September 2013

Western States Consortium ONC State Health Policy Consortium Project

Final Report

Prepared for

Office of the National Coordinator for Health Information Technology
U.S. Department of Health and Human Services
300 C Street SW
Washington, DC 20201

Prepared by

RTI International
3040 Cornwallis Road
Research Triangle Park, NC 27709

RTI Project Number 0212050.007.000.500.004

RTI Project Number
0212050.007.000.500.004

Western States Consortium ONC State Health Policy Consortium Project

Final Report

September 2013

Prepared for

Office of the National Coordinator for Health Information Technology
U.S. Department of Health and Human Services
300 C Street SW
Washington, DC 20201

Prepared by

RTI International
3040 Cornwallis Road
Research Triangle Park, NC 27709

This report was funded under Contract No. HHSP23320095651WC, Order No. HHSP23337007T. The contents of this report do not necessarily reflect the opinions or policies of ONC.

Contributing Authors

Alaska
Paul Cartland
State of Alaska Department of Health and Social Services

Arizona
Lorie Mayer
State of Arizona HIT Coordinator for Arizona Strategic Enterprise Technology (ASET) and Arizona Health Care Cost Containment System (AHCCCS)

Ryan Sommers
Senior IT Project Manager
ADOA – Arizona Strategic Enterprise Technology (ASET) Office, State of Arizona

California
Cassandra McTaggart
Chief of Health Information Policy Division
California Office of Health Information Integrity
California Health and Human Services Agency

Kerry Cataline
Chief, Privacy & Security Standards Branch
California Office of Health Information Integrity
California Health and Human Services Agency

Martin Love
Chief Executive Officer
Humboldt-Del Norte Foundation for Medical Care Independent Practice Association | North Coast Health Information Network

Robert M. Cothren, PhD
Technical Director, California Health eQuality Institute for Population Health Improvement
UC Davis Health System

Aaron Seib
2311, LLC
California Office of Health Information Integrity
California Health and Human Services Agency

Nagesh (Dragon) Bashyam
Drajer, LLC

Hawaii
Greg Suenaga
Project Director
Hawai'i Health Information Exchange

Nevada
Lynn O'Mara, MBA
State Health IT Coordinator
NV Dept. of Health and Human Services

Stefani Hogan, MS
Office of Health IT
NV Dept. of Health and Human Services

New Mexico
Craig Hewitt
Chief Information Officer
New Mexico Health Information Collaborative (NMHIC)

Mark Butler
IT Project Manager
New Mexico Health Information Collaborative (NMHIC)

Oregon
John Hall
Krysora LLC

Christy Lorenzini-Riehm
Office of Health Information Technology
Oregon Health Authority

Pete Mallord
Office of Health Information Technology
Oregon Health Authority

Mindy Montgomery
Krysora LLC
Carol Robinson
Robinson & Associates Consulting LLC

Utah
Matt Hoffman, MD
Medical Informatics Manager
UHIN

Wu Xu
Director, Office of Public Health Informatics
Utah Department of Health

RTI International
Alison Banger
Stephanie Rizk
Robert Bailey

Subject Matter Experts
Vicki Estrin, C3 Consulting
Sarah Stewart, C3 Consulting

Colorado*
Liza Fox-Wylie
Policy Director
CORHIO

Florida*
Walt Culbertson
Agency for Health Care Administration

Carolyn Turner
Government Analyst
Agency for Health Care Administration

Georgia*
Kelly Gonzalez
Director, Division of Health IT
State Health IT Coordinator
Georgia Department of Community Health

Lynne P. Hillabrant
Health Information Technology Policy, Privacy & Security Officer
Georgia Department of Community Health

Idaho*
LaDonna Larson
Health Information Technology Coordinator
Idaho Department of Health and Welfare

Washington*
Rick Rubin
President & CEO
OneHealthPort

*Satellite states as of January 1, 2013

The WSC also acknowledges the contributions of Jeff Blair (Retired, Formerly Director of Health Informatics at Lovelace Clinic Foundation), Caitlin Csakai (formerly Senior Program Manager, Public Sector Initiatives, CORHIO), and Dave Perry (Chief Information Officer at Lovelace Clinic Foundation)

Contents

Exhibits

1. EXECUTIVE SUMMARY

The Western States Consortium (WSC) was formed in October 2011 with support from the State Health Policy Consortium (SHPC) project funded by the Office of the National Coordinator for Health IT (ONC). Founded by eight core states and two satellite states, the WSC was created to establish a set of policies and technical solutions to support Direct exchange between Health Information Service Providers (HISPs) and advance health information exchange (HIE) across state borders.

Acknowledging that to tackle the full spectrum of interstate HIE activities and models would expand the scope of the project beyond the available timeline and funding, the WSC chose to focus their work on enabling point-to-point exchange between participating states using Direct Project protocols. The primary goal of the WSC was to develop the necessary policies and procedures to create an appropriate level of trust between different HISPs operating in different states, creating a multi-state, scalable solution to seamless Direct exchange. In addition, the plan included a proof of concept pilot demonstration that established a governance model to support secure exchange between health care providers in Oregon and California. The technical goals for the project focused on establishing a trust community,[1] exchanging digital certificates between HISPs through a trust anchor[2] store, and exploring ways to discover provider attributes within the provider directories of different HISPs.

The WSC developed policy solutions that addressed questions about business agreements between HISPs, security and privacy protocols, acceptable interstate uses of Direct exchange, and identity validation through registration and certificate authorities. The consortium established a governance structure based on a Memorandum of Understanding (MoU) that extended the trust environment to enable interstate Direct exchange. They developed a robust technical infrastructure that assured conformance to governance policy, and enabled secure and trusted exchange of health information between unaffiliated providers and organizations, with scalable distributed provider directory services. The WSC completed two pilot demonstrations in which Direct messages were successfully exchanged between California and Oregon, that is, across state lines and between different HISPs.

The first pilot scenario was executed between health care provider organizations in Southern Oregon and Northern California. Although it was relatively simple from a technical perspective, it laid the groundwork for the WSC governance structure by testing policies and

[1] Trust communities are defined by ONC and the WSC as a collection of organizations electing to follow a common set of policies and processes related to health information exchange. Within the WSC, these policies and processes are defined by the eligibility criteria included in the WSC Policies and Procedures.

[2] RFC 5280, section 6 defines trust anchors as public keys used to verify the signature on a digital certificate. In the context of Direct exchange, it is the public key for highest organization in the trust chain that enforces conformance to requirements for membership in the trust community.

procedures outlined in a precedent-setting interstate Memorandum of Understanding for Direct exchange. In this scenario, Direct addresses for each provider in the exchange were known to each other at the outset and the policies in place enabled the digital "handshake" to occur between HISPs.

The second pilot scenario went further from a technical perspective and overcame a more realistic challenge where providers who want to share protected health information (PHI) in a secure fashion are not aware of each other's Direct addresses. In this pilot, the providers from California and Oregon were able to connect to and search the provider directories in different HISPs and locate the Direct address for the intended receiver of a Direct message. This pilot demonstrated the potential value of a broadly federated provider directory where providers could take advantage of easy search functions and begin to use Direct exchange to push PHI to other caregivers in new, more coordinated models of care, whether in a community or across state lines. A live demonstration of the data exchange between the initial pilot sites was provided at the HIMSS13 conference, which is captured in a subsequent Web demonstration (available online[3,4]). ***Appendix A*** provides a text-based description of this demonstration which describes real-world integration of the WSC's approach to enable exchange between provider practices in multiple states and concludes with delivery of the structured patient record to the subject's Personal Health Record.

During the writing of this report, five of the core states had executed the MOU and completed the on boarding process to join the WSC governance body. A total of 15 states are recognized by the Governance Body as either participating in the work of the WSC or observing, while a number of others have expressed interest in becoming participants.[5]

The WSC will continue to extend the pilot testing of new use cases based on the trust community[6] established by the pilot. The WSC will continue to extend the pilot testing of new use cases based on the current trust community and expects to execute additional pilot tests as additional use cases are identified and prioritized by the WSC's Governance Body. As more states and their associated HISPs join the WSC, the consortium envisions an ever-increasing federation of participants representing more modes of exchange and types of participants.

---

[3] A number of WSC partners demonstrated both scenarios of the Pilot at the ONC's HIMSS Interoperability Showcase. This group also recorded the demonstration which is available on line at this location: https://cc.readytalk.com/cc/playback/Playback.do?id=5o4mmb.

[4] Also see http://www.wsctrust.org for this and other content related to the pilot and ongoing work of the WSC.

[5] During clearance of the report, the states involved to form a not-for-profit named the National Association for Trusted Exchange. Commonly known as NATE, the organization continues to support multi-state initiatives and convene states to better collaborate on health information exchange.

[6] Trust communities are defined by ONC and the WSC as a collection of organizations electing to follow a common set of policies and processes related to health information exchange. Within the WSC, these policies and processes are defined by the eligibility criteria included in the WSC Policies and Procedures.

2. INTRODUCTION AND BACKGROUND

2.1 Background on the Western States Consortium

The American Recovery and Reinvestment Act (The Recovery Act) of 2009, and the Health Information Technology for Economic and Clinical Health (HITECH) Act obligated over $22 billion of Federal support for health IT. Under HITECH, the Federal Government established a range of programs to support the adoption of electronic health records (EHRs) and accelerate the implementation and availability of mechanisms for providers and health systems to exchange information rapidly and securely.

Among these programs are the State Health Information Exchange Cooperative Agreement Program (State HIE Program) and the State Health Policy Consortium (SHPC). The State HIE Program has provided over $547 million in grant support to States and/or State Designated Entities to establish health information exchange (HIE) capacity among health care providers and hospitals, while SHPC supports multistate initiatives to develop solutions to policy challenges specific to interstate HIE. Both initiatives are funded and led by ONC.

With support from SHPC, the WSC project convened in October 2011 with participants representing Oregon, California, Arizona, Hawaii, Utah, Nevada, Alaska, and New Mexico (referred to in this report as core states). WSC focused on how state-level trust services and provider directories can be federated at a regional level to promote privacy and security and facilitate interstate exchange. California and Oregon participated in two proof of concept pilot demonstrations to show how local agreements and trust structures can be established to support interstate HIE with federated provider directory services. In addition to the 8 core States, Washington and Idaho joined the consortium as satellite states[7] and were later joined by Colorado, Florida, Georgia, Michigan and Ohio.

The project was divided into three main phases: an analysis of the status of HIE in each state as of late 2011 and potential options for interstate health information exchange; development of materials to support the pilot implementation; and execution of the pilot between Oregon and California. The analysis of the status of HIE involved reviewing each state's HIE Strategic/Operational Plan Approval Status, approach to trust services and

[7] During the initial phases of the project, specific distinctions were drawn between core and satellite states in order to streamline the scope and overall process undertaken by the WSC. Core states were defined as those with a signed commitment, via a Memorandum of Understanding and/or various contractual agreements, to perform a specific scope of work as part of the project. They were expected to be active participants in all activities defined by this scope and had specific responsibilities to complete the work. Satellite states were those that expressed an interest in the work of the group but did not, for various reasons, commit to a specific scope of work through a Memorandum of Understanding. Satellite states were included in communications between the core members of the group, and were invited to participate in regular status meetings. Due to the fact that the core states would be executing the work most immediately, satellite states were invited to submit comments regarding the work but did not actively participate in decision points for the WSC.

provider directories described in each state's HIE Plan, HIE service offerings, and HIE services request for proposal (RFP) status.

The underlying assumption of this three-phase process was that the execution of the pilots would provide adequate demonstration of feasibility to the other core states. Thus, their participation in the development of the policies upon which the pilot was established would result in those states being able to quickly execute and adopt the outcomes of the pilot.

Over the course of the project, WSC met monthly via teleconference and held five in-person meetings to complete more in-depth work and discuss key issues. See ***Appendix B*** for in-person meeting details.

2.2 Issues Related to Interstate Exchange Using Direct Exchange Services

Launched in March 2010 as a part of the Nationwide Health Information Network (NwHIN), the Direct Project was created to specify a simple, secure, scalable, standards-based means for sending authenticated, encrypted health information directly to known, trusted recipients over the Internet. Using protocols described in the Applicability Statement for Secure Health Transport[8] and the XDR and XDM Direct Messaging Specification,[9] the technical specifications for Direct exchange were largely in place by mid-2011.

In that same mid 2011 time frame, states around the nation began to move forward with implementation of their ONC-approved Strategic and Operational Plans (SOPs) to establish Direct exchange services within their states. States took different approaches; some elected to launch statewide HISPs and provide Direct exchange services through vendor contracts, others provided grant funds to regional health information organizations (RHIOs) to serve as HISPs, while still others chose to facilitate those services through a state-approved marketplace. See ***Appendix C*** for a description of required and optional HISP capabilities.

As the market of HISPs began to develop in states, whether through contracts, grants or marketplace standards, it became clear that the conditions for ensuring a scalable trust framework had not been fully realized in the initial Direct Project development. Across the country, states evaluating the legal and practical considerations of how HISPs might interoperate using Direct exchange protocols began to discover cause for concern stemming from variability on a number of critical factors, including:

- Standards within business associates agreements (BAAs) between HISPs and their member organizations

[8] http://wiki.directproject.org/file/view/Applicability+Statement+for+Secure+Health+Transport+v1.1.pdf

[9] http://wiki.directproject.org/file/view/2011-03-09%20PDF%20-%20XDR%20and%20XDM%20for%20Direct%20Messaging%20Specification_FINAL.pdf

- Identity validation policies and procedures for organizations and users of Direct exchange through registration authority and certificate authority policies[10]
- Security and privacy protocols of HISPs and of Direct exchange users
- Policies for acceptable uses of Direct exchange

While much of the role of the HISP is technical in nature, the points of responsibility for judging trustworthiness of certificates issued or maintained by other HISPs raised questions on the legal agreements that would need to be in place to ensure the fidelity of each HISP's operations, before trust anchors would be broadly shared across HISPs.

The WSC states, as they came together to consider how to develop a regional network for Direct exchange across states, began to see these issues as the basis for their work. While some states participating in the WSC were developing their own contractual relationships with Direct exchange vendors to address these issues, others were considering how to support a broad network of private sector HISPs without contractual authority for any actions taken by HISPs or by certificate authorities operating on behalf of HISPs. At the time of this report, only one state within the WSC, Nevada, is likely to have statutory authority to regulate the actions of a HISP.[11]

The variability across states created a set of parameters that the WSC needed to define in order to achieve success in an interstate pilot environment. Any solutions agreed upon would need to be based on a nonregulatory structure, i.e., be voluntary on the part of HISPs, because some states were without any contractual ability to set policies and standards for acceptable uses for Direct exchange or ensure that organizations participating within a HISP would be required to meet certain criteria.

Any agreements put into place for the WSC pilots would need to be based on attestation and would not have "teeth" to enforce as a consortium because there are no national standards for the accreditation of a HISP. Also, state accreditation programs would introduce more variability and encounter difficult legislative hurdles. Therefore, the states participating in the pilots would need to have an agreement in place to ensure compliance of those HISPs brought into the trust community of the WSC to a set of agreed-upon policies, and would need to agree to remove a HISP from the trust community if it was found to be noncompliant with the WSC policies.

