Global Knowledge®

Expert Reference Series of White Papers

Your Prescription for a Robust Healthcare IT Disaster Recovery Plan

Your Prescription for a Robust Healthcare IT Disaster Recovery Plan

Ross A. Leo, CISSP

"I just love it when a plan comes together. But any plan that is not tested and proven is not a plan that can."

– Ross A. Leo, Certified Information Systems Security Professional

Introduction

All too often, organizations experience events that cause devastating compromises to their operations. These events demonstrate that a quick and effective response can make the difference between an incident and a catastrophe. More importantly, they show that proactive planning and advance preparation are crucial elements of an effective response. While disaster recovery planning is essential for all industries, it is critical within the healthcare field. This paper explores the disaster recovery planning process within the healthcare setting.

Why Invest in a Disaster Recovery Plan

Disaster recovery planning appears time- and resource-consuming without any obvious or direct link to the bottom line. What frustrates planners even more is that the result of their labor - a workable plan that protects and preserves the operation - shows no return on investment (ROI) unless there is a disaster that calls for its use. Certainly, no organization hopes for a disaster, but the need for this crucial plan remains real and unavoidable.

Healthcare organizations want their dollars to ensure the best and most timely treatment of patients. This goal makes investment in projects like disaster recovery planning or continuity of operations plans (COOPs) seem less important than facilities expansion or acquisition of the latest diagnostic instruments. Nearly everyone can agree that adding improved diagnosis and treatment capabilities will improve patient health. It may be harder to get everyone to agree that preserving and protecting those tools and technologies is equally important. But keep this in mind: Any tool that cannot be used due to an incapacitating event is of no value to anyone. And a healthcare operation out of service even temporarily, regardless of the cause, can put many lives at risk.

An effective COOP can ensure that vital tools are kept in service or restored to service rapidly, under even adverse conditions. With laws requiring the creation of these plans, revenues being squeezed from all sides, and unrelenting pressure to keep the doors open under all conditions, one question remains foremost on the minds of those charged to make it happen: Where do I begin? This project's scope can seem like trying to eat an elephant all at once. But just like eating an elephant, a project of this size is accomplished one bite at a time.

How and Where to Begin Developing Your COOP

The Health Insurance Portability and Accountability Act (HIPAA) requires that all healthcare provider organizations plan for contingencies and outages. An effective plan to sustain the operation is the final output of the planning process. HIPAA also requires that these organizations use a "risk management" approach for their plans. This approach means that risks and events that may cause such outages must be identified, analyzed, and mitigated or compensated for. This in-depth process can be complex. Laying the proper foundation through a project management methodology is the best way to ensure you don't miss a step.

Well-planned and executed projects begin with a clear understanding of objectives, constraints, and other factors that will affect the project and its outcome. Clearly, the final outcome to be produced is a complete, tested, and proven plan.

To start, you must clarify scope, budget, scheduling issues, and resources. These are the basic components that will form the framework of a workable plan.

The project manager must first define scope and resources in ways that are unique to a COOP. COOPs are very specific to a business unit, location, facility, or other operational component. The plan must consider the work done by the operation, the information used, staffing, geography, weather, time horizon, and many other factors. Resources include those things available to build and test the plan, and those items available when the plan is activated. The project manager needs to define the following categories.

- **Assets:** human, physical, informational, technological
- **Potential threats and their sources:** human, natural, technological
- **Vulnerabilities:** flaws or other shortcoming (including absence) in a control or asset

After identifying the above, you will know the primary elements that can suffer from or cause a disaster. You will also know what assets are available to build your plan. To help you get started, a useful **Contingency Plan Guidelines** and **Template** are included in the Appendices.

Where Are the Risks and How Can They Derail Your Business?

Once you have defined assets, threats, and vulnerabilities, the next step is to assess risk. In fact, HIPAA requires risk assessment as part of the disaster planning process. Performing a Business Impact Analysis (BIA) is an additional step that must be taken and complements the risk assessment process.

Risk Assessment

A risk assessment must be performed (and updated annually). This assessment reviews the assets, threats, and vulnerabilities of the operation. Simply stated, assets are "things of value." These can be the tangible and intangible items that an organization acquires and uses to accomplish its mission. Intangibles may include processes,

intellectual property, image, and reputation. It can be hard to place value on intangibles, but they are often even more critical to protect than tangible assets. They often represent competitive advantages or the nearly irreplaceable company image and reputation.

The risk assessment looks at events that affect assets in terms of frequency of occurrence and magnitude of impact. When reviewing assets, there are potential pitfalls to watch. One of the first challenges is to be sure the nature of the asset is well understood, as well as its role in the business operation. For example, you should consider if the asset appreciates or depreciates in value over time. Technology typically depreciates with time, where land and buildings typically appreciate. Appreciation and depreciation will figure into your calculations when it comes time to do costing for mitigation or asset replacement.

Another potential planning hazard is failure to make calculations based on full lifecycle (LC) and total cost of ownership (TCO). Every asset valuation must include acquisition cost as well as maintenance costs. Both values are needed to determine the cost of asset replacement. To exclude both values could mean your replacement cost calculations will be undervalued, possibly grossly, and that planned funding through set-asides or insurance policies will be inadequate.

