NEW YORK STATE OF OPPORTUNITY.

Office of Information Technology Services

Department of Health (DOH)
New York State Immunization Information System (NYSIIS)
Information System Contingency Plan (ISCP)

June 21, 2023

CTO Business Continuity & Disaster Recovery

Table of Contents

Document Version History

Version	Date	Author(s)	Change Summary
1.0	5/14/2020	T. Reichl	First Draft
2.0	7/6/2020	M. Flynn	Support Staff Updates
2022	10/17/2022	N. Rose	Recert edits

Document Approval

Name	Date
Dina Hoefer	7/20/2020
Kyle Carpenter	7/20/2020

Yearly Review

Name	Date
Nicholas Rose (ITS DR Team) 6/22/2023	

1. Introduction

The New York State Immunization Information System (NYSIIS) provides a complete, accurate, secure, real-time immunization medical record that is easily accessible and promotes public health by fully immunizing all individuals appropriate to age and risk.

The application is deployed utilizing sets of UNIX LPARs. The back-end databases of NYSIIS are Oracle Relational Databases located in a network tier separated by a firewall from the application servers. Web servers are placed in a secured DMZ, also separated with firewalls from both the application and database servers.

2. Scope

NYS ITS is committed to the uninterrupted service of the NYSIIS application. Current application allows for redundancy within current CNSE Data Center.
Service:
Immunization Records

3. Approach

Information Technology Services (ITS) has an overall approach to both reduce the probability of a disaster due to known reasons as well to provide the conditions that facilitate failover in the event of a disaster. A high level of redundancy is built into the Primary Data Center as well as the Wide Area Network (WAN).

From a high-level view, the following represents major tasks required to prepare for and implement the Information System Contingency Plan:

- Have a detailed and current Information System Contingency Plan
- Identify all components required for the NYSIIS environment
- Form a Service Continuity Team including key roles and responsibilities
- Conduct Disaster Recovery (DR) kick-off meeting
- Execute the process and procedures for declaring disaster/critical incident
- Implement the process and procedures for failover
- Periodically test the Information System Contingency Plan

3.1 Recovery Objectives

Recovery Time Objective (RTO) – 2-3 Days
The NYSIIS application can be restored to user access within 2-3 days following a loss of the primary servers.

Recovery Point Objective (RPO) - 24 hours
Systems using the Enterprise Backup Solution have daily backups to support an RPO of 24 hours.

3.2 Primary and Secondary Data Centers

The NYSIIS application is configured to run in the ITS Primary Data Center with data backups copied to
The Utica data center.

3.3 Assumptions

The following assumptions are taken into account for this document and the procedures within:

- Connectivity to primary data center from all interfacing agencies and applications
- Functionality of all interfacing agencies/applications that utilize NYSIIS
- All core services are functional. See section 5.5 for a full list of dependencies.

4. Processes and Procedures

4.1 Critical Incident/Disaster Assessment

In the event of a failure at primary data center, a quick assessment will be vital in determining if any action is needed. Several factors will be instrumental in what process must occur, including the stability of the impacted data center, and the length of time it will take to restore complete functionality. Software and hardware failures will need to be investigated to assess whether the length of the repair time exceeds any defined recovery time and will thus be considered an incident. In such cases, the current incident management procedures should be adhered to.

If the failure is determined to be more than an incident, ITS has a documented process for declaring a disaster. Detailed information regarding the ITS Incident Management process and Policy can be found in the ITSM (ServiceNow) knowledge article KB0015586 via the ITS Enterprise Operations Incident Management Process and Policy. This process applies to processing locations, hardware, and software applications supported by ITS. The NYSIIS application will follow standard ITS Incident Management procedures in validating, assessing and reporting an incident by contacting the Help Desk

NYSIIS admins and/or the Duty Manager have the authority to approve changes needed for service restoration. If the incident is identified as a Priority 1 or Priority 2 issue, the Help Desk performs a warm hand-off (phone call, email) to the Service Delivery Manager (SDM).

4.2 Disaster Declaration Process

The identification of a potentially critical incident/disaster will set into motion a pre-defined process with associated notification, assessment, and decision-making phases. This process includes:

- Identification of the type and source of the problem and appropriate notification priorities such as police, fire, and facilities services
- Notification to senior management on the status of facilities/systems and service provision
- Assignment of a “DR Coordinator” to make an early assessment and determine if activation of the ITS Continuity of Operations Plan (COOP) is necessary or if current incident resolution measures are adequate
- If the ITS COOP is activated then the “declaration phase” is also activated and advanced steps are taken including the assignment of a Damage Assessment Team (DAT) to assess damage to areas including health and safety, physical structure(s), and technology infrastructure
- Once a disaster is formally declared, the Implementation Phase is initiated to execute all necessary DR activities

4.3 Continuity Strategy

The current continuity strategy for NYSIIS consists of restoring the servers and database from backups.

