



The Statewide Collaboration Process



**Statewide Health Information Network for New York
(SHIN-NY) Information Security Architecture and
Requirements V1.0**

November 3, 2008

TABLE OF CONTENTS

1.0	Summary of Information Security Architecture and Requirements	1
2.0	Information Security Policies	2
2.1	High Level Information Security Policies	2
2.2	Privacy and Security Work Group Policies	2
2.3	IHE Profile Controls	3
3.0	Review of Relevant Standards and Guidelines	3
3.1	The ISO/IEC 27000 Family	4
3.2	WS-Security: SOAP Message Security from OASIS	5
3.3	Gartner's "Best Practices Checklist for Web Services Security, 2006"	5
3.4	NHIN Draft Interface Specification: Messaging Platform v1.9	6
3.5	IHE Information Technology Infrastructure Technical Framework.....	7
3.6	HITSP TN 900 Security and Privacy.....	7
4.0	Architecture.....	7
4.1	Federation Over Three Tiers of Trust	7
4.2	Defining a Base-Line of Information Security	9
5.0	Requirements	11
5.1	Base-line Information Security	11
5.2	Consistent Time	12
5.3	Secure Nodes	13
5.4	Public Key Infrastructure (PKI).....	14
5.5	Secured Communication Channel.....	14
5.6	Entity Identity Assertion.....	15
5.7	Access Control	15
5.8	Collect and Communicate Security Audit Trail.....	16
5.9	Manage Consent Directives	17
5.10	Manage Sharing of Documents with Document Integrity	18
5.11	Nonrepudiation of Origin.....	18
	Appendix A – Detailed Checklist	19
	Appendix B – Map between 4As and Security Requirements.....	19
	Appendix C – Map between Consent Management and Security Requirements	19
	Appendix D – Protocols and Services Work Group Members	19

VERSION HISTORY

Version #	Implemented By	Revision Date	Description
0.1	Chris Shull	October 20, 2008	UPHN draft document for review by Subgroup
0.2	Chris Shull	October 28, 2008	First real SHIN-NY draft derived from UPHN draft document
0.3	Sean Kelly	November 3, 2008	Edited in conformance with NYeC Style Guide

1.0 Summary of Information Security Architecture and Requirements

The purpose of this document is to provide an overview of the information security architecture and requirements for NYS DOH HEAL 5 awardees as determined by the Statewide Collaboration Process (SCP) and the technical analysis efforts of the NYeC¹ Protocols and Services Work Group. The scope of this document is to provide a framework for HEAL 5 Awardees to implement information security policies, architecture and technologies required for participation in the Statewide Health Information Network for New York (SHIN-NY).

This SHIN-NY Information Security Architecture and Requirements document is a formal statement of security policies and measures that supplements the current activities of the Protocols and Services Work Group. It will be used for the following:

- Designing and developing systems and services that may be used on the SHIN-NY
- Evaluating the SHIN-NY
- Determining the success of the SHIN-NY project.

The SHIN-NY Information Security Architecture and Requirements document provides information for two different audiences. First is the "Policy" level for business people, clinicians and executives, followed by the "Architecture and Requirements" level for developers, implementers and operators.

Each requirement in this document has the following characteristics:

- It demonstrates that the SHIN-NY provides value to the State of New York in terms of the business objectives and business processes.
- It leaves no room for anyone involved with the SHIN-NY to assume anything not stated in the requirements.
- It is solution independent at the vendor level.
- It describes the security capabilities the SHIN-NY must provide in business terms.
- It does not describe how the SHIN-NY provides that capability.
- It is stated in unambiguous words. Its meaning is clear and understandable.
- It is verifiable.

The Requirements include base-line requirements for Information Systems seeking to meet the Security Policy goals of maintaining Confidentiality, Integrity and Availability, but focuses primarily on measures and mechanisms that are less obvious to Information Systems practitioners. Thus while system availability can generally be enhanced through use of a range of fault-tolerant technologies such as clustered servers, RAID systems, uninterruptible power supplies, and backup network connections, the Cost-Benefit Analysis to weigh a given organization's

¹ NYeC = New York eHealth Collaborative

willingness or ability to implement such protections against its tolerance or appetite for risk is beyond the scope of this document.

Organizations seeking a methodology for assessing these risks and options should see the ISO/IEC 27001 section (3.1) below.

This document will focus on base-line requirements that are most closely related to the function of the SHIN-NY.

This document relies on many diverse standards, guidelines and other documents that were intended for different audiences and application areas. As such, it is appropriate to provide greater or lesser detail or explanation when referring to these documents. Typically, the more comprehensive and directly applicable one of these source documents is to this one, the less needs to be written here, and the more the original source is simply referenced. For less connected sources, more is typically written to compensate or create the material connection.

2.0 Information Security Policies

SHIN-NY requires implementation of standard industry measures as well as additional special measures appropriate for the special needs of the SHIN-NY.

2.1 High Level Information Security Policies

The SHIN-NY requires policies to motivate the implementation of technologies and processes to protect the Confidentiality, Integrity and Availability of health information.

At the highest level, the security policies of the SHIN-NY are:

- 1) Data shall be kept confidential with access available only to duly authorized actors.
- 2) Data shall be protected from accidental and deliberate corruption or loss.
- 3) Data shall be available in a timely manner.

These high-level policies can be made more specific as NYeC and SHIN-NY participants gain greater understanding of their detailed security requirements.

