Risky Business: Complying with HIPAA and Conducting HIPAA Risk Assessments

Julie Sullivan, Esq.
Objectives

- Current HIPAA enforcement landscape
- Focus points of Office for Civil Rights
- Requirements under HIPAA for risk analysis and risk management
- How to perform a risk assessment
The Office for Civil Rights

- Since 2003:
  - 137,000+ HIPAA complaints
  - 885+ compliance reviews
  - 125,472 resolved cases
  - 24,477 corrective action plans
  - $33 million+ in settlement collections
  - 572 criminal referrals to DOJ
The Office for Civil Rights

Status of All Complaints
April 14, 2003 - July 2016

Complaints Remaining Open (4%)  5,330
Complaints Resolved (96%)  132,442
Total Complaints Received 137,772

* Referrals to DOJ - 578
The Office for Civil Rights

Total Investigated Resolutions
April 14, 2003 - July 2016

Corrective Action Obtained (Change Achieved) (69%) 24,331
No Violation (31%) 11,055

Total Complaints Investigated 35,386
The Office for Civil Rights

Colorado Enforcement Results

- Investigated: No Violation
- Resolved After Intake & Review
- Investigated: Corrective Action

HUSCH BLACKWELL
Entities Most Often Requiring Corrective Action

1. Private practices
2. General hospitals
3. Outpatient facilities
4. Pharmacies
5. Health plans
Compliance Issues Investigated Most Often

1. Impermissible uses and disclosures of PHI
2. Lack of safeguards of PHI
3. Lack of patient access to PHI
4. Use or disclosure of more than minimum necessary PHI
5. Lack of administrative safeguards for ePHI
On the rise....

- Failure to conduct adequate risk assessments
- Failure to mitigate identified vulnerabilities (risk management activities)
Requirements under HIPAA

- Risk assessment is mandated by two regulatory provisions.

  EHR Incentive Programs: meaningful use requirement for participants

  Security Rule: 45 CFR § 164.308(a)(1)
Security Rule

A covered entity or business associate must, in accordance with § 164.306:

(1)(i) **Standard: Security management process.** Implement policies and procedures to prevent, detect, contain, and correct security violations.

(ii) **Implementation specifications:**

(A) **Risk analysis (Required).** Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.

(B) **Risk management (Required).** Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).

(C) **Sanction policy (Required).** Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.

(D) **Information system activity review (Required).** Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
Vocabulary

Risk Analysis/Assessment – the assessment of the risks and vulnerabilities that could negatively impact the confidentiality, integrity, and availability of the electronic protected health information (ePHI) held by a covered entity, and the likelihood of occurrence.

- Risk analysis and risk assessment are often used interchangeably, but don’t confuse a Security Risk Assessment (which is preventive and proactive) with a Breach Risk Assessment (which is reactionary following a breach to determine if PHI was compromised).

Risk Management – implementation of security measures to sufficiently reduce an organization’s risk of losing or compromising ePHI and to meet general security standard.

- Risk management steps should be taken following a risk analysis, but these processes are beyond the scope of this presentation.
Common Question & Answer

Question: Can I conduct my risk assessment without outside help?

Answer: Yes, but....
Recommend Professional Assistance

- It is possible for small practices to do a risk assessment themselves using self-help tools. However, doing a thorough and professional risk analysis that will stand up to a compliance review will require expert knowledge that could be obtained through services of an experienced outside professional.
Consequences

- **August 2016: Advocate Health Care**
  - $5.5 million in penalties and subject to Corrective Action Plan
  - Failed to do risk assessment, failed to implement physical safeguards required by Security Rule to protect ePHI

- **July 2016: University of Mississippi Medical Center**
  - $2.75 million in penalties and subject to Corrective Action Plan
  - Failed to implement P&Ps to protect address security risks, failed to conduct risk management activities for known security risks

- **July 2016: Oregon Health & Science University**
  - $2.7 million in penalties and subject to Corrective Action Plan
  - Risk assessments performed biannually, but failed to cover all ePHI in OHSU’s enterprise, failed to act in timely manner to address identified risks to reasonable and appropriate level
What counts as a security risk assessment?

- World of unknowns:
  - When a risk assessment must be performed
  - How often it should be performed
  - What procedures or guidelines should be followed
  - What IT systems should be subject to the assessment
  - If vendors must be evaluated during the assessment
  - What to do with the assessment results
What does NOT count as a security risk assessment?

