

NwHIN Enhancements

Request #20100102

Business Requirements Document



December 2010

Revision History

NOTE: *The revision history cycle begins once changes or enhancements are requested after the initial Business Requirements Document has been completed.*

Date	Version	Description	Author
2/11/2010	.09	Initial version	Cheryl Sklar
2/17/10	1.0	Document approved by the Business Owner and ESM	Tim Cromwell, Susan Lloyd
Post Sign Off Additions – Not Included in Project Scope and Estimate			
7/7/2010	2.0	Approval of revisions made to the following sections: 1.2 Goals, Scope and Objectives, and 2.3 CPP External System Interface Requirements. Functional requirements (2.1) and non-functional requirements (2.2) reprioritized, completed and inactive requirements identified, post sign-off changes documented	Tin Wong,
7/14/2010	2.1	Approval of business owner	Tim Cromwell
12/21/10	3.0	Approved by business owner, ESM, and OI&T	Tim Cromwell and Shawn Faherty approved on 12/15/10 Brian Morgan approved on 12/21/10

Table of Contents

1. Purpose	1
1.1. Overview.....	1
1.2. Goals, Objectives, and Scope.....	6
1.3. Success Factors.....	8
1.4. Organizational Need.....	8
2. Requirements	9
2.1. Business Needs/Owner Requirements.....	9
2.2. CPP External System Interface Requirements.....	46
2.3. Related Projects/NSR.....	47
3. Other Considerations	48
3.1. Alternatives.....	48
3.2. Assumptions.....	48
3.3. Dependencies.....	49
3.4. Constraints.....	49
3.5. Risks.....	49
Appendix A. References	50
Appendix B. Models	53
Appendix C. Stakeholders and Primary/Secondary Users	57
Stakeholders.....	57
Primary and Secondary Users.....	60
Appendix D. Enterprise Requirements	62
HealtheVet Requirements Management.....	62
Security Requirements.....	62
Privacy Requirements.....	62
508 Compliance Requirements.....	62
Executive Order Requirements.....	62
Identity Management Requirements.....	63
Appendix E. Acronyms and Abbreviations	64
Appendix F. Approval Signatures	67
Appendix G. Post Sign-Off Additions	68

Business Requirements Document

1. Purpose

The purpose of the Business Requirements Document (BRD) is to capture and describe the business needs of the customer/business owner. The BRD provides insight into the AS IS and TO BE business area, identifying stakeholders and profiling primary and secondary user communities. It identifies what capabilities the stakeholders and the target users need and why these needs exist, providing a focused overview of the request requirements, constraints, and Information Technology (IT) options considered.

1.1. Overview

The Department of Veterans Affairs (VA) deployed the Nationwide Health Information Network (NwHIN) in late 2009 as a pilot project. The Veterans Health Administration (VHA) Chief Health Informatics Office (CHIO) seeks enhancement of NwHIN so that implementation can be extended beyond the original pilot to an expanded pilot. NwHIN is an initiative for the exchange of healthcare information being developed under the auspices of the U.S. Office of the National Coordinator for Health Information Technology (ONCHIT). ONCHIT has been facilitating development of NwHIN technology and standards to provide a secure, nationwide, interoperable health information infrastructure that will connect providers, consumers and others involved in supporting health and healthcare. Upon consent of the Veteran, NIHN will enable bi-directional sharing of VA and non-VA health records. NwHIN enhancements are foundational to the President's goal of development of the Virtual Lifetime Electronic Record (VLER), an open architecture, non-proprietary, standards-based approach to exchange of health care information. The initial pilot is referred to as VLER 1A; the second phase as VLER 1B.

This request addresses changes need in support of VLER 1B as well as some of the future phase work. Specifically, enhancements are requested in the following areas:

- Release of Information (ROI)/Consumer Preferences and Policy Management System (CPP)
- Identity Management
- Interoperability
- Additional Partnerships (new pilot sites)
- Additional Content Domains
- End Users/User Interface
- Performance Measurement

ROI/CPP System

- CHIO requests the ability to electronically manage, integrate, and enforce VA consumer preferences, as well as organizational and United States (U.S.) security and privacy policies relative to Health Information Exchange (HIE). At VHA health care facilities, HIE occurs through the ROI process. While some aspects of the ROI process were automated through the VLER 1A pilot, additional enhancements are needed to fully automate ROI through the CPP System. Briefly, CHIO has identified the following issues with the ROI process:
 - The ROI process is primarily manual. For example, participants complete a paper authorization form and ROI staff manually review the form to validate it. The patient's health record is manually reviewed to verify the presence or

absence of certain protected conditions before information is shared. Additionally, the process for monitoring and identifying changes in the status of protected conditions requires ongoing manual record reviews. These manual processes are very labor intensive and increase the likelihood for errors to occur. VA does not have the staffing resources to support expanded HIE in the absence of automation or a policy change that would absolve the requirement for review for protected conditions when the purpose of use is for treatment of the Veteran.

- VA currently lacks the ability to create, provision, and enforce advanced patient preferences about who will be granted access to the patient's record and what information would be shared. For example, a patient consents to HIE at a hospital where he receives care from two doctors, if the patient does not want to share mental health information with one of his doctors, that functionality is currently not supported.

Identity Management

- During the VLER 1A pilot, deterministic matching was used to correlate the identities for the health record. Deterministic matching requires an exact match for each of the traits used, for example there must be an exact match on the patient's first, middle and last names. The majority of the time, manual intervention was required to create the match and subsequent correlation. Probabilistic matching¹ is needed in order to expand the number of patients who can be matched within the framework, which then allows an exchange as intended by the patient choosing to participate in HIE during the VLER 1B pilot.
- Before data can be shared between networks, the patient's identity needs to be correlated in the VA and participating external organizations. VHA tools currently available to identify and fix discrepancies, such as a potentially misspelled last name, with external partners are limited. Analysis is needed to determine if identity management tools should be expanded nationally to enable information exchange beyond the pilot sites. In addition, within the NwHIN today, there are no specifications to support any resolution activities for HIE. VHA Identity Management Service needs to determine if adjustments to the matching algorithm are required and if any extension of the current tool set would be beneficial for the NwHIN goals.

Interoperability

- There are new interoperability NwHIN specifications that became effective January 2010 that need to be incorporated into the current system.² Additionally, as new NwHIN standards are released, they need to be incorporated into future NwHIN enhancements. Finally, shortcuts were taken to implement the pilot by the December 2009 deadline that do not adhere to existing and new standards. These shortcuts must be re-engineered.

Additional Partnerships

- It is anticipated that there will be at least one new partner for VLER 1B. Infrastructure enhancements are needed to expand exchange through NwHIN beyond the VLER 1A pilot sites. It is anticipated that there may be as many as 1,000 new partners. Architecture needs

¹ Probabilistic matching is a statistically based method for identifying matches. It allows one to use informational content of the data to identify matches. It does not require an "exact" match on all criteria, as is required with deterministic matching.

² See reference to Nationwide Health Information Network: Resources, 2010 NwHIN Final Production Specifications.

to be established so that, when a potential new community passes an interoperability test, it can be included as a new partner without further software deployment.

Additional Content Domains

- Expand the information that can be exchanged through NwHIN. A limited amount of standardized health summary information is being exchanged through a pilot project.³ The Recommendations of the Interagency Clinical Informatics Board (ICIB) regarding expanded standardized information exchange are incorporated into this proposal.⁴

End Users/User Interface

- Veterans Information Systems and Technology Architecture (VistA)Web is the user interface that displays the health information from the external entity to the VA provider. During the VLER 1A pilot, issues were identified with the usability of VistAWeb, for example, display of missing information was unclear. Improvements to the user interface are needed in order to enhance information sharing during VLER 1B.

Performance Measurement

- During the VLER 1A pilot, preliminary data were collected to determine the utilization and value of the information being shared. VLER 1A data collection processes are extremely labor intensive. For example, in order to assess the content of the potential and actual information shared, a copy of the patient information must be manually requested and retrieved for each patient. It is anticipated that limited automation of data collection processes will be provided as part of VLER 1B; more complete automation of data collection processes will be provided in the future.

Additional Background on ROI:

Under the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, a covered entity is permitted to use or disclose Individually Identifiable Health Information (IIHI) for treatment, payment, or health care operations purposes without the signed written authorization of the patient. However, any individually-identifiable information related to treatment of drug abuse, alcohol abuse, sickle cell anemia, and testing or treatment for Human Immunodeficiency Virus (HIV) has special protection under 38 U.S.C. Section 7332. VHA must have signed patient authorization in order to disclose health information for treatment, payment, or health care operations. This is different from authorization for treatment and informed consent obtained as part of participation in a research study.

VHA Handbook 1605.1 Privacy and Release of Information, defines the circumstances when written authorization by the patient or person authorized to sign for the patient is required prior to disclosing health information. Currently, VHA requires completion of VA Form 10-5345 to document authorization for ROI. This form is used to obtain the following information:

- Patient demographic information for identity management
- Description of the information to be disclosed, including disclosure of protected information (section. 7332) on drug abuse, alcohol abuse, sickle cell anemia, and testing or treatment for HIV

³ Components of Healthcare Information Technology Standards Panel (HITSP) C32 being exchanged include Patient information, emergency information, allergies, problems, active medications and source of sending system.

⁴ Additional information about ICIB recommendations is contained in the “Virtual Lifetime Electronic Record (VLER) and NwHIN July 2010 Feasibility and Analysis: Summary of Findings” and “VLER Summary Recommendations Final” documents available in the References section.

- Purpose
- Identification of the person or office requesting the disclosure
- Expiration date, satisfaction of the need for disclosure, or under a certain condition
- Signature of individual
- Date signed

VA Form 10-5345 is manually reviewed to determine the validity of the authorization based upon the information contained therein. As part of the determination of the validity of the authorization, the electronic record is manually reviewed for the presence of Title 38 U.S.C. 7332 protected information. If the patient's record does not contain Title 38 U.S.C. 7332 protected information or if the patient has authorized sharing Title 38 U.S.C. 7332 protected information, Health Information Management (HIM) staff at the specified VA Medical Center (VAMC) make a paper copy of the requested record or may, when requested, provide a copy of the record on a computer disc to the person or office identified on the authorization form.

A request has been submitted to the Office of Management and Budget (OMB) to change legislation so that 7332 diagnoses⁵ will not be protected for treatment purposes. It has been assumed that the legislation will not be changed in time for the VLER 1B pilot. Until such time as the legislation has been changed, or relief from the change in status requirement from the Office of General Counsel, ROI will need tools that allow for automated recognition of 7332 protected conditions on initial opt-in of patients to determine validity of patient authorization, and ongoing detection of protected conditions not present at the time of patient opt-in.

HIPAA also allows patients to make restriction requests regarding who may or may not see portions of their health information. Restriction requests must be in writing and signed. VHA is not mandated to grant a restriction request.

Document Storage Systems (DSS) ROI Records Management (RM) Software is used by HIM staff to maintain an accounting of disclosures. The DSS ROI RM Software allows VHA to provide patients with a summary of the disclosures. However, this software application was not designed to support other aspects of the current ROI process. For example, the software does not have the ability to retain and retrieve authorizations (VA Form 10-5345) for ROI purposes. At this time, authorizations are scanned into VistA Imaging. CHIO is requesting the development of a new comprehensive solution to support all aspects of the ROI process.

Additional Background on Identity Management:

The Healthcare Identity Management (HC IdM) Program is the data steward for VHA's patient identity information. HC IdM encompasses the business processes related to a patient or beneficiary's electronic medical record, which identify the individual using the Integration Control Number (ICN) throughout healthcare processes, enable the identification of that patient within the computer system and facilitate selection of the correct patient record, and create the longitudinal Electronic Health Record (EHR) across all VHA systems for a patient within that system (correlations). The HC IdM Program utilizes a robust set of tools and processes to perform their data quality work on patient records. VHA software is used to address potential identity management issues, including potential duplicates, overlays, and catastrophic edits to patient identity. Similar tools do not currently exist to resolve patient identity issues between VHA and external organizations.

⁵ Protected diagnoses include drug abuse, alcohol abuse, sickle cell anemia, and testing or treatment for (HIV).

Background on Pilot Projects:

This requirements document builds on pilot projects being developed and implemented at the San Diego VAMC in support of ROI capabilities and expanded health information sharing. The CPP System that is being initiated through this pilot and further developed through this request will utilize NwHIN standards, protocols, legal agreements, specifications, and services to enable the secure exchange of health information over the internet.

VLER Phase 1A Pilot:

In phase 1 of the pilot, released in December 2009, approximately 1,100 patients who receive care at the San Diego VAMC and through Kaiser Permanente (KP) were solicited for participation in the information sharing pilot. VA and KP patients who provided authorization, or opted-in, have agreed to health information sharing between these two entities for a period of up to five years. There has been an initial validation of the authorization to ensure it is correct and ongoing validation will occur to identify any possible change in the presence of Title 38 U.S.C. 7332 protected information compared to the initial authorization.

The pilot also includes HIE with the Department of Defense (DoD) and VA. Per a Memorandum of Understanding (MOU) authorization is not required prior to HIE between VA and DoD for treatment purposes.

VA Form 10-5345 is used to document the authorization to exchange health information between the VA and KP facilities. For the pilot, the purpose of the disclosure is “treatment,”⁶ which is automatically assigned, as it is the only purpose for which the health information is being exchanged. Also, the description of the information disclosed is automatically assigned; it has been predetermined that only some of the information contained in a HITSP C32 health care summary will be shared. The ROI Office will scan this form into the EHR using VistA Imaging.

Patient identities between VA and KP are correlated so that an exchange of information can occur. If the patient has opted-in to the pilot and has had a successful correlation, a display is provided in VistAWeb indicating that records are available from KP when the VA provider accesses the patient’s EHR. The patient’s KP record is queried, standard information retrieved, and displayed to the VA provider. Similarly, the VA record is displayed to the KP provider.

The ROI Office determines when a patient revokes or opts-out of HIE, or when there has been a change in the presence of Title 38 U.S.C. 7332 protected information compared to the initial authorization. The ROI Office manually documents, in the CPP System, information about patients who opt-out. Once the patient has opted-out, the System no longer allows for the exchange of health information between the VA and KP. Spreadsheets are used to track patients who opt-in and opt-out. Weekly or monthly reports of patients who opt-in and opt-out can be generated from the CPP System.

