



**Indian Health Service
Division of Information Security
National Programs, Albuquerque, NM**

**Emergency Management Plan (EMP)
for the National Patient Information
Reporting System (NPIRS)**

SOP 06-01i
July 2008

FOR OFFICIAL USE ONLY—SENSITIVE

This information is intended for IHS use only.
Disclosure may cause harm to IHS. Access is
provided by request only and is not available
via the organization's Intranet.

DOCUMENT INFORMATION

EXCEPTIONS TO PROCEDURE

None

AUTOMATIC RESCISSION DATE

This document will be rescinded three years from the date of approval.

REVIEW

This document will be reviewed annually to maintain its currency.

SUPERCEDES

SOP06-01i_COOP_NPIRS – June 2008

APPROVAL

This Standard Operating Procedure (SOP) has been approved for distribution and implementation. These new procedures are effective immediately and will be enforced. Representatives of management will be authorized to conduct periodic quality checks and audits to assure compliance with these procedures. Requests for corrections or changes to any procedures should be sent to the IHS CISO. Exceptions or exemptions to any of these procedures must be submitted in writing to the IHS CISO for approval or disapproval using the appropriate policy waiver form.

Approved by:

Kathleen E. Federico
Acting CISO, IHS

Date

Date of annual review:

Reviewed by:

TABLE OF CONTENTS

1.0	Record of Changes	1
2.0	Introduction	2
2.1	Purpose	2
2.2	Applicability.....	2
2.3	Scope	2
2.4	Planning Objectives and Principles.....	3
2.5	Emergency Operations Centers (EOC)	4
2.6	Assumptions	4
2.7	Related EMPs.....	5
3.0	Concept of Operations.....	6
3.1	System Description and Architecture.....	6
3.2	Line of Succession.....	6
3.3	Responsibilities.....	7
4.0	Notification and Activation Phase	9
4.1	Damage Assessment Procedures	9
4.2	Disaster Recovery Plan Activation Procedures.....	10
4.3	COGCON Readiness Levels	10
5.0	Recovery Operations	11
5.1	Primary Recovery Objective	11
5.2	Secondary Recovery Objective	11
6.0	Return to Normal Operations	13
6.1	Original or New Site Restoration.....	13
6.2	Concurrent Processing	14
6.3	Plan Deactivation.....	14
7.0	Appendix A: Personnel Contact List	15
8.0	Appendix B: Vendor Contact List	17
9.0	Appendix C: Equipment Specifications	18
10.0	Appendix D: Server Diagrams.....	19
10.1	Server 5 (IRCSRV5) Configuration.....	Error! Bookmark not defined.
10.2	Data Warehouse Servers Configurations	Error! Bookmark not defined.
11.0	Appendix E: Restoring the NPIRS System.....	20
11.1	Considerations.....	Error! Bookmark not defined.
11.2	Restoring Server 5.....	Error! Bookmark not defined.
11.2.1	System Requirements.....	Error! Bookmark not defined.
11.2.2	System Install/Restore	Error! Bookmark not defined.
11.3	Restoring the Data Warehouse Servers	Error! Bookmark not defined.
11.3.1	System Requirements.....	Error! Bookmark not defined.

11.3.2	System Install/Restore	Error! Bookmark not defined.
11.4	Restoring the NPIRS Web/Application Servers	Error! Bookmark not defined.
11.4.1	System Requirements.....	Error! Bookmark not defined.
11.4.2	System Install/Restore ROHAN ...	Error! Bookmark not defined.
11.4.3	System Install/Restore MORDOR	Error! Bookmark not defined.
11.4.4	System Install/Restore GONDOR	Error! Bookmark not defined.
12.0	Appendix F: Restoring the Databases.....	21
12.1	DB2 Recovery Procedures	Error! Bookmark not defined.
12.1.1	Restoring the DB2 Servers	Error! Bookmark not defined.
12.1.2	Restoring the DB2 Client	Error! Bookmark not defined.
13.0	Appendix G: Restoring Business Applications	22
13.1	Restoring the NDW ImportEngine.....	Error! Bookmark not defined.
13.2	Restoring NPIRS Web Reporting Applications	Error! Bookmark not defined.
14.0	Appendix H: OIT/NPIRS Business Impact Analysis	23
14.1	Introduction.....	23
14.2	System Point of Contacts (POCs)	23
14.3	System Architecture.....	24
14.3.1	Critical IT Resources.....	24
14.4	Critical Roles and Resources.....	24
14.4.1	Resource Outage Impact, Time, and Recovery Priority	25
15.0	Appendix I: Disaster Recovery Assessment Procedures	26
16.0	Appendix J: SLAs, MOUs, and Related EMPs	30
16.1	Service Level Agreements (SLAs) and Memorandums of Understanding (MOUs).....	30
17.0	Appendix K: References/Requirements	31
18.0	Appendix L: Abbreviations, Acronyms	33
19.0	Appendix M: Glossary	35

