<<organization>>

Contingency Plan

Effective Date:

Version History

Version #	Author	Date
1.0		

NOTE: This Contingency Plan template is designed to supplement a larger Business Continuity Plan and ensure that the Security and Privacy requirements of HIPAA and the due diligence of Risk Management are taken into account.

Purpose

The IT component of Contingency Planning is the process of ensuring that essential information processing functions (such as access to electronic health records) can be maintained throughout a variety of incidents and emergencies. The Contingency Plan endeavors to protect the confidentiality, integrity and availability of Protected Health Information (PHI). The purpose of [ORGANIZATION] Contingency Plan is to identify essential business operations or functions; the facilities, equipment, records, personnel, and other resources required to perform those functions; and the plans to enable an effective recovery from an event that affects the normal operation of [ORGANIZATION]. The purpose of the IT component of the Contingency Plan is to identify and plan for continuity of the critical IT functions and systems that support the essential business operations. IT Contingency Planning must address three types of disruptions:

- Closure of a facility (such as damage to a building);
- Reduced workforce (such as due to pandemic flu); and
- Technological equipment or systems failure (such as IT systems failure).

The contingency plan must, at a minimum, address the following IT Security requirements:

1. Identify the functional areas essential to business operations.
2. Determine how each situation, such as fire or flood, would affect these key areas, what actions would be taken and the resources needed for each one.
3. Set goals for the return to essential operations and return to full normal operations.
4. Identify each required process and document each step in the process, what needs to be done, along with the staff and other resources needed to complete the work. Develop plans for each functional area and the organization as a whole

5. Implement a communications and education plan to keep employees informed of changes and remind them of their roles and responsibilities.

This document provides the following sections to meet the requirements above:

- Business Impact Analysis
- Activation and Relocation
- Emergency Mode Operations
- Business Resumption
- Testing and Training

[ORGANIZATION] leadership has overall responsibility for contingency planning, including overseeing the effort to develop, test and maintain the plan. The [Contingency Plan Coordinator and/or Contingency Plan Leadership Team (CPLT)] have overall responsibility for developing and maintaining the plan. The Coordinator communicates with staff and trains them on the plan and their responsibilities.

The plan must be tested on a regular basis using mock situations to identify problems and areas for improvement. The plan must also be updated periodically to reflect changes in the organization and technology. Any regulatory requirements should be incorporated during the planning process.

Plan Owner

Business Continuity Plan: [Chief Operating Officer]

IT System Security Continuity Appendices: [ROLE]

Business Impact Analysis

The Business Impact Analysis phase of [ORGANIZATION]'s continuity planning process enables [ORGANIZATION] to identify and prioritize essential functions, and then to conduct a systematic assessment of the resources (people, facilities, equipment, and records) required to support those functions.

The Business Impact Analysis focuses on identifying and evaluating key systems, data and infrastructure:

- Identify essential facilities, equipment, records, and other resources required to perform essential functions;
- Identify the vital records (files, documents, and databases) that must be protected and preserved; and
- The Recovery Time Objectives (RTOs) for each essential information technology system.

IT Threats and Risks

A list of threats to critical IT business processes and data must be created. Each threat should be linked to what processes could be interrupted or terminated and what data is vulnerable. Mitigation strategies for preventing and decreasing the impact of the threat should be documented (e.g. remote storage of backup data, documentation or tested response alternatives).

IT Disaster Recovery

The IT Disaster Recovery Plan is a subsection of the Contingency Plan. It addresses the procedures to maintain or restore the essential IT services and functions. Contingency, Emergency and Disaster response are usually managed as a whole with executive empowerment of division or business unit leads to respond as quickly and decisively as necessary to meet the demands of the event. IT Disaster Recovery is generally the domain of the IT service staff or contractor. The [ROLE] is responsible for leading all IT response efforts and ensuring that plans are carried out to the best possible result. The [ROLE} must have the list of the Recovery Time Objectives mapped to the Business Impact Assessment findings so that (s)he can allocate resources to restore the business critical systems within their RTO.

