Using the CONNECT Gateway to Support HIE

Version 6.0

CONNECT Release 3.3

March 16, 2012

REVISION HISTORY

REVISION	DATE	DESCRIPTION
-	28 January 2009	Initial Release
-	25 March 2009	1. Initial Release. 2. CDRL numbers are now OBE since they were base year only deliverables.
2.0	7 July 2009	Updated to reflect Release 2.1
2.1	13 July 2009	1. Updated DURSA and Testing Sections based on guidance provided. 2. Title Change 3. Change how it is organized
3.0	18 March 2010	Updated per CONNECT Release 2.4
4.0	15 June 2010	Updated per CONNECT Release 3.0 and addition of performance related questions
5.0	14 September 2010	Updated per CONNECT Release 3.1. 2. Added Security related questions. 3. Added Introduction to the Business Case Section. 4. Updated all references of NHIN to Nationwide Health Information Network.
6.0	16 March 2012	Updated per CONNECT Release 3.3

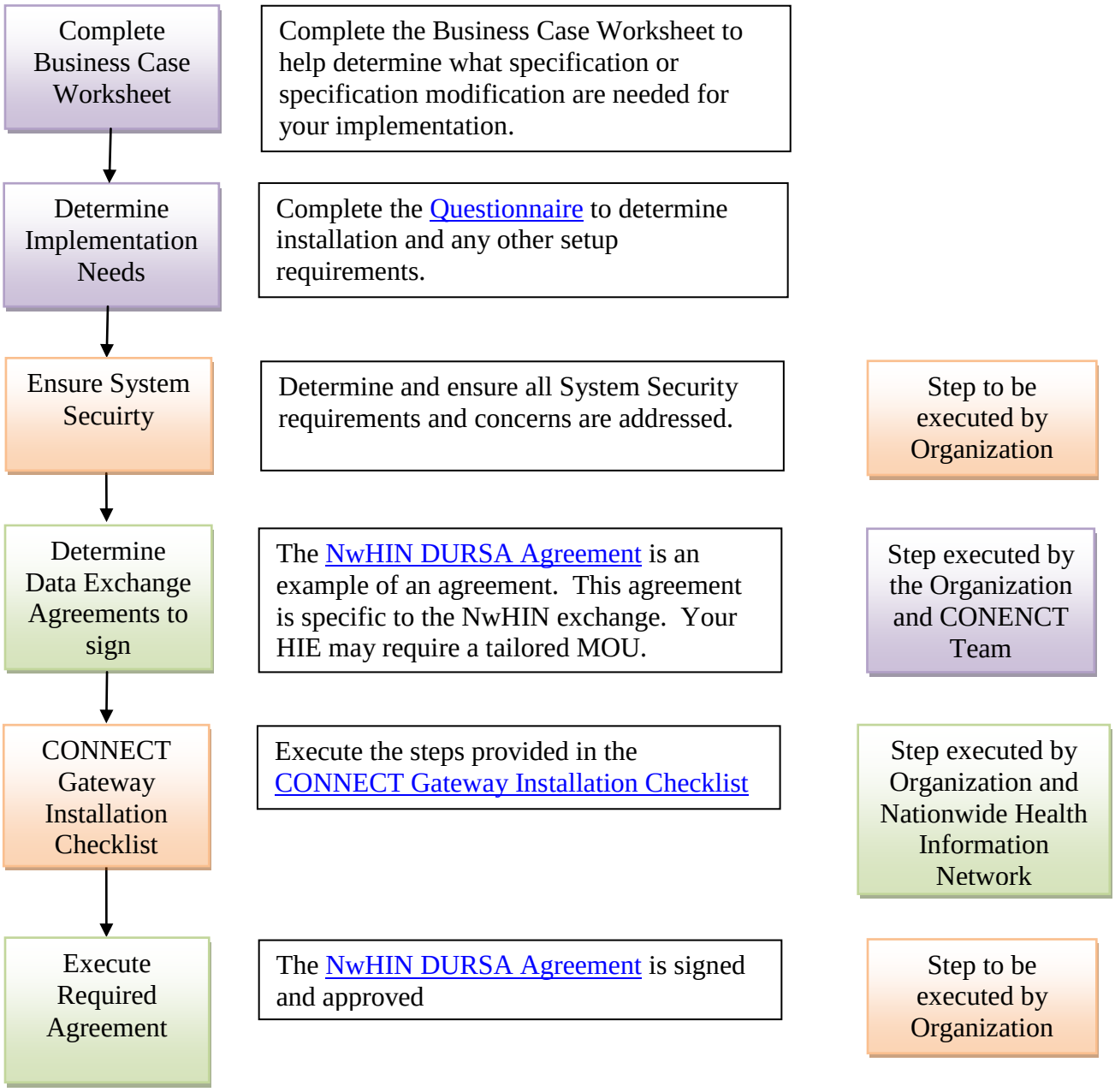
TABLE OF CONTENTS

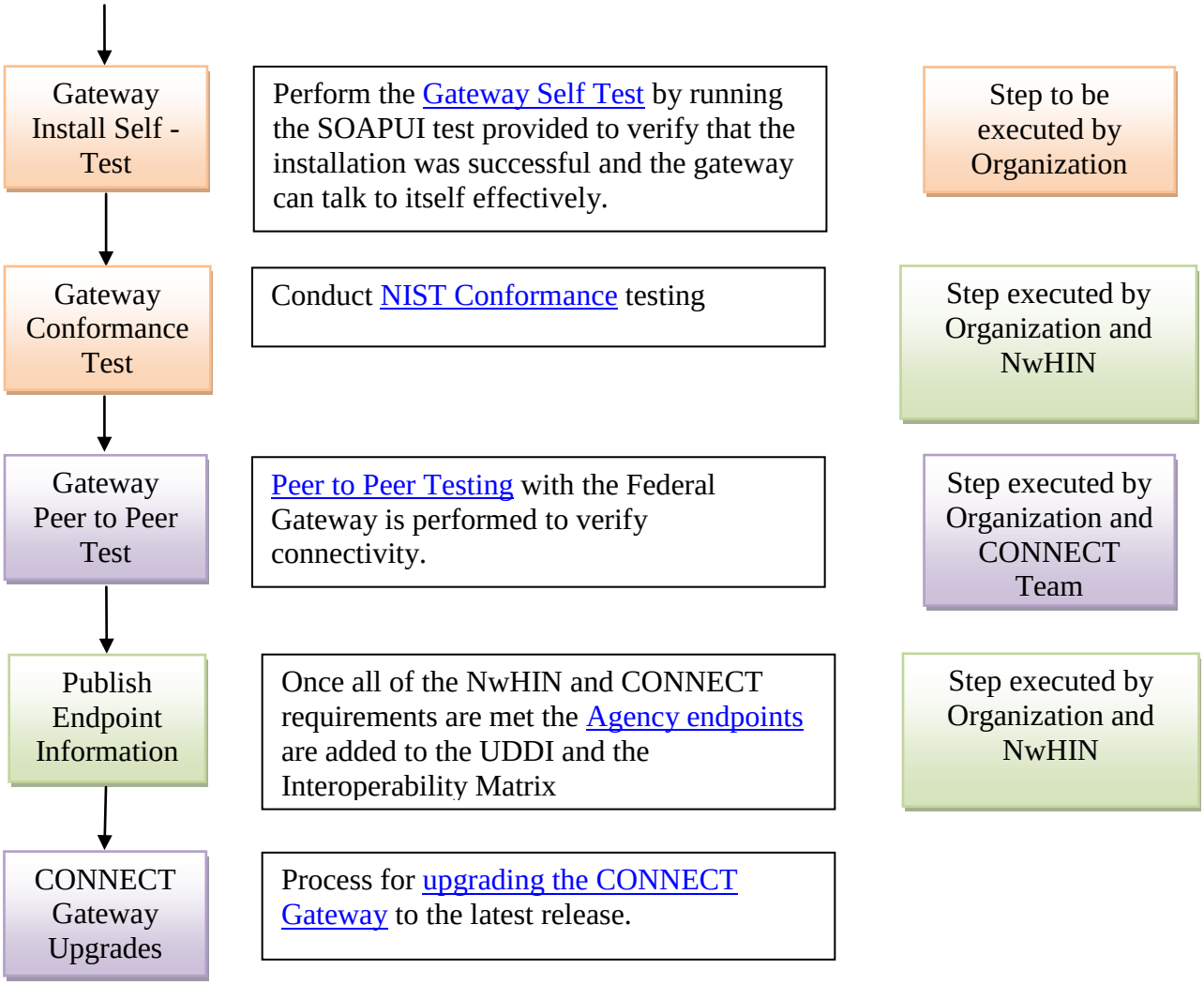
1.0 INTRODUCTION

This document serves as a guide to enabling Health Information Exchanges (HIE) using the CONNECT Solution. The Nationwide Health Information Network is one example of such an HIE. This document is intended to assist organizations with asking the key questions and determining some of the key steps to getting started. This is a living document that will be updated as processes are refined in partnership with the NwHIN, the CONNECT Team, and partnering organizations.

1.1 CONNECT Gateway Deployment Checklist

The following is a workflow/checklist that guides the organization through the steps required to use the CONNECT Solution to employ Nationwide Health Information Network (NwHIN) conventions and standards to facilitate healthcare data exchanges. This document is organized to mimic the flow of the checklist allowing for easier reference.




Gateway Install Self - Test
Perform the Gateway Self Test by running the SOAPUI test provided to verify that the installation was successful and the gateway can talk to itself effectively.
Step to be executed by Organization
Gateway Conformance Test
Conduct NIST Conformance testing