1.0 Record of Changes

Change No.	Date	Subject	Page No.
01	02/15/05	Updated SOP# and formatting	NA
02	08/26/05	Additions/Updates to: 2.3.2 Assumptions Appendix C Appendix D Appendix E Appendix F Appendix G Appendix H	9 21-23 28 34-44 46-50 52, 54-55 59-61
03	09/22/05	Updates after walkthrough to: Appendix C Appendix E Appendix F Appendix I (15.2 moved from App. G)	21-24 30-50 55 68-69
04	05/30/06	Updated	All
05	06/08/07	A - Updated Contacts List B - Updated Vendor Contact List C - Equipment List D - Deleted Server 1 diagram E - Restoring NPIRS System: used tables to consolidate Servers 2,3,5 and NDW servers information Moved "Restoring NDW Integration Engine appendix here, updated Added Section 15.5, "Restoring NPIRS Web/Application Servers G - Restoring Business Apps H - updated NPIRS system figure	17 18 19, 20 26-28 29-31 35 40-41 43
06	02/28/08	Removed all references to Legacy NPIRS and decommissioned servers IRCSR2, IRCSR3. Updated info in C, D, E, F, G, H	
07	07/30/08	Updated	All

2.0 Introduction

2.1 Purpose

The National Patient Information Reporting System (NPIRS) Emergency Management Plan (EMP) establishes procedures to recover NPIRS after 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 NPIRS operations and recover damage done to the original system
 - **Reconstitution phase** to restore NPIRS system processing capabilities to normal operations
- Identify the activities, resources, and procedures needed to carry out NPIRS processing requirements during prolonged interruptions to normal operations.
- Assign responsibilities to designated OIT/NPIRS personnel and provide guidance for recovering NPIRS during prolonged periods of interruption to normal operations.
- Ensure coordination with other OIT/NPIRS 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.

2.2 Applicability

The NPIRS EMP applies to the functions, operations, and resources necessary to restore and resume NPIRS operations as it is installed at:

5300 Homestead Rd., Albuquerque, New Mexico.

The NPIRS EMP applies to OIT/NPIRS and all other persons associated with the NPIRS, as identified under Section 3.3, “Responsibilities.”

2.3 Scope

This EMP identifies what the OIT Albuquerque must do to continue its essential functions in times of crisis. Emergency planning requires the consideration of a wide range of possible situations that could disrupt normal operations or require response to an unusual situation. These possibilities include, but are not limited to:

- A national emergency such as a war involving the United States Armed Forces, an attack on the U.S., or any threat to the continuity of the Federal Government.
- Natural and technological disasters such as radiological incidents or emergencies, hazardous materials (HAZMAT) incidents, and environmental disasters.
- Events declared by the President of the United States to be major disasters, or emergencies under Public Law (P.L.) 93-288, the “Robert T. Stafford Disaster Relief and Emergency Assistance Act,” as amended.
- Civil disorders, terrorism, or other violent acts.
- Any situation that substantially disrupts normal operations of the OIT Albuquerque Office.

2.4 Planning Objectives and Principles

Various scenarios were considered to form a basis for the plan, and multiple assumptions were made. The Emergency Management Plan for NPIRS defines two levels of emergency management: Contingency and Disaster Recovery.

The applicability of the Contingency plan is predicated on the following key principles:

- The OIT/NPIRS computer hardware and software in Albuquerque, New Mexico, are inaccessible, but the facility is available; therefore, OIT/NPIRS is unable to perform processing for the NPIRS department.
- Valid contracts exist with vendors for replacement of hardware and software at the *primary* OIT/NPIRS site in Albuquerque, New Mexico.

The applicability of the Disaster Recovery plan is predicated on the following key principles:

- The OIT/NPIRS facility in Albuquerque, New Mexico, is inaccessible; therefore, OIT/NPIRS is unable to perform processing for the NPIRS department.
- A valid contract exists with the alternate site that designates that site in Albuquerque, New Mexico, as the OIT/NPIRS *alternate* operating facility.

During an emergency situation that prevents access to the original facility:

- OIT/NPIRS will use the alternate site building and IT resources to recover NPIRS functionality.
- The designated computer system at the alternate site will be configured to begin processing NPIRS information.

- The alternate site will be used to continue NPIRS recovery and processing functions throughout the period of disruption until the return to normal operations.