The policy questions being addressed by the WSC for interstate exchange also apply to intrastate exchange between HISPs. For Direct exchange to emerge as the "ubiquitous dial tone" of HIE, these policy questions must be answered. Presently, the tenets of a scalable trust environment are being discussed in multiple forums across the country, each trying to

[10] http://en.wikipedia.org/wiki/Public-key_infrastructure

[11] Nevada plans to resolve the question of statutory authority during the Summer 2013 legislative session.

resolve the scalability challenge presented by multiple point-to-point BAAs between HISPs, both within and between states. The early work of the WSC outlined in this report demonstrates the development of a set of policies and procedures that allow HISP to HISP Direct exchange to occur without maintaining multiple BAAs between those HISPs in a pilot environment.

Although the WSC approach described in this report demonstrates that significant advances can be realized with regard to scaling trust, it is important to acknowledge that opportunities and questions remain for the WSC and others to address. Additional pilot demonstrations and policy considerations beyond what has been addressed in the first pilot exchange scenarios will be necessary to ensure a scalable trust environment.

2.3 Why Governance is Important

Governance establishes a reliable mechanism so that two parties wishing to exchange data can trust that their exchange partner has satisfied a certain set of obligations. When the exchange is between two independent entities operating in similar environments (for example, where both are required to comply with the same set of regulations) governance is generally simplified. Many such relationships exist today and are typically satisfied by mutual trust between the two parties, which may be codified in a contract. For cases where it is desirable for multiple parties to be able to exchange with one another, the conditions for trusted exchange may be facilitated by multi-party agreements, or adherence to a commonly agreed upon reference authority (such as an accrediting body or industry association) or some combination of both.

Over the past several years momentum has been building for the use of Direct to facilitate the exchange of health information between health care providers with known, trusted relationships. As Direct exchange begins to gain traction, new examples of using Direct exchange to improve health care are emerging. For example:

- In Arkansas, the Employee Benefits Division plans to use Direct exchange services to streamline their current prior-authorization processes for medical and pharmacy services.
- The Illinois Quality Improvement Organization is facilitating a care transition pilot between long-term care and acute care facilities using Direct exchange services.
- Maryland, Indiana and others are using Direct exchange services to route admission, discharge and transfer (ADT) notifications from hospitals to primary care providers and care coordinators.
- Oregon's statewide HIE is developing a pilot to facilitate electronic submission of the Physician Orders for Life Sustaining Treatment (POLST) forms from providers and hospitals into the state's electronic registry via Direct exchange services.

Unfortunately, most of these uses of Direct exchange have not easily extended across state boundaries in part due to variance in state law, regulation and practice, but also because HISP to HISP agreements have not been seen as scalable. The WSC was established by a group of states that sought to determine if a system of policies and procedures under a governance framework could be organized to help overcome the barriers to ubiquitous exchange.

2.4 WSC Governance Structure

In October 2011, when the WSC was awarded SHPC support, there were few instances of operational Direct exchange services across the country. Those that had been set up were small pilot environments serving a limited number of organizations. Most of the core states within the WSC were still in the process of finalizing their approach to enabling Direct exchange. Much of the work of the WSC in the first 6 months of the project was spent understanding the various approaches being employed by states to establish Direct exchange services and the different policies being considered to support those services. The concepts of participant agreements and individual user agreements to activate HISP services were gaining traction but still varied, depending on each state's approach to Direct exchange.

By spring 2012, as Direct exchange services began to roll out more broadly across the nation, the Consortium was able to define the scope of the policies needed for a successful pilot of interstate exchange. Extending the trust environment through policies for HISP to HISP exchange was critical to ensuring the trustworthiness of the fledgling HISPs, where legal assurances have been provided to organizations and individuals using their Direct exchange services. The framework for a governance structure began to take form with the creation of a WSC Governance Body and the development of a set of WSC Policies and Procedures linked to a memorandum of understanding (MOU), initially signed between California and Oregon.

The WSC Governance Body served the purpose of governing WSC activities related to trust and directory services during the pilot phase. The WSC Governance Body was made up of member states – each of which committed, through an MOU, to abide by the WSC Policies and Procedures. The premise of the MOU between states in the WSC was to ensure that before any HISP would be allowed to participate in the WSC trust community, the state where the HISP is operating must have attested that the HISP meets the eligibility requirements as established in the WSC Policies and Procedures.

To be eligible to participate in the WSC trust community, a HISP must:

1. Conform to all Direct Project requirements

2. Implement a business associate agreement[12] as a component of contracting with their participants
3. Have contractually binding legal agreements with their participants
4. Demonstrate conformance with industry standard practices related to meeting privacy and security regulations in terms of both technical performance and business processes
5. Minimize data collection, use, retention, and disclosure
6. Encrypt all edge protocol communications
7. Have a process to identify authorized end users
8. Have a policy that ensures similar identity verification criteria for exchange between HISPs (ensuring that a HISP does not allow independent exchange between authorized users without a HISP-to-HISP agreement in place)

While not mandatory, it was also preferable that HISPs enable Direct Project's XDR and XDM for Direct exchange.

Additional obligations that apply to the participating HISP, their participating organizations and the authorized users of their HISP services are also spelled out in the WSC Policies and Procedures. These obligations are analogous to the requirements of the participation agreements in place in many of the operational HISPs around the country, addressing responsibilities of each party such as breach notification, auditing and security practices, as well as data use restrictions and permissible uses of Direct exchange systems.

2.5 WSC Technical Infrastructure

The WSC Direct exchange pilot scenarios were supported by a thin but robust technical infrastructure that assures conformance to governance policy, and enables secure and trusted exchange of health information between unaffiliated providers and organizations. This infrastructure comprises:

1. Secure Transport – standards-based information exchange methods that support provider needs and use cases;
2. Scalable Trust – a scalable approach to identifying exchange partners who meet criteria for trusted exchange established by the WSC; and
3. Distributed Directory Services – a scalable method for discovering (a) trusted individual providers and provider organizations, and (b) the methods by which health information can be securely exchanged with them.

Membership in the WSC trust community is established technically by the creation and management of a trust bundle – the collection of trust anchors for all organizations that are

[12] If the candidate HISP is a conduit model the Governance Body may elect to exempt the HISP from the requirement to implement a BAA. The WSC Governance Body will evaluate this consideration in the future if a true conduit model HISP is identified by a Party State.

members of the trust community. The trust community provides a scalable mechanism for identifying trusted exchange partners who have elected to conform to a common set of policies and processes established by an umbrella governance organization – in this case, the WSC Governance Body. It eliminates the need for point-to-point sharing agreements between each pair of HISPs. The trust bundle provides a scalable mechanism for distributing the authentication credentials of these trusted exchange partners necessary for Direct exchange without the need for point-to-point exchange of trust anchors between each pair of HISPs.

In the absence of a national standard for trust bundles, the WSC defined a simple process for managing and distributing the collection of trust anchors, which supported the pilot exchange between California and Oregon providers. In the first scenario of the WSC pilot, the trust bundle is distributed using secure file transfer protocol (SFTP) and comprises the trust anchors present in a specific folder on the SFTP server. Each HISP retrieves the trust bundle and installs its contents into its trust anchor store. By this single act, the HISP enables bidirectional exchange with all members of the trust community. The WSC also defined a method for alerting HISPs of updates to the trust bundle via email so their trust anchor stores could be updated as necessary.

The WSC project also focused on the technical requirements for the federation of provider directories, as the core states strongly believed that Direct exchange between unaffiliated providers will not scale without this functionality. Standards development organizations such as IHE (Integrating the Healthcare Enterprise)[13], state cooperatives such as the EHR | HIE Interoperability Workgroup,[14] and the Standards and Interoperability (S&I) Framework[15] have defined a number of the building blocks for provider directories, but no nationally recognized standard exists for querying a directory.

A scalable federation of regional and state-level provider directories could support the automated discoverability of provider attributes and ensure that a specific Direct exchange address belongs to the intended receiver of a Direct message across HISPs. Early discussions within the WSC contemplated the potential financial value of provider directories within a HISP, and questions were raised about the potential for HISPs to miss an opportunity to increase sustainability with the value-add service of a proprietary provider directory. While some of the RHIOs who are beginning to offer HISP services already have robust provider directories available to their members, newly created HISPs may build those directories as users are added by participating organizations within the HISP. Ultimately, the financial value (or avoided cost value) of access to information within the provider directory of another HISP or of multiple HISPs could not be effectively determined by participating

[13] http://en.wikipedia.org/wiki/Integrating_the_Healthcare_Enterprise
[14] http://www.interopwg.org
[15] http://wiki.siframework.org

states in the WSC in the rapidly-evolving landscape of Direct exchange. Thus the question of proprietary vs. federated provider directories was settled in favor of demonstrating federation between HISPs for the purposes of the pilot scenarios.

The Oregon and California members of the Governance Body decided that testing of the federated directory functionality should move forward without finalizing formal policies and procedures for the discoverability of a provider's information within the provider directories of the participating HISPs. Numerous draft policies are in development by the WSC Governance Body and are being informed by the work of the S&I Framework Provider Directories Initiative[16] and by ONC's Provider Directory Community of Practice (CoP).

To illustrate the complexity related to a distributed network of provider directories, a list of potential policies is provided below:

- Policy on Purpose of Use
- Policy on Centralized Provider Directory v. Distributed Provider Directories
- Policy on Query v. Push Model for Directory records
- Authorization Policy
- Policy on Caching
- Policy on Data Elements
- Policy on Multiple v. Single Matching Result
- Policy on Auditing
- Policy on On-boarding HISPs for Directory Services into the WSC Trust Community

The work on federated provider directories is in the very early stages and much more will be learned as the WSC and other groups around the country continue to explore this functionality. There is high value in this work, not only for discoverability of Direct addresses, but potentially for more far reaching uses across multiple programs where access to the identity attributes of a health care provider is needed.

The WSC and California are jointly developing a query standard for directory search based on:

- Simple Object Access Protocol (SOAP) Web services over HTTP transport with TLS security,
- Healthcare Provider Directory[17] (HPD) and HPD+[18] provider directory data models, and

[16] http://wiki.siframework.org/Provider+Directories
[17] http://wiki.ihe.net/index.php?title=Healthcare_Provider_Directory
[18] http://www.interopwg.org/documents/request.html (requires registration)

- Directory Services Markup Language (DSML) for query and response format.

Through these standards, the WSC established a conceptual architecture in which each state maintains a provider directory for all Direct exchange users within the state that can be queried via Web services. This approach provides the flexibility to allow each state to create a provider directory solution that meets its needs while maintaining scalability.

2.6 Governance and Scalability: The Future of Direct Exchange

To date, the WSC has successfully executed pilot scenarios for secure, trustworthy Direct exchange between unaffiliated HISPs operating in separate states,[19] enabling providers to coordinate care across state lines. The technical components delivered in the trial implementation include a multi-state trust bundle as well as several incrementally progressive steps towards establishing a standards-based approach to federated provider directory functionality. After the pilot demonstration was completed, Alaska joined the WSC Governance Body with a signed MOU and additional WSC core states are in the process of joining. With regard to federated provider directory behavior, the WSC is working closely with other ONC initiatives to ensure alignment of the final solution with related standards as they are developed and refined.

A significant amount of progress has been made by the WSC in conceptualizing a multi-state governance structure and in executing a sufficient number of steps within that structure for the purpose of interstate pilots of Direct exchange. The technical solutions for exchanging trust bundles and querying provider directories in multiple HISPs through a federated model have been proven. Further, the WSC has endeavored to develop its policies and procedures and technical infrastructure in a manner consistent with existing recommendations of the HIT Policy and Standards Committees,[20] S&I Framework activities and State HIE Program guidelines.[21]

There is much work to be done before scalable trust between HISPs is fully realized, whether for inter – or intrastate Direct exchange. There are numerous initiatives underway that will test and improve on the Consortium's work to date. Considerations of national standards for accreditation of HISPs must move quickly, and should be a key part of the next phase of work for the WSC. Best practices when implementing legal agreements to facilitate trustworthy exchange between HISPs within and between trust communities will continue to be vetted and harmonized across the nation. In the absence of federal regulation, national standards for accreditation, or a scalable set of policies within a governance entity as envisioned here by the WSC, it is likely that some state regulators may begin to address legal and security issues raised in this report. Such a patchwork of

[19] Note that Oregon is a HIPAA only state with a statewide HISP offering while California is a HIPAA plus state with a strategic plan that does not include a statewide HISP.
[20] http://www.healthit.gov/policy-researchers-implementers/health-it-policy-committee
[21] http://www.healthit.gov/policy-researchers-implementers/state-health-information-exchange

state-by-state regulations for HIE could produce a cacophony of different standards for vendors to meet and ultimately be detrimental to interstate HIE.

Broad adoption of Direct exchange for secure point-to-point electronic HIE between health care providers will undoubtedly improve coordination in transitions of care, such as referrals between primary care providers and specialists. While that improvement is itself worthy, the promise of Direct is much broader. New use cases for Direct exchange for patients to receive their own health records, for public health reporting to be streamlined through Direct exchange, or for automated notifications of emergency department visits to care teams via Direct will also yield high value for this relatively low cost and simple way to securely send health data across the internet. Further uses in the areas of administrative transactions such as prior authorizations and claims attachments could save both money and time as the adoption of Direct exchange expands.

The work done by the WSC to explore and test policies, governance options and the federation of technical solutions has made significant progress toward a scalable environment of trust, where Direct exchange can thrive across geographic boundaries and markets.

3. PROCESS AND ASSUMPTIONS

3.1 Strategies for Defining Policy and Technology Solutions

At the outset of the WSC project, participants agreed that policy and technology issues related to creating an interstate HIE solution driven by the use of Direct exchange would need to be addressed in a comprehensive manner. Policy considerations would drive discussion, but technical issues would need to be considered in parallel to ensure that preferred policy solutions were technologically feasible. As part of the original scope of the project, the WSC had established the goal of creating interstate scalable solutions in two distinct areas: trust services and provider directories. An inventory of the then-current landscape of the WSC core and satellite states was conducted via email and reviewed on conference calls. The objective was to identify points of agreement between the states and to determine which policies could be easily aligned and which would require the consideration of multiple options before agreement could be reached.

The WSC drafted a key considerations document in February 2012 that outlined the questions and potential resources and best practices for the establishment of both trust services and provider directories.

