6 Steps to Healthcare IT Disaster Recovery
For a hospital’s IT Department, business continuity can truly be a life or death concern, because it directly affects patient care. In the case of an outage, whether it’s due to a major event or something more routine, the IT Department’s primary goal is to minimize disruptions to patient care.

This guide will help you understand the steps that the IT Department should keep in mind as it builds or modifies its disaster recovery plan.
If you would like to find out more please call 781 939 0780 or email sales.us@bridgeheadsoftware.com

Steps to Healthcare IT Disaster Recovery

1. Prioritize the criticality of systems and data
2. Perform a risk assessment
3. Estimate the cost of downtime
4. Define recovery objectives
5. Understand your data profile
6. Identify the required data protection tools

Application Environment

- Computing Software
  - HIS
  - EHR
  - Email
  - PACS
- Applications
  - Structured Data (Databases)
- End User Data
- Network Infrastructure
Prioritize the criticality of systems and data

Computer systems support and document clinical decisions, but they are only one part of a holistic view of business continuity, which also includes systems like:

- Evacuation
- Food services
- Staff management
- Telecommunications

As part of a business Impact Analysis, **prioritize the criticality of systems**. Points to consider:

- Which systems are most vital for patient care?
- What other systems may be vital to the business? Examples might include:
  - Email
  - Payroll
  - Billing/Accounts Receivable
- How quickly does each system need to be back in operation and how much data can you afford to lose? [explored in further detail in Step 4]

In addition to the criticality of systems, also consider the criticality of the data that they contain and whether the full dataset must be quickly restored in the event of a disaster, or if only the most recent data will suffice, thereby speeding the recovery process. E.g. After a disaster occurs all CT scans from your archive will not be required to be back in place, only those related to patients whose studies are currently undergoing review.

Note that this guide focuses on IT systems.
Perform a risk assessment

As part of a risk assessment, identify the threats to IT systems and how you might mitigate them. Areas to consider include (but are not limited to):

- Single points of failure
- Infrastructure
- Environmental (e.g., hurricanes, earthquakes)
- Terrorist acts
- Internal sabotage

**KEY POINT**

**APPLICATION ENVIRONMENT**

<table>
<thead>
<tr>
<th>Computing Software</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications</td>
<td>HIS EHR Email PACS</td>
</tr>
<tr>
<td>Structured Data (Databases)</td>
<td></td>
</tr>
<tr>
<td>End User Data</td>
<td></td>
</tr>
<tr>
<td>Network Infrastructure</td>
<td></td>
</tr>
</tbody>
</table>
Estimate the cost of downtime

What are the costs associated with system downtime? Costs [not only financial] to consider include:

- Lost revenue
- Lost cash flow
- Lost productivity
- Lost profitability
- Patient safety
- Patient lawsuits
- Compliance
- Community relations
- Staff recruitment and retention

KEY POINT

APPLICATION ENVIRONMENT

<table>
<thead>
<tr>
<th>Computing Software</th>
<th>Applications</th>
<th>HIS</th>
<th>EHR</th>
<th>Email</th>
<th>PACS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Structured Data (Databases)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>End User Data</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Infrastructure</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Define recovery objectives

Establish objectives for getting your critical systems operational again after a disaster occurs. Specifically:

- **Recovery Point Objective (RPO):** How much data can you afford to lose? For example, a one hour RPO means that data must be restored to within one hour of the time the disaster occurred.

- **Recovery Time Objective (RTO):** How quickly do you need to have the system back in operation? For example, a one hour RTO means that the system must be restored to acceptable service levels and available to end users within one hour of the time the disaster occurred.

As discussed in Step 1, specific systems may not require all data to be restored in order to be operational. When establishing RPOs and RTOs, focus on restoring the essential end user data; less critical data can subsequently be brought back at a granular level via the archive. Structured databases, however, typically present an “all or nothing” recovery scenario.
Understand your data profile

Understanding your data profile is essential to protecting it. When looking at your data, a key consideration is the frequency with which it is accessed and/or changed, as this factor significantly impacts your protection strategy – and associated costs.