2.5 Emergency Operations Centers (EOC)

An EOC is the location designated by this Plan where operations will continue in the event of an emergency. The alternate site will be used to continue Public Data recovery and processing throughout the period of disruption, until the return to normal operations.

OIT will use the alternate site's IT resources to recover the Public Data during an emergency situation that prevents access to the original facility.

The designated systems at the alternate site can be configured to restore the Public Data and make it available to IHS staff by Virtual Private Network (VPN).

2.6 Assumptions

Based on these principles, the following assumptions were used when developing the NPIRS EMP:

- NPIRS is inoperable at the OIT/NPIRS computer center and cannot be recovered within 72 hours.
- Key NPIRS personnel have been identified and trained in their emergency response and recovery roles; they are available to activate the Emergency Management Plan for NPIRS.
- Computer center equipment, including components supporting the NPIRS, are connected to an uninterruptible power supply (UPS) that provides 45-60 minutes of electricity during a power failure.
- Current backups of NPIRS application software and data are intact and available at the offsite storage facility.
- Equipment, connections, and capabilities required to operate NPIRS are available for delivery at the OIT/NPIRS original site in Albuquerque, New Mexico.
- Equipment, connections, and capabilities required to operate NPIRS are available at the alternate site in Albuquerque, New Mexico.
- Service agreements are maintained with NPIRS hardware, software, and communications providers to support the emergency system recovery.
- If applicable, related contingency plans are in process to include the Integration Engine and adequate communication links for receiving export data, as well as general communications.

The NPIRS EMP does not apply to the following situations:

- Overall recovery and continuity of business operations. This plan is an Annex to the Office of Information Technology Business Resumption Plan (BRP) and Emergency Management Plan (EMP), which includes the Continuity of Operations Plan (COOP).
- Emergency evacuation of personnel. Refer to the Building Emergency Management Plan for the Occupant Evacuation Plan (OEP).

2.7 Related EMPs

The following EMPs are related to this EMP.

- SOP 08-01 OIT EMP
- Albuquerque Area Office
- Building Emergency Operations Plan (AAO/OIT/NP)

3.0 Concept of Operations

3.1 System Description and Architecture

The National Patient Information Reporting System (NPIRS) stores information related to Native American patient and health care facilities. This national data repository is commonly known as the National Data Warehouse (NDW).

The NDW is the central data repository for all Indian Health systems. It provides the data for various data marts that, in turn, support IHS statutory, regulatory, and administrative obligations, including user population counts, workload reporting, epidemiological non-standard reporting, accreditation, and Government Performance and Results Act (GPRA) performance measurements to meet the mission and business requirements of the Indian Health Service.

The NDW functional areas fall into four major categories:

- (1) Operation Systems (AIX)
- (2) Database Software (DB2)
- (3) Data Movement (FTP connections and export process programming)
- (4) Web Site Reporting

3.2 Line of Succession

The Office of Information Technology (OIT) sets forth an order of succession in coordination with the order set forth by the Department, to ensure that decision-making authority for the OIT Emergency Management Plan is uninterrupted.

1. The Chief Information Officer (CIO) is responsible for ensuring the safety of personnel and the execution of procedures documented within this Emergency Management Plan.
2. If the CIO is unable to function as the overall authority or chooses to delegate this responsibility to a successor, the Deputy Chief Information Officer (DCIO) shall function as that authority.

The line of succession continues, as follows:

3. Division of Program Management and Budget (DPMB) Director
4. Division of Information Technology Operations (DITO) Director

5. Division of Information Resources Management (DIRM) Director
6. Division of Information Security (DIS) Director (CISO)
7. IHS Information Systems Security Officer (ISSO)
8. NPIRS ISSO

3.3 Responsibilities

This Emergency Management Plan has established several teams assigned to participate in recovering the NPIRS operations. The following teams have been defined and trained to respond to a contingency event affecting the IT system. Details concerning the overall Incident Command structure can be found in SOP 06-01, *OIT Emergency Management Plan*.

Team Name	Team Description
System Recovery	<p>The <i>primary recovery goal</i> of the System Recovery Team will be to restore NPIRS to functional status.</p> <p>This team is responsible for the recovery of the NPIRS computer environment, including the hardware and operating system. Members of this team include personnel who are also responsible for the daily operations and maintenance of the NPIRS servers.</p> <p>The System Recovery team leader directs the System Recovery team.</p>
Database Recovery	<p>The <i>primary recovery goal</i> of the Database Recovery Team will be to restore the NPIRS databases.</p> <p>This team is responsible for the recovery of the NPIRS database software, including retrieving and loading backups. Members of this team include personnel who are also responsible for the daily operations and maintenance of these databases.</p> <p>The Database Recovery team leader directs the Database Recovery team.</p>
Damage Assessment Recovery	<p>The <i>primary recovery goal</i> of the Damage Assessment Team will be to coordinate the damage assessment of the NPIRS system.</p> <p>The Damage Assessment Recovery team leader directs the Damage Assessment Recovery team.</p>