Key Considerations for Trust Services

- To whom may digital certificates be issued? Will they be issued to both individuals and organizations? What are the pros and cons to issuing certificates to individuals and/or organizations?
- What information must be provided to a HISP when establishing a Direct exchange messaging account to verify the identity of the individual or person responsible for committing an entity to contractual responsibilities?
- Must identity proofing by a HISP include some level of in-person verification, such as the use of a notary or other authorized party?
- Beyond identity verification, are there any additional criteria that must be met to receive a certificate? Considerations included:
  - Should Direct addresses be issued only to licensed providers or should authorized organizations determine and manage appropriate users of Direct within their organizations, including administrative staff and nontraditional health workers?
  - Should the organizations with Direct addresses be limited to use Direct services only for treatment, or for all HIPAA allowable transmissions of information?
  - Should Direct addresses be extended to other HIPAA-covered entities, such as health plans or public health offices?
- How will the minimum set of policies arising from the answers to the questions above be maintained and governed?
  - Will there be an enforcement or audit mechanism?

- Will there be a standard participation agreement, business associate agreement, user agreement and security standards for participating states?
- Are there consequences for noncompliance, and if so, what might those look like?

Key Considerations for Provider Directories

- The S&I Framework Provider Directories Initiative defined two main sets of use cases for provider directories – certificate discovery for Direct and electronic service information discovery. With the current objectives of the WSC in mind, were there use cases beyond those that need to be considered?
- The S&I Framework Provider Directories Initiative defined a set of data that should be accessible from a provider directory.
  - Are there data beyond those that need to be considered?
  - Will HISPs consider their provider directories to be of proprietary value, where making all data available to the federated network of HISPs would seem to be a risk?
- What standards should be supported for transport and query?

3.1.1 Process for Evaluating Potential Solutions

As of March 2012 the WSC had identified the following as principles to guide their process for investigating a common, scalable solution related to trust services:

1. While each participating state may have different policies with regard to trust services, the WSC should work to find a set of common policies for acceptable exchange between states and build from there.
2. All states are comfortable allowing the exchange of information for purposes of treatment and coordination of care. The WSC agreed to limit the pilot to purposes of treatment and care coordination between health care providers. While Direct exchange may be used for additional exchange related to other HIPAA allowable transactions, the WSC determined those to be out of scope for this pilot.
   a. Collectively the states are not comfortable expanding the information sharing effort to allow for information sharing for payment and operations. These require different use cases and will be addressed in the future.
   b. Coordination of care falls under treatment and operations under HIPAA. The initial use case for the WSC assumes coordination of care by the provider; however, over time the use case that addresses the role of the payer will need to be addressed.
3. The WSC must remain vendor neutral since there are a number of vendors engaged across the states.
4. The WSC needs to identify what is sufficient (not just necessary) for participants to be comfortable supporting interstate Direct exchange, in both the current environment and the "to be" environment.
5. A key piece of the puzzle would be investigating the state's role in ensuring trust. Is transparency and comparison of differences sufficient? Or are there are additional role that the states must play?

6. The timeline and extent of a Federal-level governance rule is enough of an unknown that the WSC cannot wait for conditions for trusted exchange to be established by an external entity. The work of the group will be aligned with guidance as it is established, but should not prevent the WSC from moving forward with investigating and testing a framework of trust in the absence of Federal rulemaking.

The initial discussions related to provider directories were exploratory as the WSC grappled with the considerations listed above. The group agreed to start with the Standards & Interoperability (S&I) Framework (http://wiki.siframework.org/) for data and use cases. The Provider Directory discussion revealed several issues for further consideration and discussion:

- Health plans, licensing boards, provider associations, integrated delivery systems, local health departments and state governments all struggle with keeping their own registries of providers up to date and ensuring timely, accurate information.
- While it is difficult to estimate its financial value, all participants recognized the intuitive value of streamlining numerous activities in health care settings by creating accurate provider directories. Federating access into multiple provider directories across multiple HISPs may provide such a value-add to all participating HISPs.
- Because the challenges of maintaining the integrity of a provider directory over time are well known, the WSC discussed the value of building those directories from the registration process into HISPs to help ensure the validity of the data.
- Using the national provider identifier (NPI) as a required piece of identification in provider directories, rather than as an optional field, would limit the directory to only those provider types with NPIs. There may be high value for the inclusion of nontraditional health workers, public health and other state health programs and other authorized users within a HISP in a provider directory to increase the functionality and broaden Direct use cases.

The WSC defined the business processes listed below and each state documented its status for each business process. See ***Appendix D*** for a listing of results from this exercise. For states that were moving forward with Direct, there was general alignment in technical and policy approaches. However, all states recognized that there were likely to be challenges as these issues were explored further. The business processes addressed the following topics:

- BP1 – Identity registration and maintenance by organization type
- BP2 – Identity provisioning and maintenance (including issuing certificate)
- BP3 – Verification of provider identity and secure exchange of PHI
- BP4 – Assignment of roles (for access rights)
- BP5 – Verification of accreditation
- BP6 – Authorization to access directory services
- BP7 – Authorization to exchange PHI across state lines
- BP8 – Provider Directory

3.2 Project Assumptions and Agreements

As the WSC began to make decisions about various options to enable an interstate trust framework, the group began every discussion by reviewing, expanding, and reaffirming assumptions. This level of transparency was essential to ensuring that the group focused discussion and debate on unresolved issues. The final project assumptions agreed upon by the members of the WSC were as follows:

1. The states forming the WSC do not need to agree on everything; however, there is a need to find and agree on a minimum set of specific policy agreements for acceptable exchange between states.
2. The WSC is vendor neutral and any solution (e.g., policies) must be vendor neutral.
3. The WSC should not wait for definitive guidance from ONC with regard to governance or conditions of trusted exchange to move forward.
4. The S&I Framework for data and use cases can serve as a place to start the discussion; however, it doesn't address all of the questions of the group members.
5. The individual who releases the data (sender) is bound by the laws in the sender's state (e.g., consent requirements). The individual who receives the data (receiver) is bound by the receiver's state laws in terms of access to and use of the data.
6. Although California and Oregon would be taking the lead on activities related to the proof of concept pilot, decisions made for the pilot would reflect consensus from WSC members in order to ensure the solution could be scaled once it had been proven successful.
7. The pilot project was defined as ***provider-to-provider*** exchange of clinical information ***for treatment purposes*** using the Direct mode of exchange where providers are located in different states (Oregon and California). Participating providers in each respective state would need to be associated with different HISP networks (could not be members of the same HISP). The pilot would, if at all possible, test the exchange of live or real patient data (versus the exchange of test patient data).
8. The pilot would be limited in terms of actors (providers involved in patient care); however, there would be a need to consider a more complex environment with various types of actors typically involved in exchange for post-pilot activities.
9. Standardization of the information sent between providers would be out of scope and left to each state's discretion; however, a minimum amount of data may be required for the exchange to ensure it is useful for purposes of exchanging information between providers.

4. PILOT PLANNING AND DEVELOPMENT

As a result of the planning and development activities, the scenarios to be tested in the pilot activity were defined and finalized.

Scenario 1
Exchange of information between providers where the providers' Direct addresses are known and therefore do not require the use of directory services. Use of a directory service is not required if the sender and receiver already have the information needed to complete the exchange (i.e., the Direct address and public key are in hand).
Scenario 2
Exchange of information between providers where the addresses are unknown and there is a need to discover the providers' Direct addresses.

The following agreements were also reached:

- The pilot will be Direct compliant.
- System response time for the entity requesting the data (the receiver) between Direct messages being sent and received is critical and will need to be tested in the pilot.
- Third party accreditation for HISPs is recommended but not required for interstate exchange. Accreditation (or lack thereof) is discoverable.
- Meeting the ONC Implementation Guidelines for State HIE grantees on Direct Infrastructure & Security/Trust Measures for Interoperability[22] should, for the most part, be considered aspirational for WSC participating HISPs. However, two specific guidelines were not fully endorsed by the WSC states and would need further consideration before making the recommended Implementation Guidelines a requirement for future participation in WSC pilots. Those are:
  - Guideline #6: Only facilitate Direct messages that utilize digital certificates which have been cross certified to the Federal Bridge Certification Authority (FBCA)
  - Guideline #8 for HISPs: Provide users with mechanisms to directly establish trust with another user (e.g., store the public key) to enable ad-hoc messaging even if the respective HISPs have not "white listed" each other.
- WSC needs to develop a checklist of principles or elements to be applied to the participation agreements between user and the HISP (not the vendor) where the HISP is considered to be the party who is acting as the contracting organization. For example, this may include limits on disclosure and compliance with state laws.
  - Consider a common set of definitions and terms that reflect the core components of an agreement.

[22] http://statehieresources.org/wp-content/uploads/2012/07/State-HIE-Implementation-Guidelines-for-Direct-Security-and-Trust_7-2012.pdf

- For the pilot, authorization for access to the provider directory is required.
- WSC will test Direct certificates for the pilot (California and Oregon). Participants will execute the exchange of a WSC trust bundle (which is the trust anchor for all the WSC, but will be applicable only within the WSC).
  - Inclusion of states other than California and Oregon will be completed in subsequent phases.
  - The trust anchor is **not** the organizational or individual certificate.
  - For directory service access, authorization of organizational and individual information will be recorded at the originating system for auditing purposes only. This will be a requirement included in the participation agreement.

Several approaches to the trust bundle and provider directory scenario were documented and considered, and are described in detail in below. For each of the two scenarios, a user story and set of key challenges are provided, followed by a set of proposed technical, policy, and governance solutions discussed by the WSC.

4.1 Scenario 1: Provider to Provider Information Exchange for Treatment using Direct, when Direct Addresses of participants are known to each other

User Story

A patient visits a primary care physician (PCP) in Oregon for treatment and the PCP refers the patient to a doctor in California for consultation. This is an established referral pattern in Oregon and California. The doctors involved in the referral process would like to use simple, secure Direct protocols for the referral. The doctor in Oregon is associated with Oregon's statewide HISP, CareAccord™ and the doctor in California is associated with the North Coast Health Information Network (NCHIN) HISP.

Key Challenges

The following are some of the key challenges that the providers face in enabling Direct protocols across HISPs and specifically across state lines even though they know each other and accomplish this task routinely using fax machines:

- *Concern about the ability of the receiving HISP to protect patient information:* One of the key barriers to electronic health information exchange using Direct protocols is for the sender to ascertain that the receiving HISP will follow applicable laws and regulations for information exchanged electronically and protect the patient's information to the same level as the sender. There is no automated way to discover this information currently and hence there is concern about sending the information due to potential liability issues or misuse of the system.
- *Ability to initiate the transactions when required without technical barriers:* Once the sender and the receiver are willing to trust each other based on their knowledge of how their HISPs behave, they have to cross the technical hurdle of exchanging trust anchors and adding them to their HISP in order to allow free flow of communication.

This takes multiple days once the need is recognized, and the exchange of trust anchors must be repeated for each HISP. This is not scalable given the number of providers and organizations interacting with each other.

The solutions proposed by the WSC pilot for Scenario 1 attempt to address the key challenges described above and are grouped under policy, technical and governance solutions.

4.1.1 Proposed Policy Solutions

The policy solutions proposed create a baseline set of policies for the WSC trust community, to enable trust among all the participants in the WSC and avoid requiring trust agreements between HISPs. The proposed set of policies support the ability for each state to on-board HISPs[23] into the WSC trust community. In addition to the policies for HISPs, policies are proposed on how to on-board new states to become members of the WSC. All of these policies are summarized for discussion here and are specified in greater detail in the WSC Policies and Procedures documents (see ***Appendix E***).

Policies for On-boarding HISPs

The policies for on-boarding HISPs are composed of processes and procedures used by organizations to meet and exceed HIPAA requirements, state and federal legal requirements, identity proofing, and operational processes for establishing the infrastructure used to provide HISP services. WSC considered several options for these policies.

- *Comparison of HISP's policies with each other*: In order to build trust between qualified HISPs, one option would be to compare policies between HISPs whenever they are ready to start exchanging information. While feasible, this is not a scalable approach and is highly complex because different HISPs use terminology and language differently.
- *Making policy attributes of a HISP discoverable*: There is currently no set of agreed-upon policy attributes for establishing trust. In addition, new standards and implementation guides would have to be created to enable automated discovery of policy attributes of a HISP. While feasible, this option would impact scaling of Direct exchange in the timeframe for Meaningful Use Stage 2.
- *Establishing a baseline set of policies for HISPs*: Establishing a floor set of policies and mechanisms to verify that these policies are implemented by a HISP is a feasible approach. This option aligns well with the State HIE program vision, aligns with DirectTrust.org activities, and lends itself to a scalable model depending on the implementation. It requires governance for an effective implementation.

Policies for Including New States

New states must sign both a memorandum of understanding (MOU) and a statement of authority. The MOU outlines the basic responsibilities of the state. The statement of

[23] Referred to as Qualified Entities (QEs) in the policy parlance of the WSC, QEs include all types of STAs per the Direct applicability statement. For simplicity the term HISP is used here.

authority is required for each state participating in the WSC to indicate that it has the appropriate authority to on-board HISPs within its geographical jurisdiction.

4.1.2 Proposed Technical Solutions

The technical solutions for Scenario 1 are focused on mechanisms to overcome one-off trust agreements and trust anchor exchange. They also focus on enabling trust anchor exchange across all participants within the trust community.

- *Facilitate trust anchor distribution via trust bundles:* A trust bundle is a collection of trust anchors for each HISP that is on-boarded to the WSC. This bundle can be distributed to all HISPs that have completed on-boarding to the WSC. The trust bundle is used to distribute the trust anchor of new HISPs to all the existing WSC participants, as additional HISPs on-board to the WSC trust community. In reverse, updates to the trust bundle with removed trust anchors for HISPs that have been removed by their Party State can be conveyed to all participants via the distribution of the trust bundle. This enables instant trust between the various HISPs without requiring trust anchor exchanges between any 2 individual participants. Trust anchor exchange between each participant leads to an "n^2" problem and is not scalable for Direct adoption. The technology architectures that can be used to implement trust bundle distribution can vary. Some of the initial options proposed include:
  - Distribution using File Transfer Protocol (FTP)
  - Distribution using Web Services
  - Distribution using Direct protocols
  - Distribution using Domain Name Service (DNS) and Lightweight Directory Access Protocol (LDAP)

The WSC initially used FTP as a means to distribute trust bundles as it was simple and easy for pilot participants to use. Recognizing the limitations of this method, the WSC has been working with the vendors of the participating HISPs to develop more robust methods. The WSC is currently migrating to the technical architecture being proposed by the Trust Bundle sub-work group of the Implementation Geographies workgroup.[24]

4.1.3 Proposed Governance Solutions

Paramount to each state's perspective was the importance that the resulting governance solution would not impede its local authority. Each state must retain sovereign authority to regulate the exchange of PHI within its boundaries and any multi-state governance function would have to work without the dependence on harmonization of statutory requirements to succeed. Further, significant variance between each State's HIE Program strategic plans were based on comprehensive knowledge of the state's specific environment and priorities. Preserving the flexibility for each state's ability to foster HIE within the context of its internal programs was deemed essential to any governance solution. Finally, it was

[24] http://wiki.directproject.org/Trust+Bundle+Sub+Work+Group

determined that the variance in compliance requirements within each state were statutorily inflexible (i.e., required significant lead time to change) and therefore beyond the capacity of the pilot to modify. The authority of a state to require a sender or receiver to comply with its local policy requirements is only applicable to the party that was providing treatment within its jurisdiction. For example, although a state may establish a requirement that a patient provide consent before data is exchanged electronically, the state does not have the authority to enforce that requirement on care provider who delivered the care outside of its state. Current modes of exchange used by care providers do not make it readily apparent to the receiver that the incoming data originates from out-of-state. None of the WSC states have statutes in place to prevent exchange with entities outside of its state. Thus, when a sender and receiver reside in different states the only reasonable expectation that could be placed on either party was to verify that the other party was appropriately credentialed and otherwise authorized to perform exchange in the state where the party resided. In the context of the concepts of the trust bundles and directory services that the Consortium members were investigating, the organizing elements to establish a governance process to facilitate interstate exchange began to emerge.