All VA disclosures of the patient’s EHR to KP and DoD are tracked and accounted for in accordance with the Privacy Act. The accounting of disclosures must include name of the patient, the date of each disclosure, a description of the information disclosed, the purpose of each disclosure and the name, and the address (if known) of the person or agency to whom the disclosure was made.

During the pilot, the San Diego VAMC ROI staff creates reports of disclosures made to KP and DoD using information obtained from a variety of sources. One of these sources of information is the Accounting of Disclosures Report provided by the NwHIN Development Team.

⁶ Information needed for on-going care and treatment of the patient.

Access Control Service

A Class III Access Control Service (ACS) will be used as a security and privacy solution to enforce Role-Based Access Control (RBAC) and consent directives.⁷ The ACS will be developed in collaboration with HITSP and the Organization for the Advancement of Structured Information Standards (OASIS). Portions of the solution have been accepted for use in the NwHIN and are incorporated within the NwHIN Connect Gateway.⁸ VA has purchased Commercial-Off-The-Shelf (COTS) products that can be combined to provide some of the ACS functionality. Once the Class III ACS is successfully in production at the San Diego VAMC, it will be submitted for enterprise-wide deployment via a Class III to class I New Service Request (NSR) process.

Specifically, the ACS will be used to read and parse standardized authorization assertions accompanying a request for VA HIE between the VAMC and KP. The ACS uses security and privacy rules, VA provided authorization attributes, and the requester's authorization attributes to make and enforce an access control decision regarding a request. If the access control decision is affirmative, then the requested information will be provided to the authorized recipient. If it is not affirmative, the request will be denied. The ACS may mask certain requested information in the request response. The ACS will create audit records of security-relevant events.

In addition to VA Form 10-5345 and the HIPAA restriction request process, other standards development organizations, such as HITSP and Health Level Seven (HL7) are investigating new ways for patients to create and submit consent directives electronically. VA is also investigating how patients can use forms accessed through patient portals, such as MyHealth_{Vet} (MHV) to create consent directives. Some of this investigation will occur through the second phase of the San Diego pilot project.

The ACS Pilot will allow additional patients, beyond the original ones invited to participate in the VLER phase 1A phase, to opt-in to the exchange of their records. Also in phase 2, other sites in addition to the San Diego VAMC, KP, and DoD, will be invited to participate.

VLER 1B Pilot

The VLER 1B pilot will begin in February, 2010 and complete by July 31, 2010. In addition to participation by the VLER 1A partners (San Diego VAMC, KP and DoD), one additional partner will be included in the VLER 1B pilot. Specific goals, objectives, and scope of the VLER 1B pilot are provided in section 1.2.

These projects are important first steps towards automating HIE. Additional enhancements identified in this document are needed in order to expand the information that is exchanged; expand beyond the pilot sites; analyze and automate, where possible, the HC IdM resolution process; fully automate collection of consumer (patient) authorization requirements as documented in VA Form 10-5345 as well as enforce consumer preferences as documented in consent directives and organizational policies relative to HIE.

1.2. Goals, Objectives, and Scope

Veterans receive care from both VA and non-VA facilities. In order for appropriate clinical decision making to occur, support for sharing of information between all of the entities where the patient has been treated is needed. According to the 2007 Survey of Veteran Enrollees' Health and Reliance Upon VA, 42 percent of respondents planned to use VA as their primary source of care, 12 percent would use VA as a back-up to non-VA care, and 13 percent only use VA for prescriptions. Similar results were reported in the 2005 Survey.

⁷ 2009 0331 Class III Deployment Request for the San Diego VAMC (this is not an enterprise-wide Class III request). The initiation date for the phase 2 pilot is not known at this time.

⁸ NwHIN CONNECT is a federal program to develop a standard NwHIN adaptor for exchange of information.

One goal of this request is to create an enterprise-wide electronic solution capable of supporting consumer authorization requirements, consent directives, and organizational policies on privacy and security relative to ROI. A consent directive is the record of a healthcare consumer's privacy policy that grants or withholds consent to share information. According to HITSP, a healthcare consumer may have zero to many consent directives corresponding to zero to many governing jurisdictional and organizational policy sets. Multiple consent directives may exist for the same electronic health information. A consent directive may be created, revised, or revoked. A consent directive requested by the consumer must be approved prior to its implementation. Organizational policy consists of business rules applicable to ensuring secure and private access to and sharing of protected data, systems and functions, as well as the requirements related to tracking or accounting for the disclosure resulting from health information sharing. In general, an organizational policy business rule specifies the attributes of the user (such as identification, purpose of use, user role(s), and permissions on requested objects...etc.), the constraints to be applied (location, time, cardinality⁹, separation of duty...etc.) and any obligations (such as an audit) that must be adjudicated prior to a system granting access to its protected objects. Additional goals of this request include additional analysis and automation, where possible, of HC IdM data quality and performance management processes; enhanced information exchange between VHA and an expanded list of external organizations as well as improvements to the user interface.

VA has identified the need for further development of NwHIN capabilities beyond what is being evaluated in the pilot. Specifically, the objectives of this request are to provide for:

- Patient creation and management of their own privacy preferences. This will include the ability to create and submit patient consent directives to the ROI Office, either as a paper form or electronically using emerging HL7 messaging standards, as well as management, electronic signature, and tracking of all consent directives.
- ROI Office management of patient request preferences. This will include ROI Office ability to receive, validate, store, and create reports of patient consent directives.
- ACS security and privacy policy management. This will include ACS ability to create, update, suspend, and test security and privacy policies.
- Enforcement of security and privacy policies created by ACS management services.
- Creation of an accounting of disclosures that permits the tracking of all disclosures made by VHA. Expanded standardized information sharing beyond the limited health summary exchange occurring in the pilot.
- Implementation of probabilistic matching of patient identities to increase the number of correlations to external organizations that are created without any manual intervention and minimize the number of false negative matches.
- Development of additional HC IdM data quality resolution tools to interface with external organizations, based on analysis conducted from data collected during VLER 1A. These tools will help address potential issues that may occur with external sharing partners such as shared patient data non-match issues, the need to update VHA patient traits, and managing existing correlations in support of HIE and VHA duplicate patients. These tools will not be used to add new patients to the system. If, during the NwHIN patient discovery process initiated by the sharing partner, it is determined that the patient is not found in VHA, the sharing partner will be informed that the patient does not exist. The purpose of the external relationships is to share information for existing patients only.

⁹ Cardinality is whether this is a one to one, one to many, or many to many relationship.

- Adoption of additional NwHIN specifications. This will enable information exchange to occur with Beacon Communities¹⁰ and other private parties.
- Implementation of ICIB recommendations for exchanging additional information to share additional content domains, such as vital signs and laboratory results.
- Automation of performance management activities. Manual methods used during VLER 1A will be replaced, as they are too labor intensive to be used with expanded information exchange to additional sites and additional content domains.

1.3. Success Factors

Success Factors	Measurement
Patient consent directives (patient preferences) are captured electronically.	Consent directives can be created, retrieved, and displayed electronically, upon implementation of this enhancement, 100% of the time.
Patient consent directives (patient preferences) will be electronically enforced.	Automation of HIE with individuals and other entities will incorporate patient preferences regarding opting in and opting out to disclosure of Protected Health Information (PHI), upon implementation of this enhancement, 100% of the time.
System will incorporate VA and other federal policies relative to ROI.	Automation of ROI with individuals and other entities will incorporate organizational policies regarding security and privacy, upon implementation of this enhancement, 100% of the time.
Identity management using probabilistic matching.	False negative matches will be reduced by a percent to be determined after analysis is completed.
Identity management tools for use with external partners are implemented.	Facilitate patient matching and resolve identity management issues 80-100% of the time.
Outstanding NwHIN specifications are adopted.	Phased implementation of 100% of NwHIN technical requirements by VA.
Expanded health information is shared with external partners.	Upon successful ROI and identity correlation, additional health information will be displayed to VA and non-VA providers participating in NwHIN 75% of the time.
Utilization of the information exchanged can be determined.	Automation of 15% of current manual data collection processes.

1.4. Organizational Need

The proposed NwHIN enhancements are consistent with the Eight for Excellence goal to continuously improve the quality and safety of healthcare for Veterans, particularly in those health issues associated with military service, as well as the Under Secretary's VHA Power of Performance goal to put patient care first.

Additionally, this request is consistent with the following Presidential Executive Orders (EO):

- The first is EO 13335: *Incentives for the Use of Health Information Technology and Establishing the Position of the National Health Information Technology Coordinator*. EO 13335 established ONCHIT. Since its inception, ONCHIT has led a national discussion on the role that healthcare IT can have in enabling improvements in quality, timeliness, and cost effectiveness of healthcare delivery. ONCHIT has sponsored NwHIN development

¹⁰ Beacon is a Health and Human Services (HHS) branded program that will invest in communities that have a demonstrated level of EHR capability to elevate them to full capacity of electronic HIE exchange and demonstrate the capability and benefits of this approach on a large scale.

and testing of possible architectures for interoperable, standards-based health care information exchange.

- The second is EO 13410: *Promoting Quality and Efficient Health Care in Federal Government Administered or Sponsored Health Care Programs*. This request supports the purposes of the executive order by promoting the use of Health Information Technology (HIT) and by making relevant information available to beneficiaries, enrollees, and providers in a readily usable manner.

Further, Title XIII of the American Recovery and Reinvestment Act of 2009 includes the Health Information Technology for Economic and Clinical Health (HITECH) Act. Key provisions of this Act include funding and incentives for IT adoption, codification of the ONCHIT, and strengthened privacy provisions. Privacy and security protections are essential to building public trust and encouraging the use of HIT. Electronic exchange of consumer preferences is integral for enhanced privacy, security and public trust in the exchange of health information.

Lastly, this request is consistent with the President’s request for the development of seamless health information sharing between DoD and VA through the development of VLER. VLER will provide uniform, comprehensive, and convenient access to health information as well as streamline information exchange. The proposed NwHIN enhancements will begin to provide the foundation necessary to implement VLER. This request supports the VLER/Beacon Communities Regional Health Information Network initiative on the VHA Op Plans.

2. Requirements

In the table below, each of the requirements is ranked as being required for VLER 1B, optional for VLER 1B, or long term, meaning that it has been prioritized to be addressed in the next phase or phases. For business needs 1 through 5 the term “optional” indicates requirements that are required but supportable only upon additional funding for CPP development (i.e. outside of current funded task orders). The CPP requirements corresponding with needs 2-5 correlate with the functional layers in the Reference Business Policy Management and Enforcement Model found in [Appendix B](#). These include patient privacy management, consent management, security management, and ACS.

2.1. Business Needs/Owner Requirements

Requirements unique to this request have been documented in this section. In addition, this section includes requirements from other sources so that a single consolidated list of requirements is provided. These other sources include:

- Enterprise requirements that are applicable to the CPP System and HC IdM are identified in the table below by their ENTR number.
- VA authentication services requirements as described in the Personal Identity Verification (PIV) Integration: Authentication Services BRD (#20080343) relevant to this request are identified in the table below with their PIV number.
- PIV Identity and Access Management (IAM) requirements contained in the PIV Integration: Access Control Services BRD (#20090803) relevant to this request are identified in the table below with an IAM number.

Business Need (BN)	OWNER Number	Owner Requirement (OWNER)	Ranking*: Baseline from February 2010 BRD	Ranking**: from June 2010 re-prioritization	1C

***In Column D: R=Required VLER 1Bi, O=Optional VLER 1Bi, L=Long Term**
****In Column H: 1Bii R= Required VLER 1Bii, 1B O= Optional VLER 1Bii, or L=Long Term**
RED text = requirement change or addition; Strike through denotes an inactive requirement.
Phase 1C requirements are in blue and include: Consumer Preference and Policy (CPP) Release of Information (ROI) updates, ICIB 9/9/2010 requirements and requirements identified by Jamie Bennett are identified in column I

BN 1: Transitional CPP Capabilities					
	1.1	Provide the ability to add new partners in the authorization for release. <i>(The form and the CPP users are not impacted, but the CPP interface within the adapter needs to be updated to accommodate new partners until CPP is separated from the Adapter - including the disclosure report, correlation, etc.)</i>	R	1Bii R (workaround still needed)	Completed
	1.2	Create and implement a capability that allows VA to limit the Nationwide Health Information Network partners that will participate based upon VA policy.	R	Completed	Completed
Post sign-off change	1.3	Make system changes to the CPP to enforce the VA 10-5345 10-0485 authorization to release information to allow VA patients to consent to release their records to all Nationwide Health Information Network partners.	L	Completed	Completed
Post sign-off deletion	1.4	Record the presence of protected conditions at the time of opt in.	R	Inactive	Inactive
Post sign-off deletion	1.5	Provide an automated way to detect changes in 7332 protected conditions that were not present at the time of opt in	L	Inactive	Inactive
Post sign-off deletion	1.6	Modify the opt in/opt out ROI report	R	Inactive	Inactive

Post sign-off deletion	1.6.1	Include in the opt in report the patients' 7332 status at time of opt in (same four boxes as on the 10-5345)	R	Inactive	Inactive
Post sign-off deletion	1.6.2	Include information about whether the patient has successfully correlated with each entity or not.	R	Inactive	Inactive
Post sign-off deletion	1.6.3	Include total counts of the numbers of patients who have opted in, opted out, and correlated.	R	Inactive	Inactive
Post sign-off addition	1.7	Provide the ability to support the OASIS XACML interface (i.e. an XACML Decision Request/Response) between the Adaptor and the CPP Policy Decision Point for to request/receive access control decisions for subsequent enforcement by the Gateway Policy Enforcement Point.		1Bii R	Inactive, Inserted as a technical note for requirement 5.1
Post sign-off addition	1.8	As a temporary/intermediate step, provide the ability to import ROI Office approved opt-in forms from the CPP ROI System into VistA Imaging for storage in the Veterans' patient's official health record.		1Bii O	Changed Veteran to patient R-conditional on phase for portal
	1.9	Provide in-person proofing of an identity, proofed at an appropriate level of assurance as specified by policy, to the Veteran patient identifier			R
	1.9.1	Ensure that only Veteran patients identity proofed at the level of assurance specified by policy can access the electronic consent directive capability			R
	1.9.2	If a potential duplicate is identified for a given patient, that patient cannot be shared			R

		across the N HIN.			
	1.9.3	If a patient mismatch is identified, that patient should be unlinked			R
	1.9.4	Validate that the enterprise identifier (ICN) printed on the in-person authentication (IPA) subject Veteran Identification Card (VIC) matches the correlated ICN, otherwise initiate a process to correct the VIC.			L
	1.9.5	Ensure that the consumer preferences and policy (CPP) systems are capable of accepting enterprise identifier (ICN) updates from the Master Veteran Index (MVI) system to the Veteran patient identifier.			R
	1.10	Provide the ability to batch announce a list of all shared VA/DoD patients in a VLER community.			R
BN 2: Patient Privacy Management – Patient electronic management of their own consent directives.					
Post sign-off addition	2.1	Provide a means for Veteran clients patients to express (create, modify, and cancel) and manage privacy preferences by filling in, signing, and submitting an electronic consent directive form (e.g., authorizations, restriction requests or revocations).		1Bii R	R Changed Veteran clients to patient
Post sign-off addition	2.1.1	Provide patients and authorized individuals with the ability to electronically create a consent directive by submitting a new authorization or restriction request which will negate any currently existing consent directive.		1Bii R	R Deleted "which will negate... consent directive."