4.3.1 Primary Transaction Database Server Unrecoverable

Estimated Downtime: 3-4 Hours

Remediation Steps:

1. Stop all applications.

2. DBA performs failover to secondary databases.

3. Update configuration on both server 1 and 2 to point to failover database.

4. Start all applications.

4.3.2 Secondary Transaction Database Server Unrecoverable

Estimated Downtime: No Downtime

No interruption in service, but a new failover server must be configured.

4.3.3 Primary Datamart Database Server Unrecoverable

Estimated Downtime: 3-4 Hours

Remediation Steps:

1. Stop all applications.

2. DBA performs failover to secondary databases.

3. Update configuration on both server 1 and 2 to point to failover database.

4. Start all applications.

4.3.4 Secondary Datamart Database Server Unrecoverable

Estimated Downtime: No Downtime

No interruption in service, but a new failover server must be configured.

4.3.5 Web Server 1 Unrecoverable

Estimated Downtime: No Downtime

No interruption in service, but a new web server must be configured.

4.3.6 App Server 1 Unrecoverable

Estimated Downtime: ~2 Hours

Remediation Steps:

1. Stop all applications.

2. Start RunMatch on server 2.

3. Reconfigure DX to point to new RunMatch location.

4. Update system_globals runmatch location.

5. Start Afix on Server 2.

6. Update system_globals afix location.

7. Update configuration in domain.root/ir/lib/afixproperties.

8. Start all applications.

4.3.7 Web Server 2 Unrecoverable

Estimated Downtime: No Downtime

No interruption in service, but a new web server must be configured.

4.3.8 App Server 2 Unrecoverable

Estimated Downtime: ~5 minutes intermittent downtime

Some interruption in service until web server 2 is shut down.

4.3.9 Both App Servers 1 and 2 Unrecoverable

Estimated Downtime: 2-3 days (Gainwell-owned steps)

Assumption: ITS will provide new hardware in the event that both app servers are unrecoverable.

Remediation Steps:

1. (ITS): Build new app servers on new machines.

2. (ITS): Install LPAR image from backup of previous machines (WebLogic, directory structures, configuration files, start/stop scripts, etc.).

3. (Gainwell): Refresh NYSIIS applications from GitHub.

4. (Gainwell): Restart applications/services within NYSIIS application on new server.

Start up

Start the node manager and weblogic server.

/apps/nysiis/env/prd.region/domain.root/ir/stopProdNodeManager.sh

/apps/nysiis/env/prd.region/domain.root/ir/stopProdWebLogic.sh

Weblogic --> Environment --> Servers --> Start up all apps

Data Exchange (unix command line)

IRConsole start prod-app RunMatch only on server1 validate 4 instances come up.

make sure runmatch completes before moving on.

RJM and MatchSvr need runmatch complete before they start.

IRConsole start prod-app RJM

IRConsole start prod-app (start the rest of prod-app)

IRConsole is used to show the status

ETL

cd /apps/nysiis/env/prd.region/java.root

nohup dmLoadManager.sh &

OHS

cd to /apps/nysiis/env/prd.region/domain.root

nohup ohstart.sh &

Data Backup

All servers that comprise the NYSIIS environment are backed up to the Enterprise Backup Solution. They all have weekly full backups, with incremental backups between each full.

Resuming Operations at the Primary Data Center

- **Preparing the Facility**

If failover was invoked due to damage or destruction of the Primary Data Center facility or some/all of the hardware components, necessary steps will be taken to resolve the issues that invoked the failover process in the current facility including identifying a new facility, repairing the damaged facility, and obtaining replacement hardware.

- **Assessment**

If a failover occurs and a disaster is declared, assessment activities will be driven by Executive Management and their bureau leads. The areas affected will then call upon their own disaster recovery teams to assess the scope of relocation/recovery operations. This includes the prioritization of activities and the identification of facilities. For non-disaster related failovers, a Root Cause Analysis (RCA) will be performed to ensure that a Return to Operations will be successful and will not trigger a similar event.

- **Damage or Destruction**

In the event that the failover was invoked due to damage or destruction of infrastructure or facilities, the repair or replacement of these items will be necessary before Return to Operation can be initiated.
In an effort to expedite this:

- Support to other environments may be suspended depending on the nature of the issue(s) and the resources needed to facilitate failover.
- Damage assessment efforts will leverage a process of elimination to converge on the actual root cause (damaged equipment). Through this process, equipment and parts that need replacement will be identified and compiled into a list that can be forwarded to ITS Procurement.

