The Colorado Health Foundation™

Title: Disaster Recovery Plan

Author: Shasta Community Health Center

Context for Use: This example of a comprehensive community health center information systems disaster recovery plan shows how planning can help prepare for technology-related disasters and security incidents.

Document Owner: IT Services Manager	Original Creation Date: xxxx
Approver(s): Board Member)	Date Reviewed/Approved: xxx

Printed copies are for reference only. Please refer to the electronic copy for the latest version.

Policy:

This Information Systems Disaster Recovery Plan (DRP) has been developed by Shasta Community Health Center information systems (IS) leaders to provide guidance for responding to IS disasters and other security incidents. Disasters and security incidents may threaten the organization's ability to carry out its mission as well as other operational functions

Overview

This Information Systems Disaster Recovery Plan (DRP) has been developed by Shasta Community Health Center to provide guidance for responding to ITS disasters and other security incidents. Disasters and security incidents may threaten the organization's ability to carry out its mission as well as other operational functions.

Advance planning and preparation will allow the organization to:

- Continue serving its patients and community;
- Ensure the availability of patient protected health information as well as business information;
- Minimize loss and facilitate recovery of core information systems and other business assets;
- Preserve the organization's public image and reputation within the community;
- Prevent the disaster or incident from threatening the organization's long-term stability and viability;
- Heighten organizational awareness, allow for advance preparation, and workforce education and training; and

Comply with applicable state and federal regulations and accrediting agency standards. The DRP is a collection of references, guidelines, policies, procedures, forms, and suggestions designed for responding to security incidents and disasters.

Components of this plan include:

- Disaster Recovery and Restoration - See Data Recovery Plan and Development Check List.
- Emergency Mode Operation
- Applications and Criticality Analysis
- Data Back-Up (see also supporting ITS Policies and Procedures)
- Security Incident Response (see also supporting ITS Policies and Procedures)
- Testing and Revision

Additionally, there are several documents referred to and/or appended to this plan to provide additional guidance for the management of information security, disasters and other security incidents.

Key supporting ITS policies include:

- Security Incident Response/Reporting
- Data Backup for Information Systems

Objectives of the Disaster Recovery Plan

1. To provide SCHC as an organization with a viable and maintained ITS Disaster Recovery Plan (DRP) which, when executed, will support a timely and effective resumption and recovery of all interrupted clinical and business operations.
2. To minimize possible adverse clinical outcomes, as well as financial and business impacts, to SCHC organizations as a result of an interruption of normal business operations.
3. To reduce operational effects of an information systems disaster on SCHC organization's time-sensitive business operations and functions by providing a set of pre-defined and flexible guidelines and procedures to be used in directing resumption and recovery processes.
4. To meet the needs of SCHC patients, workforce members, and other stakeholders and communities reliant on the organization's ability to provide services during and following a disaster situation.
5. To protect the public image and credibility of Shasta Community Health Center.

Applicability

The DRP has been developed to support the organization's Emergency Preparedness/Disaster Plan, providing further specificity to address ITS needs. The DRP applies to all hardware, software, workstations, applications, systems and networks (LAN, WAN, Internet, Intranet), and other components of the organization's information systems. The DRP is limited to the recovery of IT services only. The DRP does not address disaster prevention or long-term restoration of information systems. The DRP does not address the recovery of business processes that may be lost in the various departmental or business unit operations. Downtime/recovery processes are the responsibility of each department unless specifically covered in the DRP. Refer to department plans for appropriate downtime/recovery procedures (See SCHC Downtime Plan).

Key Definitions

SCHC Continuity Planning: The process that facilitates arrangements and procedures that enable SCHC to respond to an event in such a manner that critical SCHC functions continue with planned levels of interruption or essential change can be found in the Security Compliance Plan: Contingency Plan. [Found on shared: ITS/Contingency Plan.]

Disaster (Information System): An event that significantly renders the continuation of normal information system functions impossible; an event which would render the information system unusable or inaccessible for a prolonged period of time (may be departmental or organization-wide).

Disaster Recovery Coordinator (DRC): Individual assigned the authority and responsibility for the implementation and coordination of the IT disaster recovery operations.

Disaster Recovery Plan (DRP): The document that defines the resources, actions, tasks, and data required to manage the business recovery process in the event of a business interruption. The plan is designed to assist in restoring the business process within the stated disaster

recovery goals.

Recovery Time Objective (RTO): Amount of down time before outage threatens survival of the organization/mission critical processes.

Security Incident: A violation or imminent threat of violation of information security policies, acceptable use policies, or standard security practices, or an adverse event whereby some aspect of computer security could be threatened. An ITS Disaster would be considered a security incident.

Information Systems Disaster and Security Incident Response

Shasta Community Health Center recognizes an information systems disaster as a security incident and shall utilize established security incident response processes in addressing disaster response and recovery. The organization's Security Incident Response/Reporting (Reference Security Incident Response/Reporting: Security Compliance Plan) and Data Backup (Reference Information Technology Policies and Procedures for Backup of Data) policies provide a framework for this IT Disaster Recovery Plan. Additionally, other organizational information security policies and procedures support IT disaster recovery processes and may be utilized in conjunction with this plan.

A key security incident resource currently being used by SCHC is developing consistency with the *National Institute of Standards and Technology (NIST) Special Publication 800-61, Computer Security Incident Handling Guide.* This document provides guidance that SCHC can benefit from to mitigate loss and aid the organization in appropriate response to information security incidents and reflects best practices in information security.

