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*
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
• 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.
• 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.
OCR Resources
• 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 on 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 may 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

- Questions covered entities should ask:
  - 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
Evaluating Your Disaster Recovery Plan

• 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?
Evaluating Your Disaster Recovery Plan

• 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

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

Questions?
PREPARING FOR THE CMS EMERGENCY PREPAREDNESS RULE

Presented by
Hannah Gompers and Jill DeMuth
WHO DO YOU REPRESENT?
HEALTHCARE COALITIONS
WHAT IS A HEALTHCARE COALITION?

Partners with healthcare and emergency response organizations working to prepare for, mitigate, respond to, and recover from emergency and disasters.

Provides disaster and emergency management education to partners.

Provides resources to partners in the event of a disaster, emergency, or planned event.
NC Healthcare Coalitions

- Mountain Area Healthcare Preparedness Coalition
- Mid Carolina Regional Healthcare Coalition
- Triad Healthcare Preparedness Coalition
- CapRAC Healthcare Coalition
- Metrolina Healthcare Preparedness Coalition
- Eastern Healthcare Preparedness Coalition
- Duke Healthcare Preparedness Coalition
- Southeastern Healthcare Preparedness Region
COALITION ENGAGEMENT

- Community Hazard Vulnerability Assessment
- Long Term Care Workshops and Education
  - Intro to Emergency Management
  - Hazard Vulnerability Assessment/Emergency Operations Planning
  - CMS Mini Workshops
- Regional & State Partnerships
- Continuing Care Community Networking
- Regional Exercise Series
CMS EMERGENCY PREPAREDNESS RULE
WHAT IS THE CMS EMERGENCY PREPAREDNESS RULE?

“The Emergency Preparedness Requirements for Medicare and Medicaid Participating Providers and Suppliers Final Rule establishes consistent emergency prepared requirements for healthcare providers participating in Medicare and Medicaid, increase patient safety during emergencies, and establish a more coordinated response to natural and human-caused disasters.”
If your facility accepts Medicare and/or Medicaid, you are responsible for being compliant with the new CMS Emergency Preparedness Rule by....

November 15th, 2017
<table>
<thead>
<tr>
<th>Inpatient</th>
<th>Outpatient</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical Access Hospitals (CAHs)</td>
<td>Ambulatory Surgical Centers (ASCs)</td>
</tr>
<tr>
<td>Hospices</td>
<td>Clinics, Rehabilitation Agencies, and Public Health Agencies as Providers of Outpatient Physical Therapy and Speech-Language Pathology Services</td>
</tr>
<tr>
<td>Hospitals</td>
<td>Community Mental Health Centers (CMHCs)</td>
</tr>
<tr>
<td>Intermediate Care Facilities for Individuals with Intellectual Disabilities (ICF/IID)</td>
<td>Comprehensive Outpatient Rehabilitation Facilities (CORFs)</td>
</tr>
<tr>
<td>Long Term Care (LTC)</td>
<td>End-Stage Renal Disease (ESRD) Facilities</td>
</tr>
<tr>
<td>Psychiatric Residential Treatment Facilities (PRTFs)</td>
<td>Home Health Agencies (HHAs)</td>
</tr>
<tr>
<td>Religious Nonmedical Health Care Institutions (RNHCIs)</td>
<td>Hospices</td>
</tr>
<tr>
<td>Transplant Centers</td>
<td>Organ Procurement Organizations (OPOs)</td>
</tr>
<tr>
<td></td>
<td>Programs of All Inclusive Care for the Elderly (PACE)</td>
</tr>
<tr>
<td></td>
<td>Rural Health Clinics (RHCs) and Federally Qualified Health Centers (FQHCs)</td>
</tr>
</tbody>
</table>
CONDITIONS OF PARTICIPATION

- Risk Assessment and Planning
- Policies and Procedures
- Communication Plan
- Training and Testing

Emergency Preparedness Program
• A systematic approach to identifying hazards or risks that are most likely to have an impact on a healthcare facility and surrounding area
• Different types of risk assessments available for use
• CMS does not specify which HVA tool you use
• Must have facility-based and community-based HVA
Our Disaster Recovery Plan Goes Something Like This...
Develop an emergency plan based on a risk assessment or hazard vulnerability analysis.

Perform risk assessment using an “all-hazards” approach, focusing on capacities and capabilities.

Can include your current emergency operations plan, but must include risks/hazards that are pertinent to your facility and you must update the plan annually.
Develop and implement policies and procedures based on the emergency plan and risk assessment.

Must address a range of issues including subsistence needs, evacuation plans, procedures for sheltering in place, tracking patients and staff during an emergency, pharmaceutical supplies.

Review and update policies and procedures at least annually.
Develop a communication plan that complies with both Federal and State laws, including HIPAA rules

Coordinate participant care, across healthcare providers, and with state and local public health departments and emergency management systems

Review and update the plan annually
WHAT’S IN THE COMMUNICATION PLAN?

Names and contact information for:
- Staff
- Entities providing services under arrangement
- Participants physicians
- Other similar facilities
- Volunteers

- Means, in the event of an evacuation, to release client information as permitted under HIPPA
- Means of providing information about the general conditions and location of clients
- Means of providing information about the hospital’s occupancy, needs and its ability to provide assistance
TRAINING & TESTING PROGRAM

Develop and maintain training and testing programs, including initial training in policies and procedures.

Demonstrate knowledge of emergency procedures and provide training at least annually.

Conduct drills and exercises to test the emergency plan.

Provide training annually and maintain documentation of training.

All exercises and drills must be completed by November 15th, 2017.
If your facility experiences an actual natural or man-made emergency that requires activation of the EOP, the facility is **EXEMPT** from the full-scale exercise requirement.

- Occurred within the past calendar year
- Must provide AAR/IP of event to receive credit

Your facility is still responsible for completing the additional exercise requirement.

- A second full-scale exercise that is community-based or individual, facility-based
- Tabletop exercise that is led by a facilitator
INTEGRATED HEALTHCARE SYSTEMS

Demonstrate that each separately certified facility in the system actively participated in the development of the EOP

Demonstrate each certified facility is using the emergency preparedness program and is in compliance

Include integrated policies and procedures, communications plan, and training/testing programs
ADDITIONAL GENERATOR REQUIREMENTS FOR HOSPITALS, LTC, CAH

- Generator location in accordance with NFPA 99
- Generator inspection, maintenance, and testing in accordance with NFPA 110
- Generator fuel plan
THANK YOU FOR YOUR TIME!

Jill DeMuth
jill.demuth@carolinashealthcare.org
704-589-0424

Hannah Gompers
Hannah.gompers@carolinashealthcare.org
704-579-4150

www.nchealthcarecoalitions.org
www.metrolinapreparedness.org
GROUP DISCUSSION QUESTION

Out of the four CMS Conditions of Participation with Emergency Preparedness Rule, which piece is the most concerning or keeps you up at night and why?