Step executed by Organization and NwHIN
Gateway Peer to Peer Test
Peer to Peer Testing with the Federal Gateway is performed to verify connectivity.
Step executed by Organization and CONNECT Team
Publish Endpoint Information
Once all of the NwHIN and CONNECT requirements are met the Agency endpoints are added to the UDDI and the Interoperability Matrix
Step executed by Organization and NwHIN
CONNECT Gateway Upgrades
Process for upgrading the CONNECT Gateway to the latest release.

Complete Business Case Worksheet

2.0 BUSINESS CASE FOR HEALTH INFORMATION INTEROPERABILITY

The intent of having your team document the business case(s) is to provide a vehicle for your team to discuss potential projects/opportunities that could be improved with the implementation of CONNECT. The CONNECT Team welcomes a meeting with your team to facilitate completing this form. This meeting with your key program Points of Contact (POC) can help to determine if current Nationwide Health Information Network Specifications facilitate the implementation of your business case or whether new NwHIN Specifications would have to be developed. The business case will also help to determine/address some of the technical requirements/questions in the Using the CONNECT Gateway to Support HIE questionnaire and other questions as you plan the implementation. Please note that there may not be enough tables to enter all the contacts. Feel free to create additional tables as you find necessary.

Business Case Worksheet Version -2.0 March 16, 2012

Note whether your business case needs to be ready in time for a specific event:

Date: _____ __ Event: _____

Partner profile

Organization Name	
Division or Program	
Program Manager (POC)	
Address	
City, state, ZIP Code	
Phone number	
Fax number	
Web site address	

Business Lead/Sponsor:

Contact name	
Title	
Phone number	
Fax number	
E-mail address	

Technical Lead/Sponsor:

Contact name	
Title	
Phone number	
Fax number	
E-mail address	

TEMPLATE

The Story:

Please provide details on the use case. How will transitioning to electronic record exchanges help your organization provide better services to your customers?

