Business Continuity and Financial Considerations for Hospitals

Jeremy Stacy
Emergency Management Professional
Jeremy Stacy
Emergency Management Professional

Jeremy Stacy is an experienced emergency management professional with expertise in business continuity. In his previous role as the director of support services for Good Samaritan Hospital, Los Angeles, he oversaw the hospital's environment of care and emergency management programs including business continuity planning. He's also a CSTI-certified hazardous materials outreach instructor and teaches, writes, and lectures about hospital disaster preparedness and business continuity planning. He has served on the Los Angeles County EMS planning committees for evacuation and shelter-in-place and the Statewide Medical Health Exercise.
Objectives

- Identify the requirements for BCP
- Describe financial/payer issues related to BCP
- Identify the steps in continuity planning
- Describe the terminology used in BCPs (RTO, RPO, etc.)
- Demonstrate how to implement BCP at your facility

“We’re in this together!”

Bad News:
- You cannot do this on your own
- Seriously, you cannot do this alone AT ALL

Good News:
- It was really easy for me to make this fit the conference theme!
Hurricane Sandy

- 5 hospitals closed
- Hospitals were strained to make payroll
- New York Department of Health filed a $427m claim with CMS under a Medicaid 1115 waiver
- CMS denied the claim, saying that while it had merit, other federal programs were more appropriate (i.e., FEMA, SBA, etc.)

“We certainly could not afford this unexpected loss of revenue. Cash expected from the Federal Emergency Management Agency pays for repairs, not operating losses.”

-Marlene Zurack, CFO
New York City Health and Hospitals Corp.
(Bellevue Hospital’s parent company)
One day…

Your hospital:
- 400 beds
- Emergency Department
- 300 census
- Busy Ambulatory Surgery Center

OH NO!

What Now?

FEMA
BI Ins
CMS
FEMA
Who Pays for What?

- FEMA – services rendered to address the disaster
- Medicare/Medi-Cal/Private Insurance – services you provided outside the disaster
- Business Interruption Insurance – services you were unable to provide because of the disaster
- Small Business Administration – low-interest loans from the Treasury

FEMA

Emergency Work:
- ACS/Shelter operations (labor cost)
- Evacuations
- Temporary generators
- Temporary facility operations

FEMA (cont.)

Permanent Work:
- Facility repairs
- Approved Improvements
- Approved Hazard Mitigation
FEMA (cont.)

Ways FEMA can bite you:
- Capital equipment is paid for on a reimbursement basis
- Emergency Work only includes OT for your employees
- “Compensatory Time” will only be paid to exempt employees if hospital has a written policy that allows it
- FEMA does not care about OSHPD

FEMA (cont.)

Payor of Last Resort:
- FEMA will not cover anything covered by any other entity (property insurance, etc.)

California Disaster Assistance Act (CDAA)
- State-level program almost identical to FEMA (for this discussion)

FEMA (cont.)

PRIOR to a disaster (FEMA)
- Have policies on tracking disaster-related costs and compensatory time
- Establish (and document) baseline rate of utilization and labor expenses
- Have at least two $0 cost centers for expense tracking
- Drill tracking expenses
Medicare/Medi-Cal/Insurance

- IT dependent
  - Cannot generate charge tickets without ADT system
  - Cannot perform electronic submittals of charge tickets
  - Fund transfers are electronic
- At the onset of a disaster, you will have 2+ weeks of unpaid charges already submitted

Medicare

Accelerated Payments (Part A)
- Temporarily covers payments for services provided in the absence of claims
- Only provided to still-operating hospitals or those CMS believes will re-open
- Must be repaid within 90 days*
- Little clarification on consecutive approvals

* Has been extended to 180 days at times.

Medicare (cont.)

Advance Payments (Part B)
- Contingent on pre-disaster claim levels
- Only pays 80% of claims*
- Must be applied for in writing unless CMS waives requirement

* Has been increased to 100% at times.
Medicare (cont.)

PRIOR to a disaster (Medicare)

- Have template ready to request Advance payments in writing
- Drill using paper claims submittals and determine manpower needed (Clean claims still required)
- Determine impact of 90-day requirement for Accelerated payments and 20% discount on Advanced payments

Medi-Cal

Advanced Payments

- State may issue interim payments at a percentage of value (usually 75%) of claims pending in system
- State may alternatively issue interim payments based on claim history for larger/regional disasters

Private Insurance

- The Governor may issue declarations stipulating payment requirements for private insurers regulated by the state
- Negotiate a minimum data set, alternative claims process, and provisions for advancing and accelerating payments
- Ask to see their BCP/COOP
Business Interruption Insurance

NOT a substitute for BCP!
- Often takes 72+ hours to kick in
- Claim-filing time limits
- Per-incident limits
- May exclude loss of utilities if building undamaged
- May only cover a percentage of lost profits
- Share your BCPs with your insurer

Business Interruption Insurance (cont.)

Watch for these limitations/exclusions:
- Qualifying period
- Partial cessation
- Per-incident limits
- Property damage requirement
- Percentage of lost profits
- Catastrophic exclusion

Business Interruption Insurance (cont.)

