NYWIC Project

New York State Department of Health

WIC Program Services

Version: 1.1

Deliverable: NYWIC-3-09

NYWIC MIS Technical Architecture Documentation

Trademarks

Trademarked names may appear throughout this document. Rather than list the names and entities that own the trademarks or insert a trademark symbol with each mention of the trademarked name, the names are used only for editorial purposes and to the benefit of the trademark owner with no intention of infringing upon that trademark.

Contact Information

To request copies, suggest changes, or submit corrections, contact:

New York State Department of Health
Division of Nutrition, Bureau of Supplemental Food Programs
Attention: James L. Browning, Health Program Administrator 2
Phone: 518.402.7163, email: BSFP-FMS.Procure@health.ny.gov

Revision History

Date	Version	Revised By	Description
1/30/2017	0.1	3∑- Ryan Buysse	Draft version
1/14/2017	0.2	3∑-Jay Saunders	Additional detail added
3/23/2017	0.3	Jay Saunders	Responses to state feedback
4/6/2017	0.4	Jay Saunders	Responded to SFTP content and made updates as discussed. Responded to other commends and acknowledge direct terminology updates made to text.
6/9/2017	0.5	Jay Saunders	Added section 5.5 to discuss Enterprise Services and the potential for future integration with Enterprise Services under change control.
6/26/2017	0.6	Jay Saunders	Updates per IV&V requests
1/26/2018	1.0	Jay Saunders	Updating Server Requirements
3/6/2018	1.1	Jay Saunders	Responding to comments

NYWIC – MIS TECHNICAL ARCHITECTURE DOCUMENT

Deliverable Description

The contractor shall prepare and submit updated, detailed architectural diagrams with textual support for the environments within thirty (30) days of contract approval. The documents must be updated within five (5) days of any hardware and software modifications, additions, or upgrades and include, but not be limited to:

- Required servers and minimal hardware specifications per server, identifying each server by its purpose and environment
- Required software for each server, including number of licenses and versions
- Required specialized hardware and software for document scanning, UPC/PLU scanning, and capturing and filing participant electronic signatures
- Any additional hardware required, including recommended vendors, versions, and specifications
- Other hardware and software required, including the total number of licenses and the structure of pricing and usage of the licenses
- Overall detailed architectural diagram(s):
    - Diagram(s) should include detailed graphics displaying the listed components and their relative placement in the architecture
    - Vendor shall clearly mark the communication channels between architectural components, identifying features such as encryption where appropriate.
    - Required infrastructure for Local Agencies and Clinics

NYWIC – MIS TECHNICAL ARCHITECTURE DOCUMENT

TABLE OF CONTENTS

1. Glossary of Terms/Abbreviations

EBT: Electronic Benefit Transfer. Often used to reference the entire information system that facilitates the purchase of Food Benefits at authorized WIC Vendors.

EPPIC: Electronic Payment Processing and Information Control

F5: Non-specific hardware name for F5 Networks load balancers and may be used to describe load balancer in general. F5 is the most commonly used hardware load balancer and as a result, the load balancer is often described as an F5 even though other brands and units may be used.

FTP: File Transfer Protocol

IP: Abbreviation for Internet Protocol address

PDF: Portable document format

SAML: Security Assertion Markup Language

SAN: Storage Area Network.

SLA: Service level agreement

SSRS: SQL Server Reporting Services

URL: Uniform resource locator

WUMEI: WIC Universal MIS to EBT Interface. A definition of the functionality and data exchange necessary between NYWIC and Conduent to facilitate WIC EBT. The specification is defined by FNS and its partners.

2. Purpose

This document provides the details of the minimally recommended hardware and software specifications for the NYWIC management information system. Included are logical architectural diagrams that should provide an overview of the system design. Additionally, using 3 sigma software's experiences in Michigan, Indiana and Florida, this document will provide the minimal hardware specifications recommended for centralized Servers that host the system. It will detail the software required to operate the system on those servers. To summarize these recommendations a listing of each Server will be defined in detail. The Technical Architecture Document's intended audience is Information Technology Services personnel who will be administering and maintaining the system.

The NYWIC system can be supported via a variety of hosting infrastructure designs. The purpose of this document is to describe the core requirements of the NYWIC system to allow for the development of a state specific hosting infrastructure which will be influenced by several variables. These include:

- Investments in shared infrastructure components (e.g. load balancing, SAN, backup, monitoring, and DR capabilities)
- State hosting requirements based on the standards, practices, and policies enforced by the state or hosting entity
- Local security policies and the interpretation of applicable State and Federal policies regarding data privacy and security practices
- Knowledge of local usage patterns both within NYWIC and in other systems that may impact NYWIC performance
- Professional practices and preferences of the hosting team including database administration, network administration, and other technical disciplines

As with any complex system, it is challenging to predict all the possible technologies, practices, and considerations needed for deployment in a new hosting environment. This document is intended to document the key information required to develop a local hosting infrastructure plan. During deployment, questions and issues may arise. Maintaining an open and consistent communication channel will help ensure that issues are resolved in a timely and successful manner.

The document will also provide an outline of the Local Agency and Clinic infrastructure needed to operate the NYWIC system and define other specialized software requirements for these locations.