Exchange Stakeholders:

Name the organization(s) and any other entity with which you will be exchanging information.

Organization Name	
Division or Program	
Program Manager (POC)	
Address	
City, state, ZIP Code	
Phone number	
Fax number	

Organization Name	
Division or Program	
Program Manager (POC)	
Address	
City, state, ZIP Code	
Phone number	
Fax number	
Web site address	

Organization Name	
Division or Program	
Program Manager (POC)	
Address	
City, state, ZIP Code	
Phone number	
Fax number	
Web site address	

Name the Information Exchange:

Select a name that could be used by others when talking about the exchange you are planning.

EXAMPLE: Wounded Warrior

Information for Exchange:

Patient-specific diagnoses, medications, problem lists, allergies, and clinical documentation.

As a second phase, when a patient can access the disability determination results, perhaps allow the patient to securely log onto a system to access the information.

_____

_____

_____

_____

_____

Information Exchange Context:

Set the context for this information exchange:

EXAMPLE: This exchange is a bi-directional federal government to health care entity (provider of care). A provider of care may be federal, private, tribal, or other public entity.

These are federal government to business type exchanges and business to federal government return path.

Today, they are point to point in nature, from the request to the return of patient-specific information and the return acknowledgement of receipt, including the intent to pay the provider of care for the information. With business process re-engineering or the capability to query multiple providers of care to access all relevant patient-specific data, this will be an added benefit.

_____

_____

_____

_____

Business Situation

Identify the problems that you and your stakeholders are facing and why solving the information exchange challenge is important to your and/or their mission.

_____

_____

_____

_____

Is this a new information exchange for your organization? □Yes □No _____

_____

If no, explain how it is being altered.

_____

_____

_____

_____

_____

_____

Is this an intra or inter organizational exchange?

_____

_____

Anticipated Return on Investments

Identify the expected value of implementing the exchange (financials to support “the story”). For example, Will there be cost savings? Cost avoidance? Describe the basis for your expected ROI.

Technical Situation

Provide an overview of your organization's capabilities to create technical solutions for health information exchanges intra and inter organizationally. Identify what may have been uncovered during the evaluation of your systems, the technical challenges you are facing, and how you believe you can meet the challenges, including any evaluation and implementation assistance you anticipate needing.

EXAMPLE: Our current environment runs on older computers that are no longer capable of handling the bandwidth necessary for servicing a worldwide customer base. Additionally, we would like to allow customers to automate their orders and also would like to eliminate telephone and paper requests for records.

If applicable, do you have a current technology plan and/or capabilities within your organization that will assure your organization achieves the Meaningful Use Criteria in 2012 and beyond? □Yes □No _____

_____

_____

_____

_____

_____

_____

_____

3.0 QUESTIONNAIRE – DETERMINE INSTALLATION AND SUPPORT REQUIRED

The purpose of this questionnaire is to provide a framework for your teams to identify and discuss some key topics that the CONNECT team has seen previously as possible impediments. The CONNECT team recommends that you complete the questionnaire with all key players together, including, if possible, the teams that you plan to exchange data with. By using the questionnaire and jointly responding to the questions, you should be able to develop a comprehensive plan identifying key risks and impediments to overcome. Please note that there may not be sufficient room on the tables to enter all the contacts. Feel free to create additional tables as you find necessary. Please review your responses with the CONNECT team and any pertinent additions/clarifications that should be addressed.

3.1 Contacts

1. Who is your program management point of contact? (This person will be responsible for ensuring agreements are signed and determining implementation vision)

Name:	
Title:	
Phone numbers (office and cell):	
Email:	
Skype address:	
Mailing address:	

2. Who is your technical point of contact? (This person will be responsible for setting up the servers)

Name:	

Title:	
Phone numbers (office and cell):	
Email:	
Skype address:	
Mailing address:	

3. Who is the point of contact for VPN and firewall configurations?

Name:	
Title:	
Phone numbers (office and cell):	
Email:	
Skype address:	
Mailing address:	

4. Who is responsible for creating test patients within your system?

Name:	
Title:	
Phone numbers (office and cell):	

Email:	
Skype address:	
Mailing address:	

5. Who are your key stakeholders that need to be considered with your participation in the Nationwide Health Information Network?

Name:	
Organization:	
Title:	
Phone numbers (office and cell):	
Email:	
Skype address:	
Mailing address:	

6. Does your team have experience with Web services, SSL, SAML, HL7 V3, Solaris system administration, Windows system administration and VMPlayer technology? _____

Comments: Please note that depending on the type of install and whether or not your team will be modifying the adapter, having team members with certain skills sets is useful.
When installing/configuring the Gateway we recommend having the following expertise:

- Ports
- SSL certificates- creating and applying
- Access to a network administrator
- VMPlayer if you are doing the virtual installation

- System administration in the OS that your team will be installing the gateway and adapter on

For installing and customizing the adapter, we recommend having expertise in:

- Web services
- SOAP message
- HL7 v3
- CCD document structure
- Some knowledge of soapUI
- Familiarity with reviewing audit logs

Tools that are useful when setting up the adapter/gateway:

- NetBeans
- Eclipse
- GlassFish
- soapUI

3.2 Production/demo plan

7. Do you have a project plan/schedule with milestones that define the path to production/demonstration? □ Yes □ No

   _____

   Comments: Having a comprehensive plan with key milestones and owners is helpful to ensure that all of the tasks that have to be completed have been defined. The CONNECT team provides a sample schedule with each release that can assist teams in creating a comprehensive plan developed for either a demonstration, pilots or steps to production.

8. Are there any demonstrations in which you will be participating? What Nationwide Health Information Network services will be utilized in your use cases?