Specifically, **dynamic data**:
- Is frequently accessed and/or changed (e.g., HIS, recent medical images and patient records)
- Requires a more active protection strategy:
  - Daily backup is inadequate
  - Frequent recoverable data copies
  - Disk- and tape-based
  - Geo-dispersed
- Accounts for approximately 20% of all data

Conversely, **static data**:
- Is infrequently accessed and/or changed (e.g., old studies, scanned documents)
- Can be protected more cost-effectively:
  - Daily/weekly backup is sufficient
  - Multiple copies of data in a **protected archive**
    - Disk- and tape-based
    - Geo-dispersed
- Accounts for approximately 80% of all data

**KEY POINT**

**APPLICATION ENVIRONMENT**

- Computing Software
- Applications
- Structured Data (Databases)
- End User Data
- Network Infrastructure

If you would like to find out more please call 781 939 0780 or email sales.us@bridgeheadsoftware.com
Identify the required data protection tools

Finally, determine what tools are required to implement your business continuity strategy. Considerations include:

- Communication links
- Hardware
- Computing software
- Application layer

It is essential that you work with your hardware vendors and/or your reseller to devise a replacement strategy to quickly react to an event. Take, for example, a flooding event where the water was quickly removed and the data center itself is intact, but certain hardware was damaged. You will want to have a plan in place with your vendor that identifies how that hardware will be replaced and by whom. In the event of a more significant disaster, consider how you would bring up your failover environment, again in coordination with your selected vendors.

As for your computing software [e.g. operating systems, VMware], the recovery architecture and selected protection products are critical to get this layer operational again. Especially in the case of VMware, ensure that your vendor understands how to back up and restore those systems and is current with VADP, the newest generation of VMware’s data protection framework which requires far less disk space.

After an outage, bringing the application layer back up depends on the recovery architecture, including such elements as: save sets; volume copies; tools and processes for creating save sets / volume copies; and tools and processes for restoring save sets / volume copies. Your selected vendor should offer not only the tools for recovering your applications but also extensive knowledge of healthcare applications.

KEY POINT

CONTINUE
## Key Point Summary

### Step 1

Once the criticality of each system and their associated data has been prioritized, you are ready to identify the threats specific to each.

### Step 2

Identifying potential risks and mitigation strategies can help guide your business continuity drills and also get you thinking about the costs of downtime associated with each.

### Step 3

Considering the high potential cost of a system outage, you will want your business continuity plan to establish objectives for re-establishing normal operations as quickly as possible.

### Step 4

A typical hospital will have different RPOs and RTOs for its core systems, depending on the criticality of each. RPOs and RTOs are affected by the specific data sets that you choose to bring back into production first.

### Step 5

With approximately 80% of your data landing in the 'static' category, it would be sensible to incorporate data archiving into your disaster recovery strategy. Using archiving significantly reduces the cost of protecting your data while still ensuring that you can meet your business continuity objectives.

### Step 6

Even the most comprehensive disaster recovery strategy isn’t worth the paper it’s written on if the requisite tools and vendor support are not in place to support it. A robust data protection suite is an essential component. BridgeHead Software offers a comprehensive healthcare data management suite, backed up by the experience of more than 1,000 hospital implementations.
BridgeHead Software provides the solutions and industry expertise necessary to help you build or optimize your business continuity strategy.

**BH MediStore™**
BH MediStore provides hospitals with a true, standards based vendor neutral archive (VNA). Being agnostic of both the storage devices it manages and the applications it serves, BH MediStore provides a centrally managed, interoperable data repository for all hospital data.

By unlocking the storage silos caused by dedicated applications such as PACS, Electronic Medical Record (EMR) and Electronic Content Management (ECM) systems, BH MediStore delivers secure and accessible data across all applications while at the same time reducing management and storage costs. Migrating medical data into BH MediStore not only provides an indexed and searchable archive, it also releases primary storage, optimizes secondary storage and facilitates disaster recovery programs. In short, BH MediStore will be the best and the last data migration a hospital will need.

**BH MediSafe™**
Using a combination of protected archiving and refined backup techniques, BH MediSafe provides a highly scalable solution that enables healthcare organizations to implement a full and comprehensive disaster recovery strategy even in the face of exponential data growth.

Using its proven process of analyze, optimize and protect, BH MediSafe identifies, reduces and then moves static data into a fully protected archive before it implements a highly tuned backup process on the remaining dynamic data. This means that both files and/or systems can be quickly and cost effectively recovered to the correct point in time in the event of data corruption or loss. Complete disaster recovery is now attainable and affordable with BH MediSafe.

Both BH MediStore and BH MediSafe incorporate healthcare standards such as HL7, DICOM and XDS.
Contact BridgeHead to learn how our data protection software suite and seasoned professionals can help you develop or improve your disaster recovery strategy. Our field-tested healthcare IT solutions are in place at more than 1,000 hospitals worldwide, so we have the experience and knowledge to help you solve any data management challenge.

If you would like to find out more please call 781 939 0780 or email sales.us@bridgeheadsoftware.com