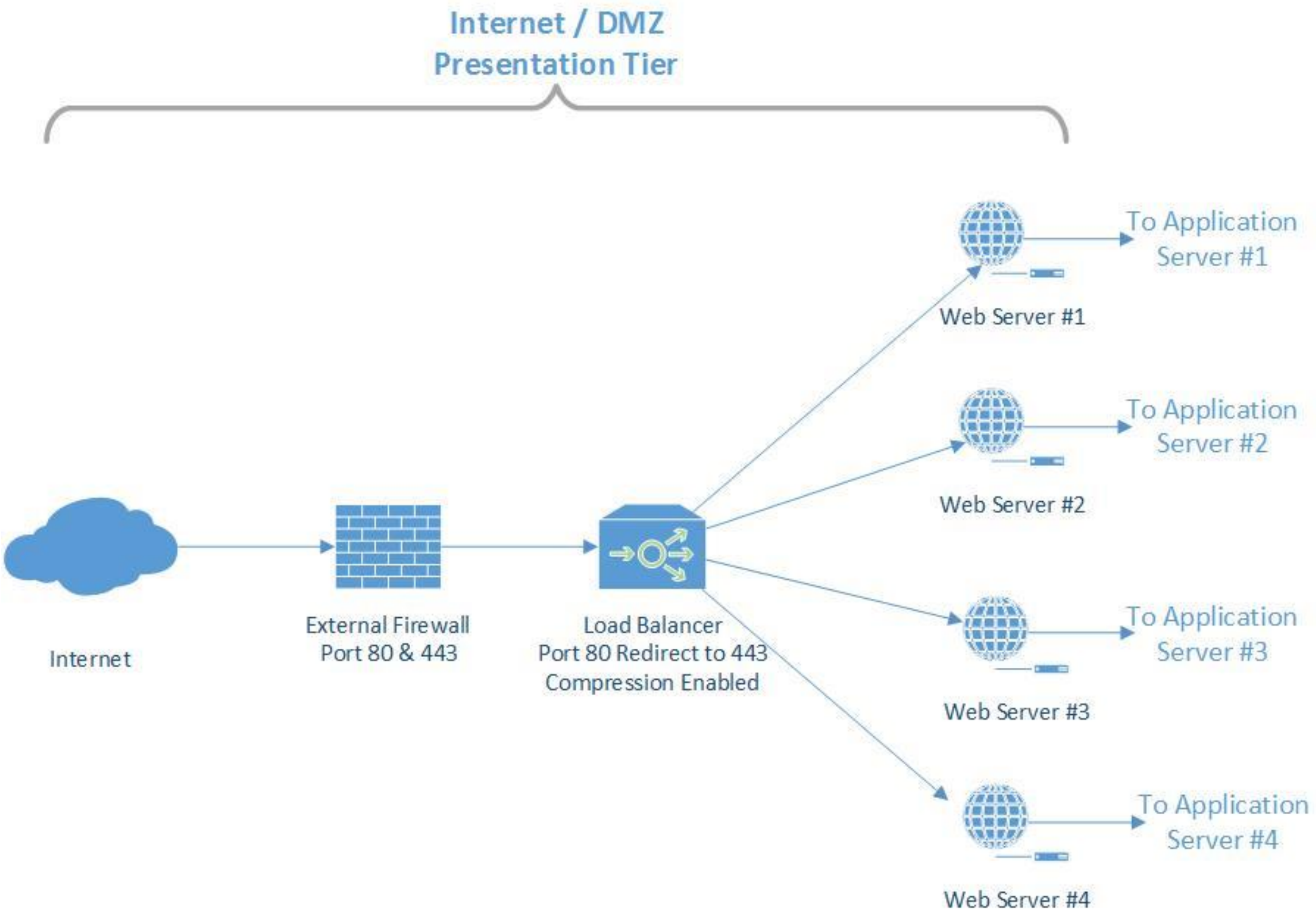
3. Architectural Diagrams

The NYWIC MIS is a centralized three-tier system; the Presentation tier, the middle or Business Service tier and the Data tier.

An end user in a Clinic, Local Agency, VMA, or State Office will interact with the presentation tier by requesting a URL from their web browser. The communication is secured in-transit by encrypting the message with secure sockets layer over HTTP.

Presentation Tier

The request is routed through NYS data center switches that serve as an outwardly facing firewall for the presentation tier. The firewall will limit incoming traffic to ports 443 (HTTPS) and 22 (SFTP). Optionally, the firewall can be configured to limit the source IP addresses to a known list of locations. The firewall can also be configured to accept port 80 (HTTP) traffic with a redirect to port 443 at the load balancer. Incoming requests continue to a load balancer. This device serves to compress and accelerate traffic as well as distribute the forwarded requests evenly across the various downstream hardware. Microsoft Windows 2012 R2 enabled Web Servers are the focal point of the presentation tier and respond to user requests by packaging web content with data retrieved from the Business Service tier and returning the data over HTTPS to the calling browser.



Business Services Tier

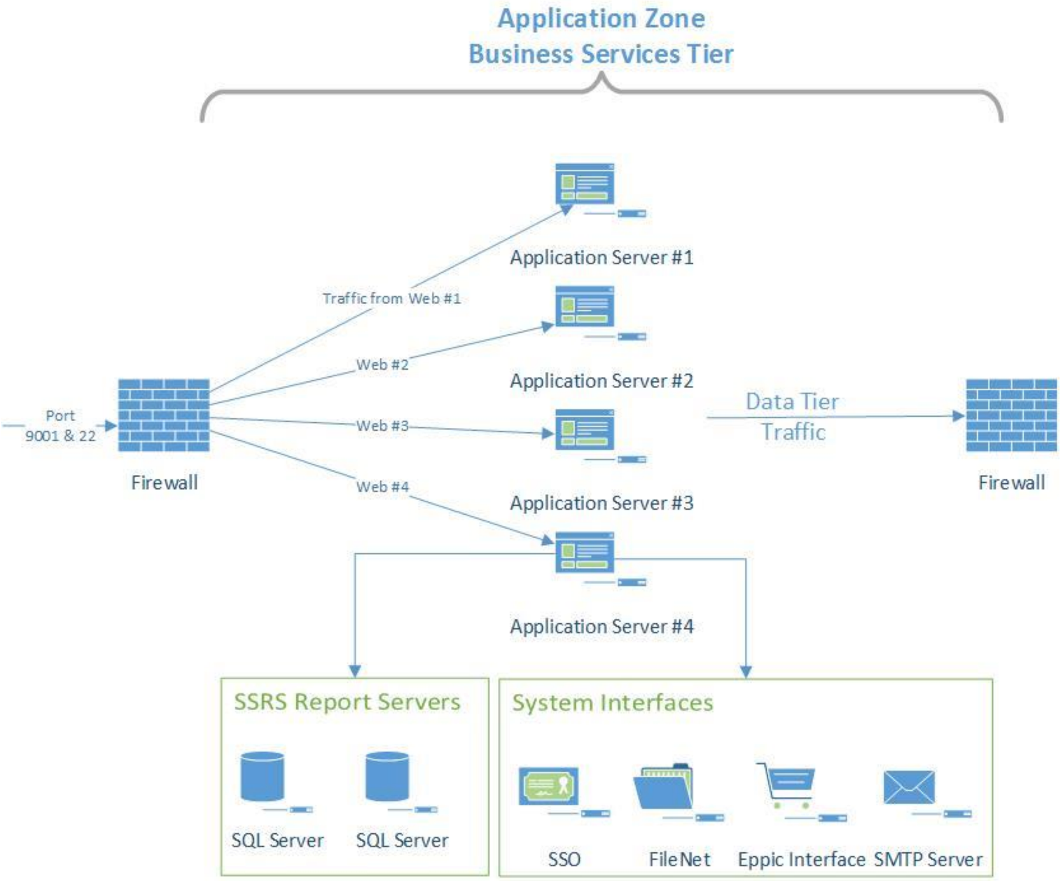
When the Web Server needs to execute a business rule, retrieve and analyze data, or save information it will do so by calling on Application Servers held within the Business Services tier. The NYWIC MIS system does this with .NET remoting, and a firewall between the Web Server and Application Server should be established to restrict this data flow to a single TCP port. The Application Servers will host the executables and libraries that make up the business rules engine.

The Application Servers need to interact with several sorts of systems to satisfy its objectives.

- For single sign on (SSO): to connect to the NYS single sign on (ny.gov) provider, the NYWIC system will need to integrate using SAML based on ny.gov specification.
- For EBT functionality: they will need a connection to CONDUENT's EPPIC system for real-time messages defined in the WUMEI.
- For EOD Operations: The NYWIC MIS has an automated component that executes End of Day (EOD) operations. This executable is hosted on Application Servers and part of its work is to automatically send and receive files to multiple external entities over a secure FTP connection.

- For ad hoc reports: they will need access to the SSRS server and for database requests the Oracle Server both held in the Data tier. Firewalls between the Application Servers and these external components can be established to further secure and segment the environment.

