HIPAA Security Best Practices

Kari Lidstone, CHP, CHSS
Network Engineer Supervisor

Trish Lugtu, CPHIMS
Technical Services Manager
HIPAA Security Best Practices

- Overview
- HITECH Breach
- Enforcement Highlights
- HIPAA Security Framework
- Risk Analysis and Risk Management
- Implementing in your Practice
HIPAA Requires Covered Entities to...

- To protect the privacy of patients’ medical information
- To control the ways they use and disclose patients’ protected health information (PHI)
- To offer patients certain rights with respect to their information
- To have certain administrative protections in place to further protect the privacy of patient’s information
Health Insurance Portability & Accountability Act of 1996 (HIPAA)
HITECH Breach (HHS and FTC)

- Defined as “the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information”
Definition of PHI

- Protected Health Information (PHI)
  - is defined as "the individually identifiable health information held or transmitted in any form or medium by these HIPAA covered entities and business associates, subject to certain limited exceptions."

- ePHI
  - electronic PHI
Who is under obligation?

- **Covered Entity (CE)**
  - A health plan, health care clearinghouse, or health care provider that transmits any health information electronically in connection with a covered transaction.

- **Business Associate (BA)**
  - A person who performs functions or activities on behalf of, or certain services for, a covered entity that involves the use or disclosure of individually identifiable health information.
Exceptions from disclosure

- When recipient of PHI would not reasonably been able to retain the information
- Certain unintentional acquisition, access, or use of PHI by employees or persons acting under the authority of a CE or BA
- Certain inadvertent disclosures among persons similarly authorized to access PHI at a CE or BA
In the event of a breach...

- Required to investigate
- Required to give notice
- Required to reprimand
- Required to record/notify Secretary
The infamous “Wall of Shame”

http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html
HHS’ Office for Civil Rights (OCS)

- **Enforcement of HIPAA**
  - Investigate complaints filed
    - [https://htct.hhs.gov/aset/](https://htct.hhs.gov/aset/)
  - Conduct compliance reviews
  - Perform education and outreach
  - Refer possible criminal violations
Enforcement Highlights

Privacy Rule Enforcement
- Since April 2003, over 53,789 complaints
  - 11,421 cases – required changes in privacy practices
  - 5,960 cases – no violation
  - 31,194 cases – ineligible

Security Rule Enforcement
- Since October 2009, over 145 complaints
  - 50 resulted in investigation and corrective action
  - Just getting started!
## HITECH Act Penalties Per Violation

<table>
<thead>
<tr>
<th>HIPAA Violation</th>
<th>Minimum</th>
<th>Maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Violation occurred even with Reasonable Due Diligence</td>
<td>$100</td>
<td>$50,000</td>
</tr>
<tr>
<td>Violation resulted from Reasonable Cause</td>
<td>$1,000</td>
<td>$50,000</td>
</tr>
<tr>
<td>Willful Neglect Corrected within 30 days</td>
<td>$10,000</td>
<td>$50,000</td>
</tr>
<tr>
<td>Willful neglect Not corrected</td>
<td>$50,000</td>
<td>$50,000</td>
</tr>
</tbody>
</table>

Notes: Annual maximum penalty of $1.5 Million; Maximum can be imposed by State Attorneys General regardless of the type of violation.
HIPAA Security Overview

- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards
- Organizational safeguards
- Policies and Procedures and Documentation Requirements
What is Information Security?

- The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction. It is achieved by ensuring the confidentiality, integrity, and availability of information.

- It is achieved by implementing policies and procedures as well as physical and technical measures that deliver CIA.
CIA Definitions

- **Confidentiality** – the protection of ePHI from unauthorized access or disclosure.

- **Integrity** – the protection of ePHI from unauthorized change (deliberate or accidental).

- **Availability** – Permits the use of ePHI as intended by ensuring it is accessible for use whenever needed – including during emergencies and disasters.
Other Important Definitions

- **Risk** – the measurable likelihood of loss from a threat – triggering or exploiting a particular vulnerability.