Team Name	Team Description
Business Applications Recovery	<p>The <i>primary recovery goal</i> of the Business Applications Team will be to ensure that the NPIRS business applications are functional.</p> <p>This team is responsible for the development and processing of the NPIRS business applications. Members of this team include personnel who are also responsible for the daily operations and maintenance of these business applications.</p> <p>The Business Applications Recovery team leader directs the Business Applications Recovery team.</p>
Tape Recovery	<p>The <i>primary recovery goal</i> of the Tape Recovery Team is responsible for coordination with the Iron Mountain offsite data vault, as needed.</p> <p>The Tape Recovery team leader directs the Tape Recovery team.</p>

The relationships of the team leaders involved in system recovery and their member teams are illustrated in the following figure.

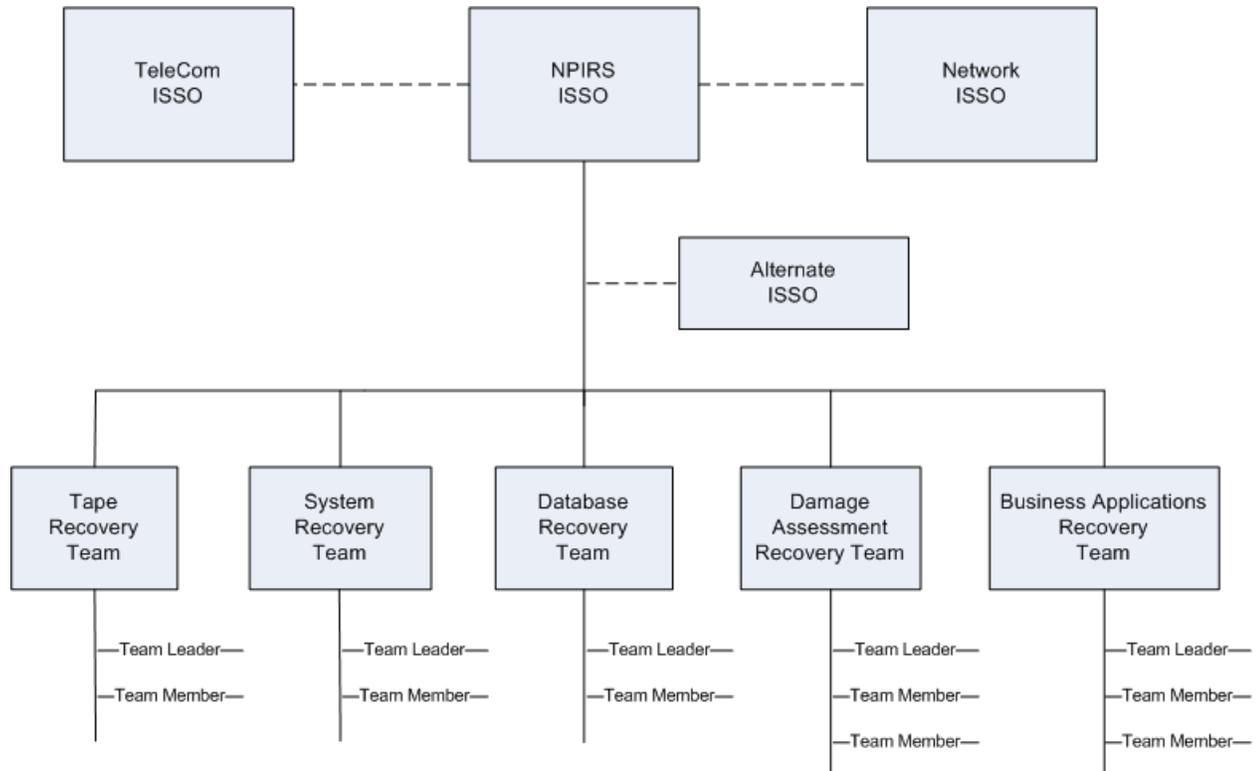


Figure 3-1: Recovery Teams/Reporting Structure

4.0 Notification and Activation Phase

This phase addresses the initial actions taken to detect and assess damage inflicted by a disruption to the National Patient Information Reporting System (NPIRS). Based on the assessment of the event, the Emergency Management Plan for NPIRS may be activated by the NPIRS Information Systems Security Officer (ISSO).

In an emergency, the top priority of OIT/NPIRS is to preserve the health and safety of its staff before proceeding to the notification and activation procedures.