The basic calculation to use is one commonly employed in the industry: single loss expectancy (SLE) x annualized rate of event occurrence (ARO) = annualized loss expectancy (ALE). The SLE represents the value of a one-time asset loss, or the average value if the same loss has occurred several times. The ARO is derived from the number of times the event has happened in the past and is called "annualized" because few of the events considered actually happen every year. The derived value equates to a decimal number less than 1.0 if the event happens less than once a year, and greater than 1.0 if more than once per year. As an example, the ARO of a hurricane happening 3 times in 5 years would be 0.60, and a power outage happening every other month would be 6.0.

The calculated value of ALE represents the potential loss anticipated to result from a particular threat or event occurring during the year. The total from all ALE calculations produces a dollar amount to be used as a budget item for countermeasures or recovery or replacement of the assets under consideration.

Business Impact Analysis (BIA)

The BIA complements the risk assessment in that it uses information generated by the risk assessment. The main difference between these analyses is that the risk assessment focuses on losses and potential adverse events, while the BIA focuses directly on the operational impacts to the business. Specifically, the BIA examines the operations and determines, once down, what direct losses are incurred, what secondary effects follow and where they appear, and how long losses can be sustained before they become operationally critical or fatal.

The BIA ranks operational elements relative to the importance of each to the organization's survival and speedy recovery. The importance of the elements is ranked highest to lowest, along with the financial impact of each. A vital part of this analysis is the discovery of non-obvious interdependence between operational elements. This discovery is critical because it reveals the potential for cascading failures that can make a minor event major, a major event a disaster, and a disaster into a catastrophe.

The analysis may be tedious, but it is extremely important. It often yields many surprising facts and interrelationships among the human, technological, and physical aspects of your business. Once done, you may wonder how you never before saw what now seems so obvious. More importantly, you will realize how vital it is that you know these facts, because in the next phases of the COOP plan preparation, the information you discovered will be put to use.

Your Action Plan -What HIPAA Requires

Regardless of the type or cause, every disaster goes through the same phases

1. Initial emergency state and reaction
2. Stabilization and damage assessment
3. Restoration and reparation
4. Reconstitution and resumption.

Depending on the disaster, the phases vary in duration. For example, an explosion is instantaneous, whereas a hacking attack is gradual, but possibly just as damaging in its own way. There are several things you can do ahead of time to become resistant to disasters and recover faster once they have happened.

Risk Mitigation

Disaster prevention will always be better than even the best recovery plan. You cannot prevent all disasters, but using the results of the risk analysis and BIA, you can make your enterprise more resilient and make disasters survivable when they do occur.

Prioritizing your organization's risks from highest to lowest, your first goal is to cost-effectively mitigate all that you can. In relation to IT systems, mitigation measures would include fully patching all platforms, hardening all publicly reachable systems, and installing redundancy measures like hot-failover or clustering. Every risk and its proposed mitigation must be considered for impact to normal operations. The goal of each mitigation should be to protect infrastructure, but without adding unnecessary or unwanted complexity or technological fragility.

One of several preparatory measures required by HIPAA includes planning and performing system backups. This can include mirroring the live system in real-time or near real-time to another identical system elsewhere, possibly to the cloud or to traditional tape drives. Backups are a well-proven method of protecting vital data. While HIPAA does not require a specific solution, it does require that you perform the function, plan it carefully, execute it consistently, and test it periodically to ensure that it works. Specially, this means periodically restoring your system from sampled tapes or mirrored files to ensure they are readable and usable.

Emergency Mode Operations Plan (EMOP)

This section of the plan deals with the initial response to the emergency and procedures for ensuring that the privacy and security of data are assured even while operating under difficult conditions. It addresses the need to continue to do business even while the emergency is in progress.

This element of the plan contains procedures to operate systems either in the original location if it is habitable or in a new location. As a HIPAA requirement, the EMOP makes it possible to operate under adverse circumstances and remain in compliance with the privacy and security requirements that HIPAA imposes. This is often difficult to achieve. In an emergency, delivering care where needed is always the priority. Even so, the law does not allow caution to be set aside when handling sensitive information. Finding an efficient balance for doing both takes advance planning, solid organization, and leadership in execution. Targeted training lays the foundation to find that balance.

Why Does Plan Testing and Revision Matter

Plans are detailed outlines of the things we want to achieve. Organizations behave like living things in that they are always changing and evolving. Because they do, plans must change with them or risk becoming outdated and ineffective. Nothing could be more deadly to an organization's surviving a disaster than an outdated COOP.

HIPAA requires that you first build a plan, but also requires the next and equally important step: Testing the plan. The plan must be tested and revised as necessary to ensure it remains relevant and current. HIPAA also requires that testing is a regular part of your business activities. This ensures that the experience is captured and documented with the goal of improving over time.

There are several tests that can be conducted to meet HIPAA requirements. Each has its benefits, either as a standalone test or as a step in maturing the overall plan. The tests include the following.