   _____

   _____

   a. When will they be? _____

   b. What do you intend to demonstrate? _____

   _____

   Comments: Determining what your team will be demonstrating will help drive what services need to be activated and documents need to be prepositioned.

9. When does your NHIE expect to go into production supporting the Nationwide Health Information Network core services, including patient discovery and

query/retrieval of records (including NwHIN summary record)?

_____

_____

Comments: It is helpful if your team develops an overall architectural diagram with the data inputs/outputs, gateway/adapter services to be used, ports, and hardware (including proxies and firewalls) that document the scenarios your team intends to take advantage of in production. This document can help communicate to the

- CONNECT team, as you may need support,
- Nationwide Health Information Network team, as you make the plan to go live, and
- Teams that you plan to exchange with, to ensure there are no issues with exchanges.

10. Are there any particular agencies, private sector partners or other health information exchanges you will initially target for production? Are these groups actively exchanging data on the Nationwide Health Information Network?

_____

_____

_____

11. What is your timeframe for rollout with workload projections?

_____

_____

_____

12. Do you have enough hardware to support all of the development and test environments necessary to proceed to demo/production? □Yes □No _____

_____

13. Does your organization require a separate test evaluation and acceptance testing processes before software can be rolled out to production? □ Yes □ No If so, what is required and have those partners been engaged in the process?_____

_____

_____

Comments: Please note that depending on the requirements by the separate testing team(s) you may need to accommodate additional documentation,

training, setup, hardware and time within your schedule to meet this milestone. You will also need to ensure that the organizations you plan to exchange with accommodate time in their schedules to test with these teams as well, if appropriate.

3.3 Security

14. Have you implemented a boundary firewall with monitoring, access control and physical restrictions, and is it locked down? □ Yes □ No

    _____

15. Have you implemented an intrusion detection and prevention system, and is it routinely updated? □ Yes □ No

    _____

16. Do you have antivirus installed? □ Yes □ No

    _____

17. Do you monitor your logs? □ Yes □ No

    _____

18. Are you locking down your operating systems and network infrastructure? □ Yes □ No

    _____

19. Are there specific security restrictions that need to be addressed? For example, firewall restrictions, limitation of port usage, server STIGing process or remote access to servers?

    _____

    _____

Comments: Depending on the security rigor within your organization, your team may need to complete particular security inspections, tests and documentation. Your team will need to allow for this rigor in your schedule as you plan your efforts to roll into production or for demonstrating. The CONNECT team has seen, at times, that the opening of ports could cause long delays when planning for demo or moving to production. In the future, the CONNECT team will be providing templates of certain security documentation that may be helpful in your efforts to meet particular security requirements. The CONNECT team will also be testing the CONNECT gateway and adapter in environments which have had the operating systems secured.

20. Is your organization required to use FIPS 140-2-compliant encryption algorithms? □ Yes □ No

    Comments: The CONNECT team provides instructions with each release to enable FIPS 140-2 on the gateway for a number of platforms. We recommend that you emphasize this request to the CONNECT team, especially if you are running on a platform that is not currently supported by the CONNECT team. You may need to add a task to your plan to ensure these instructions are completed during your gateway configuration.

21. Can we establish a VPN connection to your organization? □ Yes □ No

    _____

    Comments: Or any type of connection? The response to this question will allow the CONNECT team to determine if it can dial into your team's test/development environments to assist in troubleshooting as negotiated.

3.4 Hardware/platform

22. Do you want the CONNECT team to host the gateway, or is your organization going to provide the hardware to host the gateway? □ Yes □ No

    _____

23. Are you installing a development, demo, pilot or production server?

    _____

    _____

24. Do you currently maintain a test environment? □ Yes □ No _____

    _____

25. What operation system will you be installing on?
    - □ Windows
    - □ Solaris
    - □ Linux
    - □ Other_____

26. Is your system focused on 32-bit platforms or 64-bit platforms?

_____

27. If this is a Windows server, is hosting a VM version of the CONNECT software an option that you are exploring? _____

_____

Comments: Gateway VM installations can be configured more quickly, especially for demo purposes. If this is an option that you are exploring please contact the CONNECT team to determine if this is appropriate. The instructions for obtaining the software will be provided once discussed.

28. Do you have VMPLAYER 2.0? □ Yes □ No _____

_____

29. Does your system meet the minimum hardware configuration provided in the deployment footprint section of the installation document? □ Yes □ No

_____

30. Do you have an XML gateway or any special appliance for processing and/or transformation of XML messages? _____

_____

31. What application servers will be used in your environments (e.g., Glassfish, WebSphere, WebLogic, JBoss, etc.)? Please specify if there will be changes over the long term.

_____

_____

32. How many CONNECT gateways are planned for your network? What is the timeline to ramp up to this number of gateways?

_____

_____

33. Are there other notable HW/security/proxy nodes in your system (e.g., DataPower, Load Balancer, other network appliances)? _____

_____

34. Please describe the specific CONNECT plug-ins/adapters that will be used for your implementation. _____

_____

35. Please describe the version of CONNECT that you plan to use over the near term and long term. _____

_____

36. Please list other notable applications running on the system that may influence system performance (e.g., user interfaces, HW). _____

_____

37. Are the gateway and adapter running on the same or separate servers?
_____

_____

38. Please describe your SAN storage and associated databases.
_____

_____

39. Please describe your current or proposed configuration for the following: CPU type and clock rate, # of CPUs, memory, network and disk configuration.
_____

_____

3.5 System performance

Data transfer:

40. What is the maximum payload/size required for your implementation of CONNECT for the near term and long term (2+ years)?