The document is available at the following link and may be considered as supporting documentation to this plan:
http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf

Another useful NIST document is *Special Publication 800-34, Contingency Planning for Information Technology Systems* available at the following link:
http://www.csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf

Authority

The Disaster Recovery Coordinator (DRC), in conjunction with the SCHC's administrative leadership, shall have the responsibility and authority to take whatever steps necessary to identify, respond, contain, and eradicate the impact of an ITS disaster.

Administrative Oversight

The organization's senior administrative leadership will provide oversight in the development and management of the ITS Disaster Recovery Plan. A senior administrative leader shall also be assigned to provide support and assistance during IS disaster recovery processes. This individual shall also research the organization's disaster insurance coverage and determine available financial resources.

Organization & Notification

Activation and Administration of the Disaster Recovery Plan

Upon notification of a suspected or confirmed information security incident/disaster, the ITS leadership (e.g., management/technical analyst) shall verify, assess, and record the scope of the incident/disaster and determine the appropriate response:

- Application, system, and/or network out of operation.
- Impact localized, departmental, organizational, and/or enterprise-wide.
- Impact on mission critical operations and services.

If the ITS leadership feels that the incident meets the criteria of a "disaster," the ITS leader shall:

1. Activate of the Disaster Recovery Team (Security Incident Response Team-SIRT): xxxx
2. Identify an Individual to Act as the DRC (ITS leader/technical analyst preferred). In the absence of an ITS leader, the organization's administrative leadership shall act as the DRC and facilitate the implementation of this plan and assign the tasks involved in IS disaster plan recovery. Once an ITS Disaster has been declared and the ITS Disaster Plan activated, the DRC shall communicate such to senior administrative leaders and implement the ITS recovery steps outlined in this plan. The DRC shall determine the need to notify external resources (See Communication & Organization) including business partners and vendors to assist with ITS disaster recovery activities. These protocols are outlined in this Plan.

Disaster Recovery Coordinator (DRC)

Disaster Recovery Coordinator (DRC) **Position Description/Job Action Sheet**	
Position Assigned To:	ITS Leader or Designee
Position Reports To:	CEO or Designee
Authority Level:	Highest
Mission/Responsibility:	To implement, organize and direct information systems disaster recovery operations.

Disaster Recovery Coordinator (DRC) **Position Description/Job Action Sheet**	
Criticality Level	**Job Actions**
Immediate **(0-6 Hours)**	• Review DRC Job Action Sheet and IS Disaster Recovery Plan • Identify Disaster Recovery Command Center/Assembly Site • Notify Disaster Recovery Team Members • Assemble Team at Command Center • Assemble Resources (See Checklist) • Provide Team Briefing/Document Information Provided at • Briefing • Review Tasks to Be Performed and Assign Personnel • Notify Other Key Leaders/Workforce Members as Necessary • Notify Vendors/Stakeholders/Law Enforcement Agencies or other Emergency Government Agencies as Necessary • Determine Need for Additional Support Teams and Assign Team Leader/Members • Provide Teams with Status Report Forms • Request Team Facilitators to Track Resource Utilization on Status Report Form • Communicate Key ITS Disaster Recovery • Information/Contacts/Locations Internally • Contact External Vendors and Other Business Stakeholders • Determine Need for Media Communication • Designate Media Contact; Instruct All Others Not to Make Statements to Media • Prepare Media Statement proactively if felt necessary
Intermediate **(6-12 Hours)**	• Assess continued staffing needs/staff relief
Ongoing	• Damage assessment • Assess recovery priorities • Communicate ITS Disaster Recovery Status with Administration

	• Assess resource needs for Chief Operations Officer • Approve expenses related to recovery processes
Extended (>12 Hours)	• Assess continued staffing needs/staff relief
Follow-Up (Following Disaster)	• Facilitate "post mortem" evaluation of IS disaster and recovery processes • Revise IS Disaster Recovery Plan and Processes as Necessary • Train and educate staff on ITS DRP revisions

-

ITS Disaster Recovery Team Emergency Contact Information

Members of the ITS Disaster Recovery Team shall be contacted immediately once the ITS DRP has been activated. The following information should be provided at the time of contact:

- A brief description of the problem
- Location of the ITS Disaster Recovery Command Center
- Phone number of the ITS Disaster Recovery Command Center **xxx**
- Identification of immediate support required (Services, Equipment, Etc.)
- Information Regarding How the Facility Can be Entered (Need for Badge/Identification)
- Contact information is available as noted below.

Name of Individual	Contact information (phone number or pager number)
xxxx	**xxx**

Damage Assessment

Damage assessment shall be carried out to determine disaster recovery requirements. A preliminary damage assessment shall address:

- Cause of the emergency or disruption.
- Potential for additional disruptions or damage.
- Areas affected by the disruption.
- Status of physical infrastructure (where computer equipment is located).
- Inventory and functional status of computer equipment.
- Type of damage (e.g., water, fire, electrical surge, etc.).
- Items to be replaced (e.g., hardware, software, other).
- Estimated time to restore to normal operations.

Assessing Resource Needs for Critical Disaster Recovery Operations

Once the DRP is activated, the DRC will determine what resources are required to support critical functions. This analysis should take into consideration the following resources and potential questions:

Human Resources: Are the critical skills and knowledge possessed by the appropriate people

listed on the call roster? Can Recovery Operations staff be deployed easily get to an alternative site?

Processing Capability: Are the servers, workstations, or other hardware harmed? What happens if some of the equipment is inoperable, but not all?

