Disaster Recovery and HIPAA Compliance

Marti Arvin, JD, CHC-F, CCEP-F, CHPC, CHRC
VP Audit Strategies
Agenda

- Case Study
- HIPAA Regulations
- OCR Resources
- Process for Testing Disaster Recovery
- Questions
Case Study
Scenario 1

- Xanadu Health System*
  - Three hospital system with a total of 700 licensed beds
  - It has 70 physician clinics spread over three counties
  - There are two EHRs used by the hospitals
    - One for hospital A & B, and a third for hospital C
  - The physician practices also have a separate EHR
  - All of the EHRs are on the same network

*Xanadu Health System and the facts regarding it are all fictitious*
Scenario 1

- Xanadu Health System
  - Organization learns that the data center has been flooded with water after a heavy rain fall and the sewer system has backed up the drainage system resulting in water backing up resulting in water coming into the data center. The system attempts to fail over to the back-up system but there is a glitch in the failover and the system goes down.
  - What happens next?
HIPAA Regulations Related to Disaster Recovery
Regulations - HIPAA Security Rule

- 45 CFR 164.308(a)(7)(i) Contingency plan
  - Requires P & Ps to respond to an emergency or other occurrence that damages a system containing ePHI including
  - Data back-up plan (R)
  - Disaster recovery plan (R)
  - Emergency mode operation plan (R)
  - Testing and revision procedures (A)
  - Application and data criticality analysis (A)
Regulations - HIPAA Security Rule

• Data back-up plan (R)
  – This requires more than just documentation on paper
  – The organization must, “establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.”

• Disaster recovery plan (R)
  – Establish (and implement as needed) procedures to restore any loss of data.
Regulations - HIPAA Security Rule

- Data emergency mode operations plan (R)
  - Establish (and implement at needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

- Testing and revision procedures (A)
  - Implement procedures for periodic testing and revision of contingency plans.

- Applications and data criticality analysis (A)
  - Assess the relative criticality of specific applications and data in support of other contingency plan components.
• Data backup
  – Questions covered entities should ask:
  • Has the organization considered the various methods of back-up, including tape, disk or CD?
    ▪ In today’s environment, cloud?
  • Does the backup plan include storage of backups in a safe, secure place?
  • Is the frequency of backups appropriate for the environment?
• Disaster Recovery Plan

  – Questions covered entities should ask:
    • Are the issues specific to the covered entity’s operating environment addressed?
    • Does it identify the data to be restored?
    • Can the appropriate workforce members get the plan from more than one source?
• Emergency Mode Operations

  – Questions covered entities should ask:
    • Does the plan appropriately balance the need for the data against the need to protect the data
    • Will alternative security measures be needed to protect the data?
    • Are possible manual procedures included, if needed?
    • Does the plan include contact information for key personnel who many need to be notified and their roles and responsibilities in the process?
• Testing and Revision
  – Questions covered entities should ask
    • Are the processes for restoring data from backups, disaster recovery and emergency mode operations documented?
    • Do individuals responsible for contingency planning understand their responsibilities?
    • Has the process actually been tested?
    • Have the results of any test been documented and identified issues addressed?
Application and Data Criticality Analysis

• How often should this be done?
  – After security incident
  – Changes in the organization, i.e. new acquisitions
  – New technology

• Should there be an internal or external evaluation, or both?

• Is there appropriate documentation of the periodic evaluations, supporting material for the analysis, recommendations and subsequent changes?
Presentations from OCR

• OCR/NIST conference 2017
  – Iliana Peter’s slides focused on insufficient backup and contingency planning as a continuing OCR enforcement issue
    • Organizations must ensure adequate contingency plans (including data backup and disaster recovery plans) are in place and would be effective when implemented.
    • Cloud resources may be leveraged for certain applications and computer systems
      • Caution: this may not encompass all that is required for effective contingency planning
    • MUST test and revise as needed
Process for Testing
Disaster Recovery
Evaluating Your Disaster Recovery Plan

• Is your plan current?
• Does it account for all potential disasters that could impact your business?
  – Weather
  – Power outages
  – Network failure
  – Data compromises such as ransomware that result in loss of access
  – Human error
Does the plan have goals and objectives?

- About 25% of companies take more than 30 minutes to activate their plan.
Evaluating Your Disaster Recovery Plan

- Do all the stakeholders know their role and responsibility in the process?
  - Senior leadership
    - Do they understand the need for their availability to make decisions quickly
  - Key business unit leaders
  - External vendors
    - Are they available 24/7 if critical to the disaster recovery activity
Evaluating Your Disaster Recovery Plan

• Is there a clear communication outline as part of the disaster recovery plan?
  – Does everyone understand who needs to be notified based on the nature of the underlying disaster?
  – Is everyone clear on how the communication plan changes?
    • if the criticality of the disaster changes?
    • If decisions need to be escalated?
Evaluating Your Disaster Recovery Plan

• Does everyone understand where to find the needed documents?
  – Checklists
  – Contact lists
  – Other documents

• Does the plan clearly identify what needs to be documented and who will be responsible for the documentation?
Does everyone understand when and how where to find the needed documents?

- Checklists
- Contact lists
- Other documents

Does the plan clearly identify what needs to be documented and who will be responsible for the documentation?
Evaluating Your Disaster Recovery Plan

- Is there a post-incident debrief process?
- Where is the organization in the process of performing incident response exercises?
- How would your organization respond to inquiries from OCR regarding your compliance with the contingency plan requirement including disaster recovery?
Questions

Questions?

Marti Arvin
Marti.arvin@cynergistek.com
512.405.8550 x 7051