- **Threat** – potential violation of security

- **Vulnerability** – any weakness that could be exploited to violate a system or the information it contains
Administrative Safeguards

- Administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect ePHI and to manage the conduct of the covered entity’s workforce in relation to the protection of that information
Administrative Safeguards Standards

- Security Management Process
  - Risk Analysis (R)
  - Risk Management (R)
  - Sanction Policy (R)
  - Information System Review (R)

- Assigned Security Responsibility
Administrative Safeguards Standards

- Workforce Security
  - Authorization and/or Supervision (A)
  - Workforce Clearance Procedure (A)
  - Termination Procedure (A)

- Information Access Management
  - Isolating Healthcare Clearinghouse Functions (R)
  - Access Authorization (A)
  - Access Establishment and Modification (A)
Administrative Safeguards Standards

- Security Awareness and Training
  - Security Reminders (A)
  - Protections from Malicious Software (A)
  - Log-in Monitoring (A)
  - Password Management (A)

- Security Incident Procedures
  - Response and Reporting (R)
Administrative Safeguards Standards

- Contingency Plan
  - Data Backup Plan (R)
  - Disaster Recovery Plan (R)
  - Emergency Mode Operation Plan (R)
  - Testing and Revision Procedure (A)
  - Application and Data Criticality Analysis (A)

- Evaluation

- Business Associate Contracts and Other Arrangements
Physical Safeguards

- Facility Access Controls
  - Contingency Operations (A)
  - Facility Security Plan (A)
  - Access Control and Validation (A)
  - Maintenance Records (A)

- Workstation Use
Physical Safeguards

- Workstation Security

- Device and Media Controls
  - Disposal (R)
  - Media Reuse (R)
  - Accountability (A)
  - Data Backup and Storage (A)
Physical Safeguards

1. Is access to the building controlled at all?
2. Is access to the computers controlled?
3. Are systems protected from theft? How easy would it be to walk into your offices and steal equipment?
4. Are procedures in place now to properly dispose of confidential information?
5. Are workstations secured after hours?
6. Are the activities of the cleaning crew monitored?
7. Are data backups sent to an off-site location for safe storage?
8. Are staff members trained on key security issues?
Technical Safeguards

- **Access Control**
  - Unique User Identification (R)
  - Emergency Access Procedure (R)
  - Automatic Logoff (A)
  - Encryption and Decryption (A)

- **Audit Controls**
Technical Safeguards

- Integrity
  - Mechanism to Authenticate ePHI (A)

- Person or Entity Authentication

- Transmission Security
  - Integrity Controls (A)
  - Encryption (A)
Technical Safeguards

- Securely Configured workstations and devices
- firewalls
- Antivirus software;
- VPNs
- Encryption;
- Audit Trails
- Backups
Other Requirements

- Business Associate Contracts or Other Arrangements
  - Business Associate Contracts
  - Other Arrangements

- Requirements for Group Health Plans
  - Group Health Plan Implementation Specifications

- Policies and Procedures Standards

- Documentation Standards
  - Time Limit
  - Availability
  - Updates
Example Risk Analysis Steps

1. Identify the scope of the analysis.
2. Gather data.
3. Identify and document potential threats and vulnerabilities.
4. Assess current security measures.
5. Determine the likelihood of threat occurrence.
6. Determine the potential impact of threat occurrence.
7. Determine the level of risk.
8. Identify security measures and finalize documentation.
## Risk Level

<table>
<thead>
<tr>
<th>Probability of Occurrence</th>
<th>Potential for Damage</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>High</td>
<td>10</td>
</tr>
<tr>
<td>Medium</td>
<td>5</td>
</tr>
<tr>
<td>Low</td>
<td>1</td>
</tr>
</tbody>
</table>
Risk Management Framework

- Identify & Assess New Risks & Update Security Policies

- Monitor Effectiveness of Safeguards to ensure Confidentiality, Integrity & Availability

- Safeguards (Administrative, Physical & Technical)

- Health IT Environment (Technology, Procedures & Personnel)
PEOPLE

- People affect security.

- People are affected by security.
**Conclusion**

- Good Security requires constant vigilance.
- Effective use of deployed technology increases security.
- Technology should not drive security but support security efforts.
Conclusion

- Security reflects your clinics state of awareness and thus changes every day with the behavior and attitude of the people who interact with the systems, processes and infrastructure that support the personal health information and the organization.

- What is your security practice?
Questions?

Contact Information

Kari Lidstone, CHP, CHSS
Kari.Lidstone@mmicgroup.com
952-838-6850

Trish Lugtu, CPHIMS
Trish.Lugtu@mmicgroup.com
952-838-6844