This is the notification sequence:

1. The OIT Liaison will notify the NPIRS ISSO. All known information regarding NPIRS must be relayed to the NPIRS ISSO.
2. The NPIRS ISSO will inform the NPIRS Team Leader of the event. The NPIRS ISSO will instruct the NPIRS Team Leader to begin assessment procedures.
3. The NPIRS Team Leader will notify team members and direct them to complete the assessment procedures outlined in Section 4.1 to determine the extent of damage and estimated recovery time at the primary facility.

If damage assessment cannot be performed at the primary site because of unsafe conditions, the team members will follow the outlined procedures in Section 4.2.

See “Appendix A: Personnel Contact List” for key personnel contact information.

4.1 Damage Assessment Procedures

Upon notification from the NPIRS ISSO, the NPIRS Damage Assessment Team Leader or designee will follow procedures outlined in “Appendix I: Disaster Recovery Assessment Procedures” to coordinate the damage assessment of the NPIRS system.

When the damage assessment has been completed, the NPIRS Damage Assessment Team Leader will notify the NPIRS ISSO of the results. The NPIRS ISSO will evaluate the results and determine whether the contingency plan is to be activated and if relocation is required.

4.2 Disaster Recovery Plan Activation Procedures

The Disaster Recovery plan will be activated if either of the following criteria is met:

- (1) NPIRS will be unavailable for more than 72 hours.
- (2) The facility is damaged and will be unavailable for more than 48 hours.

Based on assessment results,

1. The NPIRS ISSO will report the assessment results to the OIT Liaison.
2. If the plan is activated, the NPIRS ISSO will notify all team leaders and inform them of the details of the event and that relocation is required.
3. Upon notification from the NPIRS ISSO, team leaders will notify their respective teams. Team members will be informed of all applicable information and will be prepared to respond and relocate.
4. The NPIRS ISSO will 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 NPIRS ISSO will coordinate with the NPIRS Tape Recovery team to ensure appropriate media is requested.
5. The NPIRS ISSO will notify the alternate site (if applicable) that a contingency event has been declared and to prepare the facility for the arrival of OIT/NPIRS.

4.3 COGCON Readiness Levels

There are four COGCON levels that can be recommended to the Senior OIT Leadership regarding COOP activation: COGCON 4, COGCON 3, COGCON 2, and COGCON 1. The OIT Liaison with input from first responder units (police and/or fire and/or the Incident Commander, if this involves more than OIT, will make the recommendation.

Detailed information about the COGCON levels of activation can be found in SOP 08-01, OIT EMP.

5.0 Recovery Operations

This section describes the efforts directed to repair damage to the NPIRS system and capabilities at either the primary site or at an alternate site. The following procedures are outlined per team required. Each procedure should be executed in the sequence it is presented to maintain efficient operations.

5.1 Primary Recovery Objective

The primary recovery objective is to restore the NPIRS system to functional status.

- **System Recovery Team Objective**

The primary recovery goal of the System Recovery team will be to restore the servers to functional status. See “Appendix E: Restoring the NPIRS System” for the procedures to restore the servers.

- **Database Recovery Team Objective**

The primary recovery goal of the Database Recovery team will be to restore the NDW databases. See Appendix F: Restoring the Databases” for the procedures to restore the databases.

- **Business Applications Team Objective**

The primary recovery goals of the Business Applications team will be to ensure that the business applications are functional and that workload and user population reports can be produced to support IHS funding requirements. The Business Applications team is responsible for running tests to ensure that the applications perform as expected. See “Appendix G: Restoring Business Applications” for the procedures.

- **Tape Recovery Team Objective**

The primary recovery goal of the Tape Recovery team will be to ensure back up tapes are retrieved from the offsite location and are available to the other teams.

5.2 Secondary Recovery Objective

Once the NPIRS system is functional, the secondary recovery objective is to recover the ability to automatically receive and process data and produce reports for NPIRS.

- **Business Applications Team Objective**

The second recovery objective of the Business Applications team is to ensure that the automatic processes are working.

- **Database Recovery Team Objective**

The second recovery objective of the Database Recovery team is to support the Business Applications team's efforts, if required.

- **System Recovery Team Objective**

The second recovery objective of the Database Recovery team is to support the Business Applications team's efforts, if required.

- **Tape Recovery Team Objective**

The second recovery objective of the Tape Recovery team is to support the other recovery teams, if required.

6.0 Return to Normal Operations

This section discusses activities necessary for restoring normal operations for the National Patient Information Reporting System (NPIRS) at the OIT/NPIRS original or new site. When the computer center at the original or new site has been restored, NPIRS operations at the alternate site must be transitioned back to the OIT/NPIRS center. The goal is to provide a seamless transition of operations.