- **Return Planning and Scheduling**

When a failover of NYSIIS is required, resuming normal operations will be initiated as quickly as conditions allow. It is recognized that failover operation does not provide a highly available service and a resumption of normal operations is imperative. Failing back to the Primary data center may cause a short disruption in service and will therefore be scheduled and communicated to end users.

4.4 Notification

Business unit management, staff, and stakeholders will be notified of the switch by one of the multiple methods listed directly below.

- Email
- Helpdesk notification
- Phone calls

The notification message will include at a minimum:

- Reason for switching to the Secondary Data Center
- Expected time of switch
- Anticipated duration for Secondary mode operations, if known
- Functionality, if any, that will not be available and for how long
- Environments, if any, that will not be available and for how long
- Any known problems or issues with the DR operations (e.g. performance degradation)

Verification of any changes made to interfacing agencies will be performed and those agencies will be notified of a switch to Service Continuity Mode. Monitoring the performance, security and availability of the Secondary data center will be accomplished with the normal production system monitoring tools.

5. Identification of Components for Service Continuity

This section identifies all necessary components to be operational Center to continue the NYSIIS services.

5.1 Facilities

SUNY College of Nanoscale, Science and Engineering (CNSE) Data Center

257 Fuller Road, Albany, NY 12203

The CNSE Data Center is currently considered to be the Primary Site and is designed to meet or exceed industry specifications for a Tier 3 data center. The following is brief list of the core capabilities provided by this facility.

- **Security:** Access to the CNSE Building is controlled by badge swipe technology combined with a keypad/PIN entry code. Data center access is provided only to those that have been cleared through the fingerprinting and State Police background checks.
- **Power:** The CNSE Data Center has Power Conditioning, dual power feeds, an Uninterruptible Power Supply (UPS) and Backup Power Generation. The Power Conditioners ensure clean power is delivered to our equipment while the UPS ensures that continuous power is available during short-term power failure. For longer-term power failures, the Backup Generator can be started to ensure continuous operation of the CNSE Data Center.
- **Fire and Flood Prevention:** The CNSE Data Center contains fire detection, fire suppression and flooding sensors in compliance with Tier 3 Data Center specifications.
- **Heating, Ventilating, and Air-Conditioning (HVAC):** Computer Room Air Conditioning (CRAC) equipment is installed for the Primary Data Center. The HVAC systems are capable of cooling the full power load in the room with an allowance for a single CRAC unit failure. The central cooling plant supporting the CRAC equipment is redundant.

Utica Data Center

1400 Noyes Street, Building 62, Utica, NY 13502

The Utica Data Center is currently considered to be the Secondary Site. The following is brief list of the core capabilities provided by this facility.

- **Security**: Access to the Utica Building is controlled by badge swipe technology and is managed by NYS Staff. Access to the Utica Data Center is controlled by badge combined with a keypad/PIN entry code. Data center access is provided only to those that have been cleared through the fingerprinting and State Police background checks.
- **Power**: Dual power feeds, Uninterruptible Power Supply (UPS) and generator keep the servers and network up and running in the event of power failure in the DR Data Center. The UPS systems are also supported by a site generator. ITS has a proactive maintenance program that assures the UPS systems are at 100%. UPS battery health is monitored
- **Fire and Flood Prevention**: The Utica Data Center contains fire detection, fire suppression and flooding sensors in compliance with Tier 3 Data Center specifications.
  Heating, Ventilating, and Air-Conditioning (HVAC): Computer Room Air Conditioning (CRAC) equipment is installed for the Utica Data Center capable of cooling the full power load in the room with an allowance for a single CRAC unit failure. There are additional overhead cooling modules that draw in hot air from the hot aisle and discharge cool air down into the cold aisle. Redundant chillers provide redundant cooling for these units. All HVAC equipment is supported by a site generator for continuous availability in a power outage

5.2 Server Components

This section describes the servers for the NYSIIS environment.