    Near term: _____

    Long term: _____

41. Approximately how many files are delivered and received on an hourly basis? Daily basis? _____

42. If known, what are your approximate peak loads on an hourly and daily basis (e.g., messages, # of files, bandwidth constraints, etc.)?_____

43. What would be the average number of files sent at any one time, since this would impact the file size being transported at any given time? _____

_____

44. Please specify the CONNECT services that these requirements apply to within your organization, assuming you include PD, XDS (e.g., DS, DQ/DR, HIEM, etc.).
_____

_____

45. Are your payload/size requirements needed for uni-directional applications or bi-directional applications? Both? _____

_____

46. Are there specific end-to-end latency requirements for retrieving and delivering files? Is there a minimum time to transfer a file upon receiving a trigger to transmit the file? _____

_____

47. Are your file transfer requirements based on synchronous transfers, asynchronous transfers or a combination? Does this depend on certain applications within your environments? If so, please explain. _____

_____

48. How many concurrent users and transactions do you expect to support from a single direction (uni-directional)? Both directions (bi-directional)? _____

_____

49. Fan out: Are you using the fan out capability? If so, how many communities do you expect to fan out to (rough estimate or everyone if broadcast)? _____

_____

NOTE: This information will allow us to know how many messages will go out at once and the responses that are expected to be aggregated.

50. Are you planning to communicate with other non-CONNECT gateways? If so, how many and what are the timelines for interworking with those gateways?
_____

_____

51. Please describe the version of CONNECT that your partners plan to use over the near term and the long term. _____

_____

52. Are any of your partners using a non-CONNECT solution to access the Nationwide Health Information Network?

_____

_____

53. If any of your partners are using a non-CONNECT solution to access the Nationwide Health Information Network, please provide details (if available) of their solutions.

_____

_____

54. Are you or do you intend to cluster instances of CONNECT gateways? Please describe the configuration.

_____

_____

55. Are your CONNECT gateways configured for HA (high availability)? Please describe the configuration.

_____

_____

3.6 Gateway Services

56. Will any data/documents be stored on the gateway? □Yes □No

Comments: If yes, you will need to follow the instructions to install MySQL adapter component or the NIST repository as described in the CONNECT installation and configuration manuals. Please refer to the documentation for the appropriate release posted at http://www.connectopensource.org .

57. Will the gateway respond to messages, or is it only a retrieval gateway?
□ Yes □ No

58. What type of MPI will you be installing?

_____

59. How would you accomplish the initial data load of the MPI? _____

_____

_____

3.7 Interfacing with the gateway

60. What message types does your system outbound?

a. What format(s) are supported?
   - □ SOAP 1.1
   - □ SOAP 1.2
   - □ Other: _____

_____

b. What format(s) are supported?
   - □ HL7 v2
   - □ HL7 v3
   - □ Other: _____

_____

_____

c. What payload format(s) are used by your EMR to send patient data?
   - □ CCD- C32, C37, , C48, C62, C84, C166, etc
   - □ HL7
   - □ ebXML
   - □ PDF
   - □ TIFF
   - □ Other: _____

Comments: Please note that the Nationwide Health Information Network exchanges are based on CCD message types.

d. Is it triggered? By what events? _____

_____

61. Can you accommodate both single message and batch updates? □ Yes □ No

_____

62. Do you currently use an interface engine? □ Yes □ No Which one? _____

_____

63. Does your existing system have any exposed interfaces for data requests?_____

_____

_____

64. Which and what type of interfaces? _____

_____

65. Do you have an existing interface control document? □ Yes □ No _____

_____

66. What is the minimum data required by your system to perform trait matching (last name, first name, middle name, sex, address, SSN)?_____

_____

_____

67. What kind of data (symptoms, diagnosis) do they send? (Utilization?)_____

_____

_____

68. Which EMR(s) is currently being used? What is the version number?

_____

69. What coding standards are employed within your EMR? Specifically, how are the allergies, medications, problems, labs, radiology reports and demographic data coded within your system? Can you transmit in HITSP C32 required elements?

_____

_____

_____

Comments: Please refer to the Nationwide Health Information Network specs for the required formats for exchange.

70. Does your system create one document for each patient encounter or one aggregated document used for all the patient's visits?
_____

_____

_____

71. What is your plan to establish a remote connection from your EMR to the gateway?

_____

_____

72. Can your system be queried for data from an outside entity (i.e., labs)?
□ Yes □ No _____

_____

73. Do you evaluate the data prior to sending? □ Yes □ No _____

_____

74. What is the general process for the evaluation? _____

_____

75. What criteria must be met to warrant sending the data? _____

_____

a. Is this process manual or automated? _____

_____

3.8 Provider support

76. What are the key attractors for your organization to the Nationwide Health Information Network? _____

_____

77. How many providers currently exchange data within your NHIE? What data do they exchange? _____

_____

78. How many providers currently exchange data outside your NHIE? What data do they exchange? With which partners?_____

_____

79. How many providers do you estimate will be able to query and retrieve a Nationwide Health Information Network summary patient record in 2012?

_____

_____

80. How many providers do you expect will be able to go live with Nationwide Health Information Network services in 2012 or 2013?

_____

_____

81. On average, how many persons does a representative provider serve? _____

_____

82. What are the barriers for providers connected to your NHIE to support the Nationwide Health Information Network summary record, including the additional data elements required by SSA? _____

_____

_____

3.9 BioSurveillance

83. Do you currently provide BioSurveillance type data to public health organizations? □ Yes □ No _____

_____

84. What are the organizations(state, local, etc.)?_____

_____

85. What kind of data (symptoms, diagnosis) do they send? (Utilization?)_____

_____

_____

86. What format is the data sent in (CCD- C32, C37, etc.)?
    - □ HL7
    - □ ebXML
    - □ PDF
    - □ Other: _____

_____

87. Do you evaluate the data prior to sending? □ Yes □ No _____

_____

88. What is the general process for the evaluation? _____

_____

89. What criteria must be met to warrant sending the data? _____

_____

    a. Is this process manual or automated? _____

_____

Ensure System Secuirty

4.0 INFORMATION SYSTEMS SECURITY FOR HEALTH INFORMAITON INTEROPERABILITY

Methods for the protection of information are an important consideration within the information system architecture. The Nationwide Health Information Network takes the approach that all applicable local operating instructions, statutes and federal laws apply to agencies or partners who implement CONNECT within their environments. Applicable federal laws may include (not limited to) the Federal Information Security Management Act, Health Information Portability and Accountability Act, and the Health Information Technology for Economic and Clinical Health Act. In some cases, a full certification and accreditation process may be completed by NwHIN participants to prove compliance if necessary.

