Navigating the Waters of Incident Response and Recovery

Lee Kim, Esq.

Tucker Arensberg, P.C.

CERT Symposium:

Cyber Security Incident Management for Health Information Exchanges

June 26, 2013

What is a Security Incident?

- HIPAA defines a security incident is the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

- A security incident need not lead to unauthorized access to protected health information (and thus, is not a breach) but is still an event that should be reported by the business associate to the covered entity.

- Each organization must define what a security incident is and how it is handled (and prioritized) depending upon the nature and sensitivity of the information, attack vectors involved, software and hardware used, etc.

Why do you need an incident response plan?

1. While there have been relatively few reported security incidents, this may be due to relatively low utilization (HIEs are relatively new) rather than risk.
2. Not having a plan may result in inconsistent or under-reporting of security incidents or breaches or not even being aware that a security incident has occurred.
3. Be proactive instead of reactive so that you know what to do if and when a problem or issue arises and be consistent & systematic.
4. Know how to handle incidents discovered by your organization and your partners (e.g., subcontractors, business associates, covered entities, etc.).
5. Provides a framework to prevent data breaches, loss, and theft by encouraging (regular) gap analysis to address any deficiencies or weaknesses and facilitating communications.

Why do you need an incident response plan?

6. Provides a framework to facilitate reporting of security incidents and breach notifications, including with regard to outside organizations.
7. Improves preparedness for the HIPAA Privacy, Security, and Breach Notification Audit Program.
8. Ensure that management has approved the use of resources and time.
9. Supports HIE implementation.
10. Compliance with applicable legal, regulatory, and contractual requirements.
11. Preserve goodwill, business operations, coordination of care, delivery of care, and may safeguard against patient harm.

HIPAA: Security Incident Handling

- HIPAA Security Rule Standard: Implement policies and procedures to address security incidents
- HIPAA Implementation Specification (Required) (45 CFR § 164.308(a)(6)(ii)):
  - Identify and respond to suspected or known security incidents;
  - Mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and
  - Document security incidents and their outcomes.

Cornerstones of an Incident Response Plan

1. Define the incident response plan
2. Identify the response team members and management/stakeholders who need to be involved
3. Inventory all “containers” of relevant information (e.g., computers, mobile devices, applications, databases, etc.) (including backups and storage that you may outsource)
4. Define the security incidents for your organization (e.g., stolen or compromised passwords, lost or stolen backups, compromised access controls, viruses, malware, etc.)
   a. You will not be aware of a security incident unless your detection means is capable of detecting it!

Cornerstones of an Incident Response Plan

5. Understand how types of security incidents can impact your organization, patients, customers, employees, etc.
6. Have procedures in place for security incidents involving healthcare information, financial information, and other types of confidential, sensitive, or proprietary information (or intellectual property), including escalation, reporting, and notification
7. Align your incident response plan with your business impact analysis, disaster recovery, contingency operations, and business continuity plans
8. Address recovery from security incidents: the goal is restoring normal operations, minimizing disruption, cost, and administrative time, while ensuring confidentiality, integrity, and availability of information

Incident Response Strategy: Incident Evaluation & Handling

- The incident response team may consider the following:
  - Has the incident actually occurred or is it likely to occur?
  - Incident in progress?
  - Criticality or sensitivity of data or information system involved?
  - Insider attack or external hack? Virus? Malware? Etc.?
  - Human error? Intentional? Crime?
  - Equipment or software failure? Misconfiguration? Bug?
  - Quick containment of incident?
  - Is there an urgent need to respond quickly? Effect on patient care or business operations?

Incident Response Strategy: Incident Evaluation & Handling

- The incident response team may consider the following:
  - How did the security incident happen?
    - Do the gap analysis to see where the deficiencies may be
  - What can be done to prevent the security incident from happening again?
    - Update policies and procedures with approval from management.
  - Can the security incident be eradicated?
    - Threat or vulnerability identification (as applicable)
    - What was done to address the threat or vulnerability (e.g., patch, update, change in configuration, training?)
  - Does the evidence need to be preserved? If so, for what purpose and what are the parameters?