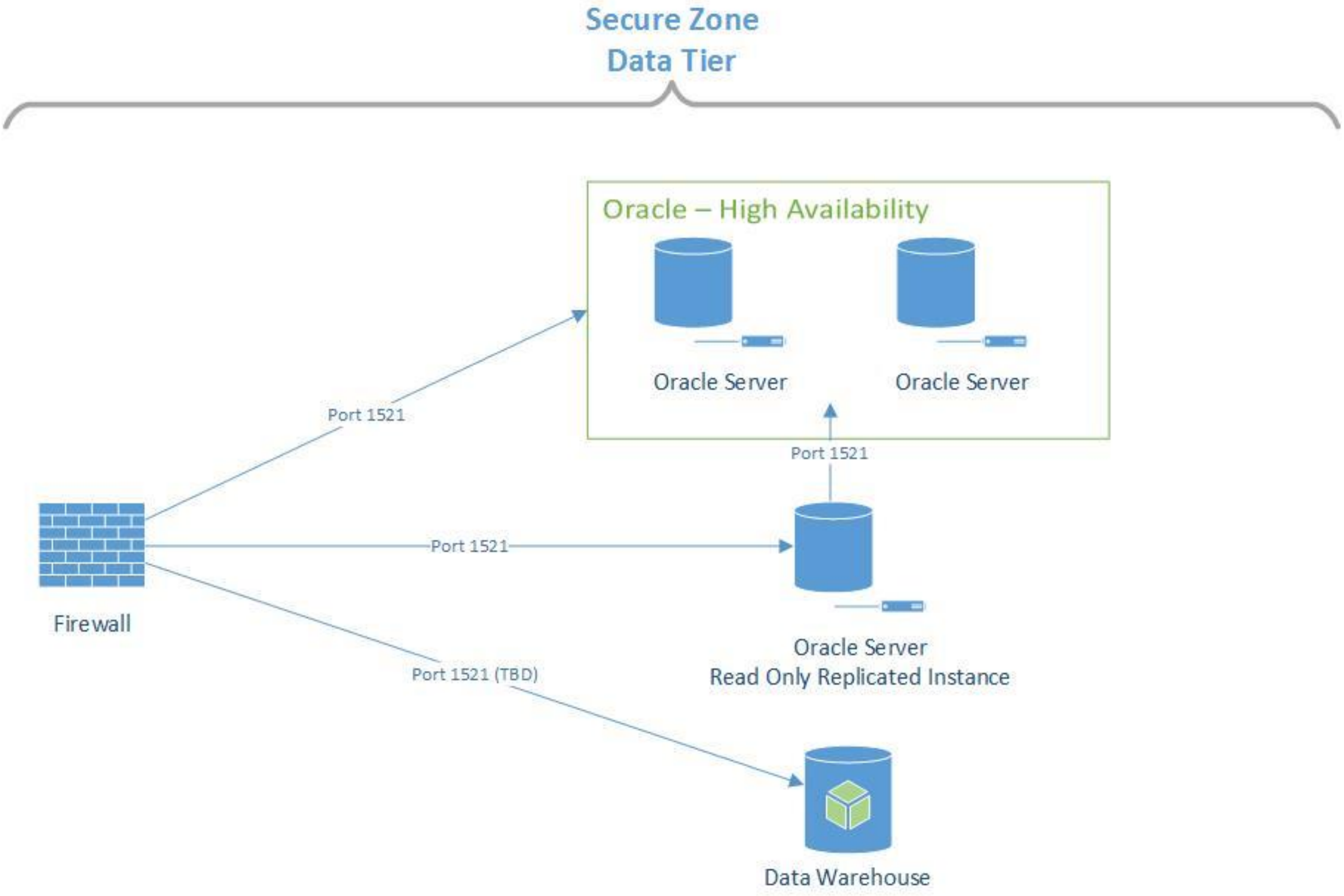
The SQL Server Reporting Service (SSRS) hardware will also operate in the business services tier. The system and ad-hoc report definitions reside on this hardware. When requests for a report are transmitted through the Presentation and Business Services tiers, SSRS will connect to the Read Only local database located in the data tier. This is done to avoid tying up the production database with complex or long running report queries. SSRS merges the queried data into the report layout and returns the formatted data to the presentation tier.



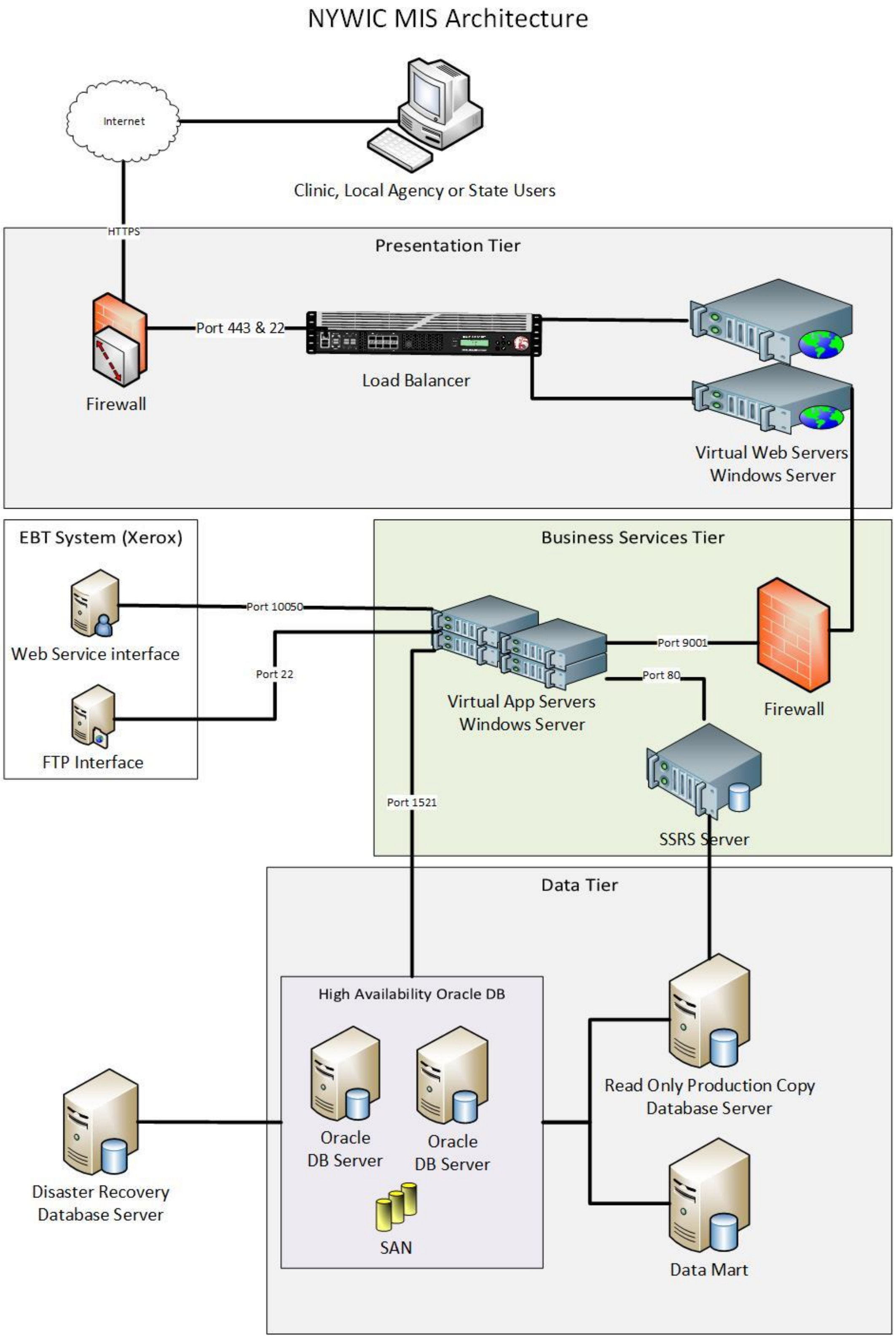
In the diagram above the authentication authority, document management and other resources are presumed to be in the Application Zone. Based on state policy they may exist in the secure zone.