6.1 Original or New Site Restoration

After start up and verification operations are performed at the original/new site, the offsite system will be shut down. Stability verification procedures can take from two days to not more than two weeks. During the stability verification period, no processing of new data will be done at the offsite location. When system stability is verified, database backups will be transferred to the original system. After the backups are restored, processing of new data will begin at the original/new site.

The following procedures are required to restore or replace the original site so that normal operations may be transferred.

- **System Resumption Team**
 - Prepare servers at new or original site.
 - Install and configure the servers. See “Appendix E: Restoring the NPIRS System” for the procedures to restore the servers.
 - Test telecommunications connections.
- **Database Resumption Team**
 - Backup databases.
 - Restore databases. See “Appendix F: Restoring the Databases” for the procedures to restore the databases.
 - Advise Business Applications Resumption team that the databases are available for use.
- **Business Applications Resumption Team**
 - Stop processing data at alternate site.
 - Notify client sites of new FTP addresses, if necessary.
- **Tape Recovery Resumption Team**
 - In joint communication with the NPIRS ISSO, retrieve necessary tapes or other media from offsite storage, if necessary.

6.2 Concurrent Processing

Concurrent processing is not required for NPIRS.

6.3 Plan Deactivation

The following procedures are required to shut down the system and clean the alternate site of any equipment or other materials belonging to the organization.

- **Database Deactivation Team**

After verification that the database has been successfully resumed at the permanent site:

- Advise Business Applications Resumption team that the databases are about to be removed.
- Drop the databases.
- Drop the instances.
- Delete DB2 files.
- Remove DB2 directories.
- Create dummy database.
- Drop logical volumes.
- Return to monitor and maintenance mode at permanent site.

- **System Deactivation Team**

The System Deactivation team should overwrite the disk to ensure that all data is removed.

- **Tape Recovery Deactivation Team**

Ensures tapes or other media, if used, are returned to offsite storage.

System and Database Deactivation team members should package, label, and ship the materials, equipment, and backup media to the new or original site, and then return to the new or original site.

7.0 Appendix A: Personnel Contact List

Name	Position	Office Number	Home Number	Cell Number	Home Email Address
Stanley Griffith	NPIRS Team Leader	(505) 248-4144			
Carlene McIntyre	Alternate NPIRS Team Lead	(505) 248-4960			
Joseph Herrera	NPIRS Information Systems Security Officer (ISSO)	(505) 248-4916			
Tape Recovery – Resumption Team					
Sam Berry	Team Leader	(505) 248-4150			
Lois Boyd	Team Member	(505) 248-8000			
System Recovery – Resumption Team					
(contractor)	Team Leader				
(contractor)	Team Member				
Database Recovery – Resumption Team					
(contractor)	Team Leader				
Joseph Herrera	Alternate Team Leader				
(contractor)	Team Member				
Damage Assessment Recovery – Resumption Team					
(contractor)	Team Leader				
(contractor)	Team Member				
(contractor)	Team Member				

Name	Position	Office Number	Home Number	Cell Number	Home Email Address
Business Applications Recovery – Resumption Team					
(contractor)	Team Leader				
(contractor)	Team Member				
(contractor)	Team Member				
(contractor)	Team Member				

8.0 Appendix B: Vendor Contact List

Note: Information in this appendix is *NOT PUBLIC* and has been removed.

9.0 Appendix C: Equipment Specifications

Note: Information in this appendix is *NOT PUBLIC* and has been removed.

10.0 Appendix D: Server Diagrams

Note: Information in this appendix is *NOT PUBLIC* and has been removed.

11.0 Appendix E: Restoring the NPIRS System

Note: Information in this appendix is *NOT PUBLIC* and has been removed.

12.0 Appendix F: Restoring the Databases

Note: Information in this appendix is *NOT PUBLIC* and has been removed.

13.0 Appendix G: Restoring Business Applications

Note: Information in this appendix is *NOT PUBLIC* and has been removed.

14.0 Appendix H: OIT/NPIRS Business Impact Analysis

14.1 Introduction

The National Patient Information Reporting System (NPIRS) stores information related to Native American patient and health care facilities. The National Data Warehouse (NDW) is the central data repository for all Indian Health systems. It provides the data for various data marts that, in turn, support IHS statutory, regulatory, and administrative obligations, including user population counts, workload reporting, accreditation and GPRA performance measurements to meet the mission and business requirements of the Indian Health Service.

14.2 System Point of Contacts (POCs)

The following table lists the positions/offices/roles within OIT/NPIRS that depend on or support NPIRS.