The governance solution proposed by WSC is to create tiered governance where trust communities can be established across the country which in turn can aggregate the participants in each trust community to a higher level trust community ending in the WSC. To facilitate the above concept, the required governance bodies are the WSC governance body and the state-level governance entities. These governance bodies are described below.

WSC Governance Body

The WSC Governance Body serves the purpose of governing WSC activities related to trust and directory services during the pilot phase. The WSC Governance Body is made up of member states – each of which has committed, through a MOU, to abide by the WSC Policies and Procedures. The purpose of the governance body is to:

- Develop and maintain policies to establish the minimum requirements in assuring the practices of qualified HISPs and include them in the trust community
- Manage the trust bundle for the WSC
- On-board new member states to participate in the WSC pilots following the Policies and Procedures established by the WSC
- Prioritize, through collaborative processes, the work plans and related activities of the projects undertaken by the members of the Consortium. The Consortium has intentionally taken small iterative steps toward completing the projects we have worked on to date with specific go\no-go criteria evaluated by the Governance Body before a project is advanced to the next stage. The WSC methods are to adopt existing standards where necessary, collaborate with all contributing participants and remain focused on approved projects. To date these activities have focused on

developing policies and technologies that are intended to increase the trustworthiness and scalability of Direct exchange across the states.

- Further refine existing policies and procedures, enhance the tools and technologies beneficial to scalable trust, and contribute to standards and accreditation concepts where appropriate following a consensus process to further mature the policies and procedures not completed to date.

State-Level Governance Entities

Referred to as Party States in the current MOU, state-level governance may take on any number of forms including a State Agency, a State Designated Entity, or another organization deemed by the State's HIT Coordinator as the most appropriate organization to handle the responsibilities of a Party State as described in the WSC pilot MOU. The Consortium has reached the maturity state where it is beginning to build lessons learned about how various forms of Party State organizations impact the overall governance of the Consortium and is finding ways to improve its policies and guidance on how new states can benefit from the lessons learned as they become signatories to the MOU. Considerations for how these entities will develop across different states with varying landscape of HIE will be an important part of the next maturity level of the WSC.

While these State-Level Entities may be different in structure and membership, the WSC Governance Body's current policy is to ensure that each state to be on-boarded to the WSC:

- Appoints a representative to the WSC Governance Body that is either the State Coordinator for Health IT under the State's Cooperative Agreement with the Office of the National Coordinator for Health IT or his or her designee
- Executes the MOU of the WSC Governance Body
- Fulfills the responsibilities of a Party State as described in the MOU

Presently, the state-level governance entities are loosely defined and have varying levels of authority (or no authority) over the actions and policies of HISPs operating within their state's jurisdiction. After on-boarding to the WSC Governance Body with a signed MOU, each state currently determines the eligibility of a qualified HISP within their state to participate in the WSC based on their attestation to the policies set and maintained by the WSC Governance Body.

In the future, the WSC hopes to further explore how each state-level governance entity might further establish its ability to satisfy the responsibilities of a Party State either through legal agreement and voluntary participation, statute or administrative rule, to ensure that the policies adopted by the WSC Governance Body are adhered to by any qualified HISP within the WSC trust community.

4.2 Scenario 2: Provider to Provider Information Exchange for Treatment using Direct when Direct Addresses of participants are not known to each other

User Story

A patient visits a PCP in California for treatment and the PCP refers the patient to a doctor in Oregon for consultation. This is a typical referral pattern that occurs between California and Oregon. The doctors involved in the referral process would like to use simple, secure, Direct protocols for the referral. The doctor in Oregon is associated with Oregon's statewide HISP, CareAccord™ and the doctor in California is associated with the NCHIN HISP.

Key Challenges – Scenario 2

The following are some of the key challenges that the providers are facing in enabling Direct protocols across HISPs and specifically across state lines even though the providers accomplish this task routinely using fax machines:

- *All of the challenges outlined in Scenario 1 are applicable to Scenario 2*
- *Ability to discover the provider's Direct Address*: One of the key barriers to electronic health information exchange using Direct protocols is for the sender to discover a provider's Direct address where a patient's information can be sent. In the above user story, the PCP in California needs to discover the Direct address of the Oregon PCP across the border. In the fax and telephone world, there are yellow pages and other websites which can be used to discover the relevant information; however this type of information is not available for Direct addresses.

The solutions proposed by the WSC pilot for Scenario 2 for this additional key challenge are grouped under policy, technical and governance solutions for ease of reading although they are all interrelated and are required for Direct exchange to scale across the country.

4.2.1 Proposed Policy Solutions and Guidance

All of the policy solutions proposed for Scenario 1 are applicable for Scenario 2. This section identifies the additional policy solutions that have been proposed for enabling Scenario 2. All of these policies are summarized for discussion here and are specified in greater detail in the WSC policy documents.

Policy on Purpose of Use

The discovered information about a provider can only be used for treatment and HIPAA related purposes of use. The technical and governance solutions are designed only for these specific uses.

- *Policy on Centralized Provider Directory versus Distributed Provider Directories:* One of the tenants of the WSC is to ensure that each state and its HISPs can operate on their own with a sustainable business model and do not require centralization of

directories or other services. This principle is adhered to by the policy decision to allow HISPs to implement, maintain and publish their directories via the WSC directory services and do not require a centralized provider directory to be created for WSC. However, a state-level directory service to discover Direct addresses is highly beneficial for interstate exchange as it facilitates disaggregation at the state level and affords performance improvements supported by a distributed query approach. This service can also federate the requests internally in the state or create a state-level directory as the state geography and requirements require.

- *Policy on Query/Retrieve versus Push Model:* The query/retrieve protocols will be used for discovery of the Direct addresses instead of the push model in order to effectively enable clinical workflows. A provider trying to refer a patient to another provider typically considers the patient's preferences in terms of geography, location and comfort level to determine the provider that can best serve the patient's treatment needs. The search therefore to identify the receiving provider is required within the clinical workflow and query/retrieve provides the best option to obtain the necessary and most current information.

- *Authorization Policy:* Although current opinion leans toward the view that the information contained in a HISP's Provider Directory is largely publicly available information, there are still some questions as to whether the HISP has the authority to make that information available to individuals that are not signatories to the same Participation Agreement (i.e., from other HISPs).[25] Because this issue remained unresolved at the creation of the current policies, the WSC has decided that entities who are on-boarded to use the directory services are the only ones who can query the various state and local directories across state lines. Thus requestors who are not on-boarded to the WSC for directory services are not authorized to query the directories of other states.

- *Policy on Caching:* The WSC has adopted a model similar to DNS in that every Direct address discovered has a TTL (time to live) parameter associated with it. This will be set to "zero" by default across the WSC participants to indicate there will be no caching of directory entries. If caching is required in the future for performance reasons, the WSC Governance Body would establish the value for TTL as informed from experience of the pilot.

- *Policy on Entities and Individuals Searches:* The WSC has decided to support both the discovery of Direct addresses for organizations and individuals.

- *Policy on Data Elements:* The WSC has agreed that there is more to be learned from executing the pilot regarding potential policy requirements for a minimum set of data elements that participants should support for both the query and the results. Based on preliminary discussions, the data elements that are most expected to provide the highest value for queries to provide sufficient context for the directory searches to

[25] For example, a policy regarding the sensitivity of different data elements that may be found in the federated query needs to be developed. Many data elements might be characterized as public information while others should only be disclosed to other providers of care or similar appropriate users. Some feel that the information in a HISP's Provider Directory is already public information while others believe that the signatory to the PA of a HISP has not given the HISP the authority to make any of that information available. At this time the WSC requires any access to the response of a query be constrained to authenticated and authorized pilot participants. We expect that as work in this area continues, a clear policy regarding this issue will help establish normative standards across the country.

return a matching result to provide sufficient context for the directory searches to return a matching result would likely involve parameters such as:

  - First name, last name, specialty, geographical information (county, city, state or ZIP code) for individuals
  - Organization name, geographical information or Entities.

  The data elements agreed upon for results returned for the query include the necessary information to enable health information exchange using Direct protocols (Direct addresses associated with the individual or the organization) and at a minimum, the query parameters that were submitted with the query.

- *Policy on Multiple versus Single Matching Result:* The WSC will return multiple results based on the query parameters (instead of providing a result only when a perfect match is found) to increase the probability of the requestor finding the right match. The requestor must have local policies on how to narrow down from multiple results to a single result as required.
- *Policy on Auditing:* The WSC has decided that there is no centralized audit log required to track the queries submitted and the results returned, however each entity involved in a directory query/retrieve transaction such as the requestor, any intermediaries such as HISPs local directory sources should log the necessary information to support reporting needs and security incident response management. The audit logs are intended to provide the required audit trail to address security incidents including HIPPA violations, accounting for disclosures and other purposes.
- *Policy on On-boarding HISPs for Directory Services:* HISPs who are interested in either publishing directory information or consuming directory information will be on-boarded explicitly for directory services.

4.2.2 Proposed Technical Solutions

The technical solutions proposed for Scenario 1 are reused for Scenario 2. This section describes the technical solution for Scenario 2, which focuses on mechanisms to create directory queries/receive results, and ensures only authorized requestors are accessing the directory services. The technical solutions are aligned with internet standards and protocols to ensure the interoperability, scalability and adoptability of the solution. The following are the protocols and standards recommended for the various components of the directory service solution:

- *Message Integrity and Confidentiality*: Message integrity and confidentiality between the various endpoints including the intermediates is achieved using the Internet Transport Layer Security (TLS) 1.0 standard and specification.
- *Authentication*: TLS mutual authentication (both client and server authentication) Internet protocols are followed to authenticate the client and server to each other.
- *Authorization*: Authorization is achieved by the on-boarding processes, coupled with the issuance of the necessary Public Key Infrastructure (PKI) certificates which will be used for both authentication and authorization.
- *Query Request/Response Header Structure*: For the WSC pilots, the query/response headers will be structured using Simple Object Access Protocol (SOAP) 1.2 standard.

This standard is also used by the Integrating the Healthcare Enterprise (IHE) Healthcare Provider Directory (HPD) specification. This may be reconsidered further after the pilots to see if a RESTful approach is more desirable vs. the SOAP-based Web services.

- *Query Request/Response Body Structure*: For the WSC pilots, the query/response body will be structured using Directory Services Markup Language (DSML) 2.0 structures leveraging the data element definitions from the IHE HPD specification supplemented by the S&I Framework Provider Directory Electronic Service Discovery User Case definitions. This may be further evaluated after the pilots for refinement based on the real world pilot experience.

4.2.3 Proposed Governance Solutions

The WSC employs the Direct method of exchange and its related requirements to ensure the security of data and transport. The complexity of the governance function is driven upward by a number of factors. The most pertinent to be considered in the case of the WSC include:

- The differences between state environments, specifically, the difference between the sets of obligations that a sender and receiver located in different states would need to satisfy.
- The presence of an accreditation process that could reflect these differences and the recognition that providers cannot afford to wait until a fully vetted and broadly available accreditation market emerges.
- The breadth of abilities and business models of entities abilities likely to benefit from participating in exchange, including, ultimately, independent organizations operating Direct exchange directly from their certified EHRs.

The governance solutions proposed for Scenario 1 are supplemented with the following additional governance functions. These additional functions are performed by the previously established governance bodies without the addition of any new governance bodies.

WSC Governance Body

In addition to performing the governance functions outlined for Scenario 1, the WSC governance body finalizes and provides the floor set of policies to each state to be used during the on-boarding of HISPs for directory services.

State-level Governance Body

In addition to performing the governance functions outlined for Scenario 1, the state-level governance body determines the eligibility of a HISP within the state to participate in the WSC and either use or publish directory services.

5. PILOT IMPLEMENTATION AND IMPLICATIONS

This section describes the policy and technology implementation details of the WSC pilots that were conducted during the SHPC project timeframe. Scenario 1 demonstrated sending and receiving a Direct message between providers in unaffiliated HISPs across state lines when the Direct addresses are known to each other. Scenario 2 demonstrated the ability to discover a Direct address in the provider directory of a different HISP across state lines in order to send and receive a Direct message when the providers' Direct addresses are unknown to each other.