2.2 Privacy and Security Work Group Policies

The simple high-level policies are also being enhanced by policies from the Privacy and Security Work Group. Directly applicable to Confidentiality, Integrity and Availability are the requirements from the 4As Subgroup.

The 4As Subgroup has published a set of Policy Requirements, mapped to CCHIT requirements as appropriate, and to an Implied Functional Requirement for EHR, HIE and PHR Technologies. In general these address the need for system and application supports in the areas of Access/Breach, Audits, Authorization and Access Controls. Specific requirements are mapped to the sections of this document that address them in the table in Appendix B.

Policies from the Consent Management Subgroup are similarly important inputs and will guide implementation of Consent Management functions described in Section 5.9 below. Specific requirements are mapped to the sections of this document that address them in the table in Appendix C..

A policy is still needed to guide and govern transition periods for implementation of vital security requirements. This will be true during the initial deployment of the SHIN-NY, and as requirements evolve and require technologies and processes to evolve with them. Initially this transition period will have to be on a best effort basis, with much information sharing to help ensure consistent, or at least comparable and compatible levels of implementation across different organizations. Eventually a formal audit or review process should be established to ensure compliance with security requirements.

2.3 IHE Profile Controls

The "IHE IT Infrastructure White Paper - HIE Security and Privacy through IHE Profiles", Version 2.0, August 22, 2008 provides an expanded list of controls necessary to protect the security and privacy of health information:

- 1) Accountability Controls – The controls that can prove the system is protecting the resources in accordance to the policies. This set of controls includes security audit logging, reporting, alerting and alarming.
- 2) Identification and Authentication Controls – The controls that prove that a system or person is who they say that they are. For example: personal interactions, Digital Certificates, security assertions, Kerberos, and LDAP.
- 3) Access Controls – The controls that limit access by an authenticated entity to the information and functions that they are authorized to have access to. These controls are often implemented using Role Based Access Controls.
- 4) Confidentiality Controls– As sensitive information is created, stored, communicated, and modified; this control protects the information from being exposed. For example: encryption or access controls.
- 5) Data Integrity Controls – The controls that prove that the data has not changed in an unauthorized way. For example: digital signatures, secure hash algorithms, CRC, and checksum.
- 6) Non-Repudiation Controls – The controls that ensure that an entity cannot later refute that they participated in an act. For example author of a document, order of a test, prescribe of medications.
- 7) Patient Privacy Controls – The controls that enforce patient specific handling instructions.
- 8) Availability Controls – The controls that ensure that information is available when needed. For example: backup, replication, fault tolerance, RAID, trusted recovery, uninterruptible power supplies, etc.

3.0 Review of Relevant Standards and Guidelines

Much work has been done by many groups and organizations to provide standards and guidelines in support of these Policies. This section provides a quick overview of some of the most relevant ones.

Several standards and best practice guidelines speak to these needs -- from general IT Security Management to Health Information Exchange specific needs:

- 4.1 The ISO/IEC 27001 family (most notably 27001 and 27002)
- 4.2 OASIS's "Web Services Security: SOAP Message Security" version 1.1 also known as WS-Security or WSS
- 4.3 Gartner's "Best Practices Checklist for Web Services Security, 2006"
- 4.4 NHIN Draft Interface Specification: Messaging Platform v.1.9
- 4.5 IHE Information Technology Infrastructure Technical Framework
- 4.6 HITSP TN 900 Security and Privacy

3.1 The ISO/IEC 27000 Family

The standard for information systems security in general is the ISO/IEC 27000-series. Also known as the 'ISMS Family of Standards' or 'ISO27K', which comprises information security standards published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Wikipedia notes:

"The series provides best practice Requirements on information security management, risks and controls within the context of an overall Information Security Management System (ISMS), similar in design to management systems for quality assurance (the ISO 9000 series) and environmental protection (the ISO 14000 series).

The series is deliberately broad in scope, covering more than just privacy, confidentiality and IT or technical security issues. It is applicable to organizations of all shapes and sizes. All organizations are encouraged to assess their information security risks, and then implement appropriate information security controls according to their needs, using the guidance and suggestions where relevant. Given the dynamic nature of information security, the ISMS concept incorporates continuous feedback and improvement activities, summarized by Deming's "plan-do-check-act" approach, that seek to address changes in the threats, vulnerabilities or impacts of information security incidents.

The published standards to date in the ISO 27K family are:

1. ISO/IEC 27001 - the certification standard against which organizations' ISMS may be certified (published in 2005)
2. ISO/IEC 27002 - the code of practice with good practice advice on ISMS (previously known as ISO 17799 and before that BS 7799 Part 1 (last revised in 2005, and renumbered ISO/IEC 27002:2005 in July 2007)
3. ISO/IEC 27006 - a guide to the certification/registration process (published in 2007)"

(Source: Wikipedia. http://en.wikipedia.org/wiki/ISO/IEC_27000-series)

Overall, the ISO/IEC 27000 standards provide a comprehensive approach, process and guide any organization can use to establish the policies, procedures, people and technologies necessary and appropriate for that organization and the risks it faces.