Post sign-off change	2.3.8 2.1.2	Provide patients and authorized individuals with the ability to electronically revise a consent directive by submitting a new authorization or restriction request, which will negate the original.	R	1Bii R	R
	2.1.2.1	Provide the ability to pre-populate the consent directive with information submitted from previous electronic consents.			R
	2.1.2.2	Provide the ability to pre-populate the consent directive with authoritative demographic information.			L
Post sign-off change	2.3.9 2.1.3	Provide patients and authorized individuals with the ability to electronically cancel a consent directive by submitting a new authorization or restriction request, which will negate the original.	R	1Bii R	R Deleted "by submitting ...original." "
Post sign-off addition	2.1.4	Receive and validate an authorization preferences that has been provided by external trusted partners.		L	L Changed preference to authorization
	2.1.5	Detect a change in the patient's preferences from the external trusted partner, and automatically update the CPRS status (technical note: attempt to re-correlate patient fails)			L
Post sign-off change	2.2.4 2.2	Provide the patient with the ability to restrict ROI based upon attributes defined by the current version of the Nationwide Health Information Network NHIN standards setting organizations (for example, the patient may want to restrict exchange of mental health information).	L	1Bii R	R
CPP/ROI Update	2.2.1	Display pre-approved policies in the user interface as options that the patient can select.			R

Post sign-off change	2.2.7 2.3	Provide the capability to patient with the ability for the patient to restrict ROI based upon standard attributes such as name, role, purpose of use, organization, and location. OASIS XSPA to a requesting approved partner.	L	1Bii R	R
Post sign-off change	2.2.6 2.4	Provide patients and authorized individuals access to consent directive management processes (e.g., creating, modifying, or revoking their privacy information, options and policies) through a VA authorized the MHV portal (e.g., MHV or e-Benefits), leveraging the delegation feature already scoped within MHV.	R	1Bii R	R
Post sign-off addition	2.4.1	Provide the Veteran patient an online consent packet that can be printed and mailed-in.		1Bii R	R Changed Veteran to patient
Post sign-off addition	2.4.1.1	Allow additional identifier information to be appended to the form when completed online.		1Bii R	R
Post sign-off change and CPP/ROI update	2.3.1 2.4.3	Provide patients with the ability to electronically generate a printable report of current and previously created, changed, and revoked consent directives.	O	1Bii R	R
CPP/ROI Update	2.4.3.1	Provide patients with the ability to print and download draft consent directives in humanly readable format as a file (pdf).			R
CPP/ROI Update	2.4.3.2	Provide patients with the ability to download signed (current and historical) and submitted consent directives in humanly readable format as a file (pdf)			R

Post sign-off change and CPP/ROI update	2.3.2 2.4.4	Provide patients with the ability to begin a consent directive online and complete it at a later session and delete a draft without re-entering information.	O	1Bii R	R
Post sign-off change and CPP/ROI update	2.3.3 2.4.5	Provide patients with the ability to review all consent directives submitted, or approved, or in progress and allow them to create, update, and delete revoke them.	O	1Bii R	R
CPP/ROI Update	2.4.6	Provide patients with the ability view frequently asked questions (FAQ) for basic assistance in completing forms and clarifying participation requirements .			R
Post sign-off change and CPP/ROI update	2.3.4 2.4.6 2.4.6.1	Provide patients with the ability to submit on-line queries for basic help desk assistance in completing forms, clarifying participation requirements, and follow-up on the status of consent directives (use of help desk should be consistent with portal being used).	O	1Bii R	L
Post sign-off change	2.3.6 2.4.7	Provide patients with an electronic display of created, changed, and revoked consent directives.	O	1Bii R	R
Post sign-off change	2.4 2.5 PIV 4.2	Provide Line of Business consumer (e.g. patient) digital signature capability for integration with Line of Business consumer applications.	R	1Bii R	R
Post sign-off change	2.3.5 2.5.1 PIV 2.3	Provide patients and authorized individuals with the ability to electronically digitally sign consent directives as part of a larger VA managed service.	R	1Bii R	R Replaces 2.9
Post sign-off change and CPP/ROI update	2.2 2.6 IAM 4	Consumer Reporting Requirement: Provide the ability for patients to request and view a report of who, on the Nationwide Health Information Network, has seen or tried and failed to see (access denied)-information enforced by their consent	O	1Bii O	O Added accounting of disclosures

		directive(s) (accounting of disclosures).			
Post sign-off change	3.5.8 3.7.8 IAM 56 2.6.1	For service to its health care users (e.g. patients), reporting under the Consumer Reporting Requirement shall include relevant demographic information (name, location, information accessed) presented in a natural language format (no technical/specialized knowledge required to read).	L	L	L
Post sign-off change	2.2.1 2.7	Provide patients and authorized individuals with the ability to submit both paper and electronic consent directives.	R	1Bii R	R
Post sign-off change	2.2.2 2.7.1	Allow manual methods to be used by the patient or authorized individuals to create, revise, or revoke consent directives.	R	1Bii R	R
Post sign-off change	2.2.3 2.7.2	Allow manually created authorizations consent directives to be input into the electronic system.	R	1Bii R	Inactive
Post sign-off change	2.2.6.1 2.8	Provide a capability to identify and link shared patients across VA and selected partners. shared capability to identify patients across VA and DoD.	R/L	Completed	Completed
Post sign-off change	2.5 2.9	Provide support for implementation of an electronic consent directive signature capability as specified by the Office of General Counsel (OGC) for recognition as a legally acceptable signature.	R	1Bii R	Inactive Replaced by 2.5.1
Post sign-off deletion	2.1	Provide patients with the ability to make and manage requests regarding personal privacy preferences concerning access and use of the electronic health information.	R	Inactive	Inactive
Post sign-off deletion	2.2.5 IAM 59	Provide the capability for a patient to express consent directives based upon a	R	Inactive	Inactive

		healthcare user's structural role(s):			
Post sign-off deletion	2.3 IAM 58	Provide a means for healthcare consumers (Veteran patients) to express (create, modify, and cancel) privacy preferences by filling in, signing, and submitting an electronic form (authorizations, consent directives, or restriction requests):	R	Inactive	Inactive
Post sign-off deletion	2.3.7	Provide patients and authorized individuals with the ability to electronically create consent directives.	R	Inactive	Inactive
BN 3: Consent Management – Administrator electronic management of organizational security and privacy policies.					
Post sign-off addition and CPP/ROI update	3.1	Provide the ability for the ROI Office to process electronically submitted consent directives opt-in submissions .		1Bii R	Completed
Post sign-off addition and CPP/ROI update	3.1.1	Provide the ability for ROI system to process pre-approved, as defined by policy, simple electronically submitted opt-in consent directives submissions .		L	R
Post sign-off addition and CPP/ROI update	3.1.2	Provide the ability for the ROI system to receive, review and process complex electronically submitted consent directives opt-in submissions not pre-approved by policy.		L	R
CPP/ROI Update	3.1.2.1	Provide the ROI Office with the ability to input manually created consent directives into the electronic system.			R
CPP/ROI Update	3.1.2.2	Provide the ability to change to a default opt-in in response to legislative relief for 7332 protected conditions			L

CPP/ROI Update	3.1.2.3	Provide the ROI Office with the ability to view electronically submitted consent directives in a humanly readable format.			R
CPP/ROI Update	3.1.2.4	Provide the ROI Office with the ability to print electronically submitted consent directives.			R
CPP/ROI Update	3.1.2.5	Provide the ROI Office with a view of current and historical signed consent directives (created, changed, and revoked).			R
CPP/ROI Update	3.1.2.6	Provide the ROI Office with the ability to download current and historical signed consent directives (created, changed, and revoked) in humanly readable format as a file (pdf)			R
Post sign-off addition	3.1.3	Upon successful electronic submission of a consent directive opt-in , associate append an identifier (such as an ICN) to the patient information.		1Bii R	R
Post sign-off addition	3.1.4	Allow the ROI office to retrieve the patient consent directive look up the opted-in patient using the additional identifier (such as ICN).		1Bii R	R
Post sign-off addition	3.2	Provide the ability for ROI to process a complex set of restrictions and revocations.		L	Inactive
Post sign-off addition	3.2.1	Provide the ability for ROI to process a limited set of restrictions and revocations.		1Bii R	Inactive
Post sign-off addition	3.3.3 3.3	Provide the ability for the system to generate and send an electronic notification to the Veteran patient.		1Bii R	R Changed Veteran to patient
Post sign-off addition	3.3.1	Notify Veterans patients, via the portal, ahead of the go live date for a new partner that their information will be shared with a new partner.		L	R Changed Veteran to patient and other rewording
Post sign-off addition	3.3.2	Provide the ability for the system ROI office to notify the Veteran patient when the latest submitted consent directive has been		1Bii R	R

		approved or denied. he/she has been successfully opted in.			
Post sign-off addition	3.3.3	Provide the ability for the system to generate a notification letter to be printed/mailed to the Veteran patient.		1Bii R	R Changed Veteran to patient
	3.3.4	Provide the ability for the system to generate and send an electronic notification to the Veteran patient, at defined intervals, when their consent directive is about to expire.			L Changed Veteran to patient
	3.3.5	Provide the ability to automatically set a consent expiration date of 5 years for consent directives (opt-in and restrictions).			R
Post sign-off change	3.5.9 3.7.9 3.3.6	Provide the ability to automatically opt-out (stop sharing) those patients whose authorizations have expired until a new authorization is entered.	L	L	R
Post sign-off change- Moved to BN 4.4	3.1	Provide the ability to download and integrate approved patient privacy policies from Consent Management Services to create composite security and privacy policy sets for ACS enforcement.	L	Inactive	Inactive
Post sign-off change	3.2 3.4 ENTR1 165	Consent Administration: Provide consent management services to administer organizational and patient privacy policies.	L	L	L
Post sign-off change	3.2.1 3.4.1	Provide consent management administrators with the ability to centrally administer cross-cutting patient authorizations consent directives for all VA healthcare systems under their control.	L	L	L

Post sign-off change	3.3 3.5	Provide properly authorized privacy policy consent management administrators with the ability to centrally manage validate, authorize, and approve (grant, modify, or revoke) patient consent directive requests and privacy policies and attributes (validate, authorize, preapprove or deny).	L	L	L
Post sign-off change	3.3.1 3.5.1	Provide an automated receipt of consent directive requests so that they can be reviewed and validated by authorized privacy administrators consent management administrators.	L	L	R As soon as the patient has the ability to electronically submit this requirement is also required.
Post sign-off change	3.3.2 3.5.2	Provide consent management administrators with the ability to validate patient requests to create, modify, or revoke delete consent directives.	L	L	R As soon as the patient has the ability to electronically submit this requirement is also required.
Post sign-off change	3.3.3 3.5.3	Provide consent management administrators with the ability to periodically re-validate information submitted in a patient's request to create, modify, or revoke delete a consent directive.	L	L	R As soon as the patient has the ability to electronically submit this requirement is also required.

Post sign-off change	3.3.4 3.5.4	Provide consent management directive administrators with the ability to review all patient and VA-created privacy policies for inconsistent, duplicate, or conflicting rules prior to actually approving them for enforcement.	L	L	R As soon as the patient has the ability to electronically submit this requirement is also required.
Post sign-off deletion	3.2.5	Provide the ability to compare Title 38 U.S.C. 7332 protected information status between the health record and the consent directive to ensure that no PHI is released without proper authorization on file	L	Inactive	Inactive
Post sign-off deletion	3.2.6	Provide the ability to trigger re-validation of consent directives by detecting Title 38 U.S.C. 7332 protected information status changes as they occur.	L	Inactive	Inactive
Post sign-off change	3.3.7 3.5.5	Upon validation by consent directive administrators, trigger discovery of VA patients that have authorized their participation in cross-enterprise health care information exchange through the Nationwide Health Information Network.	L	1Bii R	R
CPP/ROI Update	3.5.6	Upon approval of consent directive changes by the ROI Office, provide an electronic notification to external partners if approved changes modify the conditions of the previous consent directive.	Mike will contact HHS to ask about status of HITSP TP 30		L

Post sign-off change	3.4 3.6	Provide consent directive administrators with the ability to create an automated accounting of disclosures over the Nationwide Health Information Network to include: 1) A list of disclosures of health information 2) The date of each disclosure 3) The description of the information disclosed 4) The purpose of each disclosure or a copy of a written consent directive 5) Name and address (if known) of the person or agency to whom the disclosure was made.	L	1Bii R	Completed
Post sign-off change	3.4.1 3.6.1	Provide the ability to search and sort through the accounting of disclosure by patient and date range and to print the accounting of disclosures for a specific patient.	L	L	R
Post sign-off change	3.5 3.7	Provide consent directive administrators with the ability to create, retain, and forward electronic reports and records as required.	L	L	L
Post sign-off change	3.5.1 3.7.1	Provide consent directive management administrators with the ability to automatically collect, collate, and analyze audit information for privacy breach notification reporting purposes.	L	L	L Added "automatic ally"
CPP/ROI Update	3.7.1.1	Provide the ROI Office with the ability to create canned and ad hoc reports, including reports by individual patient, patients by facility, VISN and nationwide (for example: count and /or list of patients in an opt-in status, count/list of patients in an opt-out status, patients whose consent directives are expiring in a specified timeframe, restriction requests by category, Accounting of Disclosures, consent directives pending approval, and consent directives denied).			L

CPP/ROI Update	3.7.1.2	Provide the Information Access & Privacy Program Office as well as the Health Information Management Program Office with the ability to create reports (see 3.7.1.1)			L
CPP/ROI Update	3.7.1.4	Provide the ROI Office with different views of electronically submitted consent directives (ad hoc report, facility/station, date, status, expiration date, all of the pending consent directives needing processing, search by patient)			L
Post sign-off change	3.5.1 3.7.2	Provide the ability to produce an automated report of the disposition of patient requests to create, modify, or revoke consent directives.	L	L	R As soon as the patient has the ability to electronically submit this requirement is also required.
Post sign-off change	3.5.3 3.7.3	Provide the ability to report selected patient and VA privacy information policy and management information activities to VA and VA business partners (such as KP and DoD).	L	L	L
Post sign-off change	3.5.4 3.7.4	Provide reports of the date the consent directive was signed by the patient and the date and time it was approved by the consent management administrator.	L	L	L
Post sign-off change	3.5.5 3.7.5	Provide reports of patients whose consent for participation in Health Information Exchange (HIE) is within a specific expiration window.	L	L	L
Post sign-off change	3.5.6 3.7.6	Provide the ability to report failed validations and the reason for failure occurring in the consent directive validation process. (Note: validation means approve, deny, and reconcile the patient's request)	L	L	L

Post sign-off change	3.5.7 3.7.7 IAM 4	Consumer Request: Provide the ability to respond (via a report) to a healthcare consumer (e.g. patient) request to know who has seen or tried and failed to see (access denied) information enforced by their consent directive.	L	1Bii O	Completed
Post sign-off addition	3.7.10 3.7.9	Provide the ability to reconcile patient consent directives with VA policy.	L	L	L
Post sign-off addition	3.7.11 3.7.10	Provide the ability to notify patients of the status of approval, disapproval, or any conditions VA requires regarding adjudication of their consent directive requests as a result of the reconciliation process whereby the consent is compared with VA policy.	L	L	R
BN 4: Security Management – Provide security management services					
	4.1	Provide the ability for an Access Control System (ACS) to download/receive organizational security and privacy policies from security management services.	R	1Bii R	R
Post sign-off change	4.1.1 IAM 21	Provide the ability to grant, modify, delete, or suspend one or more structural roles for each, selectable, or all internal users accessing VA healthcare systems as defined by American Society for Testing and Materials (ASTM) E1986.	O	1Bii O Added "internal"	R
	4.1.2 IAM 23	Provide the ability to grant, modify, delete, or suspend one or more structural roles for each, selectable, or all users accessing healthcare systems as defined by the HL7 RBAC Permission Catalog standard.	O	1Bii O	L
	4.1.3 ENTR1 166	Provide the ability to administer security and privacy policies and procedures that create, modify, delete, or suspend an end-user's right of access to PHI.	O	1Bii O	R

	4.1.4 IAM 62	Provide the ability to create, modify, delete, or suspend organizational security and privacy access control policies or obligations for enforcement by access control services.	O	L	L
	4.1.5 IAM 66	Provide the ability to test policies created under the “Policy Administration Requirement” in an offline mode, whereby the action of the policy can be observed by the line of business policy administrator for verification of proper operation prior to actually enabling enforcement by security systems.	O	L	L
	4.1.6 IAM 24	Provide the ability to manage cross-cutting security and privacy policy based upon a purpose of use defined by the OASIS Cross-Enterprise Security and Privacy Authorization (XSPA) Security Assertion Mark-Up Language (SAML) Profile.	O	1Bii R	L
	4.1.7	Provide security administrators with the ability to manage (create, update, revoke, suspend, and delete) organization and jurisdiction mandated security and privacy policies.	O	1Bii O	R
	4.1.8	Provide the ability to create an audit trail of organizational security and privacy policy events taken during administration of security management application processes.	O	1Bii O	R
	4.1.9	Provide security administrators with the ability to query the ACS to determine if specific transactions are permitted.	O	1Bii O	R
	4.2	Provide security administrators with the ability to download organizational security and privacy policies from ACS.	O	1Bii R	Inactive-duplicates 4.1.7
Post sign-off change	4.3	Provide security administrators with the ability to upload deploy organizational security and	O	1Bii R	R

		privacy policies to ACS.			
Post sign-off change- Moved from 3.1	4.4	Provide the ability to download and integrate approved patient privacy policies from Consent Management Services to create composite security and privacy policy sets for ACS enforcement.	L	L	R
CPP/ROI Update	Technical Note	Provide the ability to extract attributes from approved requests and store them with corresponding policies			R
BN 5: Access Control - Support enforcement of VA approved security and privacy policies					
Post sign-off change	5.1 PIV 1.4	Provide authorization and access control as a common service with the goal of eliminating the need for individual application accounts and for managing and enforcing access control in each application. (Technical note: Provide the ability to support the OASIS XACML interface (i.e. an XACML Decision Request/Response) between the Adaptor and the CPP Policy Decision Point for to request/receive access control decisions for subsequent enforcement by the Gateway Policy Enforcement Point.)	O	1Bii O/L	R Inserted requirement 1.7 as a technical note
	5.1.1	Provide the ability to verify that access control decision information meets or exceeds composite business security and policy requirements prior to fulfilling requests that involve release of PHI.	O	1Bii R	Inactive Included in other requirements
	5.1.2 PIV 1.6	Provide the ability to enforce Line of Business cross cutting, purpose of use-based, hierarchical security and privacy policy, including attribute and RBAC.	L	1Bii R	L

	5.1.3 PIV 1.7	Provide the ability to enforce line of business approved individual privacy preferences/consent directives applied to purpose of use, persons (if feasible), roles, and selected data.	R	1Bii R	L
	5.1.4 PIV 1.7	Provide the ability to enforce line of business approved individual privacy preferences/consent directives applied to sensitivity.	L	L	L
CPP/ROI Update	5.1.5	Provide the Information Access & Privacy Program Office as well as the Health Information Management Program Office with the ability to nationally approve privacy policies			R
CPP/ROI Update	5.1.5.1	Translate pre-approved policies into user interface options that ROI Office can activate (Veteran's view of the policy and ROI Office view should be the same. ROI portal for manual entry of pre-approved policies should also match).			R
	5.2	Provide the ability to ensure that protected information is only accessible to entities possessing authorizations that meet or exceed information security and privacy policy access control decision attributes.	R	1Bii R	R
	5.2.1	Except in an emergency (see 5.2.4), provide for the secure electronic exchange of health information with a requesting organization only if the patient has executed an "opt-in" policy as a prerequisite to evaluating any other policies authorizing such exchange.	R	1Bii R	R
	5.2.2	Provide the ability to mask (such as delete or hide) specific patient-specified information from standard response messages (e.g., HITSP C32, C37) in accordance with VA composite security policies prior to the release of information.	L	L	L

	5.2.3	Provide the ability to deny exchanges of health information with a requesting organization if VA has accepted a patient's request to prevent such exchange with a specific named individual (if feasible) or group of individuals in an accepted role.	R	1Bii R	R
	5.2.4	In an emergency (defined as a situation involving possible death or injury/harm), Service Provider authorization and access control services shall support the capability to enforce access privileges and consent directives to appropriate policies defined by the purpose of use of "emergency access".	R	1Bii R	R
	5.3	Provide the capability to utilize and interpret external information requests (including attached access control decision information) received via the CPP -VA Nationwide Health Information Network NHIN Gateway interface.	R	1Bii R	R
Post sign-off addition	5.4	Provide the ability to identity proof Veterans patients, and VA employees, contractors and affiliates.		1Bii R	R Changed Veteran to patient
Post sign-off addition	5.5	Provide the ability to support use of PIV and Common Access Card (CAC) methods of identity proofing.		1Bii R	R
BN 6: Support VA enterprise identity management requirements					
	6.1 ENTR 1097	Person related applications/services shall use Identity Management services as the authoritative source for maintaining person identities.	R	Completed	Completed
	6.2 ENTR 1098	Person related applications/services shall use Identity Management services as the authoritative source for creating Enterprise Person Identities.	R	1Bii R	Completed

	6.3 ENTR 888	Applications/services that collect data related to a person from systems that are correlated to an Enterprise Person Identifier shall store the Source Identifier with the collected data.	R	Completed	Completed
	6.4 ENTR 889	Applications/services authorized to edit person identity traits shall provide the ability to revert back to the person's primary view when identity trait edits are deemed to be catastrophic.	R	Inactive	Inactive
	6.5 ENTR 890	Applications/Services shall process update notifications to person identity traits received from the authoritative source for Identity Management.	R	1Bii R	R
	6.6 ENTR 925	Person related applications/services shall be capable of processing a fully qualified Enterprise Person Identifier.	R	1Bii R	Completed
	6.7 ENTR 927	Applications/services that persist person related data shall register persons of interest with the authoritative source for Identity Management.	R	1Bii R	R
	6.8 ENTR 929	Applications/services that persist persons of interest-related data shall process person identity Link (Resolve Duplicate) notifications received from the authoritative source of Identity Management.	R	1Bii R	R
	6.9 ENTR 93	Applications/services that persist persons of interest related data shall support person identity Move Correlation (Resolve Mismatch) notifications received from the authoritative source of Identity Management.	R	Inactive	Inactive
	6.10 ENTR 937	Applications/services that consume person based transactions/messages from a source/input system that is correlated to an Enterprise Person Identifier shall maintain the Source Identifier from the originating system along with the person data.	R	Inactive	Inactive

	6.11 ENTR 939	Applications/services authorized to edit person identity traits shall provide the ability to revert back to the person's primary view when identity trait edits are rejected.	R	Inactive	Inactive
	6.12 ENTR 941	Applications/services that consume person based transactions/messages from a source/input system that is correlated to an Enterprise Person Identifier shall include the Source Identifier within all messages containing person related data that are sent to other VA systems.	R	Inactive	Inactive
BN 7: Enhancement of identity management processes between VA and external entities					
	7.1	Support probabilistic matching between VA and external entities.	R	Completed	Completed
	7.1.1	Support querying containing multiple patient names. Support correlation of patient identities between VA and external entities using multiple aliases per the CONNECT production specifications.		1Bii R	L
	7.1.2	Support management of multiple assigning authorities			R
	7.2	Provide tools to support analysis of matches and potential matches.	R	Completed	Completed
	7.2.1	During patient discovery, if there is no authoritative match between VA and the external entity provide a display of patient traits that are a potential match with the VA patient.	O	Completed	Completed

	7.2.2	Provide support for an internal ad-hoc query of patient demographic information received from the external partner (demographics in an identity management context). Provide response from system when insufficient traits are provided (i.e. name, dob and gender (minimum required, yet insufficient) from the sender which prompts for addition of SSN which is necessary for definitive matching.	L	L (Per Sara Temnitz, tools needed to resolve data quality issues are not available yet)	L (Per Beth Franchi, CONNECT specification does not exist yet)
	7.2.2.1	For the inbound patient discovery, create a report for each time an announcement is made and the patient correlation was not successful (received patient demographics, reason for failed correlation)			R
	7.3	Provide tools to support unlinking of correlations.	R	Completed	
	7.3.1	Do not satisfy a query if the correlation is incorrect and/or a correlation has been unlinked.	R	Completed	
Post sign-off addition	7.3.2	Provide a capability to undo an unlink of a correlation if has been determined that the unlink should not have occurred.	-	1Bii R	Completed/ Inactive (see 7.3.3)
	7.3.3	Deactivate tools created to support unlinking of correlations (7.3)			R
	7.4	Provide the ability to view /support a patient's record when there are multiple identities within the same community-(multiple assigning authorities).	R	1Bii R	Deleted view and added multiple Completed
	7.5	Provide special support for DoD patient discovery process to include additional patient information.	R	Completed	Completed
	7.6	Create a report, by VA facility number, that provides a count of the number of VAMC patients who are correlated with each CONNECT partner			R-highest priority

	7.7	Upon manually opting-in the patient, send a patient discovery announce message to CONNECT partners to enable establishment of the patient correlation		Completed	Completed
	7.7.1	The user interface used to manually opt-in patients shall display information explaining the opt-in function (opt-in initiates a CONNECT patient discovery announcement)		Completed	Completed
	7.8	For all correlated patients, provide a list (VistA report) of the patients, by facility, and all of their future appointments			O
BN8: Interoperability enhancements.					
	8.1	Update to the latest version of the Nationwide Health Information Network NHIN specifications as required by the Data Use and Reciprocal Support Agreement (DURSA) (for example, this includes HITSP C32 and patient discovery).	R	1Bi R Note: Gateway CONNECT 3.1 will not be available in time to meet 1BiR deadline	R
	8.2	Add the ability to obtain data from VA systems of interest (roll out to all VA systems).	R	Completed	Completed
	8.3	Add the ability to obtain standardized, translatable data.	R	Completed	Completed
	8.4	Provide terminology translation as specified within the content standards (such as HITSP standards).	R	1Bi R	R
	8.5	Enable Identity Management to support the separation of the following concepts: assigning authority, record location, facility, and Nationwide Health Information Network NHIN association.	R	1Bi R	Completed
	8.6	Create a tool to monitor the functioning of the system.	R	To be met via the MOU being developed with Service Coordination	Completed AITC provides a dashboard

	8.6.1	If the tool identifies a problem with the system, notify the Austin Information Technology Center (AITC) and the users.	R	To be met via the MOU being developed with Service Coordination	Completed AITC provides a dashboard
	8.7	Provide a patient discovery report that lists announcements sent, and response, or lack of response from each partner			R
BN 9: Support the addition of new partners					
Post sign-off change	9.1	Support exchange of production patient data between San Diego VAMC, DoD, KP, and other selected partners on the Nationwide Health Information Network NHIN. the additional Hampton partners. In the VLER 1A pilot, the exchange with DoD is limited to test data and exchange with KP is limited to the pilot population.	R	1Bii R	Completed
	9.1.1	Provide a new institution number for each new partner.			R
Post sign-off change	9.2	Support discovery and progress of a new partner.	R	1Bii R (if no coding changes are required)	Completed-send patient discovery to known partner
	9.2.1	Provide a mechanism for detecting a new partner.	R	1Bii R (if no coding changes are required)	R
	9.2.2	Provide the ability to place the potential new partner in a queue for testing.	O	L	R
	9.3	Provide the ability to authorize a new partner.	R	1Bii R	Completed
	9.3.1	Provide confidence testing prior to authorization of a new partner.	R	1Bii R-CPP interim solution	Completed
	9.3.2	Create authorization execution to allow exchange to occur.	R	Completed	Completed
	9.3.3	Provide new partner integration into the production deployment with no system down time.	O	Completed	Completed

	9.4	Provide the ability to monitor and detect problems with the new partner.	R	1Bii R Workaround (notify each other; long term ONC)	R
	9.4.1	Provide match/no match rates.	O	Completed	Completed
	9.4.2	Provide the ability to drill down to assess potential problems.	R	L	Inactive
CPP/ROI Update	9.5	Enable the CONNECT to leverage existing VA-DoD patient correlations that may have been established through other programs (for example, North Chicago, BHIE, addition of DEERS identifier to MPI).			R
BN 10: Expand information sharing beyond subset of HITSP C32 information currently shared in the VLER 1A pilot					
	10.1	Share Provide translated standardized allergies, problems, and medications using standardized terminology.	R	1Bii R	R
	10.1.1	Provide a problem list using standardized terminology			R
	10.2	Share Provide translated vital sign information using standardized terminology.	R	1Bii R	R
	10.3	Share chemistry and hematology laboratory test results using standardized terminology.	R	Completed	Completed
Post sign-off change	10.4	Share standardized immunization information.	L	1Bii R	R
		Consults and Referrals			

	10.6.1 Renumbered as 10.5	Share list of consults (date, time, referring service)		-	Completed
	10.6	Share consult/referral documents (notes). (ICIB 9/9/2010)	L	1Bii R if included in HITSP C32 Summary	R
		Discharge Summaries		-	
	10.7	Share list of discharge summaries (date, time, author, document title)		-	Completed
	10.5 Renumbered as 10.8	Share discharge summaries documents (notes). (ICIB 9/9/2010)	L	1Bii R if included in HITSP C32 Summary	R
		Results of Diagnostic Studies		-	
	10.9	Share results of diagnostic studies (ICIB 9/9/2010)			R
		Procedure Notes			
	10.7 renumbered as 10.10	Share procedure notes (ICIB 9/9/2010)			L
		Histories and Physicals			
	10.11	Share Histories & Physicals (ICIB 9/9/2010)			L
		Continue to build out the Summary of Care Document (prioritized order)*			
		List of Encounters			
	10.12	Share list of encounters (ICIB 9/9/2010) (date, time, location, but not the note content)			R (partially completed in 1Bii)
	10.13	Share encounter notes			R
		List of Surgeries			
	10.14	Share list of surgeries (ICIB 9/9/2010) (CPT code, name, date, time, note title, but not the note content)			R
		Pregnancy			
	10.11	Share pregnancy status (ICIB 9/9/2010)			L
		Advance Directive			

	10.12	Share advance directive (ICIB 9/9/2010)			L
		Plan of Care			
	10.13	Share plan of care (ICIB 9/9/2010)			L
Post sign-off addition	10.8	Share encounters information		1Bii R if included in HITSP C32 Summary	Inactive, rewritten as BN 10.5
BN 11: Enhance user interface					
	11.1	Provide clarifying information on reports explaining query date ranges.	O	Completed	Completed
Post sign-off change	11.1.1	Remove the query parameters from VistA Web queries.		1Bii R	Completed-removed date range from C32 data
Post sign-off change	11.2	Notify providers end users when information is available from new partners and when new functionality is available via the Nationwide Health Information Network NHIN .	R	1Bii R	Completed-VW Sites & Notices page
	11.3	When HITSP C32 information is not available, display the words "no data found" instead of skipping that section (will need confirmation of the Computerized Patient Record System [CPRS] Clinical Workgroup).	R	Approved per CPRS Clinical Workgroup on 4/28/2010 1Bii R	Completed (VistA Web not Adapter)
	11.4	Support transition to new interface platforms if/when they become available (such as AViVA).	O	L	L
	11.5	Upgrade the C32 information displayed to the user to accommodate any differences between the entities.	R	Completed	Completed
	11.6	Upgrade the display style sheet and the aggregated views in VistA Web to incorporate new content and additional Nationwide Health Information Network NHIN document types (see BN 10) to include DoD Vitals, Lab Results Chemistry, Lab Results organizer, History	R	1Bii R	Completed CPP 'View C32' tab

		of encounters, History of procedures.			
	11.7	Allow the Nationwide Health Information Network query to continue to perform while reports for VistA, Health Data Repository (HDR), and Bidirectional Health Information Exchange (BHIE) are being generated.	O	Completed	Completed
	11.8	Remove redundancies from the same source of data when providing the display (for example, multiple DoD allergies coming from same DoD source).	R	1C	L
Post sign-off addition- Moved to non-functional requirements	11.9	Identify/highlight duplicate entries in aggregated List: Meds, Problems, Allergy, Labs (for example, multiple prescriptions for the same medication) (business owner to provide additional detail)/	-	1C	Inactive Moved to non-functional requirements
Post sign-off addition- Moved to non-functional requirements	11.10	Identify/highlight duplicate entries in aggregated List: Meds, Problems, Allergy, Labs (for example, multiple prescriptions for the same medication) (business owner to provide additional detail)/	-	1C	Inactive Moved to non-functional requirements
Post sign-off addition	11.11	Support performance evaluation study by providing user interface audit logs and click streams.		1Bi R	R
Post sign-off addition	11.12	CPRS will inform the end user that there may be outside clinical information to view. (Currently done by a local Clinical Reminder)		1Bi R	R

	11.12.1	Provide an automated notification to the end user of CPRS and VistA Web that there is Nationwide Health Information Network information to review. (Note: For providers who do not use clinical reminders, provide an alternative automated notification mechanism to inform them that there is CONNECT information to review.)			R
	11.12.2	Provide an accurate, up to date notification to the end user of the availability of the CONNECT information (incorporate change from authorization to revoke).			R
	11.12.3	Inform the end user when the latest update has been made, and/or when the information is new, perhaps via a date stamp. (Need to confirm that information has not been changed since it was viewed)			R
BN 12: Performance Measurement automation for evaluation of utilization of information sharing.					
	12.1	Automate extraction of core set of evaluation data for opt-in and opt-out patients from multiple sources from the CPP application, such as CPRS, enrollment files, and appointments.	R	1Bii O	R
Post sign-off change. Header moved.	12.2	Generate an HITSP 32 summary:	R	1Bii O	Inactive
	12.2.1	Generate an HITSP C32 summary automatically upon opting in of the patient	R	1Bii R	L
	12.2.2	Generate an HITSP C32 summary on demand	R	1Bii R	Completed
	12.2.3	Generate a HITSP C32 summary automatically in response to trigger events, such as a scheduled visit	R	1Bii R	R

	12.3	Remove PHIs from each HITSP C32 summary generated for performance measurement purposes.	R	1Bii O	L
	12.4	Create a report tool to analyze VA C32 summary access logs containing information already captured in the logs (e.g., retrievals, timestamp, requestor ID, specific contents received) as well as queries.	R	1Bii R	Completed
	12.5	Archive each HITSP C32 summary document received by VA.	R	1Bii R	Completed
BN 13: Patient Privacy Management Non-Functional Capabilities					
	13.1	Provide for the storage of all variants/forms of original patient consent directives including final versions approved by privacy administrators.	O	1Bii R	R
	13.2	Provide for the creation and storage of a humanly readable form of patient consent directives.	R	1Bii R	R
	13.3	Provide for the creation and storage of an electronically computable form of patient consent directives.	R	1Bii R	R
	13.4	Provide for the creation and storage of an HL7 standard Clinical Document Architecture (CDA) Release 2 (R2) attribute form of patient consent directives.	O	1Bii R	R
Post sign-off change	13.5	Support proper level of assurance with regard to patient's use of a VA authorized the MHV portal.	R	1Bii R reworded	R
Post sign-off change	13.5.1	Enforce rule that patients who choose to use VA provided electronic consent directives must have a current MHV portal account.	R	1Bii R Changed MHV to portal	R
Post sign-off change	13.5.2	Enforce rule that patients who choose to use VA provided electronic consent directives must be identity proofed at the appropriate NIST SP 800-63 defined level of assurance-3.	R	1Bii R Added "appropriate"	R

	13.5.3	Enforce rule that patient consent directives shall be digitally signed with a signature representing the patient or the patient representative.	R	1Bii R	R
Post sign-off deletion	13.5.4	Enforce rule that patient's handwritten signatures recorded electronically shall be protected from identity theft by binding the consent directives to a known notary digital signature.	R	Inactive	Inactive
BN 14: Consent Management Non-functional Capabilities					
	14.1	The ROI application shall be capable of receiving and using an electronic HL7 CDA R2/Release 3 (R3) formatted consent directive.	R	1Bii R	R
	14.2	For Nationwide Health Information Network NHIN versions not fully compliant with the OASIS XSPA SAML specification, the ROI office CPP ROI system shall provide an electronic file that includes the full identifier of providers authorized to query for VHA patient information, their National Provider Identifier (NPI), and their structural role as specified in ASTM E1986.	R	1Bii O/L	Inactive
	14.3	Upon completion and approval of a patient consent directive, the ROI office CPP ROI system shall place the approved HL7 CDA R2 consent directive in a Cross Enterprise Document Sharing (XDS) repository for provisioning to the ACS.	R	L	L
	14.4	Organizational security policies will be available in a humanly readable format.	R	1Bii R	R
	14.5	Organizational privacy policies will be available in a humanly readable format.	R	1Bii R	R
BN 15: Security Management Non-Functional Capabilities					

	15.1 IAM 6	HITSP Collect and Communicate Security Audit Trail Requirement: VA security services shall comply with the HITSP Collect and Communicate Security Audit Trail Transaction (T15) to provide assurance that security policies are being followed or enforced and that risks are being mitigated.	R	1Bii O/L	L
	15.2 IAM 160	VA Security Services will comply with the HITSP Manage Consent Directives Construct (TP30) to ensure the capture, management, and communication of rights granted or withheld by a consumer to one or more identified entities in a defined role to access, collect, use, or disclose IIIH.	R	1Bii R	L
	15.3 IAM 33	VA security services shall decide and enforce security and privacy authorizations for external healthcare information requests in accordance with the specifications contained in the HITSP TP20 Access Control Construct.	R	1Bii R	L
BN 16: Identity Management and CPP System Non-Functional Capabilities					
	16.1	Provide ability to support the use of Integration Control Numbers (ICNs) to uniquely identify patients.	R	1Bii R	Completed
	16.2	Provide capability to look up and enforce security and privacy policy based upon the ICN of the patient identified in the information request.	R	1Bii R	Completed
	16.3	Provide capability to include ICN of the patient in its audit events where applicable.	R	1Bii R	Completed
	16.4	As necessary, comply with the Baker memo regarding EDIPI, for future requirements			L
BN 17: Additional Non Functional Requirements: (These requirements are not ranked at this time)					

	17.1	In accordance with the enterprise HC IdM Requirements, person-related applications/services will use the enterprise identifier (ICN), as appropriate, which does not include the use as an internal identification or as a Primary Key in any database or repository developed.			
Post sign-off change	17.2	Leverage the VA facility MHV portal coordinator at the next VLER Health Communities (e.g., Hampton, VA Virginia Tidewater Project) to also administer the Nationwide Health Information Network NHIN authentication and consent processes.		Changed MHV to portal	
	17.3	Nationwide Health Information Network NHIN will utilize an enterprise level, shared patient identification and authentication service, when available.			
	17.4	Demographic information will be exchanged using HITSP standard terminologies.			
	17.5	Ensure performance as new Nationwide Health Information Network NHIN partnerships (additional opportunities with external entities) are incorporated.			
	17.6	Separate CPP responsibilities from the Adapter.			
Post sign-off change	17.7	The Establish a standard response time for a new partner to join is 7 seconds.			
		VistA Web			
	17.8	Modify VistAWeb to accommodate slow response time from the Nationwide Health Information Network NHIN .			
	17.8.1	Improve performance of the display of data to display within 7 seconds.			
	17.8.2	Separate into different “threads” the request/display of data in the aggregated domains. At the very least split the data into two groups, VA data and Nationwide			

		Health Information Network data.			
	17.8.3	Display either “thread” of data as soon as it is available.			
	17.8.4	Merge data that is received “2nd” into the tabular view.			
	17.8.5	Provide a visible indicator that the different “threads” are waiting for data.			
	17.8.6	Provide an indication that the "thread" succeeded or failed. Technical note: For a user session for a single patient the cached the Nationwide Health Information Network C32 data should not be cleared or removed. There is no need to discard this cache as the contents are not going to change based on moving between medical domains. The data range of data from our partners is constant. If possible, start a Nationwide Health Information Network query/retrieve thread for the selected patient “immediately” after the patient is selected and the sites/notices page is displayed. (when the patient has Nationwide Health Information Network correlations). This “thread” could replace the above mentioned multi-thread.			
Post sign-off change	17.9	The opt in confidence test should be completed within one week.		Inactive	Inactive
	17.10	The authorization process to turn on communications between VA and a new partner that has passed the opt-in confidence test should take no more than one minute.			
	17.11	VA and partners are functionally complete by mid May 2010 for VLER 1B.		Completed	Completed