Data Tier

When the Business Services tier needs to persist or query data it will make an ODBC connection to the Oracle 12c database server. The recommendation is for High Availability Oracle database solution with active/active configuration provides redundancy and failover support to guard against transaction loss and ensure synchronization of the data. A ITS supported solution will replicate data updates real-time to an off-site disaster recovery site and a Read Only database locally. A scalable Storage Area Network (SAN) physically stores the data and is configured to perform database backup and recovery using ITS supported backup technologies.



The Data tier may also consist of a dedicated SAN for the storage of scanned documents, signature images and other large files that are imported into the system.


NYWIC MIS Architecture
Internet
Clinic, Local Agency or State Users
HTTPS
Presentation Tier
Firewall
Port 443 & 22
Load Balancer
Virtual Web Servers
Windows Server
EBT System (Xerox)
Web Service interface
FTP Interface
Business Services Tier
Port 10050
Port 22
Virtual App Servers
Windows Server
Port 9001
Port 80
Firewall
SSRS Server
Port 1521
Data Tier
High Availability Oracle DB
Oracle
DB Server
Oracle
DB Server
SAN
Read Only Production Copy
Database Server
Data Mart
Disaster Recovery
Database Server

4. System Interfaces

Document Management

The NYWIC application is currently designed to store all documents and images in Oracle BLOB fields located in a table structure intended to support document storage. Larger states, like New York, may elect to move document storage into a document management system. If this is needed, a custom integration with the NYS document management system (expected to be FileNet) would be required. This would replace existing database integration with web service integration to the document management services.

Three Sigma would recommend that this approach be limited to true document management. This would include scanned documents and attached documents. The recommendation would be to exclude signature images which are collected as part of certification and issuance processes. The reasons for this recommendation are as follows:

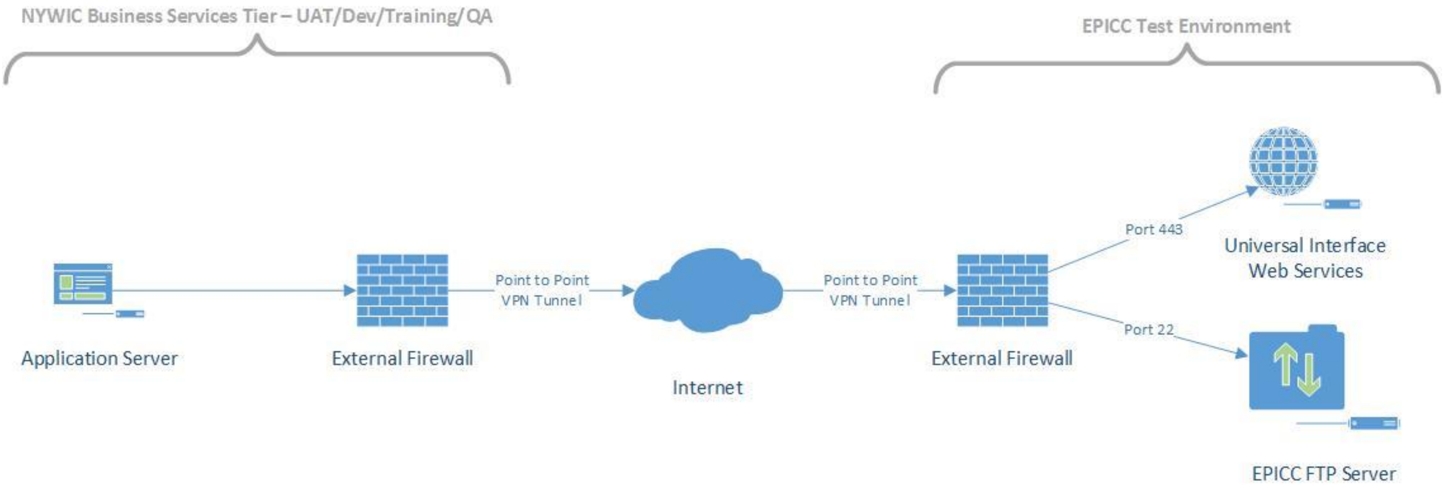
1) The images are very small, approximately 6K
2) Images may be on a limited retention policy
3) Signature capture is an important WIC policy requirement. Using a third-party service would potentially increase the potential for a system outage. Losing access to document attachment would not interrupt WIC operations but a loss of signature capture has significant policy implications.

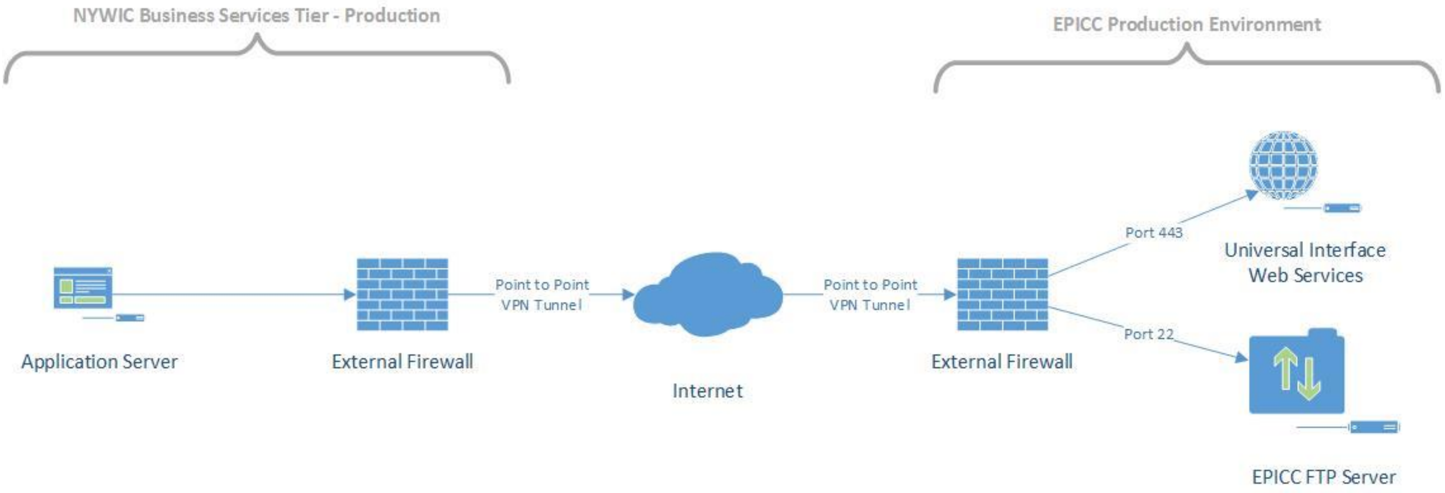
Conduent EBT Interface

The Conduent Electronic Payment Processing and Information Control (EPPIC) interface will consist of two major components. The first is a real-time interface involving communication with the EPPIC system using web services hosted by Conduent. NYWIC will send real time card issuance, benefit issuance, and other messages to the EPPIC system. Messages are initiated from the NYWIC business services tier on an encrypted HTTPS request.

The second major component are batch FTP communications to the Conduent hosted FTP server. These communications allow NYWIC to send and receive nightly batch files. The files include data like daily redemptions, authorized food updates, and authorized vendor updates. These communications occur on port 22 and are based on a SFTP protocol.

All communications with Conduent must be conducted over a secure point to point VPN tunnel between the NYWIC data center and the Conduent data center. A separate end point will be provided (by Conduent) for the production and develop/test Conduent environments.





FTP

Based on conversations with NYS WIC and NYS ITS, Three Sigma does not expect to host an FTP server for use by the NYWIC system. However, the NYWIC system will need to communicate with a variety of third-party providers using a Secure FTP client. The NYWIC system includes the capability to initiate a SFTP data transfer during daily batch processes from the business services tier. For initial rollout, the only expected communication partner is Conduent for EBT batch files.