- **Checklists**
  - Although they are useful tools, they are not enough to satisfy systematic assessment, implementation, and documentation requirements

- **Implementation and maintenance of certified EHR, even when completed by a third-party vendor**
  - Vendors are not the party legally responsible for the security of your ePHI
  - Electronic PHI includes more than just EHR (i.e., emails, scans, copier hard drives, billing statements, practice financials, etc.)
Recommended 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.
9. Develop and implement a risk management plan.
10. Implement security measures.
11. Evaluate and maintain security measures.

Risk Analysis

Risk Management
When? How often?

- **Required:**
  - The Rule requires covered entities to update and document security measures “as needed.”

- **Good Practice:**
  - Analyze security risks when planning and implementing new technologies and business operations.
  - The risk assessment process should be ongoing.

Source: 45 CFR § 164.306(e).
Recommended 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.
1. Identify the scope of the analysis.

- Remember your goal:
  - to assess potential risks and vulnerabilities to the confidentiality, availability, and integrity of all ePHI that you receive, maintain, or transmit
1. Identify the scope of the analysis.

- **ALL** electronic media (defined at 45 CFR § 160.103)

(1) Electronic storage material on which data is or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card;

(2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission.
1. **Identify the scope of the analysis**

1. Map the path of ePHI, finding everywhere it is stored, transmitted, created or received.
2. Include in the assessment every device, media, network or workstation that ePHI touches.
2. Gather data.

- Focused continuation of scope identification
- Where is ePHI received, stored, or transmitted?
  - Conduct a full inventory and analysis of the use and disclosure of ePHI.
2. Gather data.

1. Collect specific ePHI data to identify the true amount of data in play.

2. Analyze the characteristics of the ePHI that is part of the scope (e.g., full medical records, partial medical records, including of SSNs, financial information, etc.)

3. Further define the nature, type, location and use of the data to be assessed.
3. Identify and document potential threats and vulnerabilities.

VULNERABILITY

- “a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system’s security policy”

Source: NIST SP 800-30
3. Identify and document potential threats and vulnerabilities.

**VULNERABILITY**

<table>
<thead>
<tr>
<th>Technical</th>
<th>Non-Technical</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Holes, flaws or weaknesses in the development of IT systems</td>
<td>• Ineffective or non-existent policies, procedures, standards or guidelines</td>
</tr>
<tr>
<td>• Incorrectly implemented or configured IT systems</td>
<td>• Lack of training</td>
</tr>
</tbody>
</table>
3. Identify and document potential threats and vulnerabilities.

VULNERABILITY

- Sources of Information:
  - previous risk analysis documentation
  - audit reports or security review reports
  - assessments of IT systems
  - IT system security testing
  - publicly available vulnerability lists and advisories
3. Identify and document potential threats and vulnerabilities.

**VULNERABILITY**

- Examples:
  - No back-up generators for data centers
  - Unencrypted emails

Vulnerabilities are generally triggered by threats, which ultimately can lead to security breaches.
3. Identify and document potential threats and vulnerabilities.

**THREAT**

- “the potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability”

Source: NIST SP 800-30
3. Identify and document potential threats and vulnerabilities.

<table>
<thead>
<tr>
<th>Natural Threats</th>
<th>Human Threats</th>
<th>Environmental Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flooding</td>
<td>Network or computer-based attacks</td>
<td>Power failures</td>
</tr>
<tr>
<td>Earthquakes</td>
<td>Malicious software upload</td>
<td>Pollution</td>
</tr>
<tr>
<td>Tornados</td>
<td>Unauthorized access/ Hackers</td>
<td>Chemicals</td>
</tr>
<tr>
<td>Landslides</td>
<td>Inadvertent data entry or deletion</td>
<td>Liquid leakage</td>
</tr>
<tr>
<td></td>
<td>Inaccurate data entry</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
3. Identify and document potential threats and vulnerabilities.

**Sources of Information:**
- History of system break-ins
- Security violation reports
- Ongoing input from systems administrators
- Help desk personnel
- User community
4. Assess current security measures.

- What is a security measure?
  - Controls to mitigate the risk created by the organization-specific threats and vulnerabilities
  - Includes technical and non-technical systems and policies
    - access controls, identification, authentication, encryption, automatic log-offs and audit controls, policies and procedures, standards, guidelines, accountability, physical and environmental security measures
4. Assess current security measures.