Additional riders worth considering:
- Civil Authority
- Ingress/Egress (incl. Tenants)
- Contingent or Dependent Business
- Accounts Receivable
- Payroll
- R&D
Small Business Administration

Economic Injury Disaster Loans
- Low-interest loans for small businesses to maintain/restore operations
- Does not require damage, only economic injury
- Capped at $2 million

Physical Disaster Loans
- Covers damage insurance doesn’t
- Capped at $2m + 20% for mitigation

Links

CMS FAQ on disasters:
- Or, go to www.cms.gov and search “disaster FAQ”
- www.callhospitalprepare.org/continuity-planning

Business Continuity Planning

Wheel of Necessary Graphics

Why?
Revise
Write
Develop
Who?
Why perform business continuity planning?

Why?

HIPAA

- 164.308(a)(7)(ii)(A) – Data Backup Plan
- 164.308(a)(7)(ii)(B) – Disaster Recovery Plan
- 164.308(a)(7)(ii)(C) – Emergency Mode Operations Plan
- 164.308(a)(7)(ii)(D) – Testing & Revision Procedure
- 164.308(a)(7)(ii)(E) – Applications and Data Criticality Assessment

Why?

IM.01.01.03

1. The organization has a written plan for managing interruptions to its information processes.
   - The organization plans for continuity of its information management processes.
   - The plan for managing interruptions to electronic information systems addresses the following:
2. Scheduled and unscheduled interruptions.
3. Training for staff and licensed independent practitioners on alternate procedures to follow when systems are unavailable.
Why?

IM.01.01.03 (cont.)

4. Backup of the electronic information systems.
5. The organization's plan for managing interruptions to electronic information systems is tested for effectiveness according to time frames defined by the organization.
6. The organization implements its plan for managing interruptions to information processes to maintain access to information needed for resident care, treatment, and services.

Why?

Title 22 – 22 CCR § 70746

- (a) Each hospital shall develop a written plan to be used when a discontinuance or disruption of services occurs.

Why?

Because the unexpected happens and it could be worse than you imagined.
Why?

The average time period (days) to restore to normal operations is 45 days.

Also: Angela Devlin’s presentation last year (thanks!).

Developing the Plan(s) – Groundwork

Planning Team

- Executive Sponsor
- Department Directors
- BCP Management Team – IT, Risk, Facilities, Disaster Coordinator, etc.
- Internal Subject Matter Experts
  - Poll your staff to see who has experience with disasters – Northridge, San Francisco, Los Angeles riots, etc.
Contracted Services

Several Departments that are critical to continuity may be outsourced:

- Food Service
- Environmental Services
- Patient Transportation
- Sterile Processing
- Facilities and Engineering
- IT

Contracted Services (cont.)

To do:

- Review contracts for “Acts of God” or “Catastrophe” clauses
- Revise contracts to detail critical nature of continuity in disaster
- Involve legal counsel
- Integrate into BCP program as any other department
- If possible, leverage the size of the outsourced entity to your advantage

Methodology

Organizational: One BCP for the entire organization

- Good for small businesses or focused businesses

Departmental: One BCP per department

- Good for large organizations with several critical components
Methodology

1. Perform a Risk Assessment
2. Perform a Business Impact Analysis
3. Design Response and Recovery Strategies
4. Develop and Distribute Plan
5. Test and Maintain Plan

Risk Assessment

Use hospital HVA
- The HVA does not replace your need to do a Risk Assessment
- That which impacts the hospital overall may have minimal impact on your department’s ability to function
  - Example – a casualty surge will not affect IT the same way it affects the hospital

Risk Assessment (cont.)

Take the threats from the HVA one-by-one and consider:
- Speed of onset: sudden or gradual?
- Forewarning: yes or no?
- Preparedness of your critical vendors: prepared or unprepared?
- Preparedness of your own staff: prepared or unprepared?
Business Impact Analysis

- How would each threat affect your department in 3 ways:
  - How likely is the event?
  - How much impact would it have on your ability to operate?
  - How long would it impact your operation?
- Rate each on a scale of 0–3, with 3 being highest/longest

Business Impact Analysis (cont.)

<table>
<thead>
<tr>
<th>Event Risk</th>
<th>Likelihood</th>
<th>Impact on Ability to Operate</th>
<th>Impact on Operation Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Natural Disasters</td>
<td>Low</td>
<td>Medium</td>
<td>Low</td>
</tr>
<tr>
<td>Cyber Threats</td>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
</tr>
<tr>
<td>Internal Errors</td>
<td>High</td>
<td>Low</td>
<td>High</td>
</tr>
</tbody>
</table>

Severity of Consequence

- Area of major concern

Business Impact Analysis (cont.)
Business Impact Analysis (cont.)

- What are your critical business functions?
- What are functions you perform to support other department’s critical business functions?
  - Resources needed
  - Impact on Safety/Operations
  - Financial impact
  - Customer/Reputation impact

Recovery Time Objective (RTO)

- How long can the organization survive without your critical business function?
  - Current business day?
  - Tomorrow?
  - A week?
- What resources are needed to ensure the restoration of the function within the RTO?
Recovery Point Objective (RPO)

- For data-reliant processes, how current does the data need to be once systems are restored?
  - Last night’s backup?
  - Last transaction?
- If you have a manual backup, how long is it feasible to run the manual backup before restoration is impossible?