In the future, communications with third parties could grow to include:

1) EBT provider
2) Rebate provider
3) Local agencies (auto dialer data)
4) Other systems like nutrition education, FNS, etc.

If the number of outbound communications becomes significant, the decision may be made to redirect communications through the ITS Managed File Transfer solution. This change would centralize communications to a single end point. This change may require changes to NYWIC to deliver and receive files from the Managed File Transfer solution.

The NYWIC system will need permissions to communicate over port 22 as required for system interfaces from the business services tier. These permissions could be limited to trading partner IP's as needed.

SMTP

The NYWIC application will generate SMTP based emails to various entities. Access to the ITS SMTP server from the business services tier will be required

Single Sign On

The NYWIC system will integrate with NYS SSO provider (ny.gov) using SAML. The design for this integration is under development and will be documented separately.

5. Data Center Environment

5.1 Bandwidth

Bandwidth inside the data center should meet the following requirements:

- Data center components connectivity should be 1 Gbps or faster. Virtual machines should allow 1 Gbps or faster for each virtual host.
- SAN connectivity should be Fibre Channel or 10 Gbps Ethernet
- Database server connectivity should be Fibre Channel or 10 Gbps Ethernet

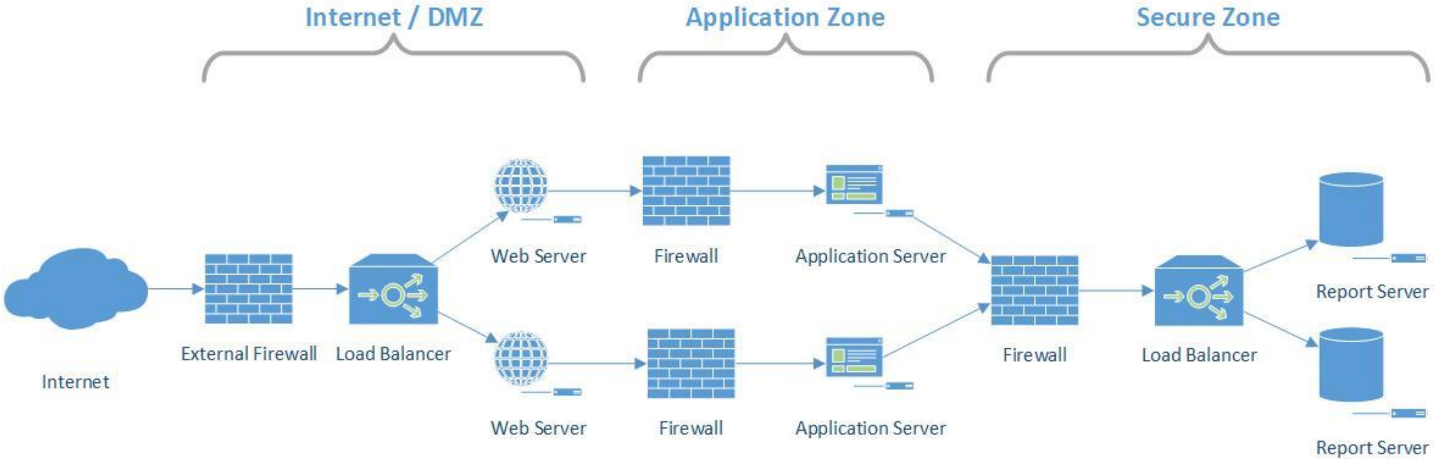
5.2 Firewalls

Each zone in the data center should be protected using an enterprise-grade firewall. The setup and configuration of firewalls is outside of the scope of this document will utilize existing ITS infrastructure. Where appropriate, this document will identify ports and protocols used in communications between infrastructure components to allow for firewall configuration.

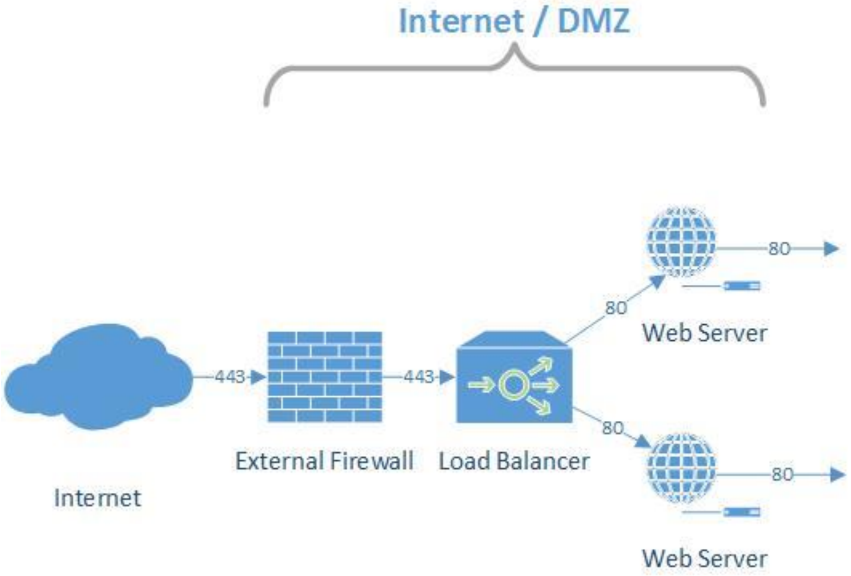
5.3 Load Balancing

Load balancing is a critical element in allowing the NYWIC system to support user workloads necessary for the NYS WIC program. There are several key elements of load balancing for the NYWIC system. These include the following:

- The load balancer in the DMZ should be configured to balance load across the web servers in the environment.
  - Hardware compression of outbound traffic should be enabled.
  - Least connections is likely the best model for balancing traffic.
  - If desired, port 80 traffic should be directed to port 443 by the load balancer.
- The application servers are paired with a web server and are not independently load balanced. Session state is stored in memory for maximum performance which prevents separate load balancing between the web and application tiers.
- A secure zone load balancer can optionally be used to load balance traffic to the SSRS report servers. Alternatively, these servers can be directly assigned to application servers.



There are several models available for encryption in this architecture. In the first, all traffic in and out of the DMZ is required to be encrypted SSL traffic on port 443. Decryption occurs at the externally facing load balancer and all internal traffic proceeds on unencrypted port 80 communications. This is the most common method used by states and offers both security and optimal performance. This approach is depicted below:



The second approach is to decrypt and re-encrypt traffic at every stop. This requires the installation of SSL certificates on every element of the infrastructure including load balancers, web, application, and database servers. This approach results in a significant added latency to data center response. The encryption methodology used is dependent on state security policies.

The data center should utilize two physical load balancing devices to maintain redundancy in the event of failure. The same physical load balancers can be used to balance traffic in multiple data center tiers. The web server and report server load balancing can be performed with the same physical hardware.

5.4 Storage Area Network

The NYWIC system will utilize the hosting data centers SAN infrastructure for:

- Transactional and reporting database files
- Mapped virtual server disks
- File storage for archived imported and exported files to external systems (e.g. EBT batch files)

The performance of the NYWIC system is dependent on the availability of reliable high-speed SAN resources. This infrastructure should include the following elements:

Connectivity – All SAN communications should be over Fibre Channel or 10 Gb Ethernet connections.

Database Files – Must be supported by high-speed low latency SAN storage. Documentation of best practices for the configuration of database access to SAN storage is outside of the scope of this document. It is critical that best practices be utilized the for separation of database file elements, LUN management, file growth configuration, and other considerations.