The Department of Commerce, National Institute of Standards and Technology, has developed a set of special publications that provide a framework for information systems security through a combination of technical, operational and managerial controls to protect the confidentiality, integrity and availability of information. This NIST SP 800-53 rev3 is the latest recommended security controls for federal information systems and organizations. This publication serves as a national standard for the implementation of security controls and cross-references with other agency and international standards.

The Nationwide Health Information Network Data Use and Reciprocal Support Agreement (DURSA) is the legal agreement between two testing entities to ensure that responsibilities and limitations to liability are met and clearly understood (see Section 10.0) when exchanging on the NwHIN. The CONNECT application provides reasonable safeguards to protect information through the application of FIPS 140-2 compliant encryption algorithms and also supports other modes of operation for the purpose of testing. The use of clear text data should be avoided and live patient data should never cross hostile boundaries in the clear. Since CONNECT is configurable and adaptable to a wide range of information systems and enterprise architecture, a review of all applicable installation and configuration guidelines is recommended to ensure the highest level of data integrity.

The intent of information system security is not to provide a barrier to entering business communications, but to instill a lasting sense of surety to the information owners that their information is not inadvertently used or disclosed. It should be clear that the ownership of Personal Health Information can be none other than the person whose attributes it belongs. It is the intent of CONNECT to provide the best business case for the transfer of electronic medical records securely, maintaining privacy to the information owner and reliability to the care provider at a lower cost.

Here are a few considerations to make when securing a system:

1. Have you implemented a boundary firewall with monitoring, access control, physical restrictions, and is it locked down?

A firewall is a first and crucial step in securing a network. How it is implemented and configured is another story and can be unique to each HIE. Considerations may include vendor security patching, security technical implementation guidelines, logical access controls lists / firewall rules, systems of least privilege, physical access and monitoring. Just having a firewall is not enough. It must be implemented correctly.

2. Have you implemented an intrusion detection and prevention system (IDS/IPS), and is it routinely updated?

   An IDS/IPS is a system used to detect or prevent known or suspicious activity on an information system, or individual host. Some systems are enterprise based, and others reside individually on the host. The bad news about IDS is that an attack has either already occurred or is in progress. The good news is that at least you know you have been exploited and can provide some forensic evidence to the cyber crime investigators regarding the intrusion or exfiltration. An IPS system is more preventative and proactive and stops the attack before it occurs. Unfortunately, neither of these systems is effective unless they are monitored and have updated signatures.

3. Do you have antivirus installed?

   An Antivirus (AV) program detects known or certain variants of malicious code using heuristic analysis of code and comparing it to a known (or close) hash value (signature). Since most signature-based systems rely on heuristics, the potential for false positives may result. That said, an AV program without the latest signature database is only marginally better than not having antivirus at all, so make sure it is up to date!

4. Do you monitor your logs?

   In a system of large scale, it is almost impractical for any one person to continuously monitor logs day in and day out. It makes sense to implement a log server, pull data from all sources, and only flag on things that are out of the norm. Another case is compliance monitoring, and there are applications out there that can help maintain a trusted state by monitoring all system changes in the environment.

5. Are you locking down your operating systems and network infrastructure?

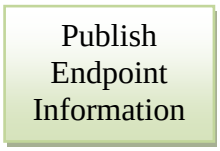
   The DoD community knows this as STIG'ing. You can "gold disk" it or script it automatically; but often when you disable certain functionality in a system, it is likely to break something else. So proceed with caution. Note that the HHS prefers to use the HHS Minimum Configuration Guideline for securing systems.

5.0 LEGAL AGREEMENTS

For the protection of the patient and the organization, each entity pursuing the endeavor of exchanging healthcare data should determine what legal agreements need to be signed between the entities performing the exchange. In some cases a document as simple as a Memorandum of Understanding (MOU) may suffice for creating a comprehensive agreement needed to legally bind the entities to the exchange and define the terms of the exchange. The Nationwide Health Information Network Limited Production DURSA is just one example of such a legal agreement. More information on the DURSA is provided in the Appendix of this document.

5.2 Execute the Legal Agreement

The Legal Agreement should be determined and drafted as early as possible, but does not need to be executed to start the installation process.