	17.12	Meet the Enterprise and Infrastructure Engineering (EIE) requirements for release, operations support, and resources throughout the lifetime of the project (Go/No Go [GNG] Testing and Release Checklist).			
	17.13	Comply with Office of Enterprise Development (OED) Testing Service and EIE Operational Readiness Testing.			
	17.14	Comply with EIE Release Management Procedures, including development of operational acceptance and post-release support, responsibility, and procedural documentation.			
	17.15	Establish a Capacity to address new partners.			
	17.16	Investigate and produce statistics on Nationwide Health Information Network NHIN system load.			
	17.17	Develop a Service Level Agreement (SLA) regarding availability of the system.			
	17.18	Provide the ability to retain the accounting of disclosures for 75 years, as required by Privacy Act as the life of the EHR is 75 years.			
	17.18.1	Provide the ability to retain consent directives for 75 years.			
	17.19	Meet NIST 800-63 level 3 electronic authentication guidelines.			
Post sign-off change	17.20	End-user (patient) response time for interface to the CPP System (MHV) (via the portal) will be 7 seconds or less.		Added interface and changed MHV to portal	
	17.21	The CPP System response time for VA staff using the system will be consistent with Nationwide Health Information Network specifications.		Completed	
Post sign-off change	17.22	The System will be able to support simultaneous use by 5 a population of approximately 6 million active Veteran patients.		Reworded	Changed Veteran patients to patients

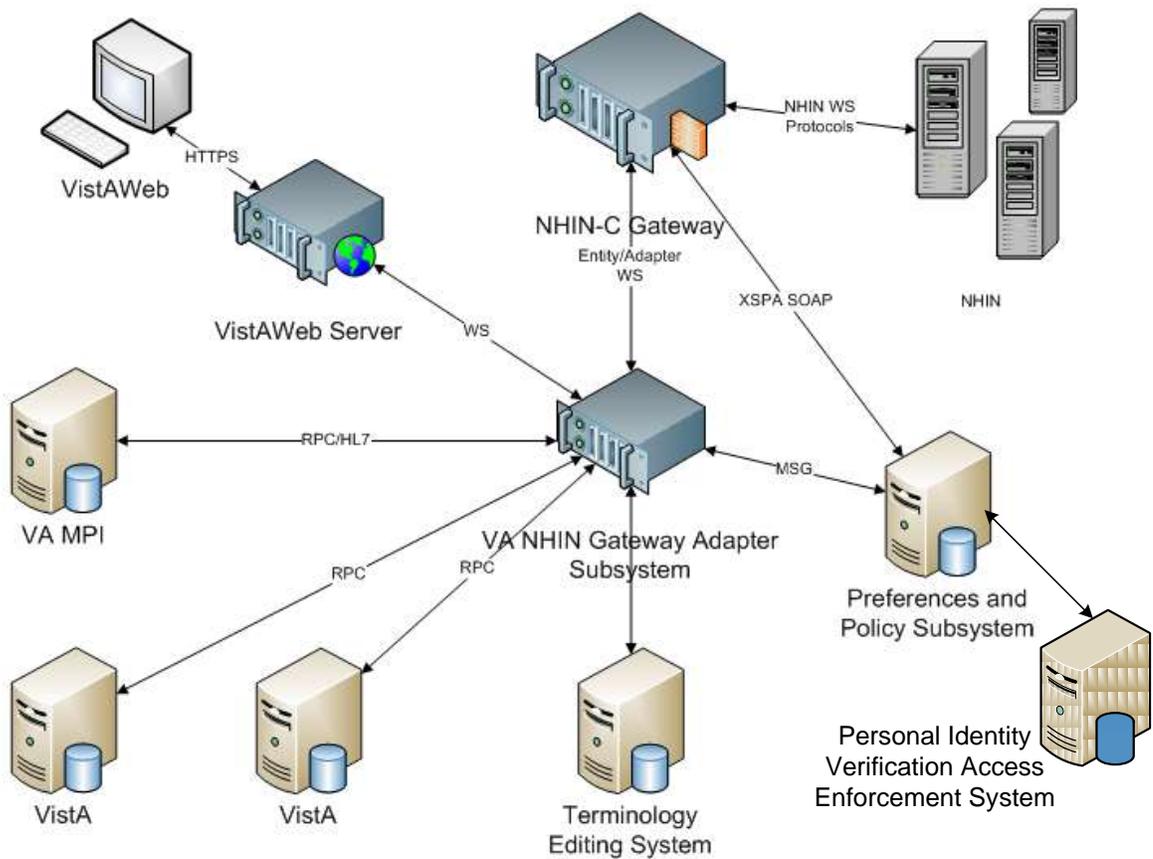
Post sign-off change	17.23	Patients will be provided with on-line help, access to Frequently Asked Questions (FAQ) with answers, as well as access to a national help desk for questions about the CPP system. Staff will be provided with tutorials and FAQs with answers for questions about the CPP System and VistAWeb.		1Bii R Reworded	
Post sign-off change	17.24	Provide user and technical manuals for the CPP System and VistA Web changes		1Bii R Reworded	
	17.25	Provide process and policy documentation to share with new Nationwide Health Information Network NHIN partners.			
Post sign-off addition	17.26	Automate processing list of Nationwide Health Information Network NHIN partners-- communicate this information to CPP, VistA Web.			
Post sign-off addition	17.27	Improve system latency of information sharing by VA to the end user of the Nationwide Health Information Network NHIN . Appropriate processing times to be defined by the business owner.			
Post sign-off addition	17.28	Improve system latency of information sharing by from the Nationwide Health Information Network NHIN to the VA user. Appropriate processing times to be defined by the business owner.			
Post sign-off addition- Moved to non-functional requirements	11.9 17.29	Identify/highlight duplicate entries in aggregated List: Meds, Problems, Allergy, Labs (for example, multiple prescriptions for the same medication) (business owner to provide additional detail)/	-	1C	

Post sign-off addition	17.30	From user request to availability of Nationwide Health Information Network document(s) list over VLER (first pass), accessible over VLER 5 seconds 90% of the time, and within 10 seconds 99% of the time, and 15 seconds 99.99% of the time.			
Post sign-off addition	17.31	1) Single Document request will be returned/displayed within 5 seconds 90% of the time, and within 10 seconds 99% of the time, and 15 seconds 99.99% of the time. 2) If requested document(s) is/are over 500 KB, it will be returned/displayed within 10 seconds, 90% of the time, and within 15 seconds 99% of the time, and 20 seconds 99.99% of the time.			

2.2. CPP External System Interface Requirements

The diagram provided below illustrates the CPP subsystem in the context of integration with other systems (primarily the Gateway and Gateway adaptor) that are expected to be integrated to provide the VA NwHIN-C Gateway Adapter deployment.

- The CPP system will need to interface with the VA NwHIN Adapter located at the Austin Information Technology Center (AITC) and the NwHIN gateway for communication with external systems.
- The Gateway integrates directly with the CPP for authorization, since the orchestration in the gateway has the call to the Policy component. The CPP Subsystem integrates with the Adapter for the enforcement of preference changes.



2.3. Related Projects/NSR

Related requests include:

- Nationwide Health Information Organization NSR ([20070210](#)) and corresponding VA NwHIN Adapter project ([VA OED – Project Notebooks](#)) is being developed to provide exchange of textual reports and computable data between VA and other government and private sector health organizations. Initial data exchanged includes: outpatient pharmacy, allergy, conditions, and demographics. The exchange is conducted compliant with national standards as defined by HITSP and NwHIN.
- Consumer Preferences and Policy Management NSR ([20090624](#)) requirements have been incorporated into this request.
- PIV Integration: Authentication Services ([20080343](#)) requirements relevant to this request have been previously identified in the Business Needs/Owner Requirements table with a PIV number.
- PIV IAM requirements contained in the PIV Integration: Access Control Services ([20090803](#)) requirements relevant to this request have been previously identified in the Business Needs/Owner Requirements table with an IAM number.
- Online Identity Proofing for My Health_eVet Web Portal NSR ([20090913](#)) requirements will provide online capability to Identity Proof Veteran users. The current in-person Identity Proofing (In-Person Authentication [IPA]) will not be replaced, but it will provide

Veterans an alternate means to meet this requirement. This functionality is needed in order for VA to meet the NIST 800-63 level 3 electronic authentication guidelines.

3. Other Considerations

3.1. Alternatives

The only identified alternative is to utilize the San Diego VAMC pilot project enhancements as the enterprise solution. However, the enhancements provided through the pilot projects would have the following disadvantages:

- The pilot projects do not provide a fully automated solution.
- Patient records would need to be manually flagged when the patient opts-in and the flag would need to be manually removed when the patient opts-out.
- There would not be an automated record of patients opting-in and opting-out.
- Consent directives would not be viewable in the electronic record.
- There would be no interface between the consent directives and organizational security and privacy policies.
- There would not be an automated way to compare Title 38 U.S.C. 7332 protected information status between the health record and the consent directive to ensure that no PHI is released without proper authorization on file.
- Limited information would be exchanged.
- The processes developed for the San Diego VAMC pilot are very labor intensive; therefore, they are not scalable for national deployment.

3.2. Assumptions

- The development of any tools, repositories, or applications in support of the NwHIN goals and processes must adhere to the VHA Healthcare Identity Management enterprise requirements, to ensure that the integrity of the patient correlations is of the highest level and that no degradation of VHA patient information is experienced.
- Comply with the OGC requirements regarding due diligence, namely ongoing record review, to detect the presence of protected conditions not originally included in the authorization.
- NwHIN will continuously upgrade to utilize the most recent, stable NwHIN Gateway (2.3[4]) and required NwHIN specification changes.
- Provide for the creation and storage of an HL7 standard CDA R2 attribute form of patient consent directives.
- Leverage standard definitions to ensure a collective understanding of HITSP data elements.
- Standardized data will be shared among NwHIN partners.
- Assumes that contracting resources will be available for support of ACS requirements.
- Incorporate two new subsystems into NwHIN: Service Registry and Certificate Authority.
- Precursor CPP business requirements include adherence to HHS, ONCHIT accepted HITSP constructs TP 30 Manage Consents Directive, and TP 20 Access Control. The intent is to

adopt the HITSP standards, though implementation may need to occur using a phased approach.

- Security requirements will be reviewed and approved by the Security Requirements Steering Committee so that they can be incorporated as enterprise-wide policies.
- Privacy requirement compliance with all applicable federal laws, regulations, and policies.
- As a result of the HITECH Act provisions of the American Recovery and Reinvestment Act (ARRA) of 2009, the HIPAA Privacy Rule will be revised to require an accounting of disclosures for the exchange of electronic health information. This HIPAA Privacy Rule revision may have an impact on the requirements of this document.

3.3. Dependencies

- The enhancement is dependent upon successful implementation of the pilot projects between the San Diego VAMC, KP, and DoD.
- Gateway and Adapter dependencies are as discussed in the External System Interface Requirements ([see section 2.3](#)).
- PIV dependencies are identified in the Business Needs and Owner Requirements ([see section 2.1](#)).

3.4. Constraints

- The system shall comply with HITSP requirements established in the Enterprise Requirements Repository (ERR).
- The enhancement will be compliant with the NwHIN authorization interface specification.

3.5. Risks

- Due to the compressed time frames used to elicit and document the requirements for this NSR, there is the inherent risk that the requirements do not capture the full scope of the request.
- Inability of the VA to efficiently manage authorizations and restrictions for health information exchange between VA and non-VA providers on a national level; as phase 1 and phase 2 pilot solutions are not scalable.

Appendix A. References

- 2005 Survey of Veteran Enrollees' Health and Reliance Upon VA.
<http://vaww4.va.gov/vhaopp/report01/SOE/SOE05ExcSum.pdf>
- 2007 Survey of Veteran Enrollees' Health and Reliance Upon VA.
<http://vaww.va.gov/vhaopp/report01/SOE/2007SOEReport.pdf>
- 2009 0331 Class III Deployment Request.
<http://vista.med.va.gov/pasdocs/supportinfo/20090624%20Consumer%20Preferences%20&%20Policy%20Management%20System.zip>
- 38 U.S.C. 7332-Confidentiality of certain medical records.
<http://uscode.house.gov/download/pls/38C73.txt>
- American Recovery and Reinvestment Act of 2009.
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_bills&docid=f:h1enr.pdf
- Consumer Preferences and Policy Management System NSR
http://vista.med.va.gov/nsrd/Tab_GeneralInfoview.asp?RequestID=20090624
- Consumer Preferences, Draft Requirements Document, October 5, 2009. U.S. Department of Health and Human Services, ONCHIT.
http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10779_891071_0_0_18/20091005_Consumer%20Preferences_Draft_Requirements_Document.pdf.
- Executive Order 13335-Incentives for the Use of Health Information Technology and Establishing the Position of the National Health Information Technology Coordinator, *Federal Register*, Friday, April 30, 2004.
<http://edocket.access.gpo.gov/2004/pdf/04-10024.pdf>
- Executive Order 13410-Promoting Quality and Efficient Health Care in Federal Government Administered or Sponsored Health Care Programs, *Federal Register*, Monday August 28, 2006.
<http://edocket.access.gpo.gov/2006/pdf/06-7220.pdf>
- HIPAA Privacy Rule
<http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/adminsimpregtext.pdf>
- HITSP Access Control Transaction Package, August 27, 2008, Version 1.2
<http://www.hitsp.org/Handlers/HitspFileServer.aspx?FileGuid=c9083325-4afb-4b41-8452-304a1011eb0a>
- HITSP Glossary
<http://publicaa.ansi.org/sites/apdl/hitspadmin/Reference%20Documents/HITSP%20Glossary.pdf>
- HITSP Lab Report Document Component, HITSP/C 37, July 8, 2009, version 2.3.
<http://www.hitsp.org/Handlers/HitspFileServer.aspx?FileGuid=00da94f5-d731-4faf-aa86-f31519873302>
- HITSP Manage Consent Directives Transaction Package, July 8, 2009, Version 1.3.
<http://www.hitsp.org/Handlers/HitspFileServer.aspx?FileGuid=35f77485-abac-4d34-855a-ded10aa91448>
- HITSP Summary Documents Using HL7 Using Continuity of Care Document (CCD) Component, HITSP/C32, July 8, 2009, version 2.5.
<http://www.hitsp.org/Handlers/HitspFileServer.aspx?FileGuid=e1b99525-a1a5-48f6-a958-4b2fc6d7a5c7>