1. Identify existing security controls.
   - Administrative safeguards
   - Technical safeguards
   - Physical safeguards
2. Evaluate effectiveness of controls.
3. Identify gaps in controls.
4. Ensure existing controls are maximized via proper configuration and implementation.

Be realistic: 100% security is unreachable.
5. Determine the likelihood of threat occurrence.

1. Use the information gathered in Steps One through Four to evaluate the likelihood of the threat to actually occur and trigger a vulnerability.

2. Rate the probability.
   - Use any scale you prefer: high/medium/low, 1-10, etc.
   - Define your ratings as objectively as possible in your documentation.
6. Determine the potential impact of threat occurrence.

- What will be the result of an exploited vulnerability?
  - **Example:** If an unencrypted email is intercepted, what will happen to the ePHI?
  - **Example:** If a flood hits your area and your servers are drowned, how can emergency access to ePHI be obtained? Use the information gathered in Steps One through Four to evaluate potential outcomes.

- **HIPAA Consideration:** compromise to ePHI, loss of ePHI, unauthorized use/disclosure of ePHI (violation, and likely a reportable breach)

- **Business Consideration:** Resultant loss of capital
6. Determine the potential impact of threat occurrence.

- Use the information gathered in Steps One through Four to evaluate potential outcomes.
  - Recall the focus of the HIPAA Security Rule: confidentiality, availability, integrity of ePHI
  - Common outcomes include unauthorized access to or disclosure of ePHI, permanent loss or corruption of ePHI, temporary loss or unavailability of ePHI, loss of financial cash flow, loss of physical assets
    - How will your organization cope with such outcomes?
7. Determine the level of risk.

- Risk is…
  “the net mission impact considering (1) the probability that a particular threat will exercise (accidentally trigger or intentionally exploit) a particular vulnerability and (2) the resulting impact if this should occur”

Source: NIST SP 800-30
7. Determine the level of risk.

- The holy grail of the risk assessment.
- Integrate the evaluation of the likelihood of threat occurrence (Step Five) with determining the potential impact of the threat (Step Six).

**High-likelihood threat + high-severity impact = high-level risk**
Risk Level Matrix
Risk Level Matrix

Risk Rating = Likelihood x Severity

- Catastrophic: 5
- Significant: 4
- Moderate: 3
- Low: 2
- Negligible: 1

Likelihood:
- Improbable: 1
- Remote: 2
- Occasional: 3
- Probable: 4
- Frequent: 5

Factors:
- Catastrophic: STOP
- Unacceptable: URGENT ACTION
- Undesirable: ACTION
- Acceptable: MONITOR
- Desirable: NO ACTION

HUSCH BLACKWELL
8. Identify security measures …

- What can we do to reduce risk to a reasonable and appropriate level?
- Evaluation, prioritization, modification, and implementation of these measures will follow as part of the risk management plan/process.
- Consider:
  - effectiveness of security measures, legislative or regulatory requirements, organizational policies and procedures
- Document corrective action(s) to be taken for each threat that poses an unacceptable level of risk.
8. ... and finalize documentation.

- Ensure you create and maintain documentation of results for each step of the process.
- Formally state what security capabilities will be implemented to lessen risk to acceptable levels.
- Create a timeline for implementation.
- Provide an explanation for risks left as-are.
- Clearly call out roles and responsibilities, and state when the plan will be reviewed and/or updated.
HIPAA Risk Assessment, Summarized

- HIPAA risk assessment process isn’t unique in its methodology or approach
- What IS unique to HIPAA is the types of data you have to identify and track, and the security requirements that must be implemented
- The NIST-800-30 method is tried-and-true and is a solid foundation for HIPAA risk assessment activities
Other Resources

- **Office of Health IT**
  - Provides free Security Risk Assessment Tool for practices with one to ten healthcare providers
    - iPad application available.
    - The SRA Tool does not guarantee compliance.

- **National Institute of Standards and Technology (NIST)**
  - Publishes free guidelines on industry-standard business practices for securing ePHI
Julie Sullivan, Esq.
Partner
Husch Blackwell LLP
1801 Wewatta Street, Suite 1000
Denver, CO 80202
Direct: 303-749-7255
Email: Julie.Sullivan@huschblackwell.com