Incident Response Strategy: Notification & Communications

- Factors to consider may include the following:
  - Who needs to be notified of the security incident? And, what timeframe applies?
    - Law enforcement?
    - Covered entity? Business Associate? Individual? HHS? Etc.
  - What is the business impact? What is the contingency or disaster recovery plan? What is the business continuity plan?
  - Establish and deploy a systematic response to the type of security incident and regulations/laws involved.

Incident Response Strategy: Evidence Preservation

- In developing a plan, factors to consider may include the following:
  - Defining the forensic actions that should or should not take place depending upon the circumstances (including the type of information involved)
  - Collection and proper handling of evidence
  - Preserving the integrity of the information and information systems, devices, etc.
  - Maintaining the chain of custody for the evidence
  - Storing the evidence appropriately
  - *Securely sharing* the evidence as appropriate!

Incident Response Strategy: Documenting the Incident

- How incident was discovered
- How incident occurred
- Priority of incident
- Compliance
  - Consider what regulation is involved: E.g., HIPAA, PCI, etc.
- Response plan steps as executed
- Effectiveness of the incident handling and response

Incident Response Strategy: Post-Incident Steps

- Discuss and implement appropriate corrective or preventative actions
  - Keep in mind business continuity, patient care, coordination of care, etc. and the need for confidentiality, integrity, and availability of the information
  - Document the lessons learned
- Training or retraining as appropriate
- Disciplinary Procedures
  - Including and up to termination
- Involving law enforcement as appropriate
- Incident Response Procedures should be routinely reviewed, updated, and tested
- Workforce members should receive regular security awareness training, including on security incident handling

Incident Response Strategy: Recovery

- Recovery process must be quick and efficient to minimize disruption to operations (including delivery of care and coordination of care) and investment of administrative time
- Eradicate the incident and validate that it has been eradicated
- Understand the lessons learned from the incident (and the eradication of it)
    - Leverage data analytics for security incident predictions and detection
- Restore information systems/equipment/software/etc. to normal operations
- Minimize data loss, theft, or other harm to data, applications, and/or information systems

HIPAA: Incident Reporting & Breach Notification

- HIPAA Omnibus Rule requires the following:
  - Reporting of security incidents occurs upstream (should be done without unreasonable delay (some business associate agreements state 5 days)
    - Subcontractor of business associate must report security incident to business associate
    - Business associate must report security incidents to covered entity
  - Business associates include health information exchanges
  - Business associates and covered entities (as applicable) must perform risk assessments
  - Covered entities must conduct breach notification (if warranted by the risk assessment) without unreasonable delay and 60 days from the date of discovery of breach

HIPAA: Breach Notification

- Risk assessment analysis to determine if breach notification is required under HIPAA:
  - The nature and extent of the Protected Health Information involved, including the types of identifiers and the likelihood of re-identification;
  - The unauthorized person who used the Protected Health Information or to whom the Protected Health Information was disclosed;
  - Whether the Protected Health Information was actually acquired or viewed; and
  - The extent to which the risk to the Protected Health Information has been mitigated.
- Even if not a reportable breach, the covered entity/business associate must document this.

Final Recommendation: Proactive >> Reactive

- Security awareness and training for workforce members on a recurring basis
- Validate, test, and update (as needed) security access controls
- Update your incident response plan regularly (and document)
- Monitor evolving, emerging, **and** new threats & vulnerabilities for “containers” (where the data is) and “conduits” of information (e.g., networks and channels of communication)
- Conduct regular risk analysis and risk management (inside your organization and outside organizations)
- Encourage reporting of security incidents and breaches and communications

Questions?

Lee Kim, Esq.
Tucker Arensberg, P.C.
1500 One PPG Place
Pittsburgh, PA 15222
(412)594-3915
lkim@tuckerlaw.com

References

- NetDiligence Data Breach Cost Calculator: http://www.eriskhub.com/risk-calc/calc/
- HIPAA Privacy, Security, and Breach Notification Audit Program: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/
- ISO/IEC 27002: http://www.iso27001security.com/html/27002.html
- SANS Security Incident Handling Forms: http://www.sans.org/media/security-training/mgt512/secinc_forms.pdf
- Computer Security Incident Handling Guide: http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf

References

- SANS InfoSec Reading Room – Incident Handling: http://www.sans.org/reading_room/whitepapers/incident/
- Guide to Integrating Forensic Techniques into Incident Response:

  http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf
- Security Breach Notification Laws: http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx