distribute Gap Report to System Owners

New Systems Implementation – WE NEED YOU!!

- Include IT in process
  - RFI/RFP
  - Contract/BAA
  - Backups/Firewalls
  - Role based access controls
  - Authentication
  - Audit trails/login monitoring
  - Business continuity/DR requirements
  - Data center needs


FIFI
Links

To view the actual regulations:
Vanderbilt HIPAA webpage:
http://www.mc.vanderbilt.edu/toolVume.php?site=HIPAA
For HIPAA Overall:
Health and Human Services:
http://aspe.hhs.gov/admnsimp/index.shtml
American Hospital Association HIPAA site:
http://www.hospitalconnect.com/aha/key_issues/hipaa/index.html
Guidelines for Academic Medical Centers:
http://www.aamc.org/members/gir/gasp/

Questions?