Making Sense of the HIPAA Contingency Planning Requirements

HIPAA Collaborative of Wisconsin
April 12, 2013
Scott P. Owens, PMP, CBCP
Owner, Managing Director

Agenda

• What is Contingency Planning?
• Industry Lexicon
• Importance of Contingency Planning
• Overview of HIPAA Security Rule CFR Part §164.308(a)(7)
  — Implementation Specifications
  — Key Thoughts
  — OCR Audit Protocol
  — Practical Considerations & Best Practice Guidance
• What Does a Great Contingency Plan Include?
• Compliance & Readiness Assessment
• Organizations, Standards, Resources

What is contingency planning?
Industry Lexicon

- **Continuity.** An uninterrupted connection, succession, or union

- **Business Continuity.** “A program which develops, exercises and maintains plans to enable the organization to:
  - respond to a disruption with minimum harm to life and resources;
  - recover, resume and restore functions within time frames which ensure continuing viability; and
  - provide crisis communications to all stakeholders.”
  
  Source: Disaster Recovery Journal, 2011

Industry Lexicon

- **Disaster.** “A sudden, unplanned catastrophic event causing unacceptable damage or loss. An event that compromises an organization’s ability to provide critical functions, processes, or services for some unacceptable period of time.”
  
  Source: Disaster Recovery Journal, 2011

- **Electronic Protected Health Information (ePHI).** Individually identifiable health information that is (i) transmitted by electronic media; (ii) maintained in electronic media.
  
  Source: 45 CFR Section 160.103
### Industry Lexicon

- **Contingency Plan.** Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster.

  Source: NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems

- **Emergency Mode Operation Plan (AKA Continuity of Operations Plan).** A predetermined set of instructions or procedures that describe how an organization's essential functions will be sustained for up to 30 days as a result of disaster event before returning to normal operations.

  Source: NIST Special Publication 800-66 Revision 1, Resource Guide for Implementing the HIPAA Security Rule

### Industry Lexicon

- **Applications & Data Criticality Analysis (AKA Business Impact Analysis).** The process of analyzing business functions, processes, and the supporting IT systems to characterize the effect that a business disruption might have upon them, their respective contingency requirements and priorities.

  Source: Hybrid Definition from Business Continuity Institute 2012 and NIST Special Publication 800-66 Revision 1, Resource Guide for Implementing the HIPAA Security Rule

### Industry Lexicon

- **Disaster Recovery.** "The strategies and plans for recovering and restoring the organizations technological infra-structure and capabilities after a serious interruption."

  Source: Business Continuity Institute, 2012

- **Disaster Recovery Plan.** A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities.

  Source: NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems
Industry Lexicon

- **Recovery Time Objective (RTO).** "The period of time within which systems, applications, or functions must be recovered after an outage. RTO includes the time required for: assessment, execution and verification. RTO may be enumerated in business time."
  
  Source: Disaster Recovery Journal, 2011

- **Recovery Point Objective (RPO).** "A point in time at which data or capacity of a process is in a known, valid state and can safely be restored from."

  Source: Business Continuity Institute, 2012

---

Industry Lexicon

- **Maximum Tolerable Period of Disruption (MTPD).** "The duration after which an organization's viability will be irrevocably threatened if a product or service delivery cannot be resumed."

  Source: Business Continuity Institute, 2012

---

Sample Disaster Timeline

A Sample Disaster Timeline is provided to illustrate the sequence of events following a disaster event, including:

- **Recovery Time Objective (RTO)**
- **Recovery Point Objective (RPO)**
- **Damage Assessment**
- **Health & Safety**
- **Technology Recovery**
- **Alternate Site Decision**
- **Systems Back Online**

Each step in the timeline is critical for ensuring a smooth recovery process and minimizing downtime.
Why is business continuity and contingency planning important?

Importance of Contingency Planning

“Small businesses that don’t have a plan in place generally don’t survive after a disaster, whether it’s a flood or a tornado. We see that anywhere from 40-60 percent of those that are hit like that simply don’t come back to business,” said David Paulison, former executive director of the Federal Emergency Management Agency (FEMA).