Any organization would do well to review the complete standards, and the ISO27K Toolkit available at http://iso27001security.com/html/iso27k_toolkit.html to ensure it is following best practices, but for the purposes of the SHIN-NY, focusing on the following is appropriate:

- Clause 10: Communications and Operations Management
- Clause 11: Access control
- Clause 12: Information Systems Acquisition Development and Maintenance

- Clause 13: Information Security Incident Management
- Clause 14: Business Continuity Management

Each of these areas suggests methods and mechanisms by which risk can be managed and policies supported. The processes for risk management and security policy are covered in Clause 4 and 5 respectively, but are generally outside the scope of this document.

However, going back to the three high-level policies from above, the clauses each deal with various threats to our core goals, that:

- 1) Data shall be kept confidential with access available only to duly authorized actors;
- 2) Data shall be protected from accidental and deliberate corruption or loss; and
- 3) Data shall be available in a timely manner;

3.2 WS-Security: SOAP Message Security from OASIS

WS-Security (Web Services Security or WSS) from the Organization for the Advancement of Structured Information Standards (OASIS) is a protocol for applying security to Web services. The protocol contains specifications on how integrity and confidentiality can be enforced on Web services messaging. The WSS protocol includes details on the use of SAML and Kerberos, and certificate formats such as X.509. WS-Security describes how to attach signatures and encryption headers to SOAP messages and how to attach security tokens, including binary security tokens such as X.509 certificates and Kerberos tickets, to messages. By including security features in the header of a SOAP message at the highest (application) level of the protocol stack, it ensures end-to-end security.

In point-to-point connections data confidentiality and integrity could additionally be ensured through the use of Secure Sockets Layer (SSL) or Transport Layer Security (TLS). However, WS-Security maintains integrity and confidentiality of messages even when they are stored and after they are transmitted.

See <http://www.oasis-open.org/specs/index.php#wssv1.1> for an overview of WSS and <http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf> for the full text of the Core Specification.

3.3 Gartner's "Best Practices Checklist for Web Services Security, 2006"

Gartner's "Best Practices Checklist for Web Services Security, 2006" zeroes in on web services security risks not called out by ISO27K. These risks are really special cases of others that are in the ISO standard, but due to the role Web Services play in the SHIN-NY design and implementation, it is important to focus on these operational and developmental risks.

3.4 NHIN Draft Interface Specification: Messaging Platform v1.9

The Nationwide Health Information Network (NHIN), Interface Specifications, Messaging Platform, V 1.9, 06/16/2008 is based on the use of web services, using interoperability profiles from the Web Services Interoperability Organization (WS-I). The WS-I Basic Profile and WS-I Basic Security Profile together define a common platform for secure and reliable exchange of messages between HIEs in a vendor independent framework.

The Messaging Platform describes the common web service protocols that should underlie every message transmitted between HIEs.

The Platform is based on the following architectural principles:

1. There shall be a common transport layer for all messages.
2. Messages between NHIEs must be secure from end to end, recognizing that there may be intermediate nodes in the message delivery process.
3. The common message envelope must support assertions about security and trust between NHIEs.
4. All NHIE participants shall use a common standard for authentication and non-repudiation. All NHIE to NHIE messages must be digitally signed for purposes of authentication and non-repudiation.
5. The NHIN shall be based on interoperability profiles that have been fully approved as an industry interoperability standard and are capable of being implemented by NHIN Trial Implementations using available SOA platforms.

Note that only principles 2, 3 and 4 are explicitly related to security.

These requirements drove selection of the following underlying messaging standards for communication between NHIEs using an SOA platform:

1. Messages: SOAP
2. Service Descriptions: WSDL
3. Service Discovery: UDDI
4. Attachments: MTOM
5. Addressing/Routing: WS-Addressing
6. Security: WS-Security
7. Authorization Assertions: SAML
8. WS-I Basic Profile
9. WS-I Basic Security Profile

Note that only standards 6, 7 and 9 are explicitly related to security.

3.5 IHE Information Technology Infrastructure Technical Framework

IHE's Information Technology Infrastructure Technical Framework (IHE ITI TF) provides invaluable guidance for the organizations seeking to actually deploy secure health information exchange systems.

Section 9 Audit Tracking and Node Authentication (ATNA) is the critical portion of the IHE ITI TF. It ensures that every actor allowed access to the IHE is known and that all actions with implications for security – confidentiality, integrity or availability – are recorded in a secure audit trail to ensure appropriate behaviors by actors.

The key subsections of ATNA are:

- Section 9.1 Authentication
- Section 9.2 Audit Trails
- Section 9.3 Audit Trail Transport

3.6 HITSP TN 900 Security and Privacy

HITSP TN 900 Security and Privacy consolidates the security and privacy details from several other HITSP document in one location. The source documents are:

- HITSP/T15 - Collect and Communicate Security Audit Trail
- HITSP/T16 - Consistent Time
- HITSP/T17 - Secured Communication Channel
- HITSP/C19 - Entity Identity Assertion
- HITSP/TP20 - Access Control
- HITSP/TP30 - Manage Consent Directives
- HITSP/TP13 - Manage Sharing of Documents with Document Integrity inserted as an option
- HITSP/C26 - Nonrepudiation of Origin

These HITSP standards are essential components of the SHIN-NY ESB, although they also contain requirements which are not strictly security related.

More will be said about the role each plays in the sections on Architecture and Requirements.

4.0 Architecture

4.1 Federation Over Three Tiers of Trust

The Information Security Architecture of the SHIN-NY is a networked federation of nodes that operate independently but collaboratively over three tiers or levels of trust.