5.1 Scenario 1: Provider to Provider Information Exchange for Treatment using Direct, when Direct Addresses of participants are known to each other

5.1.1 Policy and Governance Implementation

Multiple policy and governance artifacts were developed as part of the WSC Scenario 1 pilot implementation. Each of these artifacts serves a specific purpose within the pilot and can be further leveraged as templates that can be used to scale the implementation model for the country. In addition to these artifacts many processes were developed to on-board HISPs and manage the trust bundle. The following is a list of policy/governance artifacts and entities created for the pilot implementation:

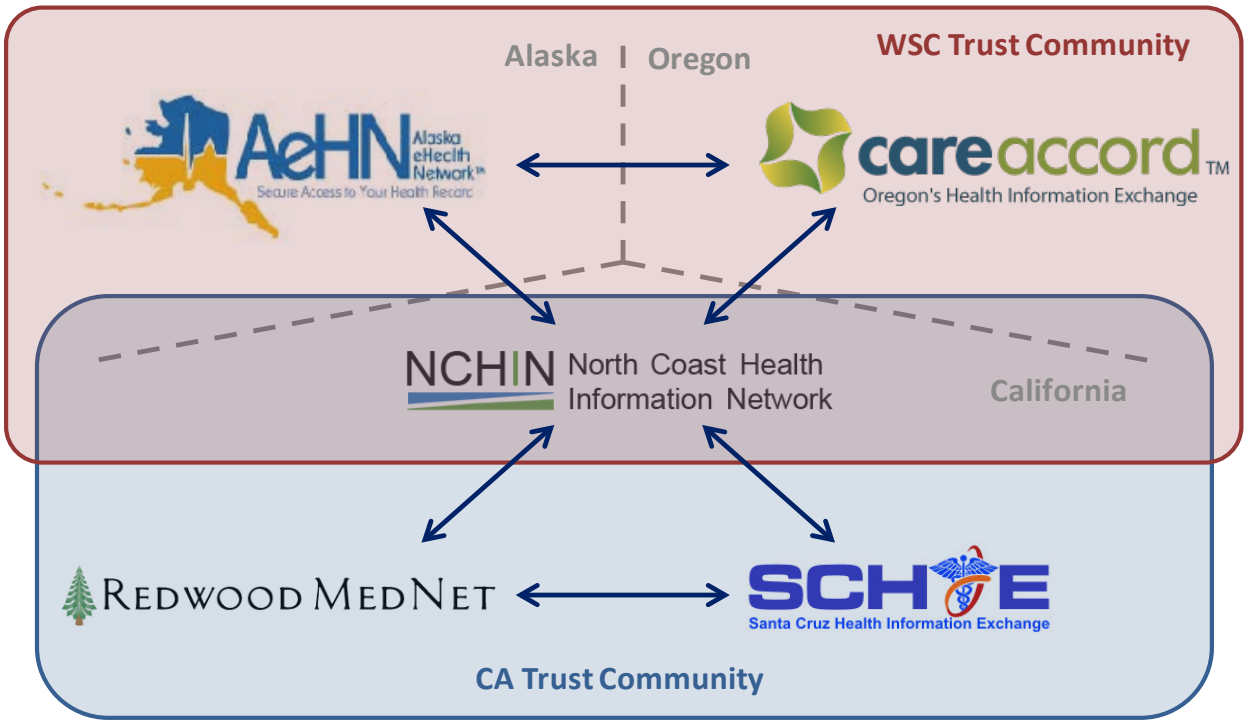
- *MOU*: This policy/governance artifact is used to on-board new states to the WSC (see ***Appendix F***).
- *Statement of Authority*: This policy/governance artifact is used to ascertain that the entity participating in the WSC on behalf of a particular state has the necessary authority to represent its geographical jurisdiction (see ***Appendix G*** and ***Appendix H***).
- *WSC Policy and Procedures Change Process*: This policy/governance artifact captures the details on how the WSC governance body can change the policies and procedures associated with the WSC.
- *WSC HISP On-boarding Process*: This policy/governance artifact captures the details on how the WSC member states can on-board HISPs within their state to participate in the WSC.
- *WSC Communication Plan*: This policy/governance artifact provides communication guidelines to the WSC member states for effective outreach and adoption of WSC directory and Trust Services.
- *WSC Governance Body:* This governance body has been established with current membership representation from California and Oregon. These members are performing and implementing the policies outlined in the previously discussed policy/governance artifacts.
- *Oregon State-level Governance Body*: The governance functions were managed by the Oregon State Coordinator for Health IT, without the formalization of a

governance body as envisioned in future-state WSC pilots. The State HIT Coordinator performed the state-level governance functions outlined in the WSC policy and procedures document within the state of Oregon.

- *California State-level Governance Body*: This governance body performs the state-level governance functions outlined in the WSC policy and procedures documents within the state of California.
- *WSC Trust Bundle Coordinator*: The trust bundle coordinator manages the addition, removal and distribution of trust anchors. These trust anchors are added or removed based on the WSC governance body decisions and notifications are provided per the processes created within the WSC.

The makeup of the current WSC Trust Community created in Scenario 1 is provided in Exhibit 1 below. Scenario 1 created a WSC Trust Community with Oregon's CareAccord statewide HISP and California's North Coast Health Information Network (NCHIN) regional HISP as members. We are in the process of expanding the Trust Community to include Alaska's AeHN statewide HISP. California is in the process of establishing its own Trust Community that includes NCHIN, Redwood MedNet, and Santa Cruz HIE regional HISPs to support a demonstration at the Interoperability Showcase at HIMSS2013. Exhibit 1 shows how exchange occurs with overlapping Trust Communities.

Exhibit 1. WSC Trust Community



5.1.2 Technical Implementation

Oregon Specific Implementation: The Oregon pilot participant is CareAccord, the state-level Direct HISP. This HISP implements the Applicability Statement for Secure Health Transport, version 1.1 (the specification for Direct exchange). This ensures that the pilot participant does publish certificates as required by the Applicability Statement for Secure Health Transport v1.1, which includes both the HISP public certificate, as well as certificates at all levels for other HISPs to discover. The Applicability Statement for Secure Health Transport v1.1 also requires that certificates be issued to at least the level of health care organizations, therefore, publishing only a HISP-level certificate is not currently considered compliant by the WSC. While the WSC acknowledges that this interpretation of the requirement is not universal, the core states have chosen to align with the majority interpretation. The ability to connect with entities that have chosen to use HISP-level certificates in the implementation of Direct exchange has been offered as a future consideration to be taken up by the WSC governance body.

California Specific Implementation: The California pilot participant is the NCHIN, which provides Direct exchange services in Northern California. This HISP implements the Applicability Statement for Secure Health Transport v1.1, following the general requirements outlined above regarding certificate discovery.

WSC Trust Bundle Distribution Solution: The WSC pilot solution included a mechanism for trust anchor aggregation and distribution following the processes outlined in the policy and governance artifacts. The technology standard used for the trust bundle distribution is FTP. FTP was chosen as the technology to minimize the resources spent on the technical solution and instead focus on implementing the necessary governance and processes to manage the trust bundle and learn from the pilot implementation.

An open source FTP server called Filezilla which is a robust implementation of the FTP protocol was adopted for the pilot. The technology provides the necessary security safeguards in terms of access controls and audit logs to monitor the downloading of the trust bundle among the WSC participants.

A user account called "wscuser" was created and provided to the WSC participants for downloading the trust bundle. Only the Trust Bundle Coordinator can add/remove trust anchors into the trust bundle based on the WSC governance body decisions as documented in the process flows.

5.2 Scenario 2: Provider to Provider Information Exchange for Treatment (P2P4T) using Direct when Direct Addresses of participants are not known to each other

5.2.1 Policy and Governance Implementation

All of the policy and governance solutions implemented as part of Scenario 1 are reused as part of Scenario 2. In addition the following policy/governance artifacts and processes will be added or modified.

- *WSC HISP On-boarding Process*: The WSC HISP On-boarding Process exists from Scenario 1. However, the process will need to be modified to support the on-boarding of HISPs who are either consumers of provider directories, publishers of provider directory information or act as both consumers and publishers will be added to the process.
- *Oregon Directory Service Policie*s: The Oregon pilot entity develops policies surrounding the usage of directory services such as how should the provider resolve issues when multiple matches are found and how does the state-level directory service interact with the local directory services within the state when the query originates from outside of the state.
- *California Directory Service policies*: The California pilot entities, which are a combination of the state-level directory and the local directory implemented by NCHIN, develop policies surrounding the usage of directory services such as how should the provider resolve issues when multiple matches are found and how does the state-level directory service interact with the local directory services within the state when the query originates from outside of the state.

5.2.2 Technical Implementation

All of the proposed technical solutions in Chapter 3 for Scenario 2 are implemented as part of the technical implementation. In addition all the technical solutions outlined as part of Scenario 1 are reused in Scenario 2. The following are some of the details of the Technical Implementation.

Oregon Specific Implementation: The following are additions to the Oregon implementation to support directory services as part of WSC pilot Scenario 2.

- *Provider Directory Implementation*: The state-level HISP within Oregon is implementing a provider directory based on the HPD+ standard to support the directory services for the WSC pilot.
- *State-level Directory Services*: A new state-level directory service is implemented to interact with other states. These interactions include requesting information from other states (i.e., discover providers in neighboring states) and responding to incoming queries from other states (i.e., allow other states to discover information present in the state provider directory). All of the standards proposed for Scenario 2 as described in Section 4.2.2 are implemented as required directory service interfaces.

California Specific Implementation: In California there is no state-level HISP and so the state-level directory is a federated service that interacts with many local directories. For the WSC pilot the NCHIN local directory was used along with the state-level services. The following details describe the technical implementation of the state-level directory service and NCHIN local directory.

- *NCHIN Provider Directory Implementation*: The NCHIN HISP is implementing the provider directory based on the HPD+ standard to support the directory services for the WSC pilot.
- *NCHIN Directory Service*: The NCHIN directory service is implemented using the proposed standards for Scenario 2 to request and respond to directory requests from the state-level directory.
- *State-level Directory Service*: The state-level directory service is implemented using the proposed standards for Scenario 2 to request and respond to directory requests from other states who are members of the WSC.
- *Federation of Incoming Requests by the State-level Directory*: The state-level directory service federates incoming requests from other states to the various local directories (in the case of the pilot NCHIN is used as the local directory) using the same standards proposed for Scenario 2 and aggregates the responses from multiple directories and provides the result back to the out-of-state requestor.
- *Technology Agnostic Local Directory Interfaces*: The state-level directories and local directories all use the same standards proposed for Scenario 2 from Section 4.2.2 which eliminates any dependency on a particular provider directory implementation model as long as the interfaces and the data elements are satisfied by each implementation.

5.3 Implications for Administering a Trust Community

5.3.1 Scaling the Governance Model

There are a number of tactics that would likely accelerate the scaling of this governance model. Adding states to the governance body is expected to be easier than the initial process followed by California and Oregon. The strategic approaches employed by the states in the consortium are varied and diverse. Once all core states have been on-boarded, the governance body will have dealt with a wide variety of environments, and will be prepared to on-board additional states regardless of approach. A number of additional states not originally involved in the baseline WSC work are interested and actively engaged in discussions regarding the on-boarding procedure. This expansion of the WSC validates the work to date and supports the premise that scalable trust services are needed. The Consortium is also interested in merging with other similar initiatives as they emerge to ensure the broadest level of scalability and integration possible.

It is expected that changes in cost and technologies related to some of the requirements found in the WSC eligibility criteria will help streamline the process of maturing HIOs in

those trust communities that have strategically elected to include those HISPs that are not able to satisfy the inter-state community's expectations today. Lowering cost and concentrated technical assistance may increase the number of HISPs who meet the eligibility criteria for interstate exchange in the future.

We suspect that scaling the purposes of use supported by this approach will be significantly improved as we expand the community's ability to automate certain policy decisions by making attributes about the HISPs, organizations, or individuals found in the directories federated together as part of the governance framework.

5.3.2 Pilot Expansion

The consortium developed a governance model that would satisfy the requirements of the pilot. This model may not be sufficient to govern the future expansion of the WSC and may need to be modified, but stands as simple and effective solution that can serve as a roadmap to future development. Continued pilot testing with the on-boarding of additional states will provide essential learning opportunities, as other accreditation activities such as DirectTrust.org are explored simultaneously. Ultimately, the related artifacts from the work of the WSC will assist the national efforts to expand HISP-to-HISP exchange, both from the expansion of federated provider directories as well as with the policies that have considered state-by-state differences while still working to ensure a secure and trusted environment for Direct exchange.

6. LESSONS LEARNED

The goal of the WSC project is to expand and scale the solution to provide a continual growth of trusted exchange across the nation. During the course of this project, a number of important issues were discussed, some of which guided the decisions and outcomes of the work of the WSC, and some of which set the stage for additional work moving forward. The following are lessons learned throughout the project by WSC participants as support from the SHPC project came to a close. They are categorized to align with the major activities discussed throughout this report: Process, Technology, Policy and Governance.

6.1 Process

- It is important to define and stay within the scope of the project. It is harder to stay in scope than it appears; managing the complexity is difficult and becomes worse if the project gets too big.
- Unpopular topics such as breach, legal actions, and insurance issues must be discussed. While they may lead to detailed discussions, they may also be essential to completing the scope of work as defined. For example, discussions regarding a breach in the release of the provider directory resulted in the conclusion that it is a minimal risk as all Direct messages are encrypted so PHI will not be exposed.
- Even though each state is unique, success can be achieved if the focus remains on commonalities that enable movement forward. For example, by focusing on the *minimum requirements* for trust bundle and audit logs, the WSC participants were able to come to an agreement fairly quickly.
- Electronic exchange of health information is important and necessary for the future of health care but it does not occur unless it fits into workflow.
  - The infrastructure needs to be built into the EHR to successfully get the workflow.
  - Use cases that do not contemplate a "workable" workflow do not seem effective. Without solving issues of workflow, many of the current Direct use cases are in danger of not being executed by providers.
  - The value of information exchange to the provider does exist, but only becomes a reality after the creation of a mature legal and regulatory framework that allows for it to happen seamlessly. There is a significant amount of work to be done for this to be realized.
- It is necessary to keep stakeholders informed and engaged with HIE activities, especially policy-making. Tremendous value can be gained by recruiting physicians who can speak about saving time by using Direct or saving the life of a visitor from out of state with a HISP-to-HISP connection.
- It is imperative to find use cases of value to providers at the point of care and figure out how to communicate these use cases to providers/hospitals.

6.2 Technology

- States may have operating HISPs that may not satisfy the WSC applicability statement. Some technical work needs to be completed, as these systems are largely not built for a "plug and play" environment.

- As the number of HISPs across the nation increases and users expect rapid connections, it will be nearly impossible to know and trust each and every HISP vendor that wants to connect to an HIE. Since HIEs will bear responsibility in the event of a problem, it is important for the HIE to work proactively to vet HISPs and develop strategies for on-boarding HISPs.
- HISPs should expect to share their operational polices. If the partner HISP doesn't have operational polices, such as how they provision and validate their providers, it should be a red flag that a HISP may not be ready for inclusion into the overall trust community.

6.3 Policy

- Never underestimate the amount of time required to work together on legal agreements/documentation to accomplish an acceptable level of standardization.
- It is important to agree to a common terminology in order to have successful discussions about implementation, especially as it relates to policy and legal issues.
  - Even in the legal contract language there is a lack of common terminology between states and between organizations.
  - The lack of common policy and semantic standards impacts the ability to exchange.

6.4 Governance

- The core WSC state participants continue to struggle with difficulties in asserting authority in governments/governance and to enforce requirements with effective contractual or statutory authority.
- The WSC project was pioneering exchange in an immature landscape; there is still much to learn. For example:
  - There is much more to do even though so much has been accomplished, particularly as other types of HIE, including query-based, are included in future pilots for interstate exchange.
  - State representatives are very concerned about their role in providing entrepreneurial services as the state without more policy guidance from ONC and authorization from their state's legislatures. In each state, high-level support (from Governor's office, legislatures and high-ranking health officials) and funding will be necessary for the concept of State-level governance entities for HIE to thrive.
  - There are many opportunities for testing new options and concepts. Participating states need to be nimble and comfortable with risk, in order to be successful in establishing the connections that allow providers to exchange data more fluidly across state lines, under appropriate circumstances.

7. FUTURE AND RECOMMENDATIONS

The member states of the WSC look forward to extending the ability of the Consortium to support its multi-state governance approach, increase interoperability, decrease the cost and complexity of Direct exchange, increase trust among participants, and mobilize exchange to support patient care.

There is significant work to be done to reinforce and build on the work that the WSC has accomplished over the past eighteen months. Much of the work that has been completed is still in its initial phases and will benefit from repeated testing as more HISPs become engaged in the WSC pilot and more providers begin to use Direct exchange services.

As the WSC continues to expand its trust community with an increasing number of HISPs and participating states, it will be essential to develop a repeatable pattern of state-level governance that can be executed in a flexible way across different state environments. The states in turn must be able to provide more than an attestation for their commitment to the WSC Policies and Principles; the current MOU or other type of interstate agreement must be either be sufficiently rooted to a national accreditation standard or bound by state statute, rule or contract in order for the scaling trust community to pass legal muster over time.