Automated Applications and Data: Has data integrity been affected? To what extent? Has an application been sabotaged? Can an application run on a different processing platform?

Computer-Based Services: Can the computers communicate? To where? Can people communicate? Are information services down? Find out as soon as possible how long services will be down.

Infrastructure: Do people have a place to work? Do they have the equipment to do their jobs? Can they occupy the department/building? Documents/Paper: Can the needed records be found via another method? (See Downtime Plan re: Master Patient Index log with appointment and patient information.)

ITS Disaster Recovery Command Center

The Commend Center will function as the centralized location for ITS disaster recovery processes. The DRC will make the determination as to the location of the Command Center. The location will be determined by the disaster type and available resources. The Command Center location must be able to accommodate the necessary critical resources and equipment required for disaster recovery (see Recovery Resources Supply Checklist):

- Hardware, Software, Other Equipment
- Electrical Support
- Telecommunications Support
- Desks, Chairs, Tables, Lights

Primary Location			
Primary Location	Main Site, Redding	**Meeting Site:**	IT Department
Address:	xxx	**Fax Number:**	xx
Phone Number:	xxxx	**Phone Number:**	xx
Contact Person:	xx	**Phone Number:**	xx
Alternate Contact:	xx	**Phone Number:**	xx
Security Considerations:			

Recovery Resources Supply Checklist

<table>
<tr><th colspan="2">Recovery Resources Supply Checklist</th></tr>
<tr><td>Workspace
Desk, Chairs, Tables, Lights
Electrical Support
Telecommunications Support</td><td>Documentation
Hardware Inventory Lists and Serial Numbers
Software Inventory Lists and License Numbers
Network Schematic Diagrams
Equipment Room Floor Grid Diagrams
Contract and Maintenance Agreements</td></tr>
<tr><td>Hardware
PC’s/Laptops
Printers
Scanners</td><td>Forms
Maintenance Forms
Message Pads</td></tr>
<tr><td>Software
Back-Up Copies of Data Files</td><td rowspan="2">Other Supplies
Office Supplies (pens, paper, folders, paper clips, scissors, staplers, tape, etc.)
Office Equipment (shredder, copiers, etc.)
Camera/Video Recorder
Film/Blank Recording Media
Duct Tape
Backup Media
Flashlights and Spare Batteries
Telephone Log
Area Maps</td></tr>
<tr><td>Communications
Telephones
Cellular Phones With Chargers
Fax and Backup Fax
Dedicated Telephone Line(s)
Radios (Walkie-Talkie) As Required
Organizational Contact
Information/Directories
Telephone Directories
Telephone Log</td></tr>
<tr><td colspan="2">Other</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td colspan="2"></td></tr>
<tr><td colspan="2"></td></tr>
<tr><td colspan="2"></td></tr>
<tr><td colspan="2"></td></tr>
</table>

Recovery Team – Roles & Responsibilities

Title	Position	Responsibilities
Disaster Recovery Coordinator	Director of ITS • ITS Leader • Security Officer • CIO	See Disaster Recovery Coordinator Position Description/Job Action Sheet
Operations Recovery Coordinator	• ITS Leader or Technical Support Person	Implement ITS disaster recovery processes; facilitate recovery of ITS operations as directed by DRC.
Network Recovery Coordinator	• Local or Enterprise Network Administrator	Implement ITS disaster recovery processes; facilitate recovery of organization/enterprise network as directed by DRC.
Clinical Applications Coordinator	• ITS Clinical Applications Coordinator • Nursing Leader	Implement ITS disaster recovery processes as necessary in the absence of ITS applications and systems. See Downtime Plan.
Business Applications Coordinator	• Database Administrator • Business Leader	Implement ITS disaster recovery processes as necessary in the absence of ITS applications and systems.
Communications Coordinator	• CEO • CIO • As designated • COO	Support DRC/activities. Investigate insurance coverage and resources. Facilitate securing critical resources. Investigate legal issues.
Administrative Assistant		Provide necessary administrative and clerical support to DRC and support teams.

Communication Strategies

ITS Disaster Recovery Team Status Report

The DRC will determine the need to complete status reports. The Disaster Recovery Team and all other disaster recovery support team leaders will be responsible for completing the "ITS Disaster Recovery Status Report Form" when requested by the Coordinator. The Coordinator will compile information from the status report(s) to use in communicating to senior administrative leadership, corporate resources, and other external contacts and stakeholders (a blank template of this form is available as an attachment to this plan).

Administration
The administrative leader assigned to the disaster recovery process shall act as a liaison between the DRC/Team and administration. The leader will be responsible for communicating disaster recovery activities on an as needed basis.

Organizational/System Level
The DRC will determine the need for notification of SCHC leadership and/or Information Systems staff members. The CIO shall be notified of any disaster/security incident that:

A. Results in adverse patient care outcomes or significantly impacts operational functions;
B. Requires additional ITS resources and support beyond the scope of SCHC ITS staff;
C. Impacts more than one SCHC organization or satellites;
D. Requires involvement with local, state or federal law enforcement agencies; and
E. Results in adverse publicity and require media relations skills. The DRC may also request assistance from other SCHC partner organizations for ITS support.
F. The Coordinator may contact the organizations directly or request assistance from SCHC business partner ITS Departments in coordinating supporting services and resources from the other organizations.