At its core is the SHIN-NY ESB or "Big Bus". These systems provide the essential infrastructure services, strictly adhere to the security policies and requirements described in this document, and primarily communicate with one another and the systems in the second tier.

The second tier of trust and security is for the RHIO HIE (RHIO-managed Health Information Exchanges) ESB's, or "Little Buses". These systems provide and consume the services advertised and brokered by the SHIN-NY ESB. These systems are the essential middlemen, communicating with systems external to the RHIO through the Big Bus and directly with the various health information systems within each RHIO's jurisdiction. Little Bus nodes must be maintained as Secure Nodes (defined below) with a Base-Line of Information Security. All communications between these nodes and with nodes in the Big Bus must adhere to the security requirements of this document.

The third tier includes all other systems, including all other information systems within each RHIO's jurisdiction and those of their participating organizations. These systems communicate with RHIO HIE ESB's (Little Buses), to query for information and to provide it. The manner in which these community systems are secured and how they communicate with the RHIO HIE ESB's is outside the scope of this document, although appropriate security measures are also essential for them.

This network topology reflects the NYeC governance model: community institutions are participants in RHIO's, and RHIO's are participants in the Statewide Collaboration Process (SPC) administered by NYeC. Community systems are the endpoints that directly support clinical care. RHIO HIE systems enable interoperability of community systems, providing substantial value since most healthcare information flow today is within the community. The SCP governs the systems providing interoperability between RHIO HIE systems, enabling more efficient access to state or national resources (Medicaid, CDC) and supporting important public health efforts (such as Quality and UPHN) in addition to direct exchange of information between RHIO HIEs. There are natural segregations of system capabilities that follow. For example, some core services will be required only between nodes of the SHIN-NY ESB, such as UDDI Registry synchronizations, and will therefore be restricted to this group.

Thus the Architecture builds from a core foundation of Secure Nodes (defined below) that comprise the SHIN-NY. Each of these nodes maintains a Base-Line of Information Security, and uses modern encryption-based technologies to ensure:

- 1) that every Secure Node only interacts with other Secure Nodes,
- 2) that their communications are secure, protected not only with respect to the confidentiality they afford their messages, but their integrity and availability as well,
- 3) that documents can be shared and their integrity validated and assured, and lastly,
- 4) that the origin of documents and changes to documents cannot be repudiated.

Access Control and Entity Identities are enforced locally under a federated trust umbrella. In short, each Secure Node is responsible for authenticating and identifying its users and processes, and for determining what access is permitted for requests from other nodes, trusting those other Nodes to have properly proved the sources of those requests.

Underpinning all of this must be a robust and comprehensive security audit trail. Nearly every access and attempted access must be recorded in a special Secure Node called the Audit Repository. The Audit Repository provides storage of security audit records and is also the data source for automatic, mandatory audit alerts (such as when a "break the glass" privacy override is used), routine audit reports, and ad hoc audit reports.

Logically these requirements can be inferred to include all Health Information Systems connecting with or exchanging data with SHIN-NY systems. However, from an implementation point of view, this becomes difficult or impossible.

The question therefore arises as to where to demark the boundary between systems that must fully comply with all SHIN-NY Information Security requirements, from those that do not. This is the role of the RHIO HIE ESB (Little Bus) that provides connectivity between systems that do not meet the requirements of ATNA Secure Nodes (see Section 5.3) and those that do.

All of the architectural requirements above are clearly and completely defined by other standards as indicated in Section 5, except for "Base-Line of Information Security", which we define in the next section.

4.2 Defining a Base-Line of Information Security

Unfortunately, most healthcare-focused standards assume the existence of basic security provisions, and do little to specify security requirements.

Nevertheless, implementations must be within a context of fundamental Information Security policies, procedures and technologies.

The "IHE IT Infrastructure White Paper - HIE Security and Privacy through IHE Profiles" mentioned in Section 3.3 identifies eight key controls for ensuring security in health information technology.

The ISO/IEC 27000 series of standards provide a holistic and comprehensive approach to assessing and mitigating these risks. The standards can be used to prepare for and obtain certification or as the foundation for developing new organizational best practices. Full ISO27K certification is desirable, but generally beyond the capabilities of many organizations. And although it could be considered the best practice for Information Security management, one need not gain ISO 27000 Certification to gain considerable benefits from using its processes.

These guidelines provide for a wide range of basic protections, from doing background checks for systems administrators, to having system-level fault-tolerance for disk storage, backups for disaster recovery, practiced business continuity plans, uninterruptable power supplies, and protections against network attacks, viruses, theft or loss of mobile devices, physical intrusions, loss of cooling, and incompetent or malicious staff.

It is beyond to scope of this document to detail all the potential risks and the associated counter-measures for the SHIN-NY ESB.

That said, several Information Systems Security areas specific to a modern HIE environment warrant special attention:

- 1) Internet Connectivity and System Availability
- 2) Firewalls and DMZs
- 3) Protecting Web Services through Firewalls

1) Internet Connectivity and System Availability

An HIE environment will require highly available system and Internet connectivity, probably in the range of 99.9% to 99.99%.

Reliability Goals	Availability	Downtime per week
Five 9s	99.999%	6 seconds
Four 9s	99.99%	1 minute
Three 9s	99.9%	10 minutes
Two 9s	99%	1.68 hours

If the cost of improving reliability is prohibitive, the organization must develop procedures for dealing with routine downtime.