While grant support or funding for technical assistance, in person meetings, or other continuing work by the WSC is currently uncertain, the list of potential issues for future WSC attention is long and includes the following:

- Accreditation
  - Evaluate and recommend the role of accreditation requirements for WSC trust community
  - Work closely with DirectTrust.org; participate with at least one HISP in the Direct Trusted Agent Accreditation Program (DTAAP)[26]
- Legal Agreements
  - Evaluate and test a model multi-HISP legal agreement across multiple HISPs and/or states
- Patient Mediated Exchange
  - Participate in the promotion of Blue Button Plus[27]
  - Consider policy needs for patient mediated use of Direct exchange
- Computable Policy Services

[26] http://ehnac.org/accreditation-programs/program-dtaap
[27] http://bluebuttonplus.org

  - Evaluate how the work of the WSC on federated provider directories can be extended to enhance trust and facilitate the exchange of sensitive data in a compliant way.

- Sustainability and Organization
  - Evaluate the perpetuation of the WSC beyond ARRA funding period to include establishing the WSC as an independent entity.
  - Research organizational options under federal 501(C) regulations, analyze alternatives and present the WSC member states with options for consideration the coming year.

All of the issues outlined in this report should be advanced in collaboration with other efforts across the country, and next steps should include an evaluation of how the WSC strategies for Direct exchange fit within the context of other HIE methods currently in practice around the country. While collaboration is often challenging for states due to time demands and staff shortages, the ONC could consider a mechanism, such as a series of in-person meetings or Webinars to highlight programs and other multi-state projects similar to the WSC to support shared learning of these lessons.

Glossary

Certificate Authority (CA) – An organization that issues digital certificates. A CA has a published identity assurance, authentication, security, and (perhaps) other policies.

Direct exchange – As created and defined by the Direct Project, is a set of standards and services that, within a policy framework, enable simple, directed, routed, scalable transport over the Internet to be used for secure and meaningful exchange between known participants in support of meaningful use.[28]

DNS – Domain Name System

DSM – Directory Services Mark-up Language

FTP – File Transfer Protocol

HDP – Healthcare Provider Directory

HDP+ – A proposed profile outlining how the HDP profile can be expanded for use with the S&I Provider Directory data model

HIE – Health Information Exchange

HIO – Health Information Organization

HIPAA – Health Information Portability and Accountability Act

HISP – Health Information Service Provider

IHE – Integrating the Healthcare Enterprise

LDAP – Lightweight Directory Access Protocol

PHI – Personal Health Information

PKI – Public Key Infrastructure, aka PKI Certificates

Provider Directory – A query based interface which provides information including electronic address

Push Model – A model of health information exchange where data is sent directly from one provider upon request from another provider.

[28] http://wiki.directproject.org/file/view/DirectProjectOverview.pdf

Query-Retrieve Model (aka "pull" model) – A model of health information exchange where data from any participating provider is available via a larger network system to a provider upon submitting a query for information on a particular patient.

REST – Representational State Transfer

RHIO – Regional Health Information Organization

SOAP – Simple Object Access Protocol

TLS – Transport Layer Security

Trust Anchor – The public key of a digital certificate for the CA used to sign a HISP's certificates. All Direct endpoints signed by a CA agree to abide by its identity assurance, authentication, security, and other policies.

Trust Bundle – Collection of trust anchors bundled together for all participating organizations, creating a group of overlapping circles of trust forming a trust community.

Trust Community – A scalable mechanism for identifying trusted exchange partners who have elected to conform to a common set of policies and processes (such as Certificate Authority's identity assurance, authentication, security) established by an umbrella governance organization which distributes the authentication credentials of these trusted exchange partners necessary for Direct exchange without the need for point-to-point exchange of trust anchors between each pair of HISPs.

Appendix A—Demo Script for Webinar

Background:

The Western States Consortium (WSC) is a group of states who have created a Trust Community- collectively electing to follow a common set of processes and standards regarding the exchange of health information using Direct secure email across state lines. In the WSC, members of the pilot Party States established a set of Eligibility Criteria based on Direct standards in the Applicability Statement and through guidance from ONC.

Here, the WSC is using the secure email system to demonstrate how these policies, procedures, and technologies enable and promote scalable tools for establishing trust for interstate exchange.

Dr. Sunshine California, Mrs. Duck's Primary Care Physician in Garberville, CA:

Patient Daisy Duck is a 77 year old female resident of California. While visiting her daughter in Salem, Oregon, Mrs. Duck begins to complain of having trouble breathing. On 2/28/2013 the situation escalates and her shortness of breath leads her to the Salem Hospital Emergency Room. They are unable to quickly resolve her discomfort and she is admitted to Salem Hospital for further testing.

During her stay, Mrs. Duck is given several tests, including an echocardiogram, x-rays, and lab work. Results of these tests show findings of congestive heart failure, pulmonary edema, and a proBNP of almost 3000. Salem Hospital treats these issues accordingly and on 3/2/2013 she is discharged with instructions to follow up with her Primary Care Physician in California.

Upon safe return to her home in Garberville, California, Mrs. Duck phones her Primary Care Physician, Dr. Sunshine California, to schedule a follow-up appointment. The appointment is scheduled for 3/8/13. To prepare for Mrs. Duck's visit, Dr. California wants to review a copy of the discharge summary from Salem Hospital. He uses Direct to accomplish this.

Dr. California searches for the Direct address of the Medical Records Department at Salem Hospital using the provider search function of her Direct client.

[Pull up the dMail client, and search for Medical Records at Salem Hospital by typing in "Salem", and click Salem Hospital Medical Records direct address (medicalrecords@demo.careaccord.org).]

Dr. California locates the address for Medical Records. She composes a message to Salem Hospital Medical records as follows:

[Open a new message in dMail and cut-and-paste the following from Notepad or Word.]

To Whom It May Concern:

Please forward to my attention the discharge summary for my primary care patient, Daisy Duck (DOB: 04/27/1935) who was discharged from Salem Hospital on 3/2/2013. Mrs. Duck has a follow-up visit with me on 3/8/2013 and I would like to review the document prior to that date for continuity of care/transitional care management purposes.

Sincerely,
Dr. Sunshine California

[Send the message]

Sidebar:

The WSC has established an open-standards based method for querying provider directories using web services and the Healthcare Provider Directory (HPD) and HPDPlus data models – drawing from early work of the S&I Framework. In this demo, the HISP at NCHIN is placing a query to the HISP at CareAccord for Medical Records at Salem Hospital to retrieve a Direct address.

The traditional means of establishing trust between two HISPs to allow the exchange of messages requires them to create and sign a data sharing agreement that establishes how their processes and standards, and exchange trust anchors. However, this is not scalable to hundreds or even tens of organizations. The WSC Trust Community uses a common set of standards and processes in the Eligibility Criteria and a Trust Bundle – a collection of the trust anchors for all members of the Trust Community. Each HISP simply references this Trust Bundle to know who has agreed to the standards and processes and which whom to exchange messages.

Clerk in Medical Records at Salem Hospital:

Salem Hospital Medical Records reads the Direct message request, then locates the discharge summary and replies to Dr. California's message attaching the PDF version of the discharge summary to the reply message:

[Open a reply message and type the following, attaching the PDF discharge summary.]

> Dr. California:
>
> Please find attached the discharge summary for Ms. Daisy Duck's hospitalization at Salem Hospital. Thank you for using Direct to request this document.
>
> Medical Records
> Salem Hospital

[Send the message]

Dr. Sunshine California, Mrs. Duck's Primary Care Physician in Garberville, Ca.:

[Display the message when received. Open Practice Fusion and import the discharge summary and display it there. While waiting…]

Dr. California receives the reply and imports the discharge summary to her EHR, Practice Fusion. She reviews the discharge summary with the patient, performs new medication reconciliation, adding the Lisinopril, Spironolactone and Amoxicillin that were added during her hospital stay and refers Ms. Duck to Dr. Heart at Northern California Heart Works in Ukiah, California for this newly diagnosed CHF.

[Start a directory search and enter "Heart" as the last name.]

Dr. California uses her NCHIN dMail account to look up Dr. Heart in the provider directory. This search reveals that there are two Drs. Heart in California: one in Ukiah and one in Santa Cruz.

In order to provide a scalable means to search for provider addresses, California has established a federated provider directory – a collection of local directories created and operated by each HISP or HIO, connected via web service queries and a statewide service operated by UC Davis on behalf of the state. The statewide service stores no provider data, but orchestrates queries to other directories so each HISP does not need to know what directories are part of the WSC or California Trust Community.

Redwood MedNet and Santa Cruz HIE are part of the California Trust Community, and therefore the statewide directory service sent a query to both Redwood MedNet and Santa Cruz directories, producing a matching result from both. This could have been avoided by searching for a first name as well, which would not have produced a match at Santa Cruz, or entering Ukiah as the city in which Dr. Heart practices, which would have avoided a search of the Santa Cruz directory altogether.

[Open a new message in the dMail client addressed to Dr. Heart at Redwood MedNet.]

Dr. California selects the Dr. Heart in Ukiah and sends a referral message with a CCD from today's visit to Dr. Heart.

> Dr. Heart:
>
> Daisy Duck is a pleasant, alert long-time patient of mine who returned from a visit to her daughter in Salem, Oregon with a new diagnosis of congestive heart failure. I feel that a cardiology work up is in order. I discussed this with Daisy and she agrees. I have attached records from today's office visit and the discharge summary from Salem Hospital. I look forward to working with you.
>
> Sincerely,
> Dr. Sunshine California

Dr. California also sends a copy of the discharge summary from Salem Hospital and today's CCR to Mrs. Duck's HealthVault instance so that her daughter can help monitor her conditions and her care. Dr. California asks Mrs. Duck for her HealthVault Direct address, and enters the address directly into the message.

[Open a new message in dMail, addressed to Ms. Duck at HealthVault. Attached are the PDF discharge summary and CCR care summary.]

Sidebar:

NCHIN and Redwood MedNet are members of both the WSC Trust Community and the California Trust Community, which means they have agreed to the processes and standards required by both, and therefore have established a trust relationship and can exchange data.

Since HealthVault is not yet part of the WSC or California Trust Communities, NCHIN established a trust relationship using traditional point-to-point methods. Since it is not part of the

California federated provider directory, Dr. California asked Ms. Duck for her Direct address during her visit.

Mrs. Daisy Duck, Patient:

Mrs. Duck has previously created a free account in HealthVault and enabled messaging using its Direct capabilities. When she returns home, she logs into her account on HealthVault, and sees that she has a new message. She moves to the HealthVault message inbox, and opens the message from her Primary Care Physician. The note includes the discharge summary, which she can save as a document in HealthVault. It also includes the CCR that her physician created in her EHR. Mrs. Duck imports the CCR into HealthVault, and sees that it contains the new diagnoses for congestive heart failure and some new medications. She adds the new CHF diagnosis and new medications to her record, but chooses not to add the urinary tract infection.

Dr. Happy Heart, Cardiologist in Ukiah, Ca.:

Dr. Heart receives the referral message and notes that Mrs. Duck was seen at Salem Hospital. Using his Direct account with Redwood MedNet, Dr. Heart looks up Salem Hospital Medical Records in the provider directory and requests a copy of the echo performed during Mrs. Duck's hospital stay.

> To Whom It May Concern:
>
> Please forward the echocardiogram for my patient, Daisy Duck (DOB: 04/27/1935) who was discharged from Salem Hospital on 3/2/2013. Mrs. Duck has a consultation with me on 3/13/2013 and I would like to review the document prior to that date for continuity of care/transitional care management purposes.
>
> Sincerely,
>
> Dr. Heart

Dr. Heart sends the message and waits for a reply before scheduling his appointment with Mrs. Duck.

Sharon:

Medical records receives and reads the request for medical records. They respond by replying to the message, and including the 4D echocardiogram and the echocardiogram report.

Dr. Happy Heart, Cardiologist in Ukiah, Ca.:

Dr. Heart receives the response from medical records, and sees that they have included the echo report as a PDF which he views. They have also included a 4D mp4 of the echocardiogram, which he can also display.

Note that it would not be possible to fax a copy of 4D echo.

At this time, Dr. Heart calls Mrs. Duck and arranges a visit with her in his office, on 3/13/2013 to begin exploring treatment options to help Mrs. Duck recover and return to her previously enjoyed quality of life.

After the consultation appointment, Dr. Heart sends his consult summary back to Dr. California by attaching his summary to a reply to the initial referral request.

Dr. Sunshine California, Mrs. Duck's Primary Care Physician in Garberville, Ca.:

Dr. California receives the consult summary from Dr. Heart and reviews it. No trees were harmed. The world is a better place. ☺

Appendix B—In-person Meetings

WSC IN-PERSON MEETINGS

Date, Location and Participants	Meeting Purpose
March 8 and 9, 2012 Las Vegas, Nevada Full Consortium	▪ Discuss the options for establishing regional connections between HISP entities in each state. ▪ Discuss the options for leveraging a regional approach to trust services to support regional provider directory services. ▪ Determine which solutions core states would be most interested in pursuing during the remaining phases of the project, including the planned pilot between California and Oregon.
May 23, 2012 Portland, Oregon California and Oregon	▪ Pilot preparation
July 25 and 26, 2012 Portland, Oregon Full Consortium	▪ Review and finalize the details of the pilot, including whether sufficient consensus and technical agreement has been gained in both pilot states to test either the trust anchor concept and/or the provider directory concept. ▪ Define the pilot tasks with dates (e.g. begin, end, major milestones) where the pilot included the bidirectional exchange of real or live patient information (if possible) across state lines. ▪ Understand the requirements for establishing inter-state exchange using Direct in order to develop policies and plans for additional states to participate in the WSC following a successful proof of concept pilot.
September 27-28, 2012 San Francisco, California California and Oregon	▪ Finalize the pilot governance structure between California and Oregon ▪ Review policy and governance milestones and finalize relevant agreements ▪ Discuss Scenario 1 pilot participants, procedures and measures ▪ Discuss plan for longer-term operation post pilot, other uses cases or participants ▪ Review procedures for creating, storing, and distributing the trust bundle ▪ Review concept of operations and standard for directory services query ▪ Review proposed minimum directory services data requirements
December 10, 2012 Washington, D.C. Full Consortium	▪ Provide an update on the pilot ▪ Obtain Consortium feedback on key issues ▪ Plan final report writing.