Recovery Priorities

Criticality levels are assigned to applications systems based upon the relative importance of the applications and systems to the organization's mission and operations. During the disaster recovery process, resources will be allocated based on established criticality levels, unless otherwise determined by the DRC and/or administrative leadership. The organization must in advance review all applications, systems, networks, and critical interfaces and assign them to one of the following priority levels:

Critical/Priority 1

Applications and systems designated "Critical" are mission-critical, impact patient care or other key operations, and require immediate data recovery resources to ensure prompt restoration, recovery, and operability. Failure of these applications and systems to function for even a short period of time could have a severe impact on the organization's ability to carry out its mission and operations.

Recovery Time Objective (RTO): 0-8 Hours.

Essential/Priority 2

Applications and systems designated as "Essential" and may impact patient care, information services, finance, labor and attendance, and physical security. Failure of these applications and systems is allowable for a short period of time. RTO: 9-24 Hours.

Necessary/Priority 3

Applications and systems designated "Necessary" and may tolerate a short period of loss of availability. RTO: 25-72 Hours.

Desirable/Priority 4 (Low)

Applications and systems designated "Desirable" are a lower priority and may tolerate a significant loss of availability. Recovery will be initiated when normal IS operations are reestablished.
RTO: > 72 Hours. Pending resolution of higher priorities; allocation of resources may be questioned.

INFORMATION SYSTEM CRITICALITY ASSESSMENT

Local Applications/ System/Network Interface	Critical Priority 1 RTO: 0-8 Hours	Essential Priority 2 RTO: 9-24 Hours	Necessary Priority 3 RTO: 25-72 Hours
External		E-Mail	
Communications - Internal	Telecom IP Phone		
Decision Support/ Reporting Systems		Reporting System	
Financial	Accounting System		
Health Information	EHR		
Human Resources		EZ Labor	Halogen
Patient Care	Order Entry Transcription/Dictation EHR/portal		
Revenue	Accounting System		

Enterprise Application Systems	Critical Priority 1 RTO: 0-8 Hours	Essential Priority 2 RTO: 9-24 Hours	Necessary Priority 3 RTO: 25-72 Hours
Payroll Processor	Payroll		
Doc Editor			Editor
Photo Editor			Editor
Patient Ed		Patient Education	
Report Module	Reporting		
Remote Access	Gives Access to Computers for ITS		
Inventory Management	PO Generator for Ordering		
VPN	Transcription transfer		
Drug Lookup System	Drug lookup		
Payroll Processor	Payroll		
Finance System	Finance		
Integrisign	Signature Pads		
KPACS	XRays		
MIP	Finance		
Cisco Phone System	Telephone System		
NextGen 5.8.0.106 EPM, EHR, ICS	Electronic Health Record		
NextGen Communications Services5.8.0.106– ERX and RXHUB	Electronic Prescribing and Patient Portal Traffic		
NextGen Faxing Integrations Services (Fax Man)	Fax Prescriptions		
Security Cameras	Facility Security		
Office Suite 2007		Office Operations	
Drupal		Website Creation	
Policy Tech	Need for Policies		
Radiology DB	XRays		
Red Gate SQL Prompting			Scripting Support
Rosetta 5.6.5121639 – Labs Quest	Lab Request		
EHR Connect	Lab Interface		
Rosetta 5.6.5121639 – Imaging MDI	Image Ordering		
Mirth IF	Lab Interface		

Rosetta 5.6.5121639 – PSMG (Cortex)	Women's Health Pap Ordering		
Rosetta 5.6.5121639 – Dental	CPS Operation		
RW Care Ware		EIS Population Management	
SQL Server 2008 R2	DataBase		
Track-IT!		ITS for Tracking	
Up to Date Search	Clinical Reference		
Lync	Employee Commuication		
Symantec Antivirus	Equipment Antivirus		
Schedule Anywhere	Clinic Scheduling		
Windows 7	Operating Systems		

Recovery Processes and Procedures

1. Upon assessment of damage and activation of disaster recovery processes, the ITS leadership/SIRT will determine the appropriate data recovery strategy.

2. The data recovery processes shall reflect the organization's information system priorities. Data recovery activities shall take place in a pre-planned sequential fashion so that system components can be restored in a logical manner and should take into consideration:

   A. Personnel: The ITS leadership and workforce members, as well as the SIRT members, involved in data recovery processes will be the most valuable resource. These individuals may be asked to work at great personal sacrifice and resources shall be provided to meet their personal and professional needs.
   B. Communication: Notification of internal and external business partners associated with the organization's information systems.
   C. Salvage of Existing ITS Equipment and Systems: Initial data recovery efforts shall be targeted at protecting and preserving the current media, equipment, applications and systems. A priority shall be to identify and obtain storage media. The IS equipment shall be further protected from the elements or removed to a safe location, away from the disaster site if necessary.
   D. Designate Recovery Site: It will be necessary to determine if the data recovery efforts can be carried out at the original primary site or moved to another location (see Command Recovery Center Alternative Site section). The choice of using an internal or a remote site will be dependent on the damage and estimated recovery of the computing and networking capabilities.
   E. Backup/New Equipment: The recovery process will rely heavily on the ability of the organization's vendors to quickly provide replacements for the resources which cannot be salvaged. Emergency procurement processes will be implemented to allow the ITS leadership to quickly replace equipment, supplies, software and any others items required for data recovery.