2) Firewalls and DMZs

Firewalls are used routinely in Healthcare Organizations to restrict traffic in and out of their networks.

However, it is less common for them to partition their networks with DMZs to isolate Internet accessible servers from other critical systems and end-user computers. This is an important tool as organizations expose more services on the Internet.

3) Protecting Web Services through Firewalls

Firewalls also do little to protect systems from transactions that are actually permitted. Gartner recommends a set of processes and technologies for all across-the-firewall transactions, starting with software design requirements and development processes, through operational procedures and technologies.

Some of the most important are as follows:

- 1) Scan XML messages for generic threats including schema poisoning, routing detours, coercive parsing, XQuery injection, virus laden XML attachments and denial-of-service attacks using circular references in XML messages to consume all available memory and crash computers.

- 2) Validate WSDLs and XML messages against their descriptions and schemas using a monitoring (or filtering) application to prevent malicious or malformed information from reaching the actual Web services.
- 3) Tighten WSDL descriptions and XML schemas as much as possible, effectively narrowing their interface definitions and therefore the attack surfaces of the Web services, and simplifying the validation monitor's task of filtering out unexpected or unwanted data (see 2 above).
- 4) Make Web Service URLs generic to avoid revealing details of underlying languages, application engines and technology.
- 5) Inspect and remove unnecessary data from outbound traffic, including both application and system error messages that could otherwise reveal useful information to attackers.

Gartner's "Best Practices Checklist for Web Services Security, 2006" offers a number of other suggestions, many of which are included below. For an in-depth look at Gartner's view of the evolving overall security environment and the appropriate enterprise response, see "Requirements for Security Administration, 2006," and "Requirements for Infrastructure Protection, 2006."]

5.0 Requirements

SHIN-NY Information Security Requirements include implementation of many measures and mechanisms. These measures are all required for all SHIN-NY ESB nodes and for all communications between any combination of SHIN-NY ESB and RHIO HIE ESB nodes.

Further, these requirements are recommended for all RHIO HIE ESB nodes.

This section lists them in an order generally aligned with a sequential, building blocks approach to implementation.

- 6.1 Base-line Information Security
- 6.2 Consistent Time
- 6.3 Secure Nodes
- 6.4 Public Key Infrastructure (PKI)
- 6.5 Secured Communication Channel
- 6.6 Entity Identity Assertion
- 6.7 Access Control
- 6.8 Collect and Communicate Security Audit Trail
- 6.9 Manage Consent Directives
- 6.10 Manage Sharing of Documents with Document Integrity
- 6.11 Nonrepudiation of Origin

The following sections detail the requirements for each.

5.1 Base-line Information Security

Monitoring and Measuring Availability

SHIN-NY ESB and RHIO HIE ESB nodes shall be continuously monitored for availability and Internet connectivity, and should they consistently fall below 99.9% over different 7-day periods (that is 10.08 minutes over the period), options for improving reliability must be examined.

Develop and Practice Disaster Recovery Plans

SHIN-NY and RHIO HIE participating organizations shall develop and periodically practice Disaster Recovery Plans to mitigate the impact of disasters on availability and data integrity, and to ensure business continuity.

Firewalls and DMZs

Organizations shall use firewalls to restrict traffic in and out of their networks.

Organizations shall also partition their networks with DMZs to isolate Internet accessible servers from other critical systems and end-user computers.

Protecting Web Services

SHIN-NY ESB and RHIO HIE ESB Nodes shall:

- 1) Scan XML messages for generic threats
- 2) Validate WSDLs and XML messages to prevent malicious or malformed messages from reaching the actual Web services
- 3) Tighten WSDL descriptions and XML schemas

This is just a partial list of a few steps that are necessary to ensure the security of Web Services.

5.2 Consistent Time

Given base-line secure environments, the next building block can reasonably be Consistent Time.

Consistent Time, ensuring that all the entity systems that are communicating within the network have synchronized system clocks is essential to several security measures.

SHIN-NY and RHIO HIE nodes shall use Network Time Protocol RFC 1305 to connect to the ntp.org pool of servers at <http://support.ntp.org/bin/view/Servers/NTPPoolServers>. The standards for this requirement are HITSP/T16 Consistent Time and in Section 3.1 of ITI Technical Framework Version 4.0 Volume 2.

5.3 Secure Nodes

Given base-line secure environments and consistent time, the next building block can reasonably be "Secure Nodes". As defined by ATNA, Secure Nodes must:

- 1) Provide reasonable access controls, typically including user authentication and authorization.
- 2) Provide security audit logging to track security events.
- 3) Be authenticated as known systems with known security characteristics.

SHIN-NY Secure Nodes shall provide reasonable access controls including user authentication. Current Best Practices are required of SHIN-NY participants:

- 1) Systems shall be able to determine when authentication has occurred and log that event.
- 2) Systems shall have administrative controls and access privilege controls aligned with categories of information being accessed.
- 3) Systems shall have the ability to create unique user IDs and passwords.
- 4) Systems shall require the use of hard passwords.
- 5) Systems shall prompt user to change their password after N (configurable, but usually 90) days and prohibit re-use of previous passwords.
- 6) Systems shall lock out a user who has been denied access X (configurable, but usually 5) number of attempts.
- 7) Systems shall have a configurable inactivity timer, after which time period, a user will be logged off the system.
- 8) Systems shall support 2nd factor, out-of-band authentication methods.