Source: Property Casualty 360 (November 2009)

Importance of Contingency Planning

According to a 2010 Global Disaster Recovery Preparedness Survey by Forrester Research and the Disaster Recovery Journal, “46 percent of respondents indicated power failure was the cause of their most significant disaster declaration or major business interruption, followed by IT hardware failures (25%), network failures (19%), and IT software failures (13%).”

According to a 2011 Business Continuity Institute Supply Chain Resiliency Survey, “53% cited adverse weather as being the main cause of disruption, maintaining its prominence from the 2010 report. Unplanned IT and telecommunication outages was the second most likely disruption affecting 41%.”
Importance of Contingency Planning

According to the Forrester Research / Disaster Recovery Journal 2010 Global Disaster Recovery Preparedness Survey, on average, "it took organizations 18.5 hours to recover from a (disaster) event", …"and organizations lost 4.5 hours' worth of data".

October 2012: Hurricane Sandy
260 deaths, $74B in damages
Photo Source: AP

March 2011: Japan Earthquake & Tsunami
110,000+ deaths, 150,000+ injured
Photo Source: National Geographic Online

June 2011: Midwest Flooding
100 miles of bridges closed / destroyed
Photo Source: GrandForksHerald.com

According to the Forrester Research / Disaster Recovery Journal 2010 Global Disaster Recovery Preparedness Survey, on average, "it took organizations 18.5 hours to recover from a (disaster) event", …"and organizations lost 4.5 hours' worth of data".

Importance of Contingency Planning

Data breaches and related fines are now becoming a significant threat as well.

Hospice of North Idaho
Unencrypted laptop stolen in 2010 with 4,411 patient records. OCR investigated in 2011, and fined Hospice of North Idaho $50,000 in December 2012 for violations of the HIPAA law.

Rite Aid
For multiple violations involving the mishandling of patient information, lack of HIPAA Privacy training for employees, and lack of a sanction policy, Rite Aid agreed to a $5 million settlement with the U.S. Dept. of Health & Human Services in 2010.

Massachusetts Eye and Ear Infirmary and Massachusetts Eye and Ear Associates
Agreed to pay the U.S. Dept. of Health & Human Services $3.5 million to settle potential violations of the HIPAA Privacy and Security Rules.

State of Alaska
In June 2012, the State of Alaska was fined $1.7 million for failing properly safeguard the ePHI of their Medicaid beneficiaries.

Data breaches and related fines are now becoming a significant threat as well.

According to the 2010 Business Continuity Institute's Supply Chain Resiliency Survey, "20% of companies suffered damage to their brand or reputation as a result of third party failures, and over 50% experienced a loss of productivity.

October 2011: Blackberry Service 4-Day Outage
Tens of millions without access to calendars & email; class action lawsuits filed
Photo Source: RIM

According to the 2010 Business Continuity Institute's Supply Chain Resiliency Survey, "20% of companies suffered damage to their brand or reputation as a result of third party failures, and over 50% experienced a loss of productivity.

April 2011: Sony PlayStation Security Breach
70 million users, personal profile & credit card information stolen
Image Source: Sony

June & October 2012: Amazon Web Services Outage
~12 hours of total downtime and approximately 11 hours of total historical data loss for customers such as Pinterest, Reddit, Foursquare, Netflix
Image Source: Amazon

According to the 2010 Business Continuity Institute's Supply Chain Resiliency Survey, "20% of companies suffered damage to their brand or reputation as a result of third party failures, and over 50% experienced a loss of productivity."
Office of Civil Rights 2012 Audit Findings

20 Initial Audits in 2012:
8 Health Plans, 3 Hospitals, 3 Physician Groups, 1 Lab, 1 Dental Practice, 1 Nursing Facility, 1 Pharmacy.