F. Reassembly Process: Salvaged and new data recovery equipment and components shall be reassembled at the recovery site to begin data recovery processes.
G. Restoration of Data from Backups: Data recovery will rely on the availability of the backup data from the storage site. Initial data recovery efforts will focus on restoring the operating systems by pre-determined priority (See Amendment A).
H. Restoration of Applications Data: ITS leadership will work with the individual departments/application owners to restore each running application. As a period of time may have elapsed between the time that the backups were made and the time of the disaster requiring data recovery, the application owners must address mechanisms to capture and restore the lost interim data.
I. Move Back to Restored Permanent/Primary Site: If the data recovery process has taken place at an alternative site, the equipment and systems that have been assembled at the alternative site will need to be returned to the original site when available.

2. Upon termination of recovery activities and once normal ITS operations are back in place, than reconstitution efforts should begin. If the original site is unrecoverable (e.g., burned in fire), then the reconstitution activities may be applied to preparing a new site to support information system requirements. Reconstitution activities should address:

A. Ensuring adequate infrastructure support, such as electric power, water, telecommunications, security, environmental control, office equipment, and supplies.
B. Installing system hardware and software.
C. Establishing connectivity and interfaces with network components and external systems.
D. Testing system operations to ensure full functionality.
E. Backing up operational data on the contingency system and uploading to restored system.
F. Shutting down the contingency system.
G. Terminating contingency operations.
H. Removing and/or locating all sensitive materials at the contingency site.
I. Arranging for recovery staff to return to the original/new facility.

Data Backup Procedures

Data backup processes shall be established through existing policy and procedures. The ITS Department is responsible for overseeing organizational data backup and recovery processes for those applications, systems, and networks under its control. Users of unique departmental and/or individual applications, systems, and networks will be responsible for data backup and recovery unless arrangements have been made in advance with the ITS Department (See Data Backup for Information Technology Systems Policy).

Electronic Health Record (EHR)

The availability of patient electronic health records (EHR) is mission critical to ensure for safe and effective communication of patient information between healthcare providers. Established

procedures shall ensure that EHR is routinely backed up and the information recoverable. In the event of downtime disruption and inability to access the EHR, the organization shall:

Communications:

1. Identify operations or services that will be impacted and make necessary notification of the unavailability of the EHR.

Access to Historical Patient Health Information:

2. Implement existing backup systems to access historical patient health information (e.g., flash drives available with a full listing of MPI directory, which includes Patient name, demographics, medication list, chronic problem list, last date seen, primary care provider, (please contact ITS for complete list of fields).
3. Identify and make available resources for retrieval, delivery, return, etc. (See SCHC Downtime Plan: Shared drive: Downtime Plan.)

Creation of New Patient Health Information:

4. Make available to healthcare providers temporary paper documentation tools including, but not limited to:

    A. MPI thumb drive (if able to access by laptop).
    B. Key patient care documentation forms:
        a. See Downtime Plan for procedure and patient care forms. (Shared drive: Downtime Plan.)

Workforce Member Education and Training

Members of the organization's workforce shall be provided periodic education and training in emergency preparedness and disaster recovery upon hire and as needed to reflect any significant changes to the organization's emergency preparedness/disaster recovery practices, including information system disaster events and security incidents. Workforce members with specific responsibilities for ITS disaster recovery shall receive the necessary education and training required to ensure that they can carry out their assigned duties in the event of an ITS disaster event.

Review and Testing of Disaster Recovery Plan

The DRP should be reviewed on an annual basis or as often as necessary to ensure that the information contained in the plan is up-to-date and reflects current workforce information (titles, names, and contact information), applications/systems, vendors, and other external contacts

information. Additionally, after each disaster incident, whether a planned drill or actual disaster, the plan should be reviewed and revised to address practical application issues.

Resources Used to Develop the IS Disaster Recovery Plan Template

"Creating an Actionable Disaster Recovery Plan," *Stone Bridge Group, HIMSS*, April 2003
"Electronic Restoration: Critical Considerations," Retrieved from: Disaster-Resource.com
"An Introduction to Computer Security: *The NIST Handbook*, Special Publication 800-12
"Disaster Recovery Plan," St. Joseph's Hospital, 1991
"Business Resumption Plan," *Disaster Recovery Journal* Website
"Disaster Recovery White Paper," *WEDI*, April 2005
"CMS Information Systems Security/Risk Assessment" Documents, 2004
"Contingency Planning Guide for Information Technology Systems," *NIST, 800-34*, June 2002

Applicable Standards/Regulations:

45 CFR §164.308(a)(7) – HIPAA Security Rule Contingency Plan

(A) Data Recovery Plan Template and Development Checklist

Use this template as a guide when performing a data disaster recovery plan assessment.

	Assessment Item	Recommended Action
	Existing data center disaster recovery plans	
☐	Review plans if available	
☐	Analyze against standards, e.g., NIST SP 800-34, BS 25777, ISO 24762	
☐	Validate based on results of assessment	
	Review previous incidents	
☐	What occurred?	
☐	What was the impact to the organization?	
☐	How did the organization respond?	
☐	What were the results of the response?	
	Threats	
	Building construction	
☐	Type of construction	
☐	Date of construction	
☐	Structural integrity	
☐	Floor loading per square foot	