The Disaster Recovery Plan (DRP) should identify the various responses based on the type of event. In some cases the recovery process may require that individuals that have not been processed through the standard security procedures and account provision process need access to sensitive systems or even ePHI to quickly restore services. The DRP should anticipate these situations and give the [ROLE] the flexibility to implement alternative controls (e.g. supervision or contracts). These mitigation options should be generalized in the Emergency Mode Operations plan and carefully limited so that the release of PHI to unauthorized personnel is minimized and where unavoidable, carefully controlled. The organization remains responsible and accountable for all releases of PHI and must follow applicable reporting requirements in the event of a PHI breach during an emergency.

Emergency Mode Operations Plan

Emergency Mode Operations are characterized by the need for management, staff and support personnel to carry out their responsibilities in alternate locations and/or beyond their assigned responsibilities. An emergency mode operations plan should identify alternative locations that may be used in an emergency. The plan must also identify how the critical IT system information including ePHI/PHI will be available to carry out their responsibilities. The plan must also identify alternate personnel to carry out the critical business processes. The [ROLE] must plan on realigning the access during emergencies to allow the alternates to execute essential business functions.

Contingency Plan Operational Phases and Implementation

The Contingency Plan Leadership Team (CPLT) is responsible for managing the Contingency Plan during each of the following four operational periods.

- **Readiness and preparedness** focuses on ensuring that the organization and contingency plans are as ready and prepared as possible to react to a disaster situation.
- **Activation and relocation** guides the initial response to a disruptive incident, with a focus on alert, notification and relocation.
- **Continuity operations** is the process of restoring essential functions by implementing orders of succession, delegations of authority or interim processes . The [ORGANIZATION] will identify and outline a plan to return to normal operations once the CPLT determines that resumption operations can begin.
- **Business Resumption** is the process by which the [ORGANIZATION] will restore all functions to at the original or replacement primary facility.

Readiness and Preparedness

Readiness and preparedness activities develop the response capabilities needed during an emergency. Planning, training and exercising are among the activities conducted under this phase. Mitigation is also an ongoing part of this phase. Mitigation activities eliminate or reduce the probability of an incident occurring. They also include actions that lessen the impact of unavoidable hazards. In support of the Business Continuity Plan, IT Security Contingency planning must prepare the detailed roles and responsibilities

Activation, Execution and Relocation

The IT Security components of the Continuity Plan support the overall business continuity objectives. As a result, the activation of any component of the Contingency Plan including Disaster Recovery and Emergency Operations is governed by the COO and the procedures documented for business continuity.

Ongoing mitigation measures include the following:

- Securing all important papers/documents at the end of the day
- Saving all electronic documents on a network drive—not on a computer's hard drive
- Maintaining accurate inventories of critical supplies
- Cross-training employees
- Ensuring Physical Security procedures are followed
- Testing system backups/restore processes
- Testing building alarm systems

Class/Level of Emergency

The Contingency Plan can be activated in part or in whole depending upon the disruption or threat. An event may force employees to evacuate a single facility for a day or two, which may require

executing only the communications component of the plan. A more serious event may include evacuation and pre-planned movement of key personnel to an alternate work location that can sustain essential functions for 30 days.

The Contingency Plan outlines a decision process for quickly and accurately assessing the situation and determining the best course of action for response and recovery. A decision matrix or flow chart has been developed that ties the organization's response to the class or level of emergency. The below classification system will be used for emergencies. However, it should be noted that essential functions with a time criticality of zero may have no acceptable disruption level.

Class/Level of Emergency	Category	Impact on <<Organization>>	Communications
I (Without relocation)	Alert	An actual or anticipated event may have an adverse impact for less than 12 hours with little effect on services or essential functions. No Contingency Plan activation required, depending on individual department requirements.	Appropriate personnel react to and remediate situation. CPLT are contacted and made aware of the situation
II (Without relocation)	Standby	An actual or anticipated event is estimated to have impact on operations for 12–72 hours, possibly requiring outside. CPLT determines if/when Contingency Plan activation is necessary, depending on individual area requirements.	Impacted area(s) alerts CPLT of situation and requests needed assistance. CPLT are placed on standby.
III (With relocation)	Limited Activation	An actual event minimally disrupts the operations of one or more essential functions or impacts critical systems for up to 7 days. Limited Contingency Plan activation. May require movement of some personnel to an alternate work location for less than a week.	Impacted area(s) notifies CPLT of situation, requests needed assistance and may send employees to alternate work location. CPLT determine extent of CP activation.
IV (With relocation)	Full Activation	An actual event significantly disrupts the operations of three or more essential functions or to the entire organization for more than a week, with the potential to last up to 30 days. Full Contingency Plan activation issued by the CPLT team.	Impacted area(s) notifies CPLT of situation, requests needed assistance and sends employees to alternate work location. Members of the CPLT activate the CP.