- Memorandum of Understanding Between the Department of Defense and the Department of Veterans Affairs for Purposes of Defining Data Sharing Between the Departments.
<http://vista.med.va.gov/pasdocs/supportinfo/20090624%20Consumer%20Preferences%20&%20Policy%20Management%20System.zip>
- Nationwide Health Information Network (NwHIN)
[HealthIT.hhs.gov: NHIN](http://healthit.hhs.gov: NHIN)
- Nationwide Health Information Organization NSR
http://vista.med.va.gov/nsrd/Tab_LinksView.asp?RequestID=20070210
- NwHIN Enhancements NSR
http://vista.med.va.gov/nsrd/Tab_GeneralInfoview.asp?RequestID=20100102
- Nationwide Health Information Network: Resources, 2010 NwHIN Final Production Specifications
http://healthit.hhs.gov/portal/server.pt?open=512&objID=1194&parentname=CommunityPage&parentid=10&mode=2&in_hi_userid=10741&cached=true
- NIST 800-63, Electronic Authentication Guideline
http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf
- Online Identity Proofing for My Health_eVet Web Portal NSR
http://vista.med.va.gov/nsrd/Tab_GeneralInfoView.asp?RequestID=20090913
- Patient Medical Records-VA, 24VA19, Privacy Act system of records
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=2009_register&docid=DOCID:fr19no09-119.pdf
- Perlin, Jonathan B. (July 2005) VHA Strategies- Eight for Excellence. Retrieved from:
http://vaww.visn5.med.va.gov/resources/career_dev/8_for_excellence.pdf
- Personal Identity Verification (PIV) Integration: Access Control Services BRD
http://vista.med.va.gov/pasdocs/analysis/20090803_Personal%20Identity%20Verification%20PIV%20Access%20Control%20Services_BRD.doc.
- Personal Identity Verification (PIV) Integration: Authentication Services BRD
http://vista.med.va.gov/pasdocs/analysis/20080343_Personal%20Identity%20Verification%20PIV%20Integration%20Authentication%20Services_BRD.doc.
- Personal Identity Verification (PIV) Integration: Access Control Services New Service Request. Request #20090803:
http://vista.med.va.gov/nsrd/Tab_GeneralInfoview.asp?RequestID=20090803
- Power for Performance
http://vaww.ush.va.gov/docs/crosswalk_strategic_framework.pdf
- Privacy Act, 5 U.S.C. 552a. THE PRIVACY ACT OF 1974, 5 U.S.C. § 552a -- As Amended
<http://www.justice.gov/opcl/privstat.htm>
- Remarks by the President on Improving Veterans Healthcare, April 9, 2009.
http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Improving-Veterans-Health-Care-4/9/2009
- Request for and Authorization to Release Medical Records or Health Information, VA Form 10-5354.
<https://www.va.gov/vaforms/medical/pdf/vha-10-5345-fill.pdf>

- TP 20 - HITSP Access Control Transaction Package
http://www.hitsp.org/ConstructSet_Details.aspx?&PrefixAlpha=2&PrefixNumeric=20
- TP 30 – HITSP Manage Consent Directives Transaction Package
http://www.hitsp.org/ConstructSet_Details.aspx?&PrefixAlpha=2&PrefixNumeric=30
- VA NwHIN Adapter
<http://tspr.vista.med.va.gov/warboard/anotebk.asp?proj=1307>
- VA NwHIN-Connect Gateway Plan B Integration Architecture
 This is a draft document not available publically.
- VHA Directive 2004-050, Mandated Utilization of Release of Information (ROI) Records Management Software.
<http://vaww.vhaco.va.gov/privacy/Documents/VHA%20Directive2004-050ROI.pdf>
- VHA Handbook 1605.1, Privacy and Release of Information.
<http://vaww.vhaco.va.gov/privacy/Documents/VHAHdbk1605-1.pdf>
- VHA NwHIN Information Sharing Policies and Procedures, San Diego Pilot (Phase 1)

 VA NHIN Privacy
 Policies 2-2-10.DOC
- VLER and NwHIN July 2010 Feasibility Analysis: Summary of Findings

 VLER full
 recommendations final
- VLER Summary Recommendations Final

 VLER summary
 recommendations final

Appendix B. Models

The following are the updated CPP models:



VLER CPP Pilot as-is
process.vsd



VLER CPP Pilot Phase
1a (San Diego) to-be



VLER CPP Pilot Phase
1b (Hampton VA) to-be



VLER CPP Pilot Phase
1bi (San Diego) update



VLER CPP long-term
solution_11_10_10.vsd

The following Activity Description Tables correspond to the updated CPP models:



VLER CPP Pilot As-Is
Activity Description



VLER CPP Pilot
Phase 1a (San Diego)

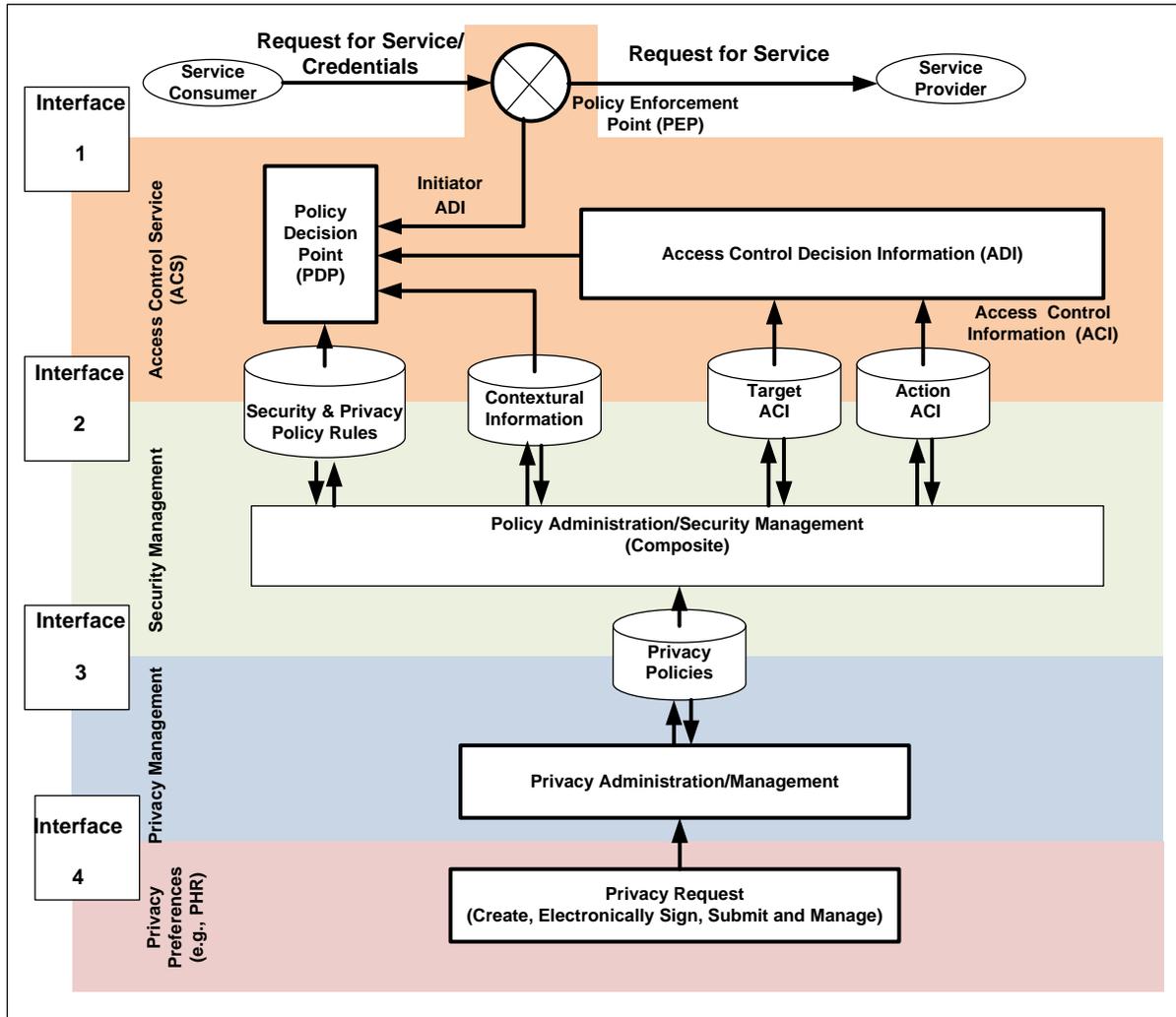


VLER CPP Pilot Phase
1b (Hampton VA) Activity



VLER CPP Pilot Phase
1bi (San Diego) Activity

Reference Business Policy Management and Enforcement Model (Future Process Model):



Technical Notes on the Reference Business Policy Management and Enforcement Model:

The Reference Business Policy Management and Enforcement model illustrates four distinct areas (layers) where business needs are described in this BRD. The model is general and follows the International Standards Organization (ISO) 10181-3 Access Control Framework standard. The model exposes authorization service in the context of generalized access control information types (per ISO) and associated Service Provider Security and Consent Management activities. The internal lines represent information flows and are not specified further. Four interfaces are identified:

1. Interface 1, is the Service Consumer to Policy Enforcement Point (PEP) interface. It is healthcare specific through the attributes contained in the Access Request Access Decision Information (ADI). Interface 1 includes the service consumer request including asserted access control attributes (ADI) that are intercepted by the Service Provider Access Control Service. Service Consumer ADI, along with Resource Access Control Information (ACI), any retained Service Consumer (e.g. Subject ADI), and associated Contextual Information are provided to the policy decision point to be combined with relevant security and privacy rules in order to make an access control decision [1]. This interface, for example, is described in the NWHIN as an SAML Attribute Assertion with a US specific Profile defined as the OASIS XSPA SAML Profile.
2. Interface 2 includes the business security and privacy policy rules and ACI stores. These policies themselves are created by the Security Management processes and provisioned to the ACS on this interface. These stores contain healthcare specific policy references and healthcare ACI/ADI value sets.
3. Interface 3 includes Consent Management. Interface 3 conveys authoritative organization agreed-to patient privacy policy to Security Management. This is interpreted to mean privacy policies accepted/agreed to by the VA that are forwarded to Security Management for integration into the VA managed composite Security and Privacy Policy Rules.
4. Interface 4 conveys EITHER a.) Patient privacy policy provided by an external business partner on behalf of a patient or a Personal Health Record (PHR) external to VA OR b.) Patient privacy policy created by patients through a Consent Management application accessed via the MHV portal, for validation by VA's privacy managers and POSSIBLE acceptance as agreed-to patient privacy policy for enforcement. Consent Management activities provide the means to deal with person privacy policies received from the outside, reflecting input from a Service Consumer, another Service Provider or from the Personal Health Record (PRH). Such policies are permitted, but require normal scrutiny and Privacy Management oversight in order to determine VA acceptance/agreement prior to enforcement.

The interleaving ¹¹Security Management layer represents that portion of the required VA internal business security and privacy management processes that links person privacy policy (from Consent Management) with Service Provider (organizational and jurisdictional) policies. Security Management bears overall responsibility for the management of organizational security and privacy policies, provisioning of Resource and Subject ACI and associated Contextual information, Privilege Management/Identity and Access Management and all other activities surrounding the maintenance and operation of VA's authoritative secure access control policies.

Security Management maps person privacy policy references in the Privacy Policy directories to executable composite privacy policy/policy sets. Security Management prepares patient originated

¹¹ Interleaving is a way to arrange data in a non-continuous way to increase performance.

policies (agreed to by VA) to enable them to be linked to existing policy rules and constraints. It is here that Consumer Privacy Policies are bound to existing organizational and jurisdictional policies to create the complete composite policy/policy sets that will be called upon in the context of a specific request. Security management is a critical business function.

Appendix C. Stakeholders and Primary/Secondary Users

Stakeholders

Type of Stakeholder	Description	Responsibilities
Requester	<ul style="list-style-type: none"> • Tim Cromwell Director, Standards and Interoperability, VHA Office of Health Information (OHI) • Theresa Hancock, Director of Veterans and Consumers Health Informatics Office (V/CHIO), VHA OHI 	Submitted request. Submit business requirements. Monitor progress of request. Contribute to BRD development.
Endorser	Linda Fischetti CHIO, Chief Health Informatics Officer	Endorsed this request.
Business Subject Matter Expert (SME)	<ul style="list-style-type: none"> • Tim Cromwell Director, Standards and Interoperability, VHA OHI • Jamie Bennett, Program Manager, Standards and Interoperability • Theresa Hancock , Director of V/CHIO, VHA OHI • Gaurav Mathur MHV, CHIO, VHA, OHI • Mike Deshazer, Privacy/Freedom of Information Act (FOIA) Officer, Acting Chief of HIM, San Diego VAMC • Stephania Griffin Director, Information Access and Privacy • Andrea Wilson Lead Privacy Specialist, Manager, VHA Privacy Office • Travis Hoffmann Health Data Systems-Data Exchange (HDS- DE), Enterprise Systems Manager (Acting) • Lena Matternas, HDS-DE Analyst, Enterprise Systems Management (ESM) Office • Randy Estes HDS-DE Analyst, ESM Office • Patrick McGrane, Senior Common Services Analyst, ESM Office • Omar Bouhaddou, Program Analyst, CHIO, NwHIN • Glen Crandall Management Analyst, CHIO, NwHIN • Nicholas Xanthakos Staff Attorney, OGC • Jonathan Wilkins, Consultant (Manager), Business Architecture (BA) 	Provide background on current system and processes. Describe features of current systems, including known problems. Identify features of enhancement.