	Assessment Item	Recommended Action
	Building location	
☐	Proximity to major highways, streets	
☐	Proximity to rail lines	
☐	Proximity to aircraft flight paths	
☐	Location with regard to bodies of water, e.g., rivers, lakes, oceans	
☐	Traffic control devices	
☐	Proximity to other buildings	
☐	Proximity to earthquake zone	
☐	Weather patterns	
☐	CCTV cameras around the site	
	Parking facilities	
☐	Parking layout	
☐	Number of entrances	
☐	Security available to inspect vehicles	
☐	CCTV cameras in place at entrances, exits and on each floor	
☐	Number of exits	
☐	Sufficient capacity for vehicles	
☐	Construction of ramps, parking space	
	Building access	
☐	Number of building entrances	
☐	Security provisions at entrances	
☐	Access methods, e.g., cards, guards	
☐	Shatterproof glass on street-level windows	
☐	Bollards in street to prevent vehicles from crashing into building	
☐	CCTV cameras	
☐	Monitoring of exterior cameras	
☐	Length of video recording for CCTVs	
	Building exits	
☐	Number and location	
☐	Method of leaving building	
☐	Access to exists from stairwells	
☐	CCTV cameras at exits	

	Assessment Item	Recommended Action
☐	Exits clearly marked and exit routes identified on each floor and hallway	
	Stairways	
☐	Number and location of stairways	
☐	Method of entry into stairwells	
☐	Method of re-entry into floors	
☐	CCTV cameras in stairwells	
☐	Emergency lighting in stairwells	
☐	Signage in stairwells	
☐	PA speakers in stairwells	
☐	Fire protection equipment	
	HVAC facilities	
☐	Location of HVAC equipment	
☐	Power supplies for HVAC	
☐	Backup HVAC systems	
☐	Monitoring of HVAC systems	
☐	Monitoring of air quality	
☐	Environmental controls on floors	
☐	Fire protection equipment	
	Utilities disruptions	
☐	Access into building for utilities: How many, where located	
☐	Secure room for utilities entry into building	
☐	Fire protection equipment	
☐	Shut-off switches	
☐	Signage at appropriate locations	
	Electric utilities	
☐	Location of entry facilities	
☐	Location of breakers	
☐	Cable routing and protection	
☐	Power distribution to floors	
☐	Firestop material at floor/wall/ceiling penetrations	
☐	Lightning protection	
☐	Grounding and bonding	
☐	Fire protection equipment	

	Assessment Item	Recommended Action
	Water and sewer	
☐	Entry points into building	
☐	Location of mains	
☐	Placement of water towers	
☐	Routing of water lines, sewer lines	
☐	Leakage notification	
☐	Fire protection equipment	
	Gas	
☐	Entry points into building	
☐	Location of mains	
☐	Routing of gas lines	
☐	Gas leak notification	
☐	Fire protection equipment	
	Telecommunications	
☐	Entry points into building	
☐	Location of mains	
☐	Routing of fiber, copper cables	
☐	Grounding and bonding	
☐	Fire protection equipment	
	Windows	
☐	Windows fixed or can be opened	
☐	Glazing to minimize ultraviolet radiation	
☐	Special covering to minimize wind or blast damage	
	Doors	
☐	Exterior doors solid and locked	
☐	Glass doors with shatterproof glass	
☐	Interior doors fire-rated	
	Interior walls	
☐	Floor-to-ceiling walls fire-rated	
☐	Movable partitions fire-rated	
☐	Dropped ceilings use fire-rated tiles	
	Fire	

	Assessment Item	Recommended Action
☐	Notification of fires to fire department or central reporting station	
☐	Building-wide fire detection system	
☐	Floor-by-floor monitors	
☐	Smoke detection equipment	
☐	Ionization detection equipment	
☐	Fire extinguishment system, e.g., dry pipe or water sprinklers	
☐	Placement of fire extinguishers	
☐	Signage indicating fire extinguishers	
☐	Regular fire drills	
☐	Building evacuation signage on each floor and in offices	
☐	Fire safety plan	
☐	Evacuation plan	
	Loss of power	
☐	Emergency power generator(s)	
☐	Emergency power outlets identified	
☐	Secure location for emergency generator	
☐	Protected fuel tank with gauge	
☐	Primary and alternate fuel suppliers	
☐	Monthly power system tests	
☐	Quarterly full-load system tests	
	Loss of lighting	
☐	Emergency lighting in all floors	
☐	Emergency lighting in stairwells	
☐	Emergency lighting by exits	
☐	Regular tests of emergency lighting	
	Loss of elevators	
☐	Elevator safety inspections	
☐	Power supply to elevators	
☐	Emergency access to elevators	
☐	All elevators return to ground floor in an emergency	
☐	Emergency egress from elevators if stuck between floors	
☐	Emergency phone in all elevators; test regularly to ensure it works	

	Assessment Item	Recommended Action

Use this checklist as a guide when structuring data center disaster plans:

	Plan Element	Recommended Action
	Table of Contents	
	Emergency response procedures	
☐	Event occurs	
☐	Initial report of event	
☐	Contact first response staff	
☐	Initial assessment	
☐	Damage assessment	
☐	Contact and assemble disaster teams	
☐	Launch call trees and/or other notification procedures	
☐	Activate emergency phone number(s)	
	Launch emergency procedures	
☐	Data protection	
☐	Data quality assurance	
☐	Data security	
☐	Data backup	
☐	Power management	
☐	HVAC management	
☐	Utility management	
☐	Initiate application-level backup procedures	
☐	Initiate hardware-level backup procedures	
☐	Initiate network backup procedures	
☐	Initiate security procedures	
☐	Initiate other backup procedures	
☐	Contact third-party organizations	
	Decision to declare disaster	
☐	Can situation be handled without staff leaving building?	
☐	If situation is deemed serious, issue evacuation orders immediately	