1. **Checklist:** All participants review checklists of steps, equipment, and other items to verify that nothing has been omitted. Gathered and collated, each round becomes more refined and more complete.
2. **Structured Walk-Through:** This is a facilitated, scenario-based group exercise. The core team members convene in a conference room and are led through the exercise and arrive at the outcome. Without the pressure of a real emergency, this enables identification of interdependencies and other subtle characteristics that, if left undiscovered, could have catastrophic impact during an actual event.
3. **Simulation:** This test involves relocation to a recovery site, but without interrupting normal operations. This works well to observe the logistics needed to set up the relocated site and begin operations. This test allows the process to be improved and confusion reduced.
4. **Parallel:** This test also involves an actual relocation, and includes opening the recovery site and initiating processing. Without closing the home site, this test involves testing the systems and equipment that will be used to recover when the time comes. Therefore, it serves as a form of non-destructive testing that provides proof-of-concept.
5. **Full Interruption:** Just what it sounds like, this test involves shutting down the home site and going to the off-site recovery location. The bad news is that this can be very costly and disruptive. This type of test can take more than a year to plan. The good news is HIPAA does not require this test.

For the best results overall, these tests should be viewed and performed as progressive steps, with each building on its predecessors. The more these tests are done, the stronger your plan becomes, and the more confident you can be about your ability to survive an adverse event.

Why Determining Application and Data Criticality Is Essential

Not every asset or system will have the same importance under emergency conditions. One of the more important steps to take in planning, and one required by HIPAA, is that of determining which systems, applications, and data are important, and prioritizing them in descending order for recovery.

In consultation with the organization's lines of operation and IT systems, it must be determined what is needed in order to function so that when disaster comes, the most critical asset or system gets immediate attention, followed by the others in order. Here are some things to consider.

1. **What is the primary system and what is it supported by?** There is a logical order of support and dependency of one system upon others. These must be identified clearly.
2. **What is a must-have and what is a would-like-to-have?** Under emergency conditions, only the most critical priorities should be addressed initially, otherwise organizational survival might be placed at risk.
3. **How long can an outage last before it becomes critical?** The length of time an operational element can be down must be determined.
    a. **Maximum Tolerable Downtime (MTD):** This metric tells how long a given organizational element can be down before operational losses become fatal.
    b. **Recovery Time Objective (RTO):** This describes the optimal amount of time it should take to get the off-site recovery location into operation.
    c. **Recovery Point Objective (RPO):** This denotes how close to true currency the data should be at the RTO.

Once those questions are answered, the next set of questions relates to what kind of facilities are needed. The following are typical facility types.

1. **Hot Site:** Fully equipped and available within hours. This is normally a subscription service, but can be provided internally, and is usually expensive.
2. **Warm Site:** This type of site is less expensive to maintain and normally requires equipment to be provided (servers, storage). Requires a longer lead time to bring on-line (up to a week).
3. **Cold Site:** This is often just a secure location that houses no equipment or data, only power, lighting, and A/C. For this type of site you need to provide everything. The lead time can be up to a month to become operational.

Clearly, the more critical the data or application, the shorter you want the outage to be. It is equally clear that cost is an important consideration. Outages and costs should be derived as outcomes from the BIA, and are based on estimated business losses. Once validated, however, the choice of recovery solution–hot, warm, or cold–should be justified by the business case loss potential.

How to Keep Your Disaster Recovery Location Safe and Secure

During these events, keeping both your primary location and your recovery location safe and secure is as important as the recovery effort itself. HIPAA also requires that you set up procedures and plans to ensure that staff working in each location are properly prepared to do the work and are trained in the necessary security and safety procedures. Of particular importance is making sure that everyone engaged in this effort is authorized to do so.

It is common in a healthcare setting for many people to come into regular contact with patient information. Under contingency conditions, the mix of personnel needed to manage the situation often differs radically from the norm. Your workforce may include people who would not normally see such sensitive information. The law regards this exposure as a breach of privacy, emergency conditions or not, and that is bad for everyone.

Knowing in advance that this may be the case, it is possible to make arrangements through confidentiality agreements and similar documents to address this and prevent the breach. This means that all of the contracts with contractors, team members, subscription recovery services, and all others involved in a recovery effort, great or small, must contain the necessary language and assurances that the confidentiality of patient information will be protected to the extent possible by all parties involved. It also means that patients must be informed that this set of conditions could occur, but that all due care will be used to protect their privacy and prevent any improper exposure.

Again, there is a need for advance preparation and specific steps are needed outside of the recovery process to ensure things go smoothly. Even from a high-level perspective, preparing for disaster and executing a recovery plan seems enormously complex. The fact is, disaster preparation and recovery is complex. There is often the added risk that those placed in charge of preparing for disasters may not be fully prepared for the challenge. This risk will exacerbate all the others. As such, it must be the first risk to be mitigated.

Preparedness Is Not Just About Plans – It's About People

It is easy to see that putting together a COOP that works to protect your business in emergencies is a complex and specialized project. Many organizations elect to bring in specialists to perform the task. But specialists won't be with you forever. After they leave, the work of maintaining and executing the plan and the accountability for its execution remains with you. The time to acquire the knowledge and build the skill to manage a project of this scope and importance is now.

Conclusion

Nothing can replace a solid plan that does its job well. But that plan cannot work without the right people in the right places who are trained to do the right things. Acquiring the knowledge and training you need now can make your disaster planning preparations easier and more successful. The time to acquire those skills is before you need them. Be sure that when the moment comes, and it will, you and your team will be ready for it.