Alert and Notification/Relocation

IT services are often relied upon to provide notifications and alerts. Procedures must be planned and followed to notify personnel of continuity disruptions that occur with and without warning and during business and non-business hours.

- With Warning – A warning may occur at least a few hours before an event. This would allow for activation of the Contingency Plan, with complete and orderly notification and deployment of key personnel.
- Without Warning – Ability to contact personnel following an event that occurs with little or no warning will depend on the severity of the event, as well as the disruption to the organization's and surrounding community's communication infrastructure.
- Non-business Hours – If the primary facility is rendered inoperable or unsafe, key personnel will be notified and deployed to a designated alternate location. Non-essential personnel will be instructed to stay home and await further instructions.
- Business Hours – If the primary facility is rendered inoperable or unsafe during business hours, all personnel will be immediately evacuated from the building. Key personnel will be deployed to the designated alternate location. Non-essential personnel will be instructed to go home and await further instructions.

Responsibilities of the IT Team During Contingency Operations

- Identify functions that can be postponed or temporarily cancelled in the event that the Contingency Plan must be executed.
- Consult with and advise the CPLT during implementation of the Contingency Plan.
- Provide direction, guidance, and objectives during an emergency.
- Manage IT contingency efforts at all alternate locations.
- Participate in training and testing of the Contingency Plan.
- Initiate appropriate notifications during contingency implementation.
- Coordinate with leadership personnel for movement of key personnel to alternate locations when the Contingency Plan is activated.

Restoration of Service

The Disaster Recovery Plan must identify the planned steps involved in restoring interrupted infrastructure, platform, application, data and communications services. In all cases, an alternative to normal operations must be planned taking into account an acceptable level of risk.

Maintenance of Plan

Long-term plan maintenance will be undertaken carefully, planned for in advance and completed according to an established schedule. The Contingency Plan will be reviewed at least annually or whenever any major organization, infrastructure or systems change occurs. The review will include:

- Contingency plans, policies and procedures
- Testing, training and exercising of the Contingency Plan
- Response to real-world contingency events

Plan revisions due to changes in [ORGANIZATION] structure, essential functions or mission should be made promptly. The CPLT has the responsibility of ensuring that the Contingency Plan is updated regularly and identifying issues that affect the Contingency Plan:

- Policy or mission changes that significantly affect essential functions or their priorities
- Changes in critical resources (technology, communication, or office systems)

- Changes in organizational structure
- Changes to specific information such as contact lists, vendor lists or succession of leadership

Contingency Training Plan

Part of emergency readiness is training, including cross training, all staff to perform their emergency duties. This ensures that the organization is prepared to meet any unusual demands that may arise when essential functions are performed with a reduced staff.

Testing and Exercising Plan

Regularly scheduled exercises are critical to ensure that the Contingency Plan can be executed in times of an emergency. Exercising is one of the most effective ways to discover and document necessary modifications. The testing and exercise plan will be progressive, building from simple, individual tests to complex, functional exercises. The plan will include activities that build on training and improve capabilities through a series of tests and exercises.

Testing is required to demonstrate the correct operation of all equipment, procedures, processes and systems that support the organization's essential functions.

Test exercises are conducted to validate elements of the Contingency Plan, both individually and collectively. Exercises should be realistic simulations of an emergency, during which individuals and agencies perform the tasks that are expected of them in a real event. Exercises should promote preparedness; improve the response capability of individuals and participating agencies; validate plans, policies, procedures, and systems; and verify the effectiveness of command, control, and communication functions. Exercises may vary in size and complexity to achieve different objectives. The various types of exercises are described below:

- **Tabletop exercises** simulate an activation of the Contingency Plan in an informal, stress-free environment. They are designed to prompt constructive discussion as participants examine/resolve problems based on existing plans. There is no equipment use, resource deployment, or time pressures. The exercise's success depends on the group identifying problem areas and offering constructive resolution alternatives. This format exposes personnel to new or unfamiliar concepts, plans, policies and procedures.
- **Drills or system tests** are coordinated and supervised activities normally used to exercise a specific operation, function or system. They evaluate response time or performance against recovery time objectives, provide training with new equipment or procedures or enable practice using current skills.
- **Functional exercises** are interactive exercises performed in real time to test the capability of the organization to respond to a simulated emergency. Functional exercises test one or more functions and focus on procedures, roles, and responsibilities before, during and after an emergency event.