	Plan Element	Recommended Action
☐	Emergency teams assess situation, make recommendation to senior management	
☐	Staff arrives at designated emergency assembly areas	
☐	Disaster declared	
	Backup and recovery procedures	
☐	Continue application-level backup procedures; launch recovery procedures as needed	
☐	Continue hardware-level backup procedures; launch recovery procedures as needed	
☐	Continue network backup procedures; launch recovery procedures as needed	
☐	Continue security procedures; launch recovery procedures as needed	
☐	Continue other backup procedures; launch recovery procedures as needed	
	Alternate site recovery procedures	
☐	Initial teams arrive at alternate data center or contracted facility	
☐	Launch application-level recovery procedures	
☐	Launch hardware-level recovery procedures	
☐	Launch network recovery procedures	
☐	Launch security recovery procedures	
☐	Launch other recovery procedures as needed	
☐	Assigned recovery staff arrive at alternate site to expand recovery	
	Primary site situation addressed	
☐	Site repaired and ready to accept data center operations	
☐	Launch application-level recovery procedures upon return	
☐	Launch hardware-level recovery procedures upon return	
☐	Launch network recovery procedures upon return	

	Plan Element	Recommended Action
☐	Launch security recovery procedures upon return	
☐	Launch other recovery procedures as needed upon return	
☐	Data center staff return to site to complete recovery and resume normal operations	
	Post-recovery activities	
☐	Validate all systems are functioning normally	
☐	Validate all network assets are functioning normally	
☐	Validate all data center infrastructure assets are functioning normally	
☐	Validate all utilities are providing normal service	
☐	Conduct review of event, how the organization responded, identify lessons learned, and summarize in report to management	

Telecommunications

General Recovery Pre-Planning

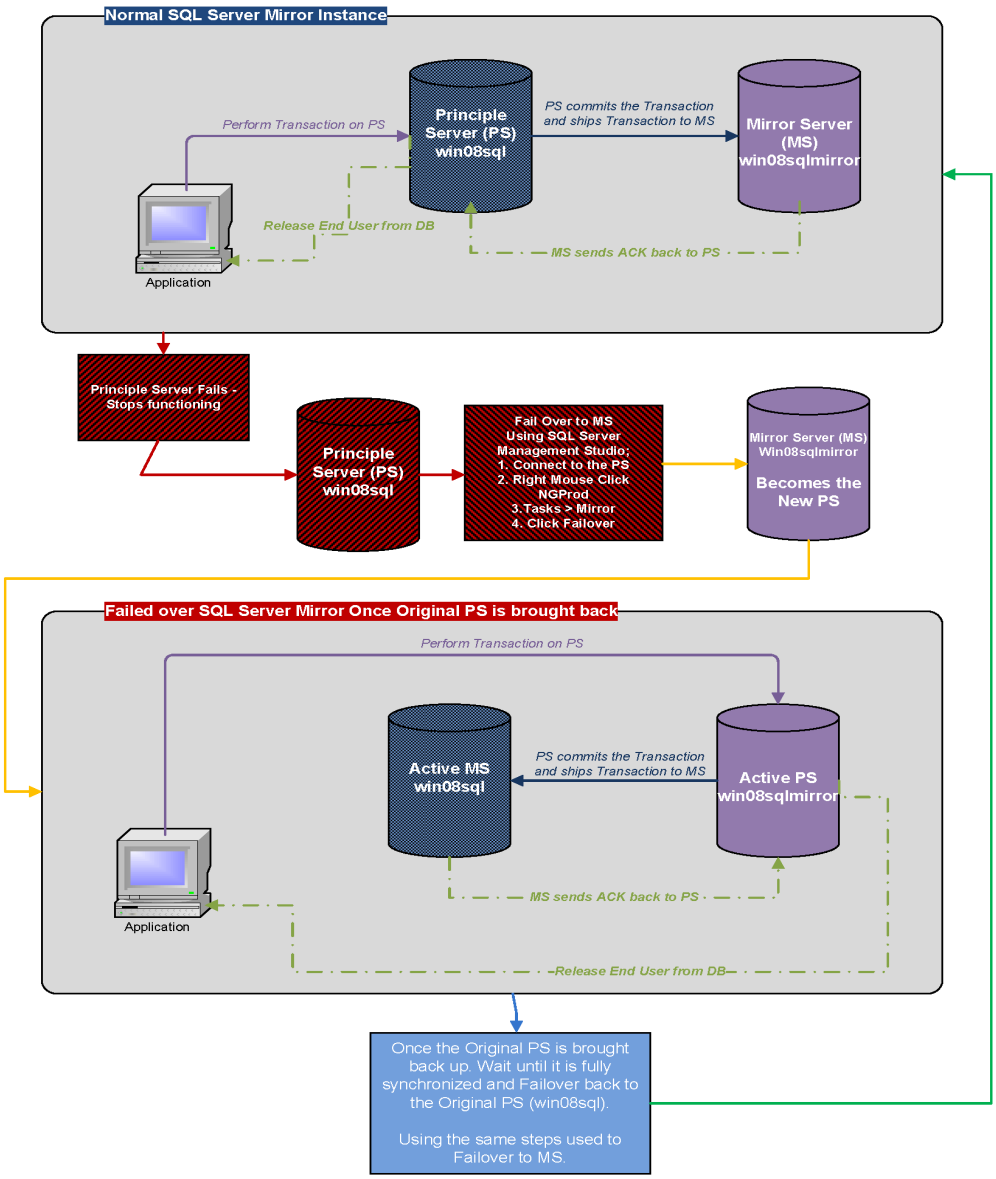
1. Critical Telecom Assets - Cisco Cube Sites
   a. Shasta Lake City: Cisco Cube 2901/K9, SN:FTX15288AS, Software Version: 15.2(1)T
   b. Happy Valley: Cisco Cube 2901/K9, SN:FTX1032W0VT, Software Version: 15.2(1)T
   c. Dental Redding: Cisco Cube 2901/K9, SN:FTX15288AJ, Software Version: 15.2(1)T
   d. Anderson: Cisco Cube 2901/K9, SN:FTX15288AM, Software Version: 15.2(1)T
   e. 980 Placer: Cisco Cube 2901/K9, SN:FTX15288AP, Software Version: 15.2(1)T
   f. 1035 Placer St: Cisco Cube 2901/K9, SN:FTX1437A0GK, Software Version: 15.2(1)T, Cisco Call Manager 8.5, Cisco Unity Connection 8.5, Cisco Unified Contact Center Express 8.5.
2. Spare parts for the Cisco are under a SmartNet Contract with Cisco which provides replacement coverage for failed part within a maximum of four hours.
3. Each Telephone Switch and devices assigned to it. See Appendix C.
4. Optional Telephone Services
   a. Primary Contacts - IT Manager, IT Project Manager.
   b. Each Satellite has two POTS lines for alternative communications installed.