Testing - Data and log file latency should be tested prior to operation of the system to evaluate and document the baseline performance prior to NYWIC database installation and use.

Security – The SAN hardware must be physically secure. All traffic to the SAN should be managed and restricted to servers with explicit authorization. File shares used by the NYWIC system should be secured with appropriate ACLs to prevent unauthorized access.

5.5 Enterprise Services

NYS maintains several Enterprise Services within the data center environment. The use of Enterprise Services may be encouraged or required by NYS policies. Three Sigma is currently working with NYS DOH and ITS to define additional NYWIC requirements to implement integration with a number of NYS Enterprise Services including:

- AKANA (Web Service Proxy)
- Managed File Services – Sterling Commerce
- FileNet – Document management and anti-virus management
- Anti-virus Scanning

Once requirements have been defined, support for Enterprise Services may be added through NYWIC project change control. If so, the scope of changes will include updating the NYWIC – MIS Technical Architecture Document to reflect approved changes.

6. Hardware Components

The following are the recommended minimal specifications for the production/ DR hardware components.

Hardware role	Hardware Configuration
Web Servers	• Virtual Server • 2.0 GHz processor • 6 vCPU • 16 GB RAM • 40 GB OS Disk Space
Application Servers	• Virtual Server • 2.0 GHz processor • 6 vCPU • 32 GB RAM • 100 GB OS Disk Space • 750 GB Shared Disk Space (Accessible by all servers)
Report Server - SSRS	• Virtual Server • 2.0 GHz processor • 6 vCPU • 64 GB RAM • 100 GB OS Disk Space • 200 GB alternate Disk Space
Database Server	• Physical Server (or equivalent) • Quad 3.5 GHz 6-core processors (24 CPU) • 192 GB RAM • 100 GB OS Disk Space • 200 GB SSD (DB Acceleration) • 600 GB ASM FC-SAN (Initial allocation)
Database Server – Read Only Instance	• Physical Server (or equivalent) • 8 vCPU • 32-64 GB RAM • 100 GB OS Disk Space • 200 GB SSD (DB Acceleration) • Data storage per capacity plan
Application Acceleration	• F5 1600 or equivalent • 1 Gbps - load balancing • 1 Gbps - maximum software compression • 500 TPS - new SSL connections • 4 Million - max concurrent connections

The following are the recommended minimal specifications for the non-production hardware components.

Hardware role	Hardware Configuration
Web Servers	• Virtual Server • 2.0 GHz processor • 3 vCPU • 16 GB RAM • 40 GB OS Disk Space
Application Servers	• Virtual Server • 2.0 GHz processor • 3 vCPU • 31 GB RAM • 100 GB OS Disk Space • 250 GB Shared Disk Space (Accessible by all servers)
Report Server	• Virtual Server • 2.0 GHz processor • 2 or 4 vCPU (assuming 2 core license pack) • 32 GB RAM • 100 GB OS Disk Space • 200 GB alternate Disk Space
Database Server	• Physical Server (or equivalent) • Single 3.5Hz 6-core processors • 64 GB RAM • 100 GB OS Disk Space • 200 GB SSD (DB Acceleration) • 600 GB ASM FC-SAN (Initial Allocation)
Application Acceleration	• F5 1600 or equivalent • 1 Gbps - load balancing • 1 Gbps - maximum software compression • 500 TPS - new SSL connections • 4 Million - max concurrent connections

7. Software Components

The software needed based on Server Type.

Server Type	Software Configuration
Web server	• Windows Server 2012 R2 Enterprise Edition • IIS • .NET Framework 4.0 • Antivirus software • Backup software (for VM not per machine)
Application server	• Windows Server 2012 R2 Enterprise Edition • .NET Framework 4.0 • Antivirus software • Backup software (for VM not per machine)
Database server	• Oracle 12c Enterprise • High availability architecture (NYS determined) • Oracle Tuning Pack • Oracle Diagnostics Pack • Oracle Transparent Data Encryption or equivalent data at rest encryption solution • Active Database replication solution • Antivirus software • Backup software
Report Server	• Windows Server 2012 R2 Enterprise Edition • SQL Server 2014 Standard Edition • Antivirus software • Backup software (for VM not per machine)

8. Oracle Hosting

The Oracle hardware recommendations in this plan are based on prior experience with dedicated and shared hosting infrastructures in states using the WOW system. NYS utilizes a RISC based hosting architecture using IBM Power Systems POWER8 technologies. NYS ITS has identified two priorities:

1) To utilize the existing Oracle hosting investments with the state's preferred RISC architecture.
2) To provision Oracle as a service and to size servers based on actual utilization

Three Sigma acknowledges that the Oracle hosting recommendations provided in this document will not map directly to the NYS Oracle hosting technologies. Unfortunately, we have limited ability to provide a proven comparative mapping of prior successful hosting configurations to NYS hosting technologies. This document has been updated to reflect NYS decisions to create a read-only Oracle database instance for reporting and to modify VM hardware specifications to current generation 2.0 GHz processors being used by the NYS data center.

Three Sigma has reviewed existing states WOW server utilization and would like to provide the following recommendations for initial server configuration:

Oracle RAC Servers Supporting OLTP for NYWIC

Based on processor utilization in multiple states, we anticipate that each server in OLTP RAC will require up to the equivalent of 24 vCPU or dedicated cores as described in the hardware configuration above. The production environment currently has 3 vCPU allocated to each server. Based on IBM literature this appears to provide the equivalent of 6 vCPU of computing power in the proposed x86 based architecture. Three Sigma does not expect this configuration to be sufficient to support production workloads.

The processor requirements of these servers may be reduced by workload moved to the read-only reporting instance. Based on NYS participant levels, compared to Florida, we expect the processing requirements to be similar. Florida has modeled their Oracle capacity to allow one node of the Oracle RAC to fail without impacting clinic operations. This capability has been needed on two occasions. If NYS elects to model based on minimum performance requirements, the Oracle RAC may not serve the intended purpose to provide failover protection without execution of the Disaster Recovery plan. We view processing capacity to be critical for initial system performance. The ability (available in hosting environment without impacting other systems or acquiring hardware) to increase processing capacity up to the original 3 Sigma requirement during rollout is an important precursor to pilot start.

Memory configurations across WOW states have more variability. The recommendation in the Hardware Specification above is based on the best available reference system, Florida. As noted above, Florida requires that either node in the Oracle RAC can support statewide volumes without service interruption or degradation. The NYWIC system may perform well with a lower level of dedicated memory. Three Sigma would recommend an initial configuration of 64GB of dedicated memory per server in the OLTP RAC. To offset this increase, we are recommending a lower initial memory allocation to the read-only instance.

NYS intends to perform a NYWIC load test. This test will be performed on a system with very limited data and the most intensive transactional activity (EBT) will be excluded from testing. The plan also calls for testing during weekend hours. Three Sigma anticipates that this test will help to evaluate the web server infrastructure performance. We do not anticipate that the test will provide an effective evaluation of database requirements. The load modeled will not simulate production workloads and the server under load will not be serving other applications. Similarly, the network and storage infrastructure will not be tested based on accurate data volumes or concurrent workload. Reducing recommended database hardware based on the results of load testing may result in operational failures during NYWIC rollout.