Appendix C—Required and Optional HISP Capabilities

REQUIRED AND OPTIONAL HISP CAPABILITIES

As presented by ONC at the April 2011 Direct Project Boot Camp[1], a HISP is defined by the following capabilities:

- A HISP must be able to assign unique Direct addresses to individuals or organizations, e.g. johndoe@direct.sunnyfamilypractice.com.
- A HISP must be able to associate X.509 certificates with full Direct address (e.g., johndoe@direct.sunnyfamilypractice.com) or Health Domain Names (e.g., direct.sunnyfamilypractice.com). The HISP may issue the certificates itself as a Certificate Authority (CA) or obtain the certificates from a trusted third-party CA.
- A HISP must provide an "edge" or "on-ramp" protocol or application/protocol combination to the user, for sending and receiving messages and attachments. The protocol must comply with a minimum set of privacy and security requirements for protection of PHI.
- A HISP must be able to format the "payload" as an RFC5322-compliant email message with a valid MIME body (RFC2045, RFC2046).
- A HISP must be able to sign, encrypt, decrypt, and verify the payload using S/MIME.
- A HISP must have a method for discovering the certificates of message recipients prior to sending a message, in order to fulfill the encryption functions of S/MIME.
- A HISP must be able to judge the trustworthiness of certificates issued by Certificate Authorities that are presented to it in the course of sending and receiving messages.
- A HISP must be able to judge the trustworthiness of leaf certificates used as trust anchors.

In addition to these requirements, it is optional that a HISP:

- Support certificate publication in a directory that is available to other HISPs.
- Utilize DNS servers to store both the users' Direct addresses and the certificates associated with them (public key only).

[1] http://wiki.directproject.org/April+12+agenda+and+session+materials

Appendix D—Business Process Tables

Term	Definitions
Identity Provider	The entity that verifies identifying materials and information and binds that information to some token to be used in Identity Management.
Relying Party	General term used for those who count on the identifying provider to have done what they were supposed to have done so that the transaction can be trusted.
Federation Operator	TBD - see WSC Subgroup Bus Proc Draft 4 10 12
Sources of Authoritative Attribute Information	TBD - see WSC Subgroup Bus Proc Draft 4 10 12
Attribute Provider	TBD - see WSC Subgroup Bus Proc Draft 4 10 12
Inter-federation Facilitator	Project structure to get something from concept to implementation until there is "governance."
Governance for Federated Provider Directory (FPD)	Documented agreement that documents the structure for how we will work together. Governance entity that assists with prioritization and standardization. Representation of federated directory operators. (Could be the same organization that did the Inter-federation Facilitator.)
Auditor	Independent role or function that produces the logs and artifacts for appropriateness according to laws and policies.
Legislator/Regulator	Those that set regulations. They can change the rules of the road. There is an ultimate authority at the state level. The (federal and state) laws are the minimum standard.
Service End Point	For the pilot this is defined as a Direct address
PHI - Protected Health Information	Individually identifiable health information that relates to a person's past/present/future physical/mental health, health care received, or payment

Business Process 1—Identity Registration and Maintenance by Organization Type*

Components	Requirements	Oregon	California	Hawai'i	Nevada
A. Registering an Individual Provider NOTE: Individuals are verified by the Organizations in a federated model. **Discussion:** How do we verify the information? Do we need to define the verification process and to what extent are they necessary for the pilot? Operationalize what can be verified in a feasible way and access to information as well as an authoritative source is an issue. This could very from state to state. In some cases attestation is the way it works. How we meet the requirements could be difficult as the devil is truly in the details. Hawaii is incorporating NPPES and fax information followed by a "face to face visit" which includes data sharing agreements, BAA and training.	– Proof of individual identity – Demographic information (to be further defined) for demographic search – Verification of demographic information – proof of organizational affiliation(s) – Service endpoints for electronic exchange (may be organizational) – Standards associated with service endpoints* (may be organizational) – Verification of service endpoint information *(Note: Service endpoint for the pilot is a direct address)	In Oregon, we use a tiered approach to registering individuals- they must affiliate with an organization that has been authorized and validated through the registration process, and then the organization's designated Point of Contact(s) must verify the identity of the individual and approve them before the individual is issued an individual account affiliated with the organization's main account. Or, if an individual provider is a sole practitioner, they can register for an organizational account. **Comments:** Approach to set up to be efficient and assumes organization and POC will verify identity.	– Proof of individual identity – Demographic information (yet to be defined) required for demographic search – Verification of demographic information – Proof of organizational affiliation(s) – Service endpoints for electronic exchange (may be organizational) – Standards associated with service endpoints (may be organizational) – Verification of service endpoint information **Comments:** Similar to OR. Intend to federate process and technology.	– Proof of individual identity using NPPS and face to face ID – Signed data sharing agreement – Verification of demographic information against state licensing board via an information sheet: practice address, phone, medical license number, administrator – Service endpoints: the PPCP is asked for their specialist network, specialists and other PCPs. **Comments:** In Hawai'i we use the hybrid mode.	– Proof of individual identity; – Demographic information (to be further defined) for demographic search – Verification of demographic information – proof of organizational affiliation(s) – Service endpoints for electronic exchange (may be organizational) – Standards associated with service endpoints* (may be organizational) – Verification of service endpoint information *(Note: Service endpoint for the pilot is a direct address) **Comments:** Similar to OR and CA. Plan is to federate process and technology, and allow sole practitioners to register for organizational accounts.

(continued)

Business Process 1—Identity Registration and Maintenance by Organization Type* (continued)

Components	Requirements	Oregon	California	Hawai'i	Nevada
B. Registering a Provider Organization	– Type of Organization – Individual memberships in the org. – Proof of organizational authorization – Demographic information (yet to be defined) required for demographic search – Individual memberships in organization – Service endpoints for electronic exchange – Standards associated with service endpoints – Verification of service endpoint information	In Oregon, we require that the organization has a valid & active state business license and they must attest to being a HIPAA-covered entity (CE) or valid Business Associate of a CE. We also check to make sure that the individual who signs the Organizational Participation Agreement on behalf of their organization (a binding contract between their organization and the HIE) is actually an officer of the organization with signing authority. **Comments:** In OR needed to define what kind of an organization it is and aligning with policy. Still not sure how to ind. Verify that they are a covered entity and they rely on attestation.	– Proof of organizational authorization – Demographic information (yet to be defined) required for demographic search – Verification of demographic information – Individual memberships in organization – Service endpoints for electronic exchange – Standards associated with service endpoints – Verification of service endpoint information **Comments:** Individual memberships in the organization - is this necessary? This is functionality that OR wants and is working with vendor to build the functionality as soon as possible. This should be in your vendor contract. Not sure this needs to be a requirement.	– Type of organization **Comments:** Our HISP can categorize the user account for type of organization; the admin - usually the IT Director assigns individuals to the accounts or group accounts; proof is not identified as necessary because we are working very closely with the organizations;	– Type of Organization – Individual memberships in the org. – Proof of organizational authorization – Demographic information (yet to be defined) required for demographic search – Individual memberships in organization – Service endpoints for electronic exchange – Standards associated with service endpoints – Verification of service endpoint information **Comments:** Similar to OR and CA. Plan to require that the organization has a valid and active state business license in good standing, and must attest to being a HIPAA-covered entity (CE) or valid Business Associate of a CE. If a health insurance plan, would also require valid and active Certificate of Authority in good standing. Agree with CA that individual memberships in the organization.

(continued)

Business Process 1—Identity Registration and Maintenance by Organization Type* (continued)

Components	Requirements	Oregon	California	Hawai'i	Nevada
C. Updating Provider Information **Discussion:** Need to produce a methodology that documents how requirements are met. Is this more procedural/contractual (see Oregon)? There seems to be a priority as to what needs to be updated (e.g. role, organization, type of access, end points, etc. are higher priority and middle name is less of an issue). CA is looking at driving the updating of information to the local/org. level. They don't want the information to get out of date. People question NPPES. Directories are difficulty to maintain and keep them up to date. On the other hand it is also to maintain information in multiple places. What are the incentives to keep it up to date? the business question is how do you get the individual to do what they are supposed to do? It could be easier to do it one time in one place. Utah is working with payers to establish the information and believe the incentive is the providers want to get paid.	– Ability to produce methodology that documents how requirements are met. – Authorization to update information – Verification of modified demographic information – Verification of modified service endpoint information	In Oregon, we make it a requirement of the Organizational Participation Agreement and the Authorized User Agreement (for individual end-users within an organization) that both the individual and the organization are responsible for keeping their information in the Provider Directory up to date, and the main responsibility lies with the Organization's designated Point of Contact. There's been some discussion of whether we should build a step in to periodically prompt and remind them of the need to update info, but that hasn't been determined yet. **Comments:** How can we tell if a message has been sitting in an inbox without opened or is there an "inactive" inbox. There is process that checks for activity to determine whether or not use should be revoked. Is this a best practice or a requirements. Need a process or method to report of users with credentials that are "inactive"	– Authorization to update information – Verification of modified demographic information – Verification of modified service endpoint information **Comments:** Procedural requirements to include contractual requirements like OR is a good one.	**Comments:** Hawai'i requires in our agreement that if anything changes for the user's account that the designated admin is required to notify the HHIE immediately and no less than 24 hrs; this assumes that the person is disgruntled and needs to be removed; for other demographic updates it should not be a problem as they are providing all the necessary fields upon sign up; change of name due to marital status can be treated the same provide that the Medical certificate is updated as it will take precedence; in the audit reports we will be looking for cases where there are no log in's for a 10 week period	– Authorization to update information – Verification of modified demographic information – Verification of modified service endpoint information **Comments:** Expect procedural requirement to include contractual requirements like OR.

(continued)

Business Process 1—Identity Registration and Maintenance by Organization Type* (continued)

Components	Requirements	Oregon	California	Hawai'i	Nevada
Inactivating a Directory Entry **Discussion:** Is this part of the previous list? There needs to be notification and is this handled through contracts to remove access?	– Authorization to inactivate entry – Effective date of inactivation	—	– Authorization to inactivate entry – Effective date of inactivation.	**Comments:** For Hawai'i, the provider would be hidden upon inactivation; date can be provide from HIE to HIE but would not be auto displayed	– Authorization to inactivate entry – Effective date of inactivation

***Definition and Considerations**

1. The full lifecycle for maintaining provider directory information.
2. For the pilot, it might make sense to limit the actors to "Individual Clinicians" and "Clinical Organizations" but we still need to think about a more complex environment which includes the following actors (listed in no particular order): Payers, Labs, Pharmacy, Patient, Researchers, Public Health, Government Agencies/Entities.

Business Process 2—Identity provisioning and maintenance (including issuing of certificates)*

Components	Requirements	Oregon	California	Hawai'i	Nevada
A. Provisioning Individual Provider Identity Credentials **Comments/Discussion:** Digital certificate issuance is the important requirement should this be included in BP1? It probably should stay separate at this point. Issuing of a digital cert could be the responsibility of a different org. ***An individual may have more than one digital certificate but they don't share digital certificates.***	– Proof of identity (outcome of BP1) – Unique(not shared) identifier in provider directory – Unique (not shared) electronic token (e.g. digital certificate) to identify the individual	For Oregon's understanding of this, see row 4 "Registering an Individual Provider": In Oregon, we use a tiered approach to registering individuals- they must affiliate with an organization that has been authorized and validated through the registration process, and then the organization's designated Point of Contact(s) must verify the identity of the individual and approve them before the individual is issued an individual account affiliated with the organization's main account. Or, if an individual provider is a sole practitioner, they can register for an organizational account. **Comments:** Oregon issues organizational certificates	– Proof of identity – Unique identifier in provider directory – Unique electronic token (e.g., digital certificate) to identify the individual **Comments**: Digital tokens are the difference	**Comments:** Hawai'i 's understanding is that HIE's are to credential the users and the HISP's are to validate the digital token.	– Proof of identity (outcome of BP1) – Unique(not shared) identifier in provider directory – Unique (not shared) electronic token (e.g. digital certificate) to identify the individual
A. Provisioning Provider Organization Identity Credentials	– Proof of identity (outcome of BP1) – Unique (not shared) in provider directory – Unique electronic token (e.g. digital certificate) to identify the organization	For Oregon's understanding of this, see row 5 "Registering a Provider Organization"	– Proof of identity – Unique identifier in provider directory – Unique token (e.g. digital certificate) to identify the organization	—	– Proof of identity – Unique identifier in provider directory – Unique token (e.g. digital certificate) to identify the organization

(continued)

Business Process 2—Identity provisioning and maintenance (including issuing of certificates)* (continued)

Components	Requirements	Oregon	California	Hawai'i	Nevada
B. Auditing Processes - logging transactions and monitoring **Discussion:** Requirements need to reflect best security practices. Does this need to be more specific than a requirement that practices are followed as a means to detect deviation from the expectations with recourse taken for the member to deal with the issue. This is one of the processes/set of requirements that we will expand as we move forward but it will be based on best practices and what we learn. If there are violations, who will be responsible for following up if it occurs across state lines? As the HIEs connect, do we need to evaluate each other's process to determine alignment? The purpose of having audits is to have something that aligns as much as can come up with and what we can live with.	– An Auditing Process exists with transparency of what is included and there are consequences when someone doesn't comply. Auditing process includes timing but the issue is that everyone has a mechanism to deal with compliance.	In Oregon, we (the HIE) reserve the right to audit participants, but do not specify if or when that will take place. **Comments:** Contractually reserve the right to audit but don't have the business requirements.	– Approved process for provisioning individuals and organizations – Records demonstrating that processes are followed **Comments:** Needs to be an audited process. Still working on the requirements.	Hawai'I reserves the right to audit participants but does not specify if or when an audit will be done.	**Comments:** Plan to do, although no requirement yet.

(continued)

Business Process 2—Identity provisioning and maintenance (including issuing of certificates)* (continued)

Components	Requirements	Oregon	California	Hawai'i	Nevada
C. Processing Violations **Discussion:** What is the authority across state lines? What is the mechanism for dealing with this?	—	—	– Organizational authority to process complaints – Published complaint process; published investigation process – Published inactivation process; published appeal process – Published reactivation process	—	**Comments:** Statutory authority to promulgate necessary regulations.
D. Revoking Individual Provider Identity Credentials **Discussion:** May be an outcome of processing violations. There are also reasons to revoke credentials such as retirement. Need a mechanism to revoke and verify. What happens in an organization/state that charges and what happens when someone doesn't pay? (Note: This last issue is not a factor for the pilot but should be considered from a planning perspective.)	– Clearly stated policies that define how accounts are terminated/revoked. – Mechanism to inactivate electronic token that identifies the individual. – Mechanism to verify that account has been suspended/revoked.	Oregon has language in the Organizational Participation Agreement for termination of access. It contains a list of reasons as to why an account would be suspended; and that the authority to revoke individual credentials lies with the organization.	– Organizational authority to revoke individual credentials – Mechanism to inactivate electronic token that identifies the individual	– Authority to revoke individual credentials – Mechanism to inactivate electronic token that identifies the individual	**Comments:** Plan to do, although no requirement yet.

(continued)

Business Process 2—Identity provisioning and maintenance (including issuing of certificates)* (continued)

Components	Requirements	Oregon	California	Hawai'i	Nevada
E. Revoking Provider Organization Identity Credentials **Comments:** Revocation is understood. Don't need to do anything new. It is applied under certain circumstances. If that address or individual org is no longer valid and certainly not safe (due to policy violation). Two broad categories exist. Mechanism to deactivate the ability to exchange and it is an urgent measure. There is also an non-urgent measure that needs to be applied as well. Not sure if these are different.	– Clearly stated policies that define how accounts are suspended/ terminated or revoked – Mechanism to inactivate electronic token that identifies organization	Oregon's Organizational Participation Agreement indicates participant is responsible for terminating access. Participant is Organization, so the authority to revoke organizational credentials lies with the organization.	– Organizational authority to revoke organizational credentials – Mechanism to inactivate electronic token that identifies the organization	—	**Comments:** Plan to do, although no requirement yet.