Server	IP Address	Role
DOH0369PA5WEB	10.108.67.72	Web Server (1)
DOH0435PA5WEB	10.108.67.73	Web Server (2)
DOH0350PA5APP	10.108.124.25	Application Server (1)
DOH0351PA5APP	10.108.124.26	Application Server (2)

5.3 Summary of Software

The web server for NYSIIS runs IBM HTTP 6.0 on an AIX 7.1 host

Following Oracle 19c Upgrade:
The web server for NYSIIS runs IBM HTTP 8.5 on an AIX 7.2 host

5.4 Database

As of 6/22/23:

Server	IP Address	DB Name	Role
DOH0352PA5ORA	10.108.124.27	nyprd1	Primary Server
DOH0371PA5ORA	10.108.124.28	Nydmp	Primary Server
PA4DH024	Admin 10.64.193.4 Prod/Data 10.64.47.6	Nyprd1	Standby Server
PA4DH025	Admin 10.64.193.6 Prod/Data 10.64.47.7	Nydmp	Standby Server

The databases for NYSIIS Oracle 11g on AIX 7.1 hosts

Following Oracle 19c Upgrade:

Server	IP Address	DB Name	Role
DOH0450PA5ORA	10.108.124.64	TBD	OLTP Server
DOH0451PA5ORA	10.108.124.65	TBD	OLTP Server
DOH0452PA5ORA	10.108.124.25	TBD	Datamart Server
DOH0453PA5ORA	10.108.124.26	TBD	Datamart Server

Not functional as of 10/26/22. Will be applicable following Oracle 19c Upgrade.

The databases for NYSIIS Oracle 19c on AIX 7.2 hosts

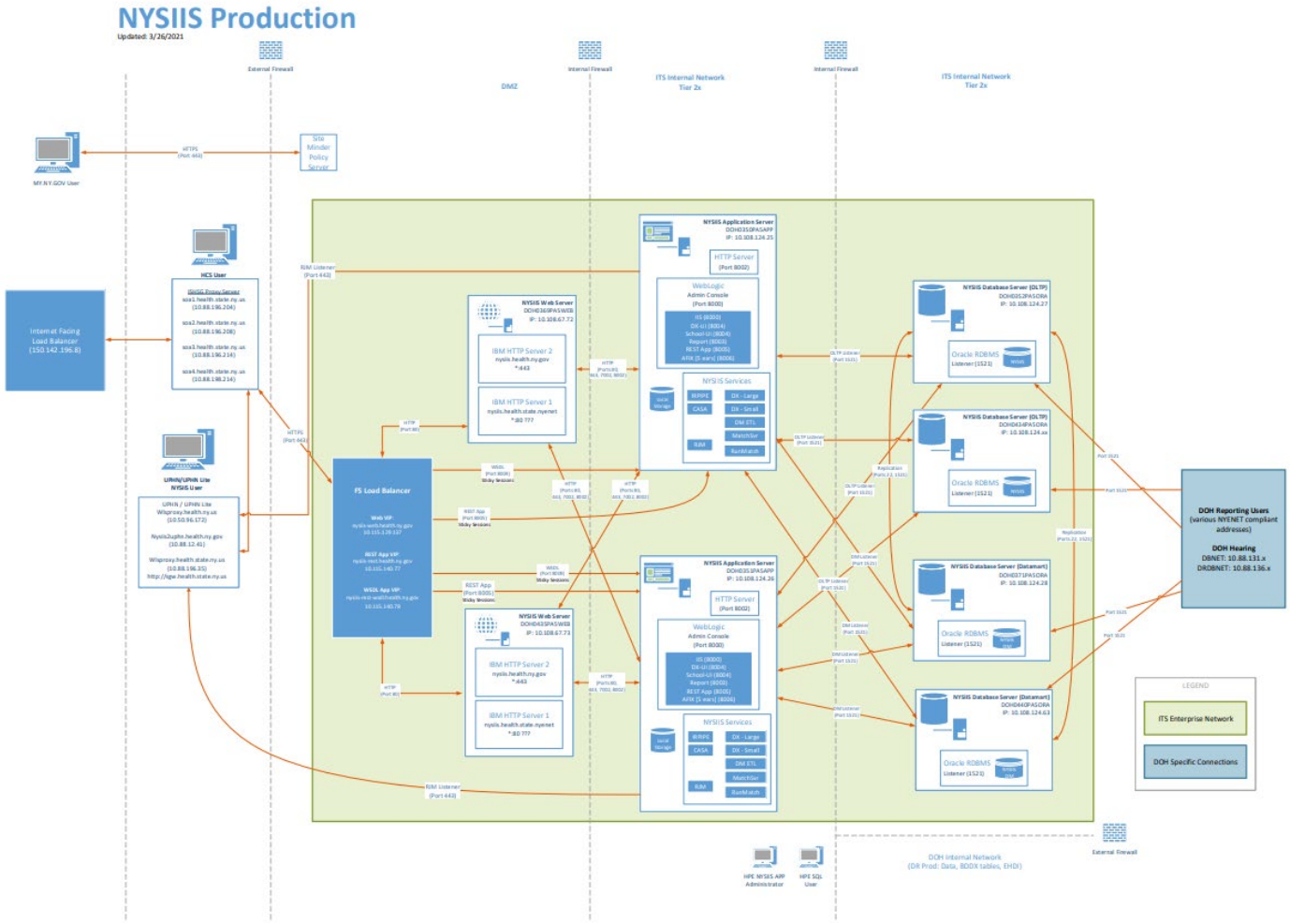
5.5 Relations

NYSIIS requires multiple internal and external services to be available to be fully functionable
Dependencies