5.2 Publish Endpoint Information

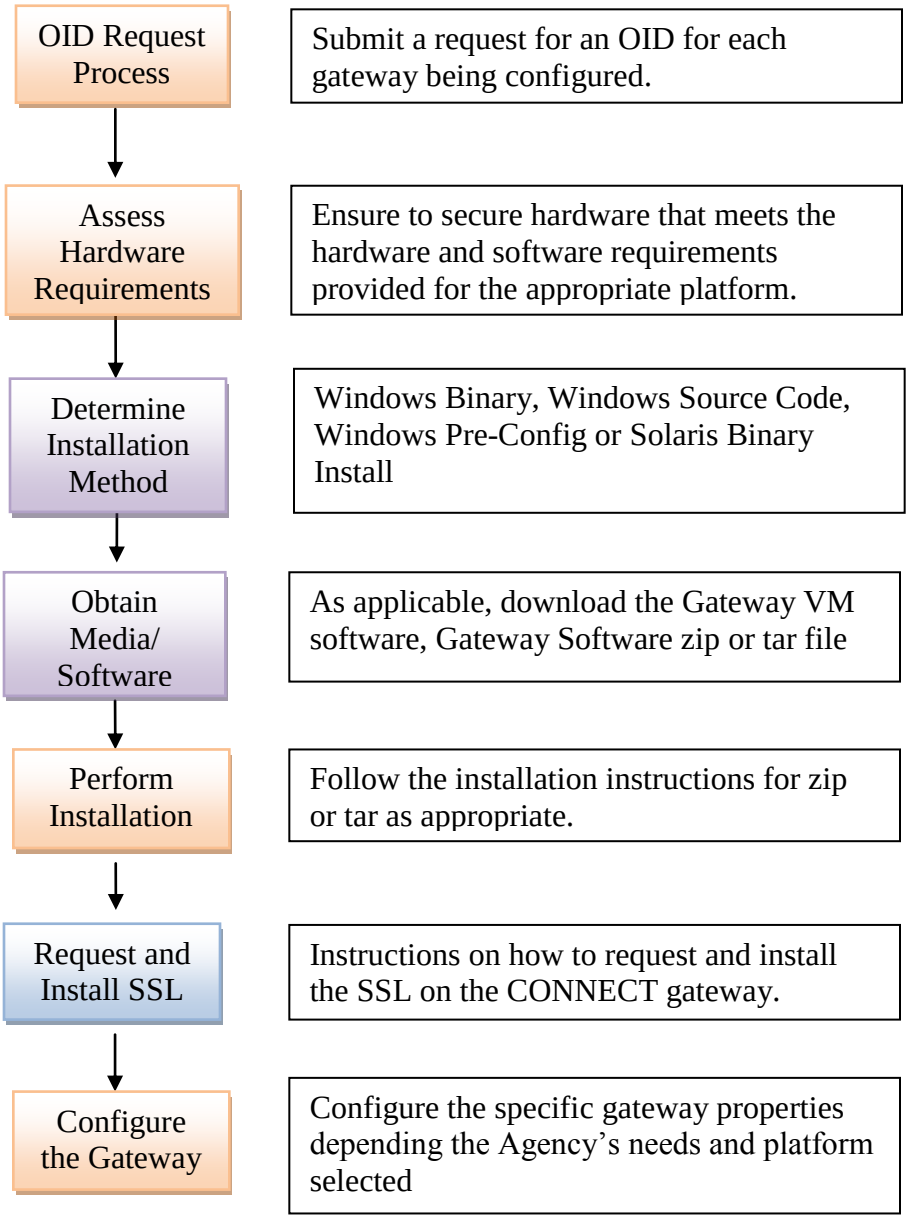
Once all the critical tasks are completed, the endpoints of the Agency's gateway will be added to the Master UDDI (Service Registry.) The critical tasks include the signing of the NHIN DURSA Agreement and the successful completion of all tests outlined (Installation Self-Test, Conformance Test, and Peer to Peer Test). Once the endpoints are added to the Master UDDI all gateways that have access to it will be able to easily access the latest endpoints. Until all of the Nationwide Health Information Network Cooperative members have access to the Master UDDI the latest endpoints will be published to them in the interoperability matrix when the critical tasks are completed.

CONNECT Gateway Installation Checklist

6.0 CONNECT GATEWAY INSTALLATION

Below is the installation workflow/checklist required to complete the installation of the CONNECT Gateway. The complete documentation of these steps can be found in the CONNECT installation and configuration manuals located on the Confluence portal.

6.1 NwHIN Installation Checklist



7.0 ADAPTER CONFIGURATION CONSIDERATIONS

Refer to the CONNECT installation and configuration manuals for how to configure adapters.

http://developer.connectopensource.org/display/NHINR31/Installations

8.0 TESTING THE GATEWAY

Once your agency has completed the installation and configuration of the gateway, you need to validate that it will communicate effectively on the Nationwide Health Information Network. There are 3 levels of testing that we have designed to assist in this validation. The first level is an isolated test that helps to ensure that the gateway is correctly installed and configured; for example, can the gateway talk to itself?

The second level of testing is to ensure the gateway communication still conforms to the standards set by the Nationwide Health Information Network. These tests should be easily passed since the Federal CONNECT team ensures that the functionality requirements are all met before performing a release. However, we have seen proxies or other configurations that could potentially affect the communication released on the basic CONNECT gateway.

The third and final level of test is a complete Peer to Peer test. This test is customized for your agency depending on the services that your agency has chosen to implement on the gateway. This test will help to ensure the agency's tailored CONNECT gateway can connect and communicate effectively to other gateways.

Gateway Install Self -Test

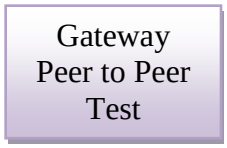
8.1 CONNECT Validation Tests

To ensure that the installation completed successfully, SOAPUI self-test scripts have been developed to validate that the gateway is functioning. These tests are a self test of the gateway and do not confirm connectivity and related functionality. The SOAPUI scripts provided utilized the free SOAPUI version. Instructions on how to run the SOAPUI scripts are provided with the scripts when they are downloaded. These instructions as well as the self-test strips can be accessed via the following link on the Confluence portal:

http://developer.connectopensource.org/display/NHINR31/CONNECT+Validation+Tests

8.2 Conformance Testing with the NIST and NwHIN Test Tools

The National Institute of Standards and Technology (NIST) in partnership with members of the Nationwide Health Information Network Cooperative have developed test tools to validate the consistent interpretation and implementation of NwHIN Specifications. The NwHIN Test Workgroup is currently working on the Conformance Tests to validate against the approved July 2011 NwHIN specifications and will provide guidance when these are ready.