Point of Contact (POC)	Relationship to NPIRS
12 Area Office Directors	Send data to and receive data from NPIRS.
HQ: IHS/OPS	Receive critical reports and manage data requirements.
IHPES	Receive incoming exports from areas. Produce reports for hospital accreditation.
Blue Cross Blue Shield (BCBS)	Receive/transmit data to update our BCBS information.
CMS	Receive/transmit data to update our Medicaid/Medicare information.
SSA	Receive/Transmit data to update our SSN information.
System Administrator	Maintains the computer systems.
Database Administrator	Maintains the database systems.
Development/Production Staff	Develop and maintain the business applications.

The following table lists the external POCs that support NPIRS.

Point of Contact (POC)	Relationship to NPIRS
System Vendor	Responds to OS hardware/software problems, as specified in vendor contract.
Database Vendor	Responds to database problems, as specified in vendor contract.
Offsite Vendor	Storage and retrieval of database backups.

14.3 System Architecture

Note: Information in this section is *NOT PUBLIC* and has been removed.

14.3.1 Critical IT Resources

The following sections list the hardware, software, and other resources that are critical to the operation of NPIRS.

Note: Information in the following sections is *NOT PUBLIC* and has been removed.

14.3.1.1 Hardware

14.3.1.2 Software

14.3.1.3 Other Resources

14.4 Critical Roles and Resources

The following table lists the roles and resources that are critical to the operation of NPIRS.

Critical Role	Critical Resources
End user	Network
System Administrator	Server, OS, backup system, network
Database Administrator	Server, OS, database, backup system
Development/Production Staff	Server, OS, database, backup system, desktop computer, network

14.4.1 Resource Outage Impact, Time, and Recovery Priority

The following table lists the critical resources, the impact of and time allowed for an outage, and recovery priority.

Resource	Outage Impact	Allowable Outage Time	Recovery Priority
Server/OS	Unable to - Access or process data - Produce user reports - Update the database - Transmit reports - Receive data	QTRs 1, 2, 3: 5 business days QTR 4: 3 business days	HIGH
Database	Unable to - Update the database - Process reports	QTRs 1, 2, 3: 5 business days QTR 4: 3 business days	HIGH
Backup	Unable to backup or restore the database	QTRs 1, 2, 3: 5 business days QTR 4: 3 business days	HIGH
Network	Users unable to transmit/receive data or reports electronically	QTRs 1, 2, 3: 5 business days QTR 4: 3 business days	Medium
Desktop computer	Unable to - Access or process data - Produce user reports	QTRs 1, 2, 3: 5 business days QTR 4: 3 business days	HIGH

15.0 Appendix I: Disaster Recovery Assessment Procedures

The use of this section is applicable during moderate or severe disruption to the NPIRS system.

During minor disruption to the NPIRS system caused by normal system problems, (this includes, but is not limited to, hardware, software, and power failure problems), a damage assessment is not required.

The form below is to be used to assess the damage of the NPIRS systems in event of a moderate or severe disaster.

During activation of the OIT EMP or Building EMP, a damage assessment of the NPIRS system would be required.

The damage assessment documents the damage to the NPIRS servers located on the 1st floor. It provides the estimated recovery time and the equipment that may be salvaged or repaired. This form may be used to notify the Incident Commander of the assessment, and coordinate equipment salvage where possible in the event of a disaster affecting the 5300 Homestead Rd. NE building and involving this system.

The purpose of the checklist below is to guide a damage review and assessment of the NPIRS system following a severe disaster. In using the checklist, consider:

- The percent of normal capacity at which the equipment is able to function.
- Actions to be taken to recover or repair damaged equipment to enable RPMS operations.
- Timeframes for repair or replacement of the damaged equipment to recover NPIRS operations.

1 st & 2 nd Floor Server Room NPIRS System		
Equipment	<input type="checkbox"/> NPIRS Servers	Description of Damage:
	<input type="checkbox"/> Network Cabling	Description of Damage:
	<input type="checkbox"/> Other Equipment	Description of Damage:
	<input type="checkbox"/> Magnetic Tape Media	Description of Damage:

ESTIMATED RECOVERY TIME

Based on the damage assessment, determine the estimated recovery time, using the following guidelines.

- Non-Disaster:** Essential damage to the facility and/or equipment. Estimated time to complete repairs is **less than 72 hours.**
- Disaster:** Moderate damage to the facility and/or equipment. Estimated time to complete repairs is **between 72 hours and 7 business days.**
- Catastrophe:** Extensive damage to the facility and/or equipment. Estimated time to complete repairs is **greater than 7 business days.**

Initials:	Date:	Time:
------------------	--------------	--------------

16.0 Appendix J: SLAs, MOUs, and Related EMPs

16.1 Service Level Agreements (SLAs) and Memorandums of Understanding (MOUs)

There are no contractual obligations with the hardware vendor beyond best efforts to restore hardware to functional status on a timely basis. Software response from IBM is two hours for production downtimes, although this does not guarantee restoration. For downtimes in excess of four hours, refer to the IHS COOP document.