SHIN-NY Secure Nodes shall also provide "least-privilege" authorization controls, limited access and permissions to the minimum, least set of privileges necessary for the performance of a user's work.

SHIN-NY and RHIO HIE Nodes shall provide security audit logging to track security events using the methods described in Section 5.8 "Collect and Communicate Security Audit Trail" (below).

SHIN-NY Secure Nodes shall only communicate with other Secure Nodes, using bi-directional certificate-based node authentication for connections to and from each node. This shall be accomplished using X.509 Certificates (see also Sections 5.4 and 5.5 below).

As noted in Section 5. "Architecture" above, the scope of this requirement logically extends to feeder systems, and then even to end-user workstations, but for the initial implementation of the SHIN-NY, these rules must be applied only to SHIN-NY ESB and RHIO HIE ESB nodes. As these systems should not be used directly by end-users, these Best Practices for user authentication apply only to systems administrator accounts. This is actually an excellent pilot user group, having both a high level of technical sophistication and compelling requirements for robust authentication.

And lastly, SHIN-NY Secure Nodes shall have known security characteristics as follows:

- 1) All systems that are members of the secure domain shall implement a Secure Node Actor for the ATNA profile.
- 2) All applications on a Secure Node shall comply with ATNA requirements, regardless of whether they are IHE Actors or not. This applies to all IT assisted activities that directly create, access, update, and delete PHI, not only those specified by IHE and performed by IHE actors.

The reference documents for Secure Nodes are IHE ITI-TF Version 4, Section 9, Audit Trail and Node Authentication; NHIN Interface Specification Messaging Platform v1.9; and the process' Privacy & Security Work Group's draft HIE and EMR 4A's Requirements.

5.4 Public Key Infrastructure (PKI)

The SHIN-NY and RHIO HIEs shall utilize a Public Key Infrastructure (PKI) to manage X.509 digital certificates for Secure Node authentication and for digital signing certificates.

The details of implementation and operations still need to be determined.

5.5 Secured Communication Channel

Communications between the secure nodes must also be secure.

SHIN-NY and RHIO HIE participants shall use X.509 Certificates from a single certificate authority (CA) to mutually establish the identity of all communications partners.

All certificates shall be signed by the common, designated CA and will serve as the basis of trust and authentication between secure nodes; all messages between Secure Nodes are both signed and encrypted using these certificates.

More complex PKI functionality such as chaining certificate authorities or certificate revocation may not be implemented initially, but this functionality will clearly need to be added in the future.

Initial implementations shall not assume a centralized identity provider exists for identity proofing and credentialing.

Only communications requiring the attributes of transmission authenticity, confidentiality and integrity need utilize this construct for session-oriented, synchronous, point-to-point communication channels.

Those communications that require the attributes of authenticity, confidentiality and transmission integrity shall either be prohibited, or be designed and verified to prevent access to Individually Identifiable Health Information (IIHI) if they are not communicated through connections that provide session- oriented, synchronous, point-to-point communication channels

There is a mutually agreed to set of policies and procedures for establishment of mutually acceptable identity credentials.

Secure Nodes shall record audit events to indicate attempted connections from nodes that are not mutually authenticated.

These requirements follow from HITSP/T17 - Secured Communication Channel v1.1.1, IHE ITI-TF v4, and NHIN Messaging Platform Interface Specification v1.9.

5.6 Entity Identity Assertion

This building block ensures that an entity is the person or application that claims the identity provided.

Relying on the User and Node Authentication requirements of Section 3.2.3 "Secure Nodes", SHIN-NY and RHIO HIE systems shall recognize the Entity Identity Assertion Construct where user identities are required.

This event shall be logged using the method of Section 5.8 "Collect and Communicate Security Audit Trail" (below), as well as the credentials issued and privileges assigned.

SHIN-NY and RHIO HIE nodes shall create audit log entries for error conditions, including errors in the verification step – malformed assertion; assertion from a distrusted identity provider; assertion from individual without enough information to perform verification; or identity provider is unknown.

The results of the authentication shall be made available to the Authentication Provider.

Authentication information that was verified shall be available.

These requirements follow from HITSP/C19 - Entity Identity Assertion v1.1.1 and IHE ITI-TF v4.0 Section 9.0.

A Statewide Collaboration Process is required to harmonize definitions of roles.

5.7 Access Control

Access Control methods ensure that an entity can access protected resources if and only if it is permitted to do so.

Pre-conditions are:

- 1) Entities must have been identified and provisioned (credentials issued, privileges granted, etc.) in accordance with Entity Identity Assertion construct.

- 2) Secure channels are established as required by policy in accordance with the Secured Communication Channel construct.
- 3) Audit services are initialized in accordance with the Collect and Communicate Security Audit Trail construct.
- 4) Entities have asserted membership in an information domain by successful and unique authentication consistent with the Entity Identity Assertion construct.
- 5) Privacy policies are identified and provisioned (consents, user preferences, etc.) in accordance with policy.
- 6) Pre-existing security and privacy policies are provisioned to access control services.
- 7) The capabilities and location of requested information/document repository services are known.

When a request for data has been received, the SHIN-NY or RHIO HIE shall determine whether access should be authorized or denied based on the requesting entity's identity and local privacy policies.

These requirements follow from HITSP/TP20 "Access Control".