Learn more about how you can develop and hone your project management expertise, expand data center management knowledge, and sharpen your IT security skills. Here is a sampling of the kinds of courses that could benefit the Continuity Planner in your organization:

1. **Project Management:** Courses with this focus provide the knowledge and skills crucial to planning and executing the COOP project successfully. You should seek courses that are aligned with the Project Management Institute® PM methodology.
2. **Data Center Management:** Knowing how the data center works under normal circumstances provides insight essential to reconstructing the data center if disaster strikes.
3. **Cybersecurity:** CISSP (Certified Information Systems Security Professional) and CISM (Certified Information Security Manager) courses provide specific knowledge that will enable you to cope with incident response and disaster recovery.

See Appendix **Contingency Plan Template** at the end of this document.

Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge. Check out the following Global Knowledge course(s):

IT Risk Management

IT Project Management

Data Center Infrastructure Management

Cybersecurity Foundations

CISSP Prep Course

CISM Prep Course

For more information or to register, visit **www.globalknowledge.com** or call **1-800-COURSES (1-800-268-7737)** to speak with a sales representative.

Our courses and enhanced, hands-on labs and exercises offer practical skills and tips that you can immediately put to use. Our expert instructors draw upon their experiences to help you understand key concepts and how to apply them to your specific work situation. Choose from our more than 1,200 courses, delivered through Classrooms, e-Learning, and On-site sessions, to meet your IT and business training needs.

About the Author

Mr. Leo has been an Information Security professional for over 30 years. He has worked internationally as a Systems Analyst/Engineer, and as a Security and Privacy Consultant. His past employers include IBM, St. Luke's Episcopal Hospital, Computer Sciences Corporation, and Rockwell International. From 1998 to 2002, he was Director of Security Engineering and Chief Security Architect for Mission Control at the Johnson Space Center. From 2002 to 2006 Mr. Leo was the Director of Information Systems, and Chief Information Security Officer for

the Managed Care Division of the University of Texas Medical Branch in Galveston, Texas. Mr. Leo continues to work in the Healthcare arena as a professional educator and management consultant.

Mr. Leo serves as a member of several university advisory boards overseeing curriculum development and programs in the Information Assurance and Engineering areas; including Texas State Technical College, DeVry University, and Voorhees College. Mr. Leo is on the Editorial Boards for Auerbach Publishing and Homeland Security Magazine (ACFEI), and the Senior Advisory Panel for eWeek Publications. Mr. Leo's most recent book, The HIPAA Program Reference Handbook, was published in January 2005. His current project is Series Editor for the *"Critical Infrastructure Protection and Cybersecurity Engineering Series."*

Mr. Leo has had many technical and operational successes through his career, including:

- Successful accomplishment of a complete HIPAA compliance program for UTMB Galveston, Managed Care Division
- Planning and execution of corporate security and compliance program plans for Healthcare, Bioengineering, Aerospace, Natural Resource, and Academic organizations
- Design, implementation, and management of the world's largest telemedicine network in Texas

Mr. Leo is a past member of the IT Security Council for the American Society of Industrial Security (ASIS). He is a member of the Project Management Institute (PMI), the Information Security, Audit, and Control Association (ISACA), the Disaster Recovery Institute (DRII), and a member of the American Board of Forensic Engineering and Technology (ABFET) for The American College of Forensic Examiners International (ACFEI). Mr. Leo holds certifications from each of these organizations.

Mr. Leo attended Graduate School at the University of Houston, and Undergraduate school at Southern Illinois University. Originally from California, Mr. Leo has lived in Texas since 1980.

Appendix A: Contingency Planning Guidelines

Information technology (IT) and automated information systems are vital elements in most business processes. Because these IT resources are so essential to an organization's success, it is critical that the services provided by these systems are able to operate effectively without excessive interruption. Contingency planning supports this requirement by establishing thorough plans and procedures and technical measures that can enable a system to be recovered quickly and effectively following a service disruption or disaster. Interim measures may include the relocation of IT systems and operations to an alternate site, the recovery of IT functions using alternate equipment, or the performance of IT functions using manual methods.

IT systems are vulnerable to a variety of disruptions, ranging from mild (e.g., short-term power outage, disk drive failure) to severe (e.g., equipment destruction, fire). Vulnerabilities may be minimized or eliminated through technical, management, or operational solutions as part of the organization's risk management effort. However, it is virtually impossible to completely eliminate all risks. Contingency planning is designed to mitigate the risk of system and service unavailability by focusing efficient and effective recovery solutions.

Within the context of HIPAA, the goal of contingency planning is to adequately protect EPHI during a contingency event, and to ensure that organizations have their EPHI available when it is needed.

This appendix, Contingency Planning Guidelines, will identify fundamental planning principles and practices to help personnel develop and maintain effective information system contingency plans. This section will be based on NIST Special Publication 800-34 Revision 1, Contingency Planning Guide for Information Technology Systems.

Contingency Planning Defined

IT contingency planning refers to a coordinated strategy involving plans, procedures, and technical measures that enable the recovery of IT systems, operations, and data after a disruption. Contingency planning generally includes one or more of the approaches to restore disrupted IT services:

- Restoring IT operations at an alternate location;
- Recovering IT operations using alternate equipment; and
- Performing some or all of the affected business processes using non-IT (manual) means (typically acceptable for only short-term disruptions).