17.0 Appendix K: References/Requirements

- IHS Circular 2002-02 Continuity of Operations Planning Program
- IHS Information Resources Management Policy Part 8, Chapter 12 - Information Technology Security
- HHS Information Security Program Policy
- Health Insurance Portability and Accountability Act
- Federal Information Security Management Act (FISMA) of 2002
- The Computer Security Act of 1987
- OMB Circular A-130, Management of Federal Information Resources, Appendix III, November 2000.
- The National Security Act of 1947, dated July 26, 1947, as amended
- HSPD-20/NSPD-51, National Continuity Policy, dated May 4, 2007
- IHS Circular 2002-02 Continuity of Operations Planning Program
- HHS Contingency Planning for Information Security Guide, 7/19/2005
- HHS Critical Infrastructure Protection (CIP) Planning Guide, 7/19/2005
- HHS Disaster Recovery Planning Guide, 7/19/05
- HHS Incident Response Planning (IRP) Guide, 7/19/2005
- Executive Order (EO) 12656, Assignment of Emergency Preparedness Responsibilities, dated November 18, 1988, as amended
- EO 12472, Assignment of National Security and Emergency Preparedness Telecommunications Functions, dated April 3, 1984
- EO 12148, Federal Emergency Management, dated July 20, 1979, as amended
- Presidential Decision Directive (PDD)-62, Protection against Unconventional Threats to the Homeland and Americans Overseas, dated May 22, 1998
- PDD-63, Critical Infrastructure Protection, dated May 22, 1998
- PDD-66, Test, Training and Exercise (TT&E) Program for Continuity of Operations (COOP), dated April 30, 2001
- PDD-67, Enduring Constitutional Government and Continuity of Government Operations, dated October 21, 1998.
- Federal Preparedness Circular (FPC) 60, Continuity of the Executive Branch of the Federal Government at the Headquarters Level during National Security Emergencies, dated November 20, 1990
- FPC 65, Federal Executive Branch Continuity of Operations, dated June 15, 2004

- 41 Code of Federal Regulations (CFR) 101-2, Occupant Emergency Program, revised as of July 1, 1998
- 36 CFR 1236, Management of Vital Records, revised as of July 1, 1998
- NIST SP 800-18, Guide for Developing Security Plans for Information Technology Systems as of December 1998
- NIST SP 800-30, Risk Management Guide for Information Technology Systems
- NIST SP 800-34, Contingency Planning Guide for Information Technology Systems
- NIST SP 800-53, Recommended Security Controls for Federal Information Systems
- National Response Plan, Department of Homeland Security, Federal Emergency Management Agency (FEMA), December, 2004
- Defense Authorization Act (Public Law 106-398), Title X, Subtitle G, "Government Information Security Reform," October 30, 2000

18.0 Appendix L: Abbreviations, Acronyms

APC	Ambulatory Patient Care (Direct Outpatient)
BRP	Business Resumption Plan
CHI	Contract Health Inpatient
CHO	Contract Health Outpatient
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMS	Center for Medicare/Medicaid Services
COOP	Continuity of Operations
CP	Contingency Plan
CPC	Contingency Planning Coordinator
DCIO	Deputy Chief Information Officer
DEPM	Division of Enterprise Project Management
DEN	Dental
DIT	Division of Information Technology
DIRM	Division of Information Resources Management
DIS	Division of Information Security
DRP	Disaster Recovery Plan
EMP	Emergency Management Plan
FTP	File Transfer Protocol
GPRA	Government Performance Results Act
HQ	Headquarters
HHS	Department of Health and Human Services
IHS	Indian Health Service
IHPES	Indian Health Performance Evaluation System
INP	Direct Inpatient
IRT	Incident Response Team
ISDM	Information Security Data Manager
ISS	Internet Security Systems
ISSO	Information Systems Security Officer
IST	IHS Security Team
IT	Information Technology
NDW	National Data Warehouse
NIST	National Institute of Standards and Technology
NPIRS	National Patient Information Reporting System
OEP	Occupant Evacuation Plan
OIT	Office of Information Technology

POC	Point of Contact
SOP	Standard Operating Procedures
SSA	Social Security Administration
SSN	Social Security Number
UPS	Uninterruptible Power Supply

19.0 Appendix M: Glossary

An online Glossary is available at the IHS Security Web Page:
<http://home.ihs.gov/ITSC-CIO/security/secpgm/SecGlos.cfm>