As discussed above, test exercises should be part of the overall review process and include a detailed analysis of successes and failures, efficiencies, costs and resources to inform the viability of the continuity procedures.

APPENDIX A

Business Impact Analysis

Use this template to perform business impact analyses. Formulate questions to elicit responses for insertion into specific categories. Organizing all columns into a spreadsheet simplifies the analysis process. This collection of data facilitates the process of identifying the most critical business functions, the financial and operational impact if they are disrupted, strategies to recover them and time frame targets to achieve recovery.

BU Name	Head Count	Process	Priority Ranking	RTO	RPO	Depends on	Required by

1. Business Unit Name – Self-explanatory
2. Head Count – Number of full-time staff in the business unit
3. Process – Brief description of the principal activities the unit performs, e.g., sales, contractor interface, or investor relationship management
4. Priority Ranking – Subjective ranking of process(es) according to criticality to the business unit
5. Recovery Time Objective – Time needed to recover the parent process to business almost as usual following a disruption
6. Recovery Point Objective – Point in time to which process work should be restored following a disruption
7. Process Depends On – Names of organizations and/or processes the process needs for normal operations
8. Process Required By – Names of organizations and/or processes that need the process for normal operations

Sub-Process	Priority Ranking	RTO	RPO	SP Depends on	SP Required by	Quantitative Impact

1. Sub-Process – Brief description of supporting activities the unit performs, e.g., sales analysis, financial analysis

2. Priority Ranking – Subjective ranking of sub-process(es) according to criticality to the business unit
3. Recovery Time Objective – Time needed to recover the sub-process to business almost as usual following a disruption
4. Recovery Point Objective – Point in time to which sub-process work should be restored following a disruption
5. Sub-Process Depends On – Names of organizations and/or processes the sub-process needs for normal operations
6. Sub-Process Required By – Names of organizations and/or processes that need the sub-process for normal operations
7. Quantitative Impact – Financial amount associated with the parent process, e.g., annual revenue generated by the process

	Time Needed to Recover Staff					
Qualitative Impact	**< 4 hrs**	**1 day**	**3 days**	**1 week**	**2 weeks**	**> 2 weeks**

1. Qualitative Impact – Non-financial impact to the company, e.g., loss of reputation, loss of customers
2. Time Needed to Recover Staff – Indicates how many staff can be recovered to "business almost as usual" within specific time frames

	Technology / Services Recovery Time						
Recovery Strategy	**< 4 hrs**	**1 day**	**3 days**	**1 week**	**2 weeks**	**> 2 weeks**	**Comments**

1. Recovery Strategy – Describes actions the business unit can take to recover to a "business almost as usual" state, e.g., work from home, relocate to an alternate area, recover to a hot site
2. Technology / Services Recovery Time – In each space list the critical systems, network services, etc. that must be recovered within the specific time frame
3. Comments – Self-explanatory

Critical Record	Location	BU	POC	Application	Backup/Archive

1. Critical Record - Name of the business critical record (e.g. tax files)
2. Location – Where the primary documents are located in Normal Operations
3. BU – Business Unit (e.g. Accounting, Scheduling, Clinical, etc)
4. POC – Point of Contact
5. Application – IT Application that is used to access or account for the records if electronic
6. Backup/Archive – The location of the backup records and archived records

APPENDIX B

Threats and Risks

Use the checklist below to reference the threats and likelihood described in the Business Continuity Plan:

Abridged Checklist of Threats to IT Services (supplement as needed)