Type of Stakeholder	Description	Responsibilities
	<ul style="list-style-type: none"> • Rakhi Varma Consultant (Business Analyst), BA • Tammy Talley, Program Analyst, BA • John (Mike) Davis, Security Architect, CHIO Emerging Health Technologies • Jennifer Teal, HIM Specialist, HIM Program Office • Beth Acker, HIM Specialist, HIM Program Office • Colleen Tribby Program Analyst, HDI • Betsy Green, VA Program Support Office, Project Manager, NwHIN, Space and Naval Warfare Systems (SPAWARS) Center Atlantic, New Orleans Office • Frank Fontaine NwHIN, SPAWARS Center Atlantic, New Orleans Office • Sara Temnitz, Data Quality (DQ) Business Product Manager, VHA OHI Health Data & Informatics (HDI) • Jackie Houston, HC IdM Program Manager, VHA OHI HDI • Pat Stallings HC IdM Analyst, VHA OHI HDI • Elizabeth Franchi, Director, DQ, VHA OHI HDI • Carol Turner, HC IdM Analyst, VHA OHI HDI • Carrie Parr Program Analyst, HDI • Paul Nichol Associate Chief of Staff (ACOS)/Clinical Informatics • Tana Defa Deputy Director Medical Informatics • Ty Mullen VHA OHI VA/DoD Health IT Sharing • Norman Lee Director of Health Services, Naval Health Clinic Great Lakes • Frank Maldonado Associate Chief of Medical Service, North Chicago VAMC 	

Type of Stakeholder	Description	Responsibilities
Technical SME	<ul style="list-style-type: none"> • Stephania Griffin Director, Information Access and Privacy • Andrea Wilson Lead Privacy Specialist, Manager VHA Privacy Office • Jamie Bennett, Program Manager, Standards and Interoperability • Anthony Mallia, System Integration Architect, Software Engineering, OED • David Staggs, JD, Certified Information System Security Professional (CISSP), VHA CHIO, Standards and Interoperability • John (Mike) Davis, Security Architect, VA CHIO Emerging Health Technologies • Greg Paige, NwHIN Office of Information and Technology (OI&T) Program Manager, VLER Program Executive Office (PEO), OI&T • Nona Hall Interagency Program Office (IPO) • Carolyn Inoa OED Program Management Support • Wally Welham OED Program Management Support • Marie Swall, Functional Analyst, NwHIN, OI&T • Edward Kort, Program Architect, Health IT Sharing Program (HITS), Interagency Integration Portfolio Management Office • Ed Ridley VistA Web Project Manager, OI&T • Gaurav Mathur MHV, CHIO, VHA, OHI • Graham Nixon, Director of Clinical Informatics, San Diego, VAMC • Bill Newhart, Security Engineer, VHA OHI HDI • Rhonna Clark, Program Analyst, Health Security, VHA OHI HDI • Tonya Drew Director Release Management • Annette Parsons Release Management • Tony Doles 	Provide technical background information about the current software and requested enhancements.

Type of Stakeholder	Description	Responsibilities
	<p>IT Specialist, OI&T EIE</p> <ul style="list-style-type: none"> • Betsy Green, VA Program Support Office, Project Manager, NwHIN, SPAWARS Center Atlantic, New Orleans Office • Frank Fontaine NwHIN, SPAWARS Center Atlantic, New Orleans Office • Glenn Sheridan VA/DoD Interagency Program Office • Danny Reed OI&T Project Manager • Jeff Podolec OI&T Project Manager • Ruth Beltran-West IT Specialist, VLER OED • Sylvia Endicott-Sullivan Implementation Manager, OI System Implementation • Elizabeth Feszczenko Deputy Director, National Data Systems 	
User SME	<ul style="list-style-type: none"> • Mike Deshazer, Privacy/FOIA Officer, Acting Chief of HIM, San Diego VAMC • Stephania Griffin Director, Information Access and Privacy • Andrea Wilson Lead Privacy Specialist • Travis Hoffmann, HDS-DE, Enterprise Systems Manager (Acting) • Lena Matternas, HDS, Data Exchange Analyst, ESM Office • Patrick McGrane, Senior Common Services Analyst, ESM Office • Omar Bouhaddou, Program Analyst, CHIO, NwHIN • Graham Nixon, Director of Clinical Informatics, San Diego, VAMC • Paul Nichol ACOS/Clinical Informatics • Tana Defa Deputy Director Medical Informatics 	Ensure that the enhancements will account for current business processes and existing software capabilities.

Primary and Secondary Users

Name	Description	Responsibilities
Primary Users	Patients and authorized individuals	Create, change and revoke consent directives.

Name	Description	Responsibilities
	Policy Administrator	<ul style="list-style-type: none"> • Create, change, and revoke organizational security and privacy policies. • Digitally sign consent directives.
	Local HIM administrative staff, including ROI staff	<ul style="list-style-type: none"> • Use tools to evaluate traits/compare data. • Use consent repository to generate reports and monitor program implementation.
	Local Security and Privacy administrative staff	Use organizational security and privacy policy repository to monitor program, generate reports, and monitor program implementation.
	NwHIN facilities/providers	<ul style="list-style-type: none"> • If Veteran has received care at their facility and consent directive allows sharing of records, share non-VA record with VA provider. • If Veteran has received care at their facility and consent directive allows sharing of records, share VA record with non-VA facility provider.
Secondary Users	<ul style="list-style-type: none"> • Enterprise HIM staff • Enterprise Security and Privacy staff 	Utilize aggregate data to make policy decisions.

Appendix D. Enterprise Requirements

HealtheVet Requirements Management

To view Enterprise-level requirements, access the web site for VHA Health Information Technology, Software Engineering and Integration, Enterprise Requirements Management located at http://vhaishwebr1:81/ReqWeb/Login_Page.jsp. For information and guidance on accessing the database, contact the VHA 19 ESM RAEM Management mailgroup.

Security Requirements

All VA and VHA security requirements will be adhered to. Cross-cutting security requirements are contained in the VA ERR.

Privacy Requirements

All VA and VHA Privacy requirements will be adhered to. Efforts that involve the collection and maintenance of individually identifiable information must be covered by a Privacy Act system of records notice. Specifically, the CPP System will conform to:

- VHA Directive 2004-050, Mandated Utilization of Release of Information (ROI) Records Management Software.
http://www1.va.gov/vhapublications/ViewPublication.asp?pub_ID=1166
- VHA Handbook 1605.1, Privacy and Release of Information.
<http://vaww.vhaco.va.gov/privacy/Documents/VHAHdbk1605-1.pdf>

508 Compliance Requirements

All Section 508 requirements will be adhered to. VHA recognizes that these are Enterprise cross-cutting legal requirements for all developed Electronic & Information Technology. To ensure that these requirements are met, they are addressed through the Enterprise-level requirements maintained by VHA Health Information Technology, Software Engineering and Integration, and Enterprise Requirements Management.

Executive Order Requirements

In keeping with the President's Executive Order: *Promoting Quality and Efficient Health Care in Federal Government Administered or Sponsored Health Care Programs*, VHA OHI must promote quality and efficient delivery of health care through the use of health information technology, transparency regarding health care quality and price, and incentives to promote the widespread adoption of health information technology and quality of care. To support this mission, to the greatest extent possible, any new IT system development or acquisition of commercial system shall:

- Use interoperability standards recognized by the Secretary of Health and Human Services, or the appropriate designated body at the time of the system update, acquisition, or implementation, in all relevant information technology systems.
- Ensure interoperability with the NwHIN.
- Comply with certification standards released through the Certification Commission of Health Information Technology (CCHIT).

The interoperability and certification standards are constantly evolving; for questions relative to these standards, contact Tim Cromwell, Acting Director, HealthePeople, Office of the Chief Health Information Officer.

Identity Management Requirements

All Enterprise Identity Management requirements will be adhered to. VHA recognizes that these are Enterprise requirements for all developed Electronic & Information Technology. These requirements are applicable to any application that adds, edits, or performs lookups on persons (patients, practitioners, employees, IT Users) to systems within the VHA. To ensure that these requirements are met, they are addressed through the Enterprise-level requirements maintained by VHA Health Information Technology, Software Engineering and Integration, and Enterprise Requirements Management.

Appendix E. Acronyms and Abbreviations

Term	Definition
ACI	Access Control Information
ACOS	Associate Chief of Staff
ACS	Access Control Service
ADI	Access Control Decision Information
AITC	Austin Information Technology Center
ARRA	American Recovery and Reinvestment Act
ASTM	American Society for Testing and Materials
BA	Business Architecture
BHIE	Bidirectional Health Information Exchange
BN	Business Need
BRD	Business Requirements Document
CCD	Continuity of Care Document
CCHIT	Certification Commission of Health Information Technology
CDA	Clinical Document Architecture
CHIO	Chief Health Informatics Office
CISSP	Certified Information System Security Professional
COTS	Commercial Off-the-Shelf
CPP	Consumer Preferences & Policy
CPRS	Computerized Patient Record System
DoD	Department of Defense
DQ	Data Quality
DSS	Document Storage Systems
DURSA	Data Use and Reciprocal Support Agreement
EHR	Electronic Health Record
EIE	Enterprise Infrastructure Engineering
EO	Executive Order
ERR	Enterprise Requirements Repository
ESM	Enterprise Systems Management
FAQ	Frequently Asked Question
FOIA	Freedom of Information Act
GNG	Go No Go
HC IdM	Healthcare Identity Management
HDI	Health Data & Informatics
HDR	Health Data Repository
HDS-DE	Health Data Systems-Data Exchange
HHS	Department of Health and Human Services

Term	Definition
HIE	Health Information Exchange
HIM	Health Information Management
HIPAA	Health Insurance Portability and Accountability Act
HIT	Health Information Technology
HITECH	Health Information and Technology for Economic and Clinical Health
HITS	Health IT Sharing
HITSP	Healthcare Information Technology Standards Panel
HIV	Human Immunodeficiency Virus
HL7	Health Level Seven
HTTPS	Hypertext Transfer Protocol Secure
IAM	Identity and Access Management
ICIB	Interagency Clinical Informatics Board
ICN	Integration Control Number
ID	Identification
IIHI	Individually Identifiable Health Information
IPA	In-Person Authentication
IPO	Interagency Program Office
ISO	International Standards Organization
IT	Information Technology
KP	Kaiser Permanente
L	Long Term
MHV	My HealtheVet
MOU	Memorandum of Understanding
MPI	Master Patient Index
MSG	Message
NHIE	National Health Information Exchange
NwHIN	Nationwide Health Information Network
NwHIN-C	Nationwide Health Information Network-Connect
NwHIN WS	Nationwide Health Information Exchange Web Services
NIST	National Institute of Standards and Technology
NPI	National Provider Identifier
NSR	New Service Request
O	Optional
OASIS	Organization for the Advancement of Structured Information Standards
OED	Office of Enterprise Development
OGC	Office of General Counsel
OHI	Office of Health Information
OI&T	Office of Information and Technology

Term	Definition
OMB	Office of Management and Budget
ONCHIT	Office of the National Coordinator for Health Information Technology
OWNR	Owner Requirement
PDP	Policy Decision Point
PEO	Program Executive Office
PEP	Policy Enforcement Point
PHI	Protected Health Information
PHR	Personal Health Record
PIV	Personal Identity Verification
R	Required
R2	Release 2
R3	Release 3
RBAC	Role-Based Access Control
RM	Records Management
ROI	Release of Information
RPC	Remote Procedure Call
SAML	Security Assertion Markup Language
SLA	Service Level Agreement
SME	Subject Matter Expert
SOAP	Simple Object Access Protocol
SPAWARS	Space and Naval Warfare Systems
TP	Transaction Package
U.S.	United States
U.S.C.	United States Code
V/CHIO	Veterans and Consumers Health Informatics Office
VA	Department of Veterans Affairs
VAMC	Veterans Administration Medical Center
VHA	Veterans Health Administration
VistA	Veterans Health Information Systems and Technology Architecture
VLER	Virtual Lifetime Electronic Record
WS	Web Server
XSPA	Cross-Enterprise Security and Privacy Authorization

Appendix F. Approval Signatures

The requirements defined in this document are the high level business requirements necessary to meet the intent of this new service request.

From: Cromwell, Tim

Sent: Wednesday, February 17, 2010 8:17 AM

To: Sklar, Cheryl (Hines OIFO)

Subject: Approve: NwHIN Enhancements Request (NSR#20100102): review and approval of BRD and Quad Chart

From: Lloyd, Susan S. (OIFO)

Sent: Wednesday, February 17, 2010 3:52 PM

To: Sklar, Cheryl (Hines OIFO); Cromwell, Tim

Cc: Hoffmann, Travis F. (HPTI); Matternas, Lena M. (HPTi); Hebert, Linda; Goyal, Pawan (EDS); Dagen, Leslie; Lowe-Bey, Farah

Subject: RE: NwHIN Enhancements Request (NSR#20100102): review and approval of BRD and Quad Chart

approved

Appendix G. Post Sign-Off Additions

The following changes in requirements pertain to Phase 1C:

For phase 1C additions and modifications to the requirements were primarily made in the following areas:

1. CPP/ROI
2. Privacy
3. Information Sharing
4. Identity Management

Additionally, all of the CPP models were updated and Activity Description Tables provided.

From: Morgan, Brian

Sent: Tuesday, December 21, 2010 12:23 PM

To: Sklar, Cheryl (Hines OIFO)

Subject: Approve: Nationwide Health Information Network Enhancements: Review and approval of revised requirements

From: Cromwell, Tim

Sent: Wednesday, December 15, 2010 8:17 AM

To: Matternas, Lena M. (HPTi)

Subject: Approve: Nationwide Health Information Network Enhancements: Review and approval of revised requirements

From: Faherty, Shawn

Sent: Wednesday, December 15, 2010 8:00 AM

To: Sklar, Cheryl (Hines OIFO)

Subject: Approve: Nationwide Health Information Network Enhancements: Review and approval of revised requirements

The following changes were reviewed and approved in June 2010:

The following revisions to section 1.2 Goals, Scope and Objectives are being made:

- Patient creation and management of their own privacy preferences. This will include the ability to create and submit patient consent directives to the ROI Office, either as a paper form or electronically using **emerging-~~HL7~~ CDA R2 consent directive for** messaging standards, as well as management, **electronic digital** signature, and tracking of all consent directives.

The following revisions to section 2.3 CPP External System Interface Requirements:

Delete the diagram as it is out of date and the following text:

~~The diagram provided below illustrates the CPP subsystem in the context of integration with other systems (primarily the Gateway and Gateway adaptor) that are expected to be integrated to provide the VA NwHIN C Gateway Adapter deployment.~~

The attached changes to the requirements were identified subsequent to the approval of this document. These changes to the requirements were not included in the project scope estimates when this request was considered for approval. They will be entered into the repository for tracking purposes.



NHIN Enhancements
Requirements 07_6_2

From: Cromwell, Tim
Sent: Wednesday, July 14, 2010 12:52 PM
To: Sklar, Cheryl (Hines OIFO)
Subject: Approve: NWHIN Enhancements Request: review and approval of revised BRD

From: Wong, Tin
Sent: Wednesday, July 07, 2010 3:29 PM
To: Sklar, Cheryl (Hines OIFO)
Subject: Approve: NWHIN Enhancements Request: review and approval of revised BRD