Types of Contingency-Related Plans

IT contingency planning represents a broad scope of activities designed to sustain and recover critical IT services following an emergency. IT contingency planning fits into a much broader emergency preparedness environment that includes organizational and business process continuity and recovery planning. Ultimately, an organization would use a suite of plans to properly prepare response, recovery, and continuity activities for disruptions affecting the organization's IT systems, business processes, and the facility. Because there is an inherent relationship between an IT system and the business process it supports, there should be coordination between each plan

during development and updates to ensure that recovery strategies and supporting resources neither negate each other nor duplicate efforts.

Types of Contingency Plans

Contingency Plan (CP)

- 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.
- Addresses IT system disruptions; not typically business process-focused

Continuity of Operations Plan (COOP)

- 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 a disaster event before returning to normal operations.
- Addresses the subset of an organization's missions that are deemed most critical; not typically IT-focused

Disaster Recovery Plan (DRP)

- A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities.
- Limited to major disruptions with long-term effects; typically IT-focused

HIPAA Contingency Planning Requirements

Standard 164.308(a)(7), 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

The Contingency Plan standard includes five implementation specifications:

1. 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.
2. Disaster Recovery Plan (R) – 164.308(a)(7)(ii)(B): Establish (and implement as needed) procedures to restore any loss of data.
3. 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.
4. Testing and Revision Procedures (A) – 164.308(a)(7)(ii)(D): Implement procedures for periodic testing and revision of contingency plans.

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

IT Contingency Planning Process

To develop and maintain an effective IT contingency plan, organizations should consider using the approach discussed in NIST SP 800-34, Contingency Planning Guide for Information Technology Systems, which proposes a step-by-step contingency planning process, and provides an in-depth discussion of technical contingency planning considerations for specific types of information technology systems. A summary of this process is detailed below.

1. Develop the Contingency Planning Policy Statement. To be effective and to ensure that personnel fully understand the agency's contingency planning requirements, the contingency plan must be based on a clearly defined policy supported by organizational leadership. The contingency planning policy statement should define the organization's overall contingency objectives and establish the organizational framework and responsibilities for IT contingency planning. Key policy elements include:

- Roles and responsibilities
- Scope as applies to the type(s) of platform(s) and organization functions subject to contingency planning
- Resource requirements
- Training requirements
- Exercise and testing, and plan maintenance schedules
- Frequency of backups and storage of backup media.

2. Conduct the Business Impact Analysis (BIA). The BIA is a key step in the contingency planning process. The BIA enables the organization to fully characterize information system requirements, processes, and interdependencies and use this information to determine contingency requirements and priorities.

The purpose of the BIA is to correlate specific system components with the critical services that they provide and, based on that information, to characterize the consequences of a disruption to the system components. Key steps include identifying critical IT resources, disruption impacts and allowable outage times, and developing recovery priorities. Results from the BIA should be appropriately incorporated into the analysis and strategy development efforts for the organization's other continuity and recovery plans, including disaster recovery and emergency mode operations plans.

3. Identify Preventive Controls. In some cases, the outage impacts identified in the BIA may be mitigated or eliminated through preventive measures that deter, detect, and/or reduce impacts to the system. Where feasible and cost-effective, preventive methods are preferable to actions that may be necessary to recover the system after a disruption. Preventive controls should be documented in the contingency plan, and personnel associated with the system should be trained on how and when to use the controls.

A variety of preventive controls are available, depending on system type and configuration; however, some common measures are listed below:

- Appropriately sized uninterruptible power supplies (UPS) to provide short-term backup power to all system components (including environmental and safety controls)
- Gasoline- or diesel-powered generators to provide long-term backup power
- Air-conditioning systems with adequate excess capacity to permit failure of certain components, such as a compressor
- Fire suppression systems
- Fire and smoke detectors
- Water sensors in the computer room ceiling and floor
- Plastic tarps that may be unrolled over IT equipment to protect it from water damage
- Heat-resistant and waterproof containers for backup media and vital non-electronic records
- Emergency master system shutdown switch
- Offsite storage of backup media, non-electronic records, and system documentation
- Technical security controls, such as cryptographic key management and least-privilege access controls
- Frequent scheduled backups.

4. Develop Recovery Strategies. Recovery strategies provide a means to restore IT operations quickly and effectively following a service disruption. Strategies should address disruption impacts and allowable outage times identified in the BIA. Several alternatives should be considered when developing the strategy, including cost, allowable outage time, security, and integration with larger organization-level contingency plans.

The selected recovery strategy should address the potential impacts identified in the BIA and should be integrated into the system architecture during the design and implementation phases of the system life cycle.

The strategy should include a combination of methods that complement one another to provide recovery capability over the full spectrum of incidents, ranging from minor service disruption to a partial or total loss of primary system operations requiring operational resumption at another location. A wide variety of recovery approaches may be considered; the appropriate choice depends on the incident, type of system, and its operational requirements, including retention requirements. Specific recovery methods may include commercial contracts with cold, warm, or hot site vendors, mobile sites, mirrored sites, reciprocal agreements with internal or external organizations, and service-level agreements (SLAs) with the equipment vendors. In addition, high-availability technologies such as Redundant Arrays of Independent Disks (RAID), automatic fail-over, uninterruptible power supply (UPS), mirrored systems, and multisite data archiving systems should be considered when developing a system recovery strategy.