HIPAA Security Audit Issues

Research

- Financial investment in disaster recovery preparedness is down.
- Disaster plans are updated less frequently.
- Fewer testing exercises and drills are performed.
- Actual recovery times from disaster events is lengthening.
- Planned recovery objectives vary significantly from actual.
- IT configurations change constantly and are not well documented, leading to chaos during disaster events.

Conclusion – Organizational preparedness and planning is trending downward

What are the HIPAA requirements for contingency planning?

Required vs. Addressable

• **Required Implementation Specification.** Similar to a standard in that a covered entity must comply with it. [Source: NIST Special Publication 800-66 Revision 1, Resource Guide for Implementing the HIPAA Security Rule]

• **Addressable Implementation Specification.** Covered entities must perform an assessment to determine whether the implementation specification is a reasonable and appropriate safeguard for implementation in the covered entity’s environment. The analysis and decision on whether the covered entity implements this or an alternate measure, or no measure related to this specification, must be fully documented. [Source: NIST Special Publication 800-66 Revision 1, Resource Guide for Implementing the HIPAA Security Rule]

HIPAA Security Rule – Contingency Planning

• § 164.308(a)(7) Standard, Contingency Plan, requires covered entities to:

  Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information
HIPAA Security Rule – Contingency Planning

- The Contingency Plan standard includes five implementation specifications:
  - Data Backup Plan
  - Disaster Recovery Plan
  - Emergency Mode Operation Plan
  - Testing and Revision Procedures
  - Applications and Data Criticality Analysis

HIPAA Security Rule – Contingency Planning

- OCR Audit Protocol
  - Existence of a formal contingency plan with defined objectives
  - Existence of a formal process for identifying critical applications, data, operations, and manual and automated processes involving ePHI
  - Evaluation of the contingency plan in relation to the content relevant to the specified criteria
  - Validation that the contingency plan defines the overall objectives, framework, roles, and responsibilities of the organization
  - Verification that the contingency plan has been approved and updated on a periodic basis
  - Verification that the process used to identify critical applications, data, operations, and manual and automated processes involving ePHI incorporates the recommended performance criteria
  - Validation that the process has been approved and updated on a periodic basis

HIPAA Security Rule – Contingency Planning

- OCR Audit Protocol
  - Verification that preventive measures are identified and deemed practical and feasible in the organization’s given environment
  - Evaluation the list of preventive measures relative to the specified criteria
  - Existence of procedures for recovering documents from emergency or disastrous events
  - Evaluation of procedures in relation to specified criteria for the recovery of documents from emergency or disastrous events
  - Determination that procedures are approved and updated on a periodic basis
Data Backup Plan

• **Data Backup Plan (R)** – 164.308(a)(7)(ii)(A): Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

• **Key Thoughts**
  - (Required)
  - Create Exact Copies of ePHI
  - Maintain Retrievable Exact Copies of ePHI

Data Backup Plan

• **OCR Audit Protocol**
  - Existence of disaster recovery and data backup plans
  - Evaluation of contents of plan documents in relation to the specified criteria
  - Determine if disaster recovery and data backup plans have been approved and updated on a periodic basis
  - Existence of written procedures to create and maintain exact copies of ePHI
  - Evaluation of procedures in relation to the specified criteria used to create and maintain exact copies of ePHI
  - Determination that the procedure regarding creation and maintenance of exact copies of ePHI have been approved and updated on a periodic basis

Data Backup Plan

• **Practical Considerations**
  - RPO & RTO tolerances (tiers)
  - Most EHR’s & enterprise systems contain extremely large amounts of data
  - Many great technology options
  - As RTO approaches zero, technology solution costs increase dramatically

• **Best Practices (Disaster Recovery Institute)**
  - Design the data backup strategy to align with Risk Assessment & BIA
  - Ideally, data backup should be stored >25 miles from the original data
Disaster Recovery Plan

- **Disaster Recovery Plan (R)** – 164.308(a)(7)(ii)(B): Establish (and implement as needed) procedures to restore any loss of data.