- Enterprise Storage
- DNS
- Enterprise Network
- DOH services/applications: HCS

Appendix A – Continuity Procedure

Production Architecture



Plan Overview

- **RISK:** Low
- **IMPACT:** High
- **Plan Owner(s):** Dina Hoefer
- **Test Schedule:** TBD

Failover Procedure

Name/Organization & contacts	Role	Responsibility
L2 NYSIIS DOH Bhnsm-wls@health.ny.gov	Operations Administrator	
L3 NET-COM DCN Its.dl.dcn@its.ny.gov	Data Center Networking	
GAINWELL TECHNOLOGIES LLC NYSIIS-Distribution@gainwelltechnologies.com (281) 385-9236 (630) 621-0532	Vendor	Gainwell supports the NYSIIS application
L2 PLAT DBA ORACLE DOH	Databases	Oracle DBA

In the event that the new servers will be engaged for use temporarily supporting one or more NYSIIS environments, the first steps in the recovery process will be build new servers containing the LPAR image from backup of previous machines. This will include any non-database file backups that must be restored to the standby servers, as well as current NYSIIS release files and configuration updates, if needed, for connection to the HCS authentication portal.

Because NYSIIS-specific application modules can be released relatively quickly, disaster recovery events will include the deployment of the most current NYSIIS application code. The source code for this release will be pulled from the release archival prepared by vender. The code release will be deployed in the same manner that regular releases to NYSIIS Production are applied, making use of the new direct VPN connection to servers that will need to be identified and made available to authorized Gainwell staff.

While the NYSIIS-specific restoration activity is on-going, the necessary network reconfigurations will also get underway to ensure that URL requests for the NYSIIS application are correctly passed to the HCS authentication module and then routed to the standby NYSIIS web server in the newly identified environment.

In the event that only the primary DB server(s) are lost, due to the ongoing DataGuard synchronization process, the transactional database(s) will already be as up to date as possible. The timing of the restore need compared to the last complete synchronization of the datamart instance(s) will be evaluated to determine whether additional updating is advised. The status of the standby transactional and datamart databases will be reviewed to confirm both are in a ready state for live access. If all DB servers are lost, Commvault backups will be utilized to restore datamart instances.

Once all files have been retrieved from archive and restored and the new network connections have been established, the new database instances will be changed from standby mode to active mode. Doing this will leave the instances available for update by the NYSIIS application and related services.

Before confirmation of the application availability is sent to the NYSIIS users community, validation of the regions will be conducted to ensure that all components are in place and available. A full checkout of the application will be performed by vender and NYSIIS Program staff before users will be advised that the application is available for continued use. This checkout will be similar in scope and detail to checkout performed following a NYSIIS software release and will include verification of all subcomponents of the application.

While the new database instances are in Active (read-write) mode, users authorized for direct access (e.g. NYS DOH Program staff) will be able to continue their use of the databases for independent querying. However, because these instances are now the primary databases attached to the NYSIIS application, any large queries submitted may

impact system performance. Therefore, it is strongly recommended that Program staff temporarily halt any in-depth activity on the database instances while they are being used with a live application.

Additionally, while the primary database instances are unrecoverable due to the disaster event and the standby instances are serving as the active instances, there will be no new standby version of the databases. No DataGuard replication will be operating on the instances. Therefore, during the disaster event, it will be important to perform nightly backups of the database instances, writing the backup data to tape or otherwise saving it to a safe location; this will be accomplished by Commvault backups. Likewise, non-database files created by the NYSIIS application while it is live on the new servers must be backed up as well. The directories in need of backup will be the same as those identified on the primary NYSIIS servers in the ITS Data Center. If all original database instances are unrecoverable due to the disaster event, the minimum configuration of DB instances will be created; there will be no new standby version of the databases initially.

Appendix B – DR Tests

The NYSIIS application was included in Disaster Recovery testing for various DOH applications. The testing to be scheduled.