5.8 Collect and Communicate Security Audit Trail

SHIN-NY ESB and RHIO HIE ESB nodes shall collect and communicate a security audit trail according to HITSP/T15.

Audit records shall be created, communicated, stored and analyzed. Communications shall be via BSD syslog -- RFC 3194, not RFC 3195.

The "provisional format" for audit records defined in IHE ATNA shall not be used.

SHIN-NY participants shall:

- 1) Develop a policy defining what is to be audited
- 2) Initialize an audit record source to the audit policy
- 3) Create and activate an audit record repository that is designated as the destination for recorded audit events
- 4) Create and enforce a policy defining the protection of the log and audit
- 5) Create, communicate, store, and analyze audit records
- 6) Take subsequent action indicated by policy, e.g., reports and other automated actions
- 7) Create audit records (Defined in ATNA section 3.20.7.1 of IHE-ITI-TF-2 v4.0)
- 8) Create Security Audit Alarms (Defined in ISO 10164-7)
- 9) Create Security Report (Defined in ASTM E2147)
- 10) Ad Hoc Queries shall be supported via web services (defined in NHIN Audit Log Query Interface IS v.1.2.1, 24-June-08)

The specific Web Services to be exposed are:

AuditLogQuery Service
FindAuditEvents Operator

SHIN-NY participants shall manage the audit log according to NIST SP 800-92 – Guide to Computer Security Log Management.

SHIN-NY and RHIO HIE systems shall use “Security Audit and Access Accountability Message XML Data Definitions for Healthcare Applications” (RFC-3881) for reporting events that are relevant to security and privacy auditing. Note that "this document consolidates previously disjointed viewpoints of security auditing from:

- Health Level 7 (HL7) [HL7SASIG],
- Digital Imaging and Communications in Medicine (DICOM) Working Group 14,
- Integrating the Healthcare Enterprise (IHE) [IHETF-3],
- ASTM International Healthcare Informatics Technical Committee (ASTM E31) [E2147], and
- The Joint NEMA/COCIR/JIRA Security and Privacy Committee [NEMASPC]. "

5.9 Manage Consent Directives

Participants in SHIN-NY shall implement consent management to assure proper confidentiality of Protected Health Information (PHI) in accordance with the requirements developed by the Privacy and Security Work Group. There are two levels of concern for implementation: between RHIO HIEs via the SHIN-NY ESB and with the community domain of a single RHIO HIE.

Within the community domain of a RHIO HIE, the HITSP Manage Consent Directives² specification shall be followed. This requires the establishment of a consent registry and uses the HITSP Manage Sharing of Documents³ specification.

In addition to the specifications of HITSP TP30, specific Web Services shall be implemented on the RHIO HIE:

ManageConsentDirectives Service
CaptureConsentDirective and RequestConsentDirective Operators

These operators correspond to the transactions defined in HITSP TP30. This will assure uniform treatment of consent management and enable service bureau capabilities that run within or across communities. It also enables publishing these services through the SHIN-NY ESB at a later date should it be decided to make these services available through the SHIN-NY.

Consent directives shall be represented using XACML as specified by the *NHIN Interface Specification – Consumer Preferences Service Interface Specification*⁴ that is part of the NHIN phase-2 collaboration.

² See HITSP/TP30 "Manage Consent Directives" v1.1.1 for more information.

³ HITSP/TP13 "Manage Sharing of Documents with Document Integrity" v.2.3.1.

⁴ This document is currently under revision and will be posted to a public site when available.

RHIO HIEs shall not directly pass any information regarding consent through the SHIN-NY ESB so that privacy and confidentiality is maintained. When a trigger event occurs that requires checking consent, the consent directives within the community domain of the RHIO HIE are processed to determine whether there is consent for the desired access. If so the function is processed, if not it is rejected with no indication to the requesting system why the request failed, so that the failure of consent checking is not visible.

5.10 Manage Sharing of Documents with Document Integrity

When sharing documents, SHIN-NY AND RHIO HIE participants shall ensure the integrity of documents that are exchanged or shared.

The Document Consumer technical actor shall validate the SHA-1 hash.

For SHA-1 hash validations which return a “no match”, the document shall be considered invalid by the supporting application.

For SHA-1 hash validations which return a “match”, the document shall be considered valid by the supporting application.

For failure to validate the hash value, the document shall be considered invalid by the supporting application.

Applications must record audit events to indicate “no match” outcomes.

These requirements follow from HITSP/TP13 "Manage Sharing of Documents with Document Integrity" v.2.3.1.

5.11 Nonrepudiation of Origin

SHIN-NY and RHIO HIE nodes shall support non-repudiation of the origin of documents.

The SHIN-NY foundational security policy of ensuring data integrity (see Section 3.1 above) implies the need for non-repudiation of the origin of documents.

SHIN-NY participants shall use digital signing certificates from the Public Key Infrastructure (PKI) to protect the integrity of documents and to allow verification of identity and intent/authority of the signer.

This requirement does not support non-repudiation of receipt.

These requirements follow from HITSP/C26 "Nonrepudiation of Origin" v.1.1.1.

Appendix A – Detailed Checklist

This Appendix is deliberately empty.

Appendix B – Map between 4As and Security Requirements

This Appendix is deliberately empty.

Appendix C – Map between Consent Management and Security Requirements

This Appendix is deliberately empty.