1. Disruption to Building Access
2. Disruption to Room Access
3. Disruption to Communications
4. Server Failure
5. Other Infrastructure Failure
6. Loss of Staff
7. Loss of Management
8. Loss of Support Contractor
9. Loss of Business Documents
10. Loss of Patient Documents
11. Loss of Business Data Processing
12. Loss of Patient Data Processing
13. Privacy Breach
14. Loss of Data Integrity

(Copy table as needed)

Threat/Risk:	
Detailed Description of Example Scenario:	
Processes Impacted (with severity of impact):	
Mitigation Strategies Planned:	
Mitigation Strategies Implemented (with Date):	

APPENDIX C

IT Disaster Recovery Plan

Disaster Recovery is the process of ensuring that essential information technology functions can be maintained throughout a variety of incidents and emergencies. The Disaster Recovery Plan endeavors to ensure the continuous operation of information systems and the protection, confidentiality, integrity and availability of Protected Health Information (PHI). The purpose of [ORGANIZATION] Disaster Recovery Plan is to identify essential information technology systems, networks, applications and infrastructure and the plans to enable an effective recovery from an event that affects the normal operation. The Disaster Recovery Plan is designed to address:

- Closure of a facility (such as damage to a building from fire, flood, etc)
- Cyber attack
- Unexpected failure of major technology infrastructure (Network, Hardware, Application)

[ORGANIZATION] leadership has overall responsibility for disaster recovery planning, including overseeing the effort to develop, test and maintain the plan. The Disaster Recovery Coordinator (DRC) and/or Security Compliance Officer (SCO) have overall responsibility for developing and maintaining the plan. The Coordinator communicates with staff and trains them on the plan and their responsibilities.

Disaster Recovery Plan (DRP) provides guidance for [ORGANIZATION] in carrying out its responsibilities and ensuring that the technology resources supporting its mission essential functions can be recovered following a catastrophic event that severely disrupts or damages critical IT systems or supporting IT infrastructure (e.g. telecommunication closets, workstations, etc.). The disaster recovery plan supports and is a component of the business continuity plan.

The purpose of the Disaster Recovery Plan is to establish processes and procedures to be used by the DRC and SCO to guide the detection and escalation of disaster. These procedures are composed of:

- Disaster Declaration Process and Procedures
  - Incident Management and Escalation
  - Internal and Commercial Declaration Procedures
- Recovery Team Logistics and Dispatch Procedures
  - Recovery Team
  - Emergency Operations Center (EOC)
- Disaster Communications and Status Management Procedures
  - Employee Safety
  - Alert Communications
  - Recovery Management and Reporting

The DRP is activated by the DRC or SCO when a disruptive event will result in a long term disruption of or damage to critical IT systems or supporting IT infrastructure. The plan will be tested on a regular basis using mock situations to identify problems and areas for improvement. The plan will also be updated periodically to reflect changes in the organization and technology. Any regulatory requirements have been incorporated into the planning process.

Organization

The Disaster Recovery plan:

1. Identifies the information technology components essential to business operations
2. Determines how each situation, such as fire or flood, would affect these key information technology resources and which actions from the emergency mode operations plan (Appendix C) should be taken;
3. Sets goals for the return to normal operations
4. Identifies each required process and documents each step in the process and what needs to be done, along with the staff and other resources needed to complete the work
5. Implements a communications and education plan to keep employees informed of changes and remind them of their roles and responsibilities

The DRP covers the following technology areas:

- IT facility infrastructure
- Data communications
- Voice communications
- Network servers
- Application servers and systems
- Workstations

Core Disaster Recovery Team members are listed below. They will work closely with the DRO and SCO in the event of an emergency. They will also be responsible for assisting in ongoing readiness and training activities.

Name	Title	Phone	Email

<<organization>>

Name	Title	Phone	Email

In the event of an emergency, alternative office will be required. The below table identifies alternative management and work sites. The Disaster Management team is responsible for verifying the availability and suitability of alternative sites at the time of disaster.

Location Name	Address, Contact Numbers	Available Seats

Suitable emergency alternative locations should meet the following design criteria:

- Chairs and table space for at least 10 people
- 2 or more telephone lines
- An audio conferencing phone
- Wireless Laptop Access
- 2 or more LAN ports
- Access to a hub or switch
- 10 or more power outlets
- Television / cable connection (optional)
- Access to office supplies
- Access to printer / fax / scanner
- Internet access
- Whiteboard

Preparation

Preparation for recovery from a disaster includes the determination of business critical data and operations that rely on it. This will determine the data backup and recovery procedures including periodic testing of all procedures commensurate with the business impact and standards for return to service.