8.3 Peer to Peer Testing with the Federal Gateway

Peer to Peer testing, also referred to as Interoperability testing, validates that multiple systems that implement a particular standard, or set of standards, can all communicate with each other. The Federal CONNECT Team conducts extensive functionality tests, validation of the messages to ensure they are semantically and syntactically accurate for all services supported, and tests to verify gateway's robustness and stability. Each agency has different network and possibly hardware configurations. The Peer to Peer testing with each agency is targeted to ensure that any connectivity configurations that could affect querying or responding through the Nationwide Health Information Network are addressed prior to using the agency's gateway for a demonstration or transitioning the agency's gateway to production. Once the agency's gateway is installed, the Federal CONNECT team will coordinate with the agency's gateway technical team to perform the extensive tests to exchange messages on the services that the agency has chosen to implement. This team will engage any other technical support team members needed to resolve any connectivity issues identified.

9.0 ACRONYMS

Acronym	Definition
CDC	Centers for Disease Control & Prevention
CMS	Centers for Medicare & Medicaid Services
DOD	Department of Defense
DURSA	Data Use and Reciprocal Support Agreement
EHR	Electronic Health Record
EMR	Electronic Medical Record
ESB	Enterprise Service Bus
FHA	Federal Health Architecture
Functional Test	This refers to the system's ability to ensure the required activities take place appropriately according to the requirements. Examples of this type of conformance include ensuring correct routing of information, actual delivery of information, employment of appropriate security measures, etc.*
HITSP	Healthcare Information Technology Standards Panel
IHS	Indian Health Services
Logical Conformance Test	This refers to the system's ability to ensure the semantically-correct content of the information being exchanged accurately fulfils the intention of the exchange. Examples of this type of conformance include queries for specific information engendering appropriate responses in kind (e.g. – ensuring a request for a lab result is not fulfilled with a medication history, or referencing the wrong patient).*
MPI	Master Patient Index
NCI	National Cancer Institute
NDMS	National Disaster Medical System
NHIE	NwHIN Health Information Exchange
NwHIN	Nationwide Health Information Network
NIST	National Institute of Standards and Technology
OID	Object Identifier or Home Community ID
ONC	Office of the National Coordinator
OS	Operating System

Acronym	Definition
Performance and Usability Test	This refers to the system's employment of appropriate and reasonable methods to fulfill the requirements. Examples of this type of conformance include fulfilling service-level agreements for availability, responsiveness, transaction levels, etc., that ensure the overall usability of the system.*
Robustness and Stability Test	This refers to the system's ability to appropriately handle exceptional operational conditions. Examples of this type of conformance include graceful handling of boundary conditions of correct operation (e.g. – high loads), negative cases, edge-system malfunction, attempted security breach, etc.*
Semantic Conformance Test	This refers to the system's ability to ensure the syntactically-correct content of the information being exchanged accurately represents the intended concepts. Examples of this type of conformance include referential-integrity checking of informational elements against prescribed vocabulary standards (e.g. – a given five digit code is actually valid within the endorsed version of the ICD-9 code set).*
SSA	Social Security Administration
SSL	Secure Sockets Layer
Syntactic Conformance Test	This refers to the system's ability to ensure the correct form of the information being exchanged based on required standards and constraints. Examples of this type of conformance include adherence to the definitions of message or document specifications, such as element length, element order, inclusion of required elements, etc.*
SDK	software development kit
VA	Department of Veterans Affairs

*Definitions provided by the NHIN Test Approach & Test Materials v.2

10.0 NwHIN DURSA AGREEMENTS

In order to transact health information with a group of Federal agencies and non-Federal organizations using an agreed upon set of national standards, services and policies developed by or under the auspices of ONC, a Federal agency or non-Federal organization must be accepted for participation by the Coordinating Committee and sign the Data Use and Reciprocal Support Agreement (DURSA). (Those who sign the DURSA are known as "Participants.") The DURSA provides an enforceable legal framework to support the exchange of individually identifiable health information among the Participants and eliminates the need for point-to-point agreements. The DURSA builds upon the various legal requirements that Participants are already subject to and describes the mutual responsibilities, obligations and expectations of all Participants under the Agreement. All of these responsibilities, obligations and expectations create a framework for safe and secure health information exchange, and are designed to promote trust among Participants and protect the privacy, confidentiality and security of the health data that is shared. All Participants are required to execute the DURSA before they are provided with the Digital Credentials that technologically enable them to transact health data with other Participants.

An initial group of Participants, including SSA, VA, MedVirginia and Kaiser Permanente, executed the DURSA in 2009 in order to support the first set of electronic health information exchange activities in production under the Agreement. Since then, other entities wishing to transact health information electronically using the agreed upon standards, services and policies have executed the DURSA. These entities include DoD, CMS and CDC as well as various non-Federal entities. Additional entities are expected to execute the Agreement over time. As a living document, the DURSA is being maintained using the process described in the Agreement. An amended and restated version of the DURSA became available in 2011. Like the 2009 version, the amended and restated version provides guidance through the Federal clearance process.

Based upon experience with the DURSA, it takes 4-6 weeks for Federal agencies to approve/execute a finalized agreement once it has gone through their clearance process. The primary driver for pushing this through the agency approval process is typically the agency's desire to exchange information in production by a date established by the agency, by contract or by Congressional mandate.

The latest information about the DURSA and the latest version can be obtained at HealthIT.hhs.gov: NHIN Resources

If you have any questions on the DURSA please email nhin@hhs.gov.

10.1 Execute the DURSA Agreement

The DURSA must be executed before the Agency can become a Participant. If an agency would like to become a Participant, it must submit an Application for Participation along with an executed DURSA Joinder Agreement and complete the application validation.