- **Key Thoughts**
  - (Required)
  - Capability to restore loss of data involves policy, procedures, technology, training, & testing

Disaster Recovery Plan

- **OCR Audit Protocol**
  - Existence of disaster recovery and data backup plans
  - Evaluation of contents of plan documents in relation to the specified criteria
  - Determine if disaster recovery and data backup plans have been approved and updated on a periodic basis
  - Existence of written procedures to create and maintain exact copies of ePHI
  - Evaluation of procedures in relation to the specified criteria used to create and maintain exact copies of ePHI
  - Determination that the procedure regarding creation and maintenance of exact copies of ePHI have been approved and updated on a periodic basis

Disaster Recovery Plan

- **Practical Considerations**
  - Procedure documentation must be revised frequently
  - Team training & testing makes a difference
  - Long range DRP’s should be aligned with continuity strategies and technology budgets

- **Best Practices (Disaster Recovery Institute)**
  - Should include recovery teams / individuals required for recovery, including logistical information regarding mobilization of resources
  - Should include detailed recovery procedures for power, climate control, hardware & telecommunication infrastructure, information security, software applications, and data
Emergency Mode Operation Plan

- **Emergency Mode Operation Plan (R) – 164.308(a)(7)(ii)(C):** Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

- **Key Thoughts**
  - (Required)
  - Continuation of critical business process (not just IT systems)
  - Protection of security of ePHI while operating in emergency mode

---

Emergency Mode Operation Plan

- **OCR Audit Protocol**
  - Existence of a policy and procedures to enable the continuation of critical business processes that protect the security of ePHI while operating in emergency mode
  - Evaluation of the content of policy and procedures used to enable continuation of critical business processes for the protection of the security of ePHI while operating in emergency mode in relation to the relevant specified performance criteria
  - Verification that the policy and procedures have been approved and updated on a periodic basis

---

Emergency Mode Operation Plan

- **Practical Considerations**
  - Team training & drills are critical to success
  - Include all processes and supporting technology
  - Short term plan may be very different than long term plan, which might require new physical space

- **Best Practices (BS 25999 Business Continuity Standard)**
  - Include a clear description of included scope (also excluded scope)
  - All roles and responsibilities for each activity should be included
  - Include specific arrangements for stakeholder communication
  - Include detailed procedures for emergency mode operations that outline what criteria must be met before engaging them
  - Include procedures for how to revert back to normal operations

---
### Testing and Revision Procedures

- **Testing and Revision Procedures (A) — 164.308(a)(7)(ii)(D):** Implement procedures for periodic testing and revision of contingency plans.

- **Key Thoughts**
  - (Addressable)
  - Periodic testing – not once and done
  - Revision of contingency plans

### OCR Audit Protocol

- Existence of a policy and procedures for periodic testing and revision of contingency plans
- Evaluation of the content of the policy and procedures used for periodic testing and revision of contingency plans in relation to the specified criteria
- Determination that the policy and procedures have been approved and updated on a periodic basis
- If the covered entity has chosen not to fully implement this specification, the entity must have documentation on where they have chosen not to fully implement this specification and their rationale for doing so

### Practical Considerations

- Team training in advance of testing is valuable
- Contingency Plan testing & drills are critical to success

### Best Practices (Disaster Recovery Institute)

- Testing should occur at least annually
- Contingency Plan revisions should occur at least annually, but also when a significant business event occurs
Disaster Simulations & Drill Scenarios

- **Goals**
  - Validate the manual recovery procedures & processes
  - Verify emergency communication
  - Design a regular schedule of testing across departments or divisions
  - Test each individual department at least every 18 months, with a full-scale, enterprise wide disaster simulation every 2 years

- **Examples**
  - Tabletop drill / Meeting to review paper based plans
  - Fire drill / building evacuation
  - Technology failure simulation
  - Pandemic simulation
  - Chemical spill drill
  - Site destruction simulation

Applications and Data Criticality Analysis

- **Applications and Data Criticality Analysis (A)**
  164.308(a)(7)(i)(E): Assess the relative criticality of specific applications and data in support of other contingency plan components.