Activation

The DRP will be activated when conditions exist that have caused or threaten severe damage or disruption to critical IT systems or supporting IT infrastructure. An event may force systems to be unavailable for short periods of time requiring execution of only the communications component of

the DRP and will not require a full activation of this plan. In another situation, IT resources could be severely damaged requiring full execution of the DRP, including evacuation and pre-planned movement of key personnel and systems to an alternate work location that can sustain essential function operations for up to 30 days.

The DRC is responsible for initiating activation of this plan and associated recovery activities. Once the damage to the IT systems and infrastructure has been assessed and reported, the DRC and/or SCO will determine if activation of the DRP is required. The chart below will be used to assess the severity level of the emergency and determine what immediate actions required. Appendix A contains a DRP Activation and Recovery checklist to be used to coordinate DRP activation activities.

Crisis and Disaster Management

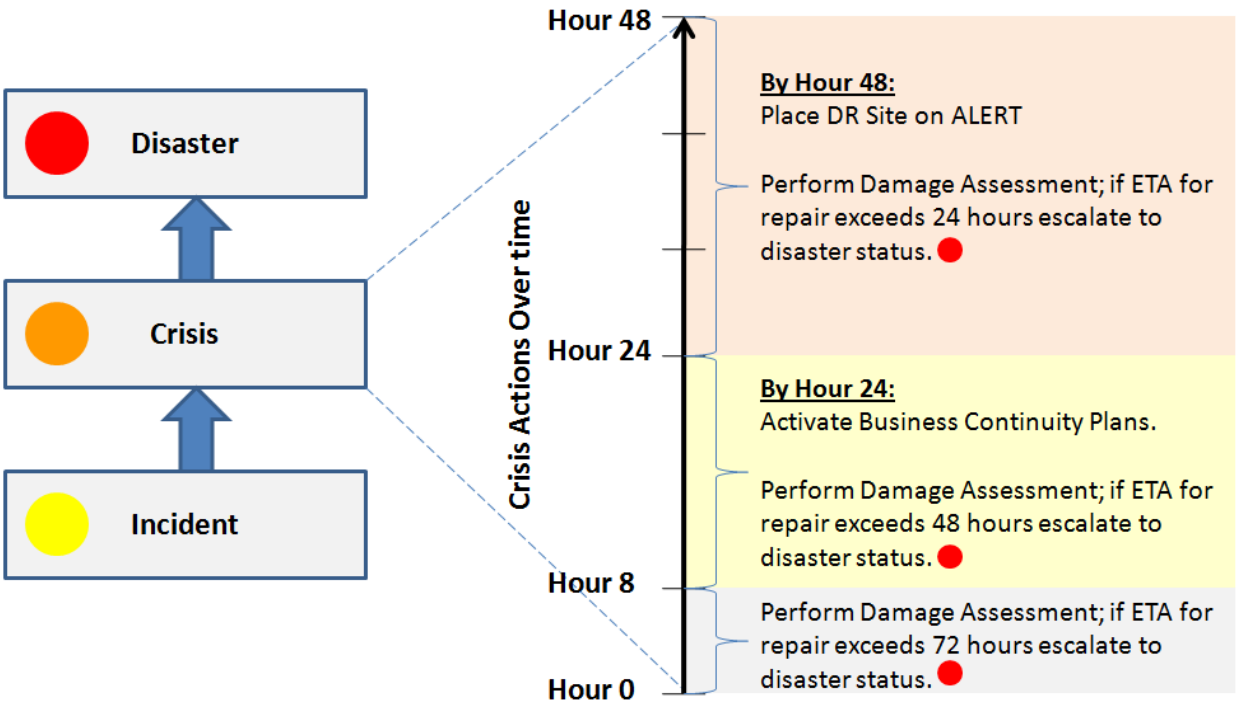
Severity Level	Criteria	Action to Be Taken
Disaster	Severe impact to several critical applications resulting in **the inability to provide critical functions**, processes or services. Outage expected to exceed (48 hrs) to resolve. *Examples*: • Complete datacenter/servers loss or significant physical damage due natural and man-made disaster. • Extended power loss to key location • Complete failure of entire network	• Immediately escalate and **Declare** (activate recovery). • **Mobilize recovery team** and begin recovery process. • **Activate business continuity plans**
Crisis	• Moderate to severe impact to one or more critical applications that has the potential to compromise the ability to provide critical functions, processes or services if not restored within 48 hours. • Outage may or may not exceed the RTO (48 hrs) to resolve. • Potential to replace damaged equipment or restore data locally within RTO (48 hrs). *Examples*: • Isolated physical damage at the datacenter/servers • Failure of applications due to data loss or an isolated availability incident	• **Assess damage** to determine the extent of the disruption • **Decide if business continuity plans should be activated** • If outage is expected to exceed RTO (48 hours) or if the impact expands to additional critical systems, **escalate to Disaster** otherwise address via incident management.