Read-Only Oracle Instance

The NYWIC system will support a large volume of user report requests. However, most requests will be relatively simple reports utilized by clinic staff. The creation of a data warehouse will move many complex report functions to other environments. Based on this understanding, Three Sigma recommends the equivalent of an 8-vCPU allocation per the Hardware Specifications above. These servers are currently allocated 80 GB of memory. Three Sigma recommends an initial allocation of 32 GB with the potential to increase to 64 GB if needed. We believe that increasing the initial allocation of memory to the transactional servers will optimize initial performance and scalability of the NYWIC system.

9. Server Listing

This section will identify and quantify of each Server type needed to support five environments; Development, Quality Assurance, UAT/Stage/Training, Production, and Disaster Recovery. There are a wide variety of server configurations that could be used to meet the needs of the NYS WIC program. Based on the proposed infrastructure in the RFP, the following assumptions have been made:

1) The quality assurance environment is intended to mirror production architecture with load balancing to allow for testing in a production configuration.
2) There is a desire for separation of development, quality assurance, UAT, training, and data conversion on separate physical/virtual servers.
3) There is relatively little discussion of disaster recovery SLA's. As a result, the proposed configuration assumes nearly 100% production capacity for continuing clinic operations.

Based on these assumptions the following server configuration is recommended:

Environment	Web	Application	Database	Report	F5
Development	1	1	1	1	0
Quality Assurance	2	2	1	1	1 or 2
UAT/Training	1	1	1	1	1
Production	4	4	2	2	2
Disaster Recovery	4	4	2	1	1

Based on the NYWIC architecture, it is relatively simple to create multiple NYWIC web site instances on the same server hardware. These sites can simply have their own URLs and associated IP addresses. One possible alternative would be to use one set of improved hardware to host all non-production (Production & DR) environments. In this configuration, the server requirements would look like the following:

Environment	Web	Application	Database	Report	F5
Development, Quality Assurance, UAT, Training, and Data Conversion	2	2	1	1	1 or 2
Production	4	4	2	2	2
Disaster Recovery	4	4	2	1	1

There are also options in the disaster recovery tier. With less emphasis on redundancy within the DR environment, the number of physical/virtual web and application servers could be reduced. An analysis of disaster recovery SLAs may allow for refinement and improvement of the recommended hardware.

Disaster Recovery Recommendation

There are a variety of options for reducing the cost of the DR environment. Three Sigma would recommend the following limitations be considered:

1) Remove the Read Only Oracle instance – During a DR event, reporting should be limited to critical clinic reports needed to deliver services to participants. These reports are generally simple in design and do not generate significant load. If the state needs to perform complex reports as part of the disaster response, they should be run off hours to avoid conflict with the daily transactions. All reports will be configured to execute against the OLTP database.
2) Remove redundancy/high availability in the Oracle server – Because the primary environment already has redundancy in the Oracle database to reduce the likelihood of failover to the DR environment, maintaining high availability in DR is a third level of redundancy. This can be removed to reduce cost while maintaining appropriate redundancy within the system.
3) Single report server – With limited report execution, the SSRS SQL Server can be limited to a single unit.
4) Web and Application servers – It is difficult to forecast the ability to reduce hardware without production statistics. In general, DR should be limited to critical operations. Three Sigma would recommend that as server utilization data is collected during rollout, a calculation of minimal web and application server hardware be derived. Emphasis should be on memory needed to cache session state and processor availability. It may be possible to reduce servers to alternatively reduce vCPU/Memory on servers. The program will also need to consider policies to limit activities to issuance which would significantly reduce transactional volumes.
5) Oracle Server – The same approach to monitor utilization during rollout and consideration of NYS WIC policies for limited usage during a disaster should be considered in reducing the capacity of the database server. Removing the distributed load of a high availability solution may already reduce computing capacity.

The production environment needs a High Availability design to provide redundancy in all three application tiers. We propose;

Count	
2	F5 load balancers or equivalent
4	Virtual Web servers
4	Virtual Application servers
1	Oracle high availability database servers (2 servers)

1 Oracle read-only database server for replicated reporting instance.

2 Virtual SSRS servers

The above list presumes that all necessary enterprise firewall, switching, SAN, and networking infrastructure is determined and in place.

This configuration will align the hardware specifications with other large States using the same system.

State	Caseload	Avg. Daily Users	# of Web/App Cores	# of DB Cores
Michigan	243,000	480	32	32
Florida	481,000	900	56	48 (2x24)
New York	554,000	1100	64	48 (2x24)

Oracle High Availability Database

The Oracle hardware recommendations within this document are based on Three Sigma's experience using Solaris based Oracle servers in a Real Application Cluster (RAC) high availability configuration. Three Sigma understands that New York will likely utilize a different high availability mechanism on AIX based Oracle servers. Three Sigma has relatively little data to map a reference Solaris RAC configuration to an alternative high availability Oracle configuration on AIX. The Three Sigma team will provide comparative real world utilization data and provide assistance to the NYS ITS team as they develop internal hardware recommendations based on the state's Oracle practices and hosting investments.

10. Clinic and Local Agency Infrastructure

10.1 Hardware Requirements

The NYWIC functionality will be accessed using a web browser. The web site operates without writing data to local storage and with memory usage consistent with normal web sites running within the selected web browser. Users of the system may have local drivers installed for scanners, printers, and signature pad hardware. These will require limited storage space and memory utilization.

Because of these limited requirements, NYWIC should run on any machine that is equipped with the Microsoft minimum recommended hardware specifications for the operating system in use. The single exception to this rule is the need for NYWIC to run in at least a 1024x768 screen resolution to have a good user experience. The current minimum hardware specifications for Windows 10 are the following:

M**icrosoft's Windows 10 Minimum Hardware specifications**

Processor: 1 gigahertz (GHz) or faster processor or SoC

RAM: 1 gigabyte (GB) for 32-bit or 2 GB for 64-bit

Hard disk space: 16 GB for 32-bit OS or 20 GB for 64-bit OS

Graphics card: DirectX 9 or later with WDDM 1.0 driver

Display: 1024 x 768 (Increased from Microsoft's 800 x 600)

Microsoft's minimum specification is far below what most commonly available PC models ship with today. As of the creation of this document, the lowest line of Dell workstations for business use starts with a 2.8 GHz Celeron processor, 4 gigabytes of memory, and a 500-gigabyte hard drive. Many of the primary considerations for hardware selection should be based on the expected additional application usage, software installation, and other concurrent activities to be conducted on NYWIC workstations while running the NYWIC web site. Likely software includes:

- Other web sites open, both professionally required (e.g. nutrition education) and non-work related.
- Microsoft Office
- Adobe Reader (PDF)
- Antivirus
- Hard disk encryption
- Others

These variables make providing a minimum recommendation challenging and the ultimate decision is best evaluated by local personnel combining the understanding of NYWIC requirements with other uses. With that limitation noted, the following specification is likely to provide reasonable performance in a clinic environment.

Reference Hardware Specification

Processor: 2 gigahertz (GHz) or faster processor or SoC

RAM: 4 gigabyte (GB) for 32-bit or 64-bit

Hard disk space: 200 GB, potentially less for a laptop or SSD equipped machine

Graphics card: DirectX 9 or later with WDDM 1.0 driver

Display: 1024 x 768

NYWIC will generally not perform significantly “better” with more memory and a faster processor but may perform slower if a workstation has either memory or CPU contention.