Appendix D – Protocols and Services Work Group Members

Last Name	First Name	Organization
Kremer	Ted	Rochester RHIO
Stein	Benjamin	LIPIX
White	Thomas	NY State Office of Mental Health
Andiel	Marc	STHL
Andrews	Brett	
Barker	Robert	NextGen Healthcare
Barrows	Randy	MedAllies
Barto	John	Sun Microsystems
Berry	Kate	SureScripts
Betor	Debra	NYS Department of Health
Bhaumik	Amitabhba	NYS Office of Mental Health
Bifulco	William	Southampton Hospital
Block	Rachel	New York eHealth Collaborative
Bourette	James	
Cardoso	Matthew	InterComponentWare
Casper	Joseph	MedPlus Inc (Quest Diagnostics)
Cole	George	Allscripts
Columbus	Suzanne	Samaritan Physicians Community HIT Collaborative
Cothren	Robert	Cognosante
Donovan	Thomas	NYS Department of Health
Dournaee	Blake	Intel, SOA Products Division
Duthe	Robert	Northeast Health
Erde, Ph.D., M.D.	Steven	NewYork-Presbyterian Hospital
Evans	John	Strategic Alliance Advisors, Inc
Evans	Lori	NYS Department of Health
Fahey	Walter	Maimonides Medical Center
Fennell	Chuck	St Joseph's Hospital Health Center
Gagnon	Mike	Strategic Alliance Advisors, Inc

Last Name	First Name	Organization
Galanis	Christina	Southern Tier HealthLink
Gilderhus	Keith	Catholic Family Center
Glickman	Michael	NYCLIX- C/O Computer Network Architects
Gotham	Ivan	NYS Department of Health
Greaker	Mark	LIPIX
Greenberg	Marlowe	Foothold Technology
Grieser	John	HealtheLink
Haar	Jaclyn	BHIX
Hale	Pat	NYS Department of Health
Hall	John	INSNC RHIO
Hare	Jonathan	Resilient Networks
Helmin	Stephen	NYS Department of Health
Hoffman	Adam	NYS Office of Mental Health
Humby	Kim	InterSystems Corporation
Johnson	Phyllis	NYS Dept of Health
Jones	Chad	Initiate
Kashyap	Anupam	eClinicalWorks
Kerl	Gary	HealthNow
Kilburn	Bill	6N Systems, Inc.
Kinel	Al	Carestream Health
Koch	Irene	BHIX
Krenitsky	Robert	HealtheLink
Kuperman	Gil	NYCLIX, Inc.
Kwan	Tim	Manatt Health Solutions
Lacal	Jose	SNOMED Terminology Solutions
LaRocca	Mike	Intersystems
Le	Linh	New York State Department of Health
Leonov	Sergei	Ping Identity
Lingayat	Sunil	Northrop Grumman
Lipton	Adam	Hudson River HealthCare
Looney	Sloan	Resilient Networks
Lorenzi	Virginia	NewYork-Presbyterian Hospital
Low	Alex	New York eHealth Collaborative
Mamkin	Boris	BHIX
Marino	Al	Interboro RHIO
Marr	Marie	Excellus
Marvin	Kevin	Kevin Marvin Consulting LLC
Mattice	Chris	HealtheLink
McGeath	Jeff	
Miller	Andrew	Carestream Health
Murphy	Ray	HIXNY/ARCHIE
Murtha	John	Linxus
Myer	Stu	VNSNY
Norman	Frank	ActiveHealth Management
Painter	Joshua	Intel
Perez	Hector	Lutheran Family Health Center
Peshok	Alon	dbMotion
Philip	Suby	Southampton Hospital
Pierce	Jennifer	ITS - Health Insurance Solutions
Plansky	Derek	MedPlus Inc (Quest Diagnostics)

Last Name	First Name	Organization
Poleto	Peter	HANYS
Popp	George	Lab Alliance of Central New York
Pucherelli	Ron	MSSNY
Pulgarin	Claudia	NYCDOHMH
Radov	Nick	Axolotl Corporation
Rankin	Jerry	Healthvision
Rathore	Zahid	Booz Allen Hamilton
Rowe	LaRon	Rochester RHIO
Rubinchik	Valentin	dbMotion/Bronx RHIO
Schell	Kate	InterSystems Corporation
Schroth	C. William	NYS Department of Health
Seale	Brian	
Shatzkin	Nance	Bronx RHIO
Silvious	Thomas	CSC
Soiman	Erika	Hebrew Home for the Aged at Riverdale
Soulakis	Nicholas	NYC DOHMH
Spurchise	Michael	Partners in Health Systems
Stanley	Kendall	Axolotl Corporation
Stuard	Susan	THINC RHIO
Subramanian	Sandeep	GSI
Suri	Rohit	Emerging Health IT
Tripathi	Micky	
Tull	Laurie	Anakam
Unger	Tom	HealtheLink
Upadhyay	Asha	THINC RHIO
Vaczy	Ted	Univ of Rochester Med Ctr
von Laszewski	Gregor	RIT
Voss	John	Cisco Systems
Walker	Holton	
Wallace	Eric	Linxus
Wan	Lin	Axolotl Corporation
Wheaton	Jason	CVPH Medical Center
Yan	Tony	NYS Department of Health
Zecchini	Edward	MediVoice, LLC
Andrews	Tim	High Pine Associates
Jones	Lee	GSI Health
Kelly	Sean	GSI Health
Lewis	Vincent	GSI Health
Shull	Chris	GSI Health