Incident Management

Severity Level	Criteria	Action to Be Taken

Critical	• An issue is considered 'Critical' when any key applications are impacted, regardless of the cause. *Example:* • Patient management interruption that is more than a delay or considered slow in processing	• Immediately email/call to communicate incident to IT Support • IT Support immediately communicates incident to users and other affected parties via email • Provide hourly status updates • If outage is expected to exceed target resolution time for critical incidents (1 business day), **escalate to Crisis** • **Consider activation of business continuity plans**
High	• While not as serious as a critical issue, high impact issues causing a major disruption in providing service to the business requiring immediate attention. *Example:* • Unable to login to applications due to application issues ; Phone lines down	• IT Support immediately communicates incident to users and other affected parties via email • Provide hourly status updates

Crisis Level Action 0-48 hrs



Communications

Following an event/disaster, communications will be coordinated to allow for both effective recovery operations and appropriate messaging throughout the recovery. Some of the internal and external communications required include:

- Employee and Contractor Awareness
- Patient and Supplier Closing Notices
- IT Vendors Emergency Assistance
- Disaster Recovery and Business Contingency Coordination
- Staff Safety Checks
- On-Going Status Updates

Disaster Recovery Process

Listed below are the plans for resumption of key technology components. It is critical that all IT application and infrastructure inventories are kept up to date to ensure smooth and successful resumption activities.

Facility Infrastructure Recovery

Without the ability to quickly provision and recover the IT infrastructure, the recovery of essential information technology systems to meet the business RTOs determined by the BIA are not achievable.

In order to manage the risk of a disaster that impacts [ORGANIZATION] IT infrastructure, the ability to quickly relocate IT infrastructure to an alternate site with similar capabilities is imperative. An alternative site to house and operate the organization's servers is a primary prerequisite for the recovery of critical IT services and applications. [ORGANIZATION] alternative operations site is located at XXXXXXX.

[ORGANIZATION] alternative technology operation site is a:

- Cold site – this is prearranged floor space that can be provisioned with power, environmental controls, rack space, network connectivity, etc. sufficient to host the IT facility that needs to be recovered. However, readying this cold site for IT equipment can take days to weeks to accomplish.
- Warm site – this is prearranged floor space that is already provisioned with power, environmental controls, network connectivity, etc. sufficient to host the IT facility that needs to be recovered. This type site is already ready to build out the computer racks and servers and can be occupied as soon as that type equipment is ready.
- Hot site – this type alternate computer space is already provisioned with the power, environmental controls, network connectivity and the like, as well as the computer racks and servers and can be occupied immediately.

The alternative site also has basic network capabilities in place to support network access and user authentication to help meet the RTOs for restoration of basic network services as well as Internet access.

Data Communications Recovery

[ORGANIZATION] is dependent on its data communications infrastructure as software application access is via this network along with transactions for claims processing, electronic prescriptions, laboratory results and data backup. The computing network infrastructure is comprised of equipment and software that provide the data communications functions and capacity. The loss of these data circuits will sever the network and disable the ability to communicate outside. The plan considers

- Loss of connectivity by the primary internet provider
- Loss of the primary site that houses the IT infrastructure and the corresponding data communications node

The ability of patients and employees to communicate with CPC following a disaster is a primary concern. In the event that voice communications are severed in an emergency, the ability to restore telephony communications will be a high priority.