5. Develop an IT Contingency Plan. IT contingency plan development is a critical step in the process of implementing a comprehensive contingency planning program. The plan contains detailed roles, responsibilities, teams, and procedures associated with restoring an IT system following a disruption. The contingency plan should document technical capabilities designed to support contingency operations. Plans need to balance detail with flexibility; usually the more detailed the plan, the less scalable and versatile the approach.

Following the approach described in NIST SP 800-34, the contingency plan comprises five main components: Supporting Information, Notification and Activation, Recovery, Reconstitution, and Plan Appendices. The first and last components provide essential information to ensure a comprehensive plan. The Notification and Activation, Recovery, and Reconstitution phases address specific actions that the organization should take following a system disruption or emergency.

- The Supporting Information component includes an introduction and concept of operations section that provides essential background or contextual information that makes the contingency plan easier to understand, implement, and maintain. These details aid in understanding the applicability of the guidance, in making decisions on how to use the plan, and in providing information on where associated plans and information outside the scope of the plan may be found.

- The Notification and Activation Phase defines the initial actions taken once a system disruption or emergency has been detected or appears to be imminent. This phase includes activities to notify recovery personnel, assess system damage, and implement the plan. At the completion of the Notification and Activation Phase, recovery staff will be prepared to perform contingency measures to restore system functions on a temporary basis.

- The Recovery Phase begins after the contingency plan has been activated, damage assessment has been completed (if possible), personnel have been notified, and appropriate teams have been mobilized. Recovery phase

- Activities focus on contingency measures to execute temporary IT processing capabilities, repair damage to the original system, and restore operational capabilities at the original or new facility. At the completion of the Recovery Phase, the IT system will be operational and performing the functions designated in the plan. Depending on the recovery strategies defined in the plan, these functions could include temporary manual processing, recovery and operation at an alternate system, or relocation and recovery at an alternate site. Teams with recovery responsibilities should understand and be able to perform these recovery strategies well enough that if the paper plan is unavailable during the initial stages of the event, they can still perform the necessary activities.

- In the Reconstitution Phase, recovery activities are terminated, and normal operations are transferred back to the organization's facility. If the original facility is unrecoverable, the activities in this phase can also be applied to preparing a new facility to support system processing requirements. Until the primary system is restored and tested, the contingency system should continue to be operated. The Reconstitution Phase should specify teams responsible for restoring or replacing both the site and the information system.

Contingency Plan Appendices should provide key details not contained in the main body of the plan. The appendices should reflect the specific technical, operational, and management contingency requirements of the information system and the larger organization. Appendices can include, but are not limited to, contact information for contingency planning team personnel; vendor contact information, including offsite storage and alternate site points of contact; standard operating procedures and checklists for system recovery or processes;

equipment and system requirements lists of the hardware, software, firmware, and other resources required to support system operations; vendor agreements, reciprocal agreements with other organizations, and other vital records; description of, and directions to, the alternate site; and the BIA.

Plans should be formatted to provide quick and clear direction in the event those personnel unfamiliar with the plan or the systems are called on to perform recovery operations. Plans should be clear, concise, and easy to implement in an emergency. Where possible, checklists and step-by-step procedures should be used. A concise and well-formatted plan reduces the likelihood of creating an overly complex or confusing plan.

6. Plan Testing, Training, and Exercises. Plan testing is a critical element of a viable contingency capability. Testing enables plan deficiencies to be identified and addressed. Testing also helps evaluate the ability of the recovery staff to implement the plan quickly and effectively. Each IT contingency plan element should be tested to confirm the accuracy of individual recovery procedures and the overall effectiveness of the plan. The following areas should be addressed in a contingency test:

- System recovery on an alternate platform from backup media
- Coordination among recovery teams
- Internal and external connectivity
- System performance using alternate equipment
- Restoration of normal operations
- Notification procedures.

Training for personnel with contingency plan responsibilities should complement testing. Training should be provided at least annually; new hires with plan responsibilities should receive training shortly after they are hired. Ultimately, contingency plan personnel should be trained to the extent that that they are able to execute their respective recovery procedures without aid of the actual document. This is an important goal in the event that paper or electronic versions of the plan are unavailable for the first few hours resulting from the extent of the disaster. Recovery personnel should be trained on the following plan elements:

- Purpose of the plan
- Cross-team coordination and communication
- Reporting procedures
- Security requirements
- Team-specific processes (Notification/Activation, Recovery, and Reconstitution Phases)
- Individual responsibilities (Notification/ Activation, Recovery, and Reconstitution Phases).

7.Maintain the plan. To be effective, the plan must be maintained in a ready state that accurately reflects system requirements, procedures, organizational structure, and policies. IT systems undergo frequent changes because of shifting business needs, technology upgrades, or new internal or external policies. Therefore, it is essential that the contingency plan be reviewed and updated regularly, as part of the organization's change management process, to ensure that new information is documented and contingency measures are revised if required.