- **Key Thoughts**
  - (Addressable)
  - Relative criticality of specific applications & data (think RTO)
  - Support of other Contingency Plan components

Applications and Data Criticality Analysis

- **OCR Audit Protocol**
  - Existence of a formal process for identifying critical applications, data, operations, and manual and automated processes involving ePHI
Applications and Data Criticality Analysis

**Practical Considerations**
- Data criticality analysis must occur at the enterprise level, with scoring assignments made in relation to other systems and processes, not simply against a standard.
- Think holistically on how data or the system affects patient safety, quality of service, potential of information breach, legal or regulatory concerns, reputation, technology, financial viability, assets (damage), environment, & more.

**Best Practices (Business Continuity Institute)**
- Assess impact over time, not just in the immediate period.
- Clearly establish the maximum tolerable period of disruption for each process and system.
- Understand the interdependencies between processes and between systems.

What should a great contingency plan include?

- Evaluation of risks and potential threats to the organization.
- Evaluation of criticality of systems, data, processes, & assets.
- Personalized continuity strategies including Data Backup Plan.
- Conditions and guidelines for declaring a disaster.
- Emergency response, incident management, and system/process/asset recovery teams.
- Communication plans for various stakeholder groups.
- Action lists with defined responsibilities through a timeline.
- Emergency mode operational procedures.
- Procedures for evaluating and recovering each critical system, process, & asset.
- Timetable of continuous improvement of the plans.
- Calendar of drills and plan testing.
- Team training plan.
How can I take the pulse of my organization’s Contingency Plan?

Compliance & Readiness Assessment

• Could your organization survive being without its key systems, people, or processes for 24 hours? 48 hours? 72 hours? Do you even know?
• What is the financial loss to your company if you were not able to admit and treat patients?
• Do you know what your most vulnerable assets are?
• Did you pass your last regulatory compliance audit?
• How do you feel about the OCR Audit Protocol questions in this presentation?
• Do your primary suppliers have solid business continuity plans to avoid a shortage of materials?
• Do you have a comprehensive crisis communication strategy that considers the top ten stakeholder groups?

Compliance & Readiness Assessment

• Do you have an active business continuity program?
• Do you have a succession plan for company executives that extends below the C-Suite?
• Does your data backup strategy reflect a balance of both recovery times and recovery points?
• Do you have an alternate working site for office staff identified?
• Is the core technology in your data recovery strategy older than 4 years?
• How frequently do you perform disaster drills? Is the frequency enough to provide adequate training?
• Do you know what your true recovery capabilities are?
The organization is unsure how to quantify risk
- The organization is not sure how to prioritize systems, processes, or critical components into the RTO scale
- The organization has 4+ systems with an RTO of less than 8 hours
- The organization has any single system with RTO of less than 2 hours
- The organization is unsure about its true recovery capabilities
- The organization is unsure about designing a strategy and recovery environment to allow itself to meet the RTO’s (remember that the RTO is a goal defined by business and is not the same as your actual capabilities)
- The organization has never performed a disaster simulation drill and therefore has no benchmark on performance

Scenarios That Add Complexity to Contingency Planning

Organizations, Standards, Resources
- Business Continuity Institute: thebci.org (Good Practices)
- Disaster Recovery Institute: drii.org (Professional Practices)
- Association of Contingency Planners: acp-international.com
- NIST SP800-34 Contingency Planning Guide: nist.gov
- ISO 23001 Business Continuity Management Standard
- National Fire Protection Association: nfpa.org (NFPA-1600)
- Federal Emergency Management Association: fema.gov
- FEMA Ready: ready.gov
- American Red Cross: redcross.org
- Do 1 Thing (to prepare for emergencies): do1thing.com
- Centers for Disease Control: emergency.cdc.gov

Action

What action will you take in the next month regarding your organization’s Contingency Plan?
Scott Owens, PMP, CBIP
Owner, Managing Director
BluTinuity LLC
blutinuity.com

414.215.9020
sowens@blutinuity.com
linkedin.com/in/owensscott
twitter.com/blutinuity