[ORGANIZATION] primary data communications are provided by <<XXXX>>. In case of an emergency, alternative data communications will be provided by <<XXXX >>

Network Servers Recovery

The network servers are those systems that support network services, such as Domain and Print servers, and common system functions, such as Blackberry administration, Microsoft Exchange, CITRIX and other administrative tools. Network management servers will be imaged to create point-in-time backups that can be written to disk and backed up for storage offsite.

In the event [ORGANIZATION] network servers become unavailable for an extended period of time, XXXXXX (Vendor) will recover the network servers using the standard system image, the backed up data and new replacement servers.

Application Server and System Recovery

[ORGANIZATION] is critically dependent on several key application systems to be able to run its business processes:

- *(List key applications)*
-

Based on [ORGANIZATION] Business Impact Analysis, which prioritized the full recovery time objectives (RTOs) for their key business functions, the application systems would have to be restored in the following sequence:

1. *(List application recovery order)*
2.

All of these application recovery tasks can be accomplished within *XXX (eg. restoring data on the servers will take about 2 to 3 days, so currently it would probably take about a day to get the*

servers, a day to reload the servers and then 2 to 3 days to reload the application and data, which would say the minimum full recovery would be 4 to 6 days) days.

Workstation Recovery

[ORGANIZATION] employs a number of different types of IT workstations that need to be recovered in a disaster situation requiring an organization to operate in an alternate environment. For immediate workstation needs, <<Organization>> would obtain the required devices from the IT Vendor or if necessary, purchase the needed devices from a nearby retail store.

Standard workstation images with up to data system patches will be maintained that can be reloaded quickly on any new workstations.

APPENDIX D

Emergency Mode Operations Plan

Alternate Facilities

When normal operations can no longer be carried out at a facility of the organization, an alternative site must be selected, prepared and communicated to staff, patience and other entities. To prepare for this the EMOP must identify each business critical facility (room or building), select one or more alternate locations, identify how long and what resources are needed prior to occupancy and plan for communicating the location to all interested parties.

Bldg/Rm	Critical Use	Alt. Location	Resources needed	Time needed	POC	Comms. Plan

Alternate IT Processing

When a critical IT system identified in the Business Impact Assessment is not available and service recovery is not certain, an alternative to the infrastructure (e.g. Network), platform (e.g. Server) or even the application must be prepared to maintain continuity of operations. The EMOP must identify the alternate infrastructure for each critical application. There should be a migration plan in place for each that defines what the source of data will be (live data from the application if available or backups if the live data is not available). Note that backup and restore capabilities should be tested and provide a failsafe path to restoration of services.

Application	Critical Use	Alternate Infrastructure	Resources Needed	Time Needed	POC	Comms Plan

Alternate Communications Channels

When a contingency requires that a facility or a portion of one becomes inaccessible and alternative location may need to be designated. In order to continue business operations, all members of the management, staff, support personnel, patients, vendors and anyone else associated with the organization need to have ready access to a communication channel that reaches the new location. The new location must also have access to the systems and resources required to support business operations. To accommodate this alternative communication channels must be planned for Emergency Mode Operations. For each alternate facility or application, a communications alternative must be available and documented.

BU	Process	Facility/Application	Alternate	Network	Telephone	POC

			Location	Communications	Communications	

1. BU - Business Unit (see the BIA)
2. Process – Critical Process (See the BIA)
3. Facility/Application – Self Explanatory
4. Alternate Location – Where the work done in the facility or application will be done
5. Network Communications – What provision has been made to ensure the location has adequate network access to conduct the business process?
6. Telephone communications - What provision has been made to ensure the location has adequate telephone access to conduct the business process?
7. POC - The Point of Contact responsible for setting up the communications in the event of an emergency

Alternate IT Role leads

Emergency Mode Operations can result in a requirement to continue business operations with a reduced staff. Planning needs to be done to ensure that the key business process roles are filled and that the persons who must assume alternate duties have the necessary access to data and systems. To address this, the Emergency Mode Operations Plan should identify who are the appropriate replacement personnel for the key roles in the organization.

BU	Process	Key Role	Primary Personnel	Secondary Personnel