The following resources may provide useful information to assist covered entities in developing contingency planning strategies to adequately protect and recover access to EPHI during a contingency event, and demonstrate compliance with the Contingency Plan standard and implementation specifications:

NIST Special Publication 800-34 Revision 1, Contingency Planning Guide for Information Technology Systems, http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf

NIST Special Publication 800-66 Revision 1, Implementing the HIPAA Security Rule, http://csrc.nist.gov/publications/nistpubs/800-66/sp800-66.pdf

HIPAA Security Series, Security Standards: Administrative Safeguards, http://www.cms.hhs.gov/EducationMaterials/Downloads/SecurityStandardsAdministrativeSafeguards.pdf

Appendix B

Contingency Plan Template

This sample format provides a template for preparing an information technology (IT) contingency plan. The template is intended to be used as a guide and should be modified as necessary to meet the system's contingency requirements and comply with internal policies. Where practical, the guide provides instructions for completing specific sections. Text is added in certain sections; however, this information is intended only to suggest the type of information that may be found in that section. The text is not comprehensive and should be modified to meet specific organization and system considerations.

1. INTRODUCTION

1.1 PURPOSE

This {system name} Contingency Plan establishes procedures to recover the {system name} system following a disruption. The following objectives have been established for this plan:

- Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:

  - Notification/Activation phase to detect and assess damage and to activate the plan;

  - Recovery phase to restore temporary IT operations and recover damage done to the original system; and

  - Reconstitution phase to restore IT system processing capabilities to normal operations.
- Identify the activities, resources, and procedures needed to carry out {system name} processing requirements during prolonged interruptions to normal operations.
- Assign responsibilities to designated {Organization name} personnel and provide guidance for recovering {system name} during prolonged periods of interruption to normal operations.
- Ensure coordination with other {Organization name} staff who will participate in the contingency planning strategies. Ensure coordination with external points of contact and vendors who will participate in the contingency planning strategies.

1.2 APPLICABILITY

The {system name} Contingency Plan applies to the functions, operations, and resources necessary to restore and resume {Organization name}'s {system name} operations as it is installed at its primary location: {Name, City, State}. The {system name} Contingency Plan applies to {Organization name} and all other persons associated with {system name} as identified under Section 2.3, Responsibilities.

1.3 SCOPE

1.3.1 Planning Principles

Various scenarios were considered to form a basis for the plan, and multiple assumptions were made. The applicability of the plan is predicated on two key principles:

- The {Organization name}'s facility in {City, State}, is inaccessible; therefore, {Organization name} is unable to perform {system name} processing for the organization.
- A valid contract exists with the alternate site that designates that site in {City, State}, as {Organization name}'s alternate operating facility.

  – {Organization name} will use the alternate site building and IT resources to recover {system name} functionality during an emergency situation that prevents access to the original facility.

  – The designated computer system at the alternate site has been configured to begin processing {system name} information.

  – The alternate site will be used to continue {system name} recovery and processing throughout the period of disruption, until the return to normal operations.

1.3.2 Assumptions

Based on these principles, the following assumptions were used when developing the IT Contingency Plan:

- The {system name} is inoperable at the {Organization name} computer center and cannot be recovered within {XX} hours.
- Key {system name} personnel have been identified and trained in their emergency response and recovery roles; they are available to activate the {system name} Contingency Plan.
- Preventive controls (e.g., generators, environmental controls, waterproof tarps, sprinkler systems, fire extinguishers, and fire department assistance) are fully operational at the time of the contingency event.
- Computer center equipment, including components supporting {system name}, are connected to an uninterruptible power supply (UPS) that provides {XX} minutes/hours of electricity during a power failure.
- {System name} hardware and software at the {Organization name} original site are unavailable for at least {XX} hours.
- Current backups of the application software and data are intact and available at the offsite storage facility.
- The equipment, connections, and capabilities required to operate {system name} are available at the alternate site in {City, State}.
- Service agreements are maintained with {system name} hardware, software, and communications providers to support the system recovery.

The {system name} Contingency Plan does not apply to the following situations:

- Overall recovery and continuity of business operations. The Business Resumption Plan (BRP) and Continuity of Operations Plan (COOP) are appended to the plan.
- Emergency evacuation of personnel. The Occupant Evacuation Plan (OEP) is appended to the plan.
- Any additional constraints should be added to this list.

1.4 REFERENCES/REQUIREMENTS

This {system name} Contingency Plan complies with the {Organization name}'s IT contingency planning policy as follows:

{Insert organization's contingency planning policy statement}

The {system name} Contingency Plan also complies with the following policies:

- Health Insurance Portability and Accountability Act (HIPAA), 1996
- {Insert other applicable policies}

1.5 RECORD OF CHANGES

Modifications made to this plan are as follows:

- Record of Changes
- Page No.
- Change Comment
- Date of Change
- Signature

2. CONCEPT OF OPERATIONS

2.1 SYSTEM DESCRIPTION AND ARCHITECTURE

Provide a general description of system architecture and functionality. Indicate the operating environment, physical location, general location of users, and partnerships with external organizations/systems. Include information regarding any other technical considerations that are important for recovery purposes, such as backup procedures. Provide a diagram of the architecture, including security controls and telecommunications connections.

2.2 LINE OF SUCCESSION

The {organization name} sets forth an order of succession to ensure that decision-making authority for the {system name} Contingency Plan is uninterrupted. The Chief Information Officer (CIO), {organization name} is responsible for ensuring the safety of personnel and the execution of procedures documented within this {system name} Contingency Plan. If the CIO is unable to function as the overall authority or chooses to delegate this responsibility to a successor, the Deputy CIO shall function as that authority. Identify and describe line of succession as applicable.

2.3 RESPONSIBILITIES

The following teams have been developed and trained to respond to a contingency event affecting the IT system.