c. Contingency for Connectivity Loss - Loss of switch should be limited to a maximum of four hours. In the interim our phone system is configured with xxxx
d. Four hours for any loss of a switch. For loss of communication line(s) or trunks we are subject to the timeline of the underlying carrier of services through xxx.

Establishing the Parameters of Timeline and Analysis of Data Loss

1. Time of outage
   a. Make note of time of outage (if this is what occurs) recording it in outage spreadsheet on S:drive or note for later input.
2. Time of loss of connectivity
   a. Time that NextGen becomes inaccessible (either by shutting down, Backup Batteries going dead or equipment failure) recording it in outage spreadsheet on S:drive or note for later input and ALL whiteboards in the IT Support Shop Area. Email the info to the DRC team.
3. Time of last t-log filing
   a. The last NGProd T log file in *Proprietary* in this format "NGProd_(Date)numbering.trn the last file with date and time is the last T log. recording it in outage spreadsheet on S:drive or note for later input.

SCHC Production Database Real-Time Mirroring Schematic



Coupled with our remote offsite backup solution, mirroring the production database is our best defense against data loss. Should it become necessary to recover items from any gap from connectivity loss to recovery status, the following procedures shall be followed:

NextGen Document Recovery Procedure
(Fill in recovery process of EHR system - proprietary)

PRESCRIPTION RECOVERY PLAN:

A. Recovery Calls
   1. Contact all local pharmacies, listed on Appendix A, to request a list of all prescriptions generated from Shasta Community Health Center on the date of the system outage.
   2. Have pharmacies fax to a central fax number. IT was where I had them faxed.

B. NextGenRoot FAX Recovery
   1. Access : *proprietary*
   2. In the Sent folder, order the faxed prescriptions by detail to get the date/timestamp information. If it is more than 6 days after the date of the failure, access the Archive folder for the date of the failure.
   3. Pick the actual date of the system failure and reconcile with the same process in section C.

C. Medication Reconciliation Process
   1. Look up each patient in NextGen that is on the prescription lists.
   2. Access the med module and determine if the prescription documentation needs to be added.
   3. Add the med to the med list checking to be sure these data elements are completed:
      a. Medication Name
      b. Dose
      c. Sig.
      d. Quantity
      e. Refills
      f. Actual Start Date (date of the system failure)
      g. Provider Name and Location
      h. Do not fax the prescription.

      4. Add a med module note stating “recreated from back up recovery records due to system failure”
      5. Click Accept and move to the next medication.

All manual data recovery procedures are dependent on timely data extractions from a primary source (Production Environment) to other locales. The following table outlines the various jobs and the intervals associated with each.

Job Activity	Occurrence	Frequency	Start	End	AVG Duration
Tracks (i2i) EHR Update	Daily	60 Min	6:45	23:59	0:08min
Tracks (i2i) AutoUpdate	Daily	30 Min	0:15	23:45	3:45min
Tracks (i2i) InHouse Lab	Daily	30 Min	0:15	23:45	0:05min
SQL – T-Log	Daily	30 Min	0:15	23:45	0:02min
Mirrored Duplicate (Real-Time)	Daily	Real-Time	--:--	--:--	--:--

Appendix A.

PHARMACY CONTACT INFORMATION	Contact Number	Contact Name
Costco	xx	xx
CVS - Placer	xx	xx
CVS - Cypress	xx	xx
Frank's	xx	xx
Lim's	xx	xx
Owen's	xx	xx
Raley's - Lake	xx	xx
Rite Aid - Cypress	xx	xx
Safeway	xx	xx
Target	xx	xx
Wal-Mart - Dana Drive	xx	xxx
Wal-Mart - Anderson	xx	xx
Walgreens	xxx	xx

Appendix B.

Scripts for i2i Data Pull

Proprietary – put in local organizational scripts

Appendix C.

Telephone Switch ID's and Attached Devices

Main Facility

Fill in proprietary - local info

Appendix C.
Telephone Switch ID's and Attached Devices
Main Facility

MAC ADDRESS

Fill in local information DESCRIPTION

Anderson Switch ID's and Attached Devices

Fill in proprietary - local info

Device Name(Line) **Description** **IP Address**

Anderson Switch ID's and Attached Devices

Device Name(Line) **Description**

Fill in proprietary - local info