10.2 Web Browsers

NYWIC will support a wide variety of current web browsers. NYS WIC may elect to limit sanctioned web browsers to reduce potential help desk support requirements across a wider variety of browsers. This decision is left up to the program based on applicable policies and the degree to which local agencies have autonomy for technology decisions. The NYWIC system is intended to work with the following web browsers:

- Internet Explorer
- Edge
- Chrome
- Firefox

It is possible and likely that the web site could operate in other browsers but this list constitutes the clear majority of the current browser market. Three Sigma cannot guarantee future support with browser updates but based on the technologies in use, a loss of compatibility that could not be resolved is unexpected. Due to the number of web browsers available to users and the pace of upgrades in the marketplace, Three Sigma would recommend that NYS use a current version or current minus one policy for its users. This approach helps to limit the number of browsers being supported and to ensure that users are working with software that is currently under support to meet evolving security threats.

10.3 Other Software

This section is intended to discuss additional software that is either required or recommended on client workstations. Drivers associated with peripherals will be discussed in a later section. Depending upon user roles the following software may also be needed for NYWIC use:

Microsoft Word – The NYWIC system allows certain users to generate mail merge templates and a broader user base to generate Word documents using mail merge functions. Users with these privileges will need to have Microsoft Word installed on their workstation. Both Office 365 and MSI based versions of Word are compatible with NYWIC.

Microsoft Excel – The NYWIC system can generate report output or file outputs in comma separated value files (CSV). Users with these privileges may require Microsoft Excel to view and work with file outputs. Both Office 365 and MSI based versions of Word are compatible with NYWIC.

Adobe Reader – NYWIC reports are generated in PDF document formats. All users of NYWIC will require the installation of Adobe Reader on their workstations to view report outputs. Three Sigma recommends that policies exist to either automate or request that users apply regular updates to their Adobe software to maintain current patch levels.

Antivirus and Anti-Malware Software – The use of antivirus software is not a direct NYWIC requirement but as with any system that maintains sensitive information, users that access NYWIC should have antivirus and anti-malware software installed that meet state and local security policy requirements. Software and definition updates should be applied on a regular basis per best practices.

Browser Extensions – Some browser extensions may interfere with the operation of the NYWIC web site. Users should be discouraged from installing browser extensions that alter the appearance or navigation within web sites

Encryption – If the state policy requires that data be encrypted at rest in the clinic setting a full disk encryption tool can be used. NYWIC is designed to not store documents and data locally but users may store files and cached data may reside on the local hard drive.

10.4 Patch / Update Management

Due to the sensitive nature of the data housed within the NYWIC system, Three Sigma recommends that all workstations used to access NYWIC be maintained to current operating system, web browser, and security patch levels per applicable state and local security policies and procedures.

10.5 Local Area Networks

For those clinics and local agencies that work on a local area network, the minimum recommended network connection would be 10 Mbps or faster and 100 Mbps of faster would be preferable, particularly for larger agencies.

10.6 Site and Clinic Internet Connections

General Recommendations

Based on typical NYWIC web request sizes (5-10 KB) and typical response sizes (25-100KB) the average NYWIC user actively navigating the system will require a relatively small amount of bandwidth. However, the generation of large reports and other less frequent activities have the potential to create intermittent demands for significantly higher bandwidth. To calculate the estimated bandwidth requirements, the peak number of concurrent NYWIC users should be calculated. Internet connectivity should be based on:

- Minimizing latency which will significantly improve performance
- A minimum of 256Kbps of downstream bandwidth should be available per NYWIC user
- Upstream bandwidth should be at least 50% of downstream requirements.
- Bandwidth requirements should be increased for locations with fewer users to prevent slow performance when transferring larger files. Downloading reports and uploading documents require higher short term bandwidth usage. User experience should be considered when working with small sites.

Competing Usage

There are a variety of common competing uses of Internet bandwidth that must be considered when estimating bandwidth requirements for NYWIC users. Common alternative uses include:

- Other public health systems utilized in the same facility
- WIC related web site access (e.g. nutrition education)
- Web meetings
- IP Phone systems
- Non-work related activities (e.g. video streaming)

Unfortunately, many of the potential competing uses of bandwidth require significantly higher bandwidth than the NYWIC system. A careful and realistic estimation of total bandwidth consumption is critical to bandwidth planning.

Asymmetric Connections

Many commercially available Internet connections provide asymmetrical bandwidth. The most common example would be Cable Modem based connections which typically feature high speed data downloads but relatively limited upload speeds. Although much of the user activity in NYWIC will require more download capacity, some key features, like document scanning, require significant upload capacity. Where possible, the use of symmetric Internet connections is recommended. Where not possible, a minimum of 128 Kbps of upstream bandwidth is recommended for each concurrent user.

Wireless Access

NYWIC will operate on any wireless network that meet the general latency and bandwidth requirements. The use of wireless networks does present additional security challenges due to the potential for misconfiguration and security vulnerabilities. Three Sigma recommends that the use of wireless connections be governed by state and local security standards and that wireless networks be audited to ensure that they are in compliance with published standards.

Quality of Service

Clinic networks may support traffic from a variety of devices including Voice-over-IP (VoIP) systems. In these environments, network routers and other equipment may need to be configured to segregate traffic by priority to ensure that competing traffic does not create interference. This process is typically referred to as applying quality-of-service (QoS) rules.

11. Other Specialized Equipment

- Signature Pad device

  The system interacts with properly installed devices that are compatible with SIGPLUS or eSign3 libraries. The following list of devices are currently supported in Production systems in other States. Experience has shown that other models by the same manufacturer have been seamlessly integrated, especially when the screen display size is the same.

  - ePad ink /USB
  - Topaz Signature Pad, model# : T-LBK755–BHSB–R

  If New York selects a newer device from this manufacturer a cursory test will be done to check compatibility. These devices install an~~d~~ ActiveX control that allow for interaction between the NYWIC web site and the signature pad hardware.

- EBT Card Reader device

  Interaction with this device does not require any special installation. The Card number is entered in text boxes as it is swiped because the device acts as a keyboard wedge. Many hardware devices will interact successfully with the NYWIC system.

  MagTek

  MagTek is one card reader that has been used by states to read EBT card IDs. The MagTek card reader is a plug-and-play device. Drivers do not need to be manually installed for this device, simply plug the device into an available USB port and Windows should recognize the new attached hardware.

  To test the device, you can swipe any normal sized magnetic strip card through the device. If the LED light on the device turns green, the magnetic strip on the card was successfully detected. Data from the card will be placed into the keyboard buffer and entered into the cursor location on any active application including NYWIC.

- Scanning device

The HP LaserJet series of scanners and many scanners compatible with the TWAIN specification are supported in the NYWIC MIS system. After following the devices' installation instructions, and confirming the device is operational using the Manufacturer software, images can be scanned directly into the application. Check the device for TWAIN or HP LaserJet compatibility.

Three Sigma recommends that NYS identify identifies either targeted models for procurement or common models already in use. Evaluation units should be obtained for testing during UAT. Targeted user instructions for installation and configuration should be developed to allow for consistent compatibility with NYWIC in field use.

- Printers

Printing in NYWIC relies on Windows underlying print spooler and print services. If Windows can send a document to a printer, NYWIC should be able to send a document to that printer as well.

- Bar Code Scanners

Should NYS WIC have a need for a bar code scanner there are hundreds of devices on the market that can scan UPC and other barcode formats. The key consideration for selection of hardware will be to identify a unit that is intended to act as in input device placing barcode data in the keyboard buffer. There are many handheld scanners that connect to a USB port capable of this function.

Devices may require a manufacturer supplied driver. Once installed, the device will allow users to scan barcodes and to record the barcode data in the cursor location. A trial unit should be procured to allow for testing and evaluation of scanner models.

- Pin Pad

Conduent does not currently offer pin pad support.