The Contingency Plan establishes several teams assigned to participate in recovering {system name} operations. Examples of teams that may be included are management team, application recovery team, operating system team, network operations team, site restoration/salvage team, procurement team, damage assessment team,

and communications team. The system environment and the scope of the recovery effort will dictate which teams will be necessary to execute the plan.

- {Team name}

{Describe each team, their responsibilities, leadership, and coordination with other applicable teams during a recovery operation. Do not detail specific procedures that will be used to execute these responsibilities. These procedures will be itemized in the appropriate phase sections.}

The relationships of the teams involved in system recovery are illustrated in Figure {XX} below.

{Insert hierarchical diagram of recovery teams. Show team names and leaders; do not include actual names of personnel.}

3. NOTIFICATION AND ACTIVATION PHASE

This phase addresses the initial actions taken to detect and assess damage inflicted by a disruption to {system name}. Based on the assessment of the event, the plan may be activated by the Contingency Planning Coordinator.

In an emergency, the {Organization name}'s top priority is to preserve the health and safety of its staff before proceeding to the Notification and Activation procedures.

Notification

Contact information for key personnel is located in Appendix A. The notification sequence is listed below:

- The first responder is to notify the Contingency Planning Coordinator. All known information must be relayed to the Contingency Planning Coordinator.
- {Insert further notification sequences specific to the organization and the system.}

Upon notification, the following procedures are to be performed by their respective teams:

Damage Assessment Procedures:

{Detailed procedures should be outlined to include activities to determine the cause of the disruption; potential for additional disruption or damage; affected physical area and status of physical infrastructure; status of IT equipment functionality and inventory, including items that will need to be replaced; and estimated time to repair services to normal operations.}

- {team name}
  - Team Damage Assessment Procedures
- {Insert additional team names and procedures as necessary}

Activation

The Contingency Plan is to be activated if one or more of the following criteria are met:

1. {System name} will be unavailable for more than {XX} hours.
2. Facility is damaged and will be unavailable for more than {XX} hours.
3. Other criteria, as appropriate:
   - If the plan is to be activated, the Contingency Planning Coordinator is to notify all Team Leaders and inform them of the details of the event and if relocation is required.
   - Upon notification from the Contingency Planning Coordinator, Team Leaders are to notify their respective teams. Team members are to be informed of all applicable information and prepared to respond and relocate if necessary.
   - The Contingency Planning Coordinator is to notify the offsite storage facility that a contingency event has been declared and to ship the necessary materials (as determined by damage assessment) to the alternate site.
   - The Contingency Planning Coordinator is to notify the alternate site that a contingency event has been declared and to prepare the facility for the organization's arrival.
   - The Contingency Planning Coordinator is to notify remaining personnel (via notification procedures) on the general status of the incident.

4. RECOVERY OPERATIONS

This section provides procedures for recovering the application at the alternate site, whereas other efforts are directed to repair damage to the original system and capabilities.

The following procedures are for recovering the {system name} at the alternate site. Procedures are outlined per team required. Each procedure should be executed in the sequence it is presented to maintain efficient operations.

Recovery Goal. State the first recovery objective as determined by the Business Impact Assessment (BIA). For each team responsible for executing a function to meet this objective, state the team names and list their respective procedures.

- {team name}
  - Team Recovery Procedures
- {Insert additional team names and procedures as necessary}

Recovery Goal. State the remaining recovery objectives as determined by the BIA. For each team responsible for executing a function to meet this objective, state the team names and list their respective procedures.

- {team name}
  - Team Recovery Procedures

- {Insert additional team names and procedures as necessary}

5. RETURN TO NORMAL OPERATIONS

This section discusses activities necessary for restoring {system name} operations at the {Organization name}'s original or a new site. When the computer center at the original or the new site has been restored, {system name} operations at the alternate site must be transitioned back. The goal is to provide a seamless transition of operations from the alternate site to the computer center.

Original or New Site Restoration

Procedures should be outlined, per necessary team, to restore or replace the original site so that normal operations may be transferred. IT equipment and telecommunications connections should be tested.

- {team name}
  - Team Resumption Procedures
- {Insert additional team names and procedures as necessary}

5.1 CONCURRENT PROCESSING

Procedures should be outlined, per necessary team, to operate the system in coordination with the system at the original or the new site. These procedures should include testing the original or new system until it is functioning properly and ensuring that the contingency system is shut down gracefully.

- {team name}
  - Team Concurrent Processing Procedures
- {Insert additional team names and procedures as necessary}

5.2 PLAN DEACTIVATION

Procedures should be outlined, per necessary team, to clean the alternate site of any equipment or other materials belonging to the organization, with a focus on handling sensitive information. Materials, equipment, and backup media should be properly packaged, labeled, and shipped to the appropriate location(s). Team members should be instructed to return to the original or the new site.

- {team name}
  - Team Deactivation Procedures
- {Insert additional team names and procedures as necessary}

6. PLAN APPENDICES

The appendices included should be based on system and plan requirements.

- Personnel Contact List
- Vendor Contact List
- Equipment and Specifications
- Service-Level Agreements and Memorandums of Understanding
- IT Standard Operating Procedures
- Business Impact Analysis
- Related Contingency Plans
- Emergency Management Plan
- Occupant Evacuation Plan
- Continuity of Operations Plan.