Gap Analysis

- Does your Facilities and IT staff have the resources to meet the RTO?
- Does your IT department have the capability to meet the RPO?
- What pre-planning can the department do to mitigate delayed response?
  - Pre-positioned supplies – go-bags and/or downtime kits
  - Pre-designated work areas

Impact Scenarios

- Loss or denial of physical space
  - Your work area has been destroyed and/or become inaccessible
- Access to space, but loss of technology or utilities
  - Your area is intact, but without data/power/water/etc.
- Both
Impact Categories

Financial
- The cost to recover all functions + loss of revenue
- Example: BP oil spill cost billions to clean + lost billions in product

Operational
- The ability to physically execute a critical business function

Impact Categories (cont.)

- Legal/Regulatory
  - The ability to be fined, sued or shut down
- Customer
  - The ability to retain customer base when operating in Emergency Mode
- Reputation
  - The ability to retain customer base when the story gets out or recovery is complete
  - BCP can make or break market share

Developing the Plan(s) – Writing
Developing the BCP

- Shoot for simple – your staff must be able to read, understand and implement the plan under stressful conditions
- A good plan doubles as a progress-monitoring tool for your recovery team
- Plans should be organized so they are easy to follow from response to recovery
- Write in plain language using only the amount of technical jargon needed

Developing the BCP (cont.)

“If you make something idiot-proof, they’ll make a better idiot.”

Basic Structure

- Introduction
- Overview
- Scenarios
- Response Team
- Response Actions (Downtime Procedures)
- Recovery Actions
- Testing and Maintenance
Introduction

- Straight-forward list of justifications (Purpose) and planning assumptions
- Most BCPs are written for a worst-case scenario that involves multiple impact types

Overview

- Identify Critical Business Functions
- Identify RTO for each
- Identify RPO for each (if applicable)
- Identify Dependencies
  - Vital Records: records that must be restored
  - Critical Computer Applications: any applications that support Critical Business Functions
Scenarios

- Response procedures for specific scenario types
- Different from Downtime Procedures
  - How would this specific scenario impact your business area? vs. How would you continue to perform your critical function?
  - Should be high-level, but still thought-through

Loss of Work Area

- Evacuation plan? Rally points?
- What technology, utilities, equipment, size, etc., are needed to function?
- Identify an alternate work area ahead of time
- Can your critical functions be performed by staff from their homes?
  - If so, are they set up to do so?

Response Team

- Detail Response Team members, leaders, and contact information
  - Should have primary and alternate leaders
  - Always include a scribe role in your Response Team to document actions!
- Identify critical vendors if they should be considered part of Response Team (i.e., data-recovery contractors)
Response Team (cont.)

Don’t win the battle only to lose the war!

- Staff:
  - Create teams by geographic region
  - Split teams into multiple, phased response groups
  - Split teams into continuity and response

Response Team (cont.)

- Disaster Response Team
  - Team members who will report directly to the frontline to assist with the disaster
- Continuity Team
  - Team members who will stay behind to handle routine functions and/or workplace relocation
- Know and drill your roles

Disaster Activation & Notification

- What triggers your BCP?
- How will staff be notified?
- What is your staff’s expected response?
  - Does everyone report at once, or is there a first response team and a relief team?
  - Does anyone report in the middle of the night?
- Downtime kits: Where are they? What’s in them?
Response Actions (Downtime Procedures)

- Where the “rubber meets the road” of the plan
- Highly specific depending on department and function
- Should be written in a way that can be understood and managed by supervisor (consider checklists)
- Should include vendor information, if not identified in Response Team

Response Actions (Downtime Procedures) (cont.)

- Dedicate one chapter to each Critical Business Function
- If applicable:
  - How will you provide for current patients?
  - How will you provide for the triage area?
- Documenting actions for patient charges is a response tactic, but processing payment charges is a recovery tactic

Recovery Actions

- Not the same as Response!
  - Response = what do we do now?
  - Recovery = how do we get back to normal?
- Most steps should be your response in reverse
- What systems/equipment need to be tested before returning to normal?
- How will vital records be rebuilt?
- Repatriation of work space
- Rebalance staff schedules
Plan Testing and Maintenance

- Orient staff to the BCP on hire
- Incorporate knowledge of BCP into job description and evaluation
- Test plan at least annually:
  - Tabletop with Response Team
  - Integrate into hospital-wide drill
  - Drill with dependent departments (IS, Facilities, etc.)
  - Drill with critical vendors

Plan Testing and Maintenance (cont.)

- DOCUMENT orientations/drills, otherwise they didn’t happen
- State where documentation is located – as an attachment, in staff meeting minutes, etc.
- If drills lead to major revisions, document those revisions in the Plan Testing and Maintenance section
- Note the last revision date and the next revision date

Thank you

Jeremy Stacy
jstacy@aya.yale.edu