***Definition and Considerations:**

The full lifecycle for maintaining provider and provider organizational identities, including issuing certificates or the equivalent. It could be a part of the registration process. Direct requires the issuance of certificates; however in the future this requirement could change.

ID Proofing requirements by type:

- Individual Provider*
- Payer
- Pharmacy
- Public Health
- Patient
- Provider Organization*
- Lab
- Researcher
- Government Agencies/Entities

Proposed Alternative BP 3: "Verification of Provider Identity" or alternatively Secure Exchange of PHI*

Components	Requirements	Oregon	California	Hawai'i	Nevada
A. Discovering Service Endpoint	—	—	– Demographic information of individual recipient of PHI or query OR unique identifier for individual OR demographic information of organizational recipient of PHI or query OR unique identifier of organization – Authorization to search provider directory – Location of "root" provider directory for search – Query/response mechanism for service discovery **Comments:** I believe this additional component to this process is necessary.	**Comments:** Not sure what this means; is it Personal Health Information or Physician Health Information; for provider information they can query.	—

(continued)

Proposed Alternative BP 3: "Verification of Provider Identity" or alternatively Secure Exchange of PHI* (continued)

Components	Requirements	Oregon	California	Hawai'i	Nevada
B. Establishing Secure Transport	—	—	– Service endpoint for system with which to exchange – Unique electronic token establishing identity of sending system – Unique electronic token establishing identity of receiving system – Agreed-up transport protocol between systems **Comments:** NwHIN takes system (gateway) identity tokens to be equivalent to organizational tokens; that is not necessary and should not be assumed.	HISP to HISP agreement to exchange data in BAA or DSA agreements.	—
C. Signing Exchange	—	—	– Authorization to send information – Unique electronic token establishing identity of sending individual OR unique electronic token establishing identity of sending organization	HISP to HISP agreement to exchange data in BAA or DSA agreements.	—

(continued)

Proposed Alternative BP 3: "Verification of Provider Identity" or alternatively Secure Exchange of PHI* (continued)

Components	Requirements	Oregon	California	Hawai'i	Nevada
D. Exchanging Information	—	—	– Common service between sending and receiving systems; – Common standards for information content. **Comments:** I believe this additional component to this process is necessary.	HISP to HISP agreement to exchange data in BAA or DSA agreements.	—
E. Logging Exchange	—	—	– Agreed-upon details of exchange that should be recorded – Authorization to record details of exchange – Process for recording details of exchange – Process for authorizing disclosure of details of exchange – Process for recording denial of authorization to exchange **Comments:** I believe this additional component to this process is necessary.	HISP to HISP agreement to exchange data in BAA or DSA agreements.	—

*__Definition and Considerations__

Exchange of health information that properly guarantees the identity of the sender and identity of the recipient, and ensures that information is secured against corruption in transport and viewing by unauthorized individuals.

Business Process 4—Assignment of Roles (for Access Rights)*

Components	Requirements	Oregon	California	Hawai'i	Nevada
A. Assignment of roles (for access rights)	—	We require participating Organizations to define access rights for the individual users within their organization, based on what is appropriate for their role in the organization. We (the HIE) do not currently have varying levels of access rights for different types of part. organizations or different types of users within the organizations. We have functionality to allow an individual and/or organization to have delegates to the individual or organization's account. Delegates are able to view, edit, and respond on behalf of the individual or organization. This is a form of access and is authorized by the individual or organization.	– Authorization to assign roles – Agreed-upon lexicon of roles **Comments**: This single component probably should be multiple components, including assignment, assertion, and verification. I've added additional components. (they are shaded)	**Comments:** For Hawai'i there are only 2 roles - non clinical and clinical.	—

(continued)

Business Process 4—Assignment of Roles (for Access Rights)* (continued)

Components	Requirements	Oregon	California	Hawai'i	Nevada
B. Discovery of permissible roles (for access rights or authorization to send) **Comments:** Component of BP added by CA	—	—	– Agreed-upon lexicon of roles – Authorization to query provider directory for permissible roles – Mechanism to query for permissible roles of an individual based on demographic information OR based on unique identifier **Comments:** I believe this is a component of this business process.	**Comments:** For Hawai'i, we are only signing up clinical roles.	—
C. Assertion of purpose (for authorization to send or authorization to request information) **Comments:** Component of BP added by CA	—	—	– Agreed-upon lexicon of purposes for exchange – Mechanism for sender in an exchange or query to assert purpose **Comments**: I believe this is a component of this business process.	**Comments:** For Hawai'i, we are only signing up clinical roles.	—
D. Assertion of role (for authorization to send or authorization to request information) **Comments:** Component of BP added by CA	—	—	– Agreed-upon lexicon of roles – Mechanism to assert role of sender in an exchange or query **Comments:** I believe this is a component of this business process.	**Comments:** For Hawai'i, we are only signing up clinical roles.	—

(continued)

Business Process 4—Assignment of Roles (for Access Rights)* (continued)

Components	Requirements	Oregon	California	Hawai'i	Nevada
E. Verification of authorization (to send or request information) **Comments:** CA suggests this might not need to be a separate component but it might be.	—	—	– Mechanism to query for permissible roles of an individual (see "discovery" above) – Local rules for authorizing disclosure considering purpose, roles, and permissible roles – Mechanism to deny authorization (dispose of transmitted PHI or deny query request) **Comments:** This may not be a separate component, but I think it is.	**Comments:** For Hawai'i, we are only signing up clinical roles.	—

***Definition and Considerations**

Role based access—different roles could have different access rights.

Roles will likely be more dynamic than other information in the Provider Directory. There will be a group of roles that establish the "treating provider"

Oregon: I think we need to define access TO WHAT here. It seems to me that "Authorization to access Directory Services across state lines" (business process 6) and "Authorization to exchange PHI across state lines" (business process 7) are components of "Assignment of Roles for Access Rights" (business process 4)

California: I believe there are business processes beyond "assignment" that include discovery and verification. I've identified those as components of assignment in what follows, but that may not be strictly appropriate.

Business Process 5—Verification of Accreditation*

Components	Requirements	Oregon	California	Hawai'i	Nevada
Accreditation	—	—	—	—	—

***Definition and Considerations**

Process for discovery of an attribute (called accreditation) that establishes the entity has met certain requirements.

California: "Certain requirements" is not really sufficient for us to define requirements for this business process. I'm not sure how to proceed, or even that this business process is necessary given the "roles" business process.

Oregon: In Oregon, it is my understanding that all of our certificates are identical- they don't contain certain attributes for some participants and different attributes for another, and I'm not sure if/how they could.

Business Process 6—Authorization to Access Directory Services Across the State Lines*

Components	Requirements	Oregon	California	Hawai'i	Nevada
A. Describing Purpose for Query	—	Oregon- I'm assuming that the "purpose" here could include for treatment, payment, health care operations, quality reporting, immunization reporting, clinical research, etc.? (so in other words, "purpose" as defined by HIPAA?) And depending on the identity/credentials/ access privileges of the requester, the purpose is either permissible or not?	Replaced with "Assertion of purpose".	**Comments:** For Provider Query, Hawai'i has that avail	—
B. Retrieving Credentials of Requester	—	Oregon- What do "credentials" consist of?- Just their certificate and its attributes? Information in the Provider Directory? Both? Anything additional?	Replaced with "Verification of authorization".	**Comments:** When HISP to HISP is concern we should be able to trust each other's HISP; If the provider doesn't trust the message they are not to open the message and if the provider does not get a response they should call by phone.	—
C. Discovery of permissible roles (for access rights or authorization to send) **Comments:** Added by CA	—	—	See above. I believe this a component of this business process.	**Comments:** When HISP to HISP is concern we should be able to trust each other's HISP; If the provider doesn't trust the message they are not to open the message and if the provider does not get a response they should call by phone.	—

(continued)

Business Process 6—Authorization to Access Directory Services Across the State Lines* (continued)

Components	Requirements	Oregon	California	Hawai'i	Nevada
D. Assertion of purpose (for authorization to send or authorization to request information) **Comments:** Added by CA	—	—	See above. I believe this a component of this business process.	**Comments:** When HISP to HISP is concern we should be able to trust each other's HISP; If the provider doesn't trust the message they are not to open the message and if the provider does not get a response they should call by phone.	—
E. Assertion of role (for authorization to send or authorization to request information) **Comments:** Added by CA	—	—	See above. I believe this a component of this business process.	**Comments:** When HISP to HISP is concern we should be able to trust each other's HISP; If the provider doesn't trust the message they are not to open the message and if the provider does not get a response they should call by phone.	—
F. Verification of authorization (to send or request information) **Comments:** Added by CA	—	—	See above. This may not be a separate component but I think it is.	**Comments:** When HISP to HISP is concern we should be able to trust each other's HISP; If the provider doesn't trust the message they are not to open the message and if the provider does not get a response they should call by phone.	—

*__Definition and Considerations__

Process to allow access to the provider directories and trust services, including access to DIRECT and DIRECT addresses for senders and receivers (individuals, organizations, and facilities)

Comments: I'm not clear on why/how access to Directory services is linked to access to trust services- does this just mean that the Directory is where certificate information/public keys are accessed? Is it necessary that the two are inextricable?

Comments: I believe this business process looks exactly like the roles process above, where at least one permissible role is "query the provider directory". I believe the implementation could be the same, but that the business processes and components certainly are.

Business Process 7—Authorization to Exchange PHI Across State Lines*

Components	Requirements	Oregon	California	Hawai'i	Nevada
A. Describing Purpose for Exchange	—	Oregon- I'm assuming that the "purpose" here could include for treatment, payment, health care operations, quality reporting, immunization reporting, clinical research, etc.? (so in other words, "purpose" as defined by HIPAA?) And depending on the identity/credentials/ access privileges of the requester, the purpose is either permissible or not?	Replaced with "Assertion of purpose".	**Comments:** Should be in DSA	—
B. Retrieving Credentials for the Requester	—	Oregon- What do "credentials" consist of?- Just their certificate and its attributes? Information in the Provider Directory? Both? Anything additional?	Replaced with "Verification of authorization".	**Comments:** Should be closely related by DSA but not by provider to provider	—
C. Discovery of permissible roles (for access rights or authorization to send) **Comments:** Added by CA	—	—	See above. I believe this a component of this business process.	**Comments:** Should be closely related by DSA but not by provider to provider	—
B. Assertion of purpose (for authorization to send or authorization to request information) **Comments:** Added by CA	—	—	See above. I believe this a component of this business process.	**Comments:** Should be closely related by DSA but not by provider to provider	—

(continued)

Business Process 7—Authorization to Exchange PHI Across State Lines* (continued)

Components	Requirements	Oregon	California	Hawai'i	Nevada
C. Assertion of role (for authorization to send or authorization to request information) **Comments:** Added by CA	—	—	See above. I believe this a component of this business process.	**Comments:** Should be closely related by DSA but not by provider to provider	—
D. Verification of authorization (to send or request information) **Comment:** Added by CA	—	—	See above. This may not be a separate component but I think it is.	**Comments:** Should be closely related by DSA but not by provider to provider	—

*__Definition and Considerations__

Process for determining whether an exchange should be allowed, including verification of authorized receivers (via Providers/Entity Directory) and verification of patient consent pursuant to sender's state laws.

Oregon comments: I think it would be ideal if every receiver had proof that the sender abided by their own states law, including those pertaining to patient consent/authorization, but I'm concerned about the actual feasibility of this. State laws are very complex (at least in Oregon they are, and I've heard much the same of our WSC partners), so other than a sender attesting to having attained any required consent /authorization, I can't imagine how this could be verified in any kind of systematic/efficient/affordable manner. And at the end of the day, the sender is legally responsible for whether they have done so, not the receiver or the HIE.

California Comments: I don't believe this process has any special requirements beyond "Secure Exchange of PHI" above, save that "local rules to authorize exchange" must include considerations for interstate exchange.

Business Process 8—Provider Discovery*

Components	Requirements	Oregon	California	Hawai'i	Nevada
A. Query/Response for Discovering an Individual Provider	—	—	– Authorization to search provider directory – Demographic information of individual provider – Location of "root" provider directory for search – Query/response mechanism for service discovery	**Comments:** Should be able to search provider directory by demographic list but not by narrative	—
B. Query/Response for Discovering a Provider Organization	—	—	– Authorization to search provider directory – Demographic information of provider organization – Location of "root" provider directory for search – Query/response mechanism for service discovery	**Comments:** Should be able to search provider directory by demographic list but not by narrative	—

*__Definitions and Considerations__

Querying the directory to identify individual or organization providers.

Oregon: I don't understand how this is different from "Authorization to Access Directory Services Across State Lines". Maybe the difference is in determining who can do what (authorizing who can use the directory) versus performing the actual function of doing it (using the directory). If that's the case, the we should have "inter-network exchange" listed as an additional business process as the function counterpart to "Authorization to Exchange PHI Across State Lines".

California: I've answered this as if this is for pure directory services, and not for the purposes of electronic exchange. The latter is described as part of "Secure Exchange of PHI" above when considering endpoints.

Appendix E—Policies and Procedures

Western States Consortium Policy Approval Log

Document	Party State Representative	Date Rep Approved	Date effective
WSC Policy Procedure 1.3 - WSC P&P Change Process	Cassie McTaggart, CA	10/31/2012	10/31/2012 ~SEIB
WSC Policy Procedure 1.3 - WSC P&P Change Process	Carol Robinson, OR	10/31/2012	10/31/2012 ~SEIB
WSC Policy Procedure 2.4 - WSC P&P Onboarding Process with Addendum	Cassie McTaggart, CA	10/31/2012	10/31/2012 ~SEIB
WSC Policy Procedure 2.4 - WSC P&P Onboarding Process with Addendum	Carol Robinson, OR	10/31/2012	10/31/2012 ~SEIB
WSC Policy Procedure 3.3 - WSC P&P Communications	Cassie McTaggart, CA	10/31/2012	10/31/2012 ~SEIB
WSC Policy Procedure 3.3 - WSC P&P Communications	Carol Robinson, OR	10/31/2012	10/31/2012 ~SEIB
WSC-GB Policy Decision 1.0 – Statement of Authority	Cassie McTaggart, CA	11/26/2012	11/28/2012 ~SEIB
WSC-GB Policy Decision 1.0 – Statement of Authority	Carol Robinson, OR	11/28/2012	11/28/2012 ~SEIB
WSC-GB Policy Decision 2.0 – WSC-GB role in signing 3Rd Party Agreements	Cassie McTaggart, CA	11/26/2012	11/28/2012 ~SEIB
WSC-GB Policy Decision 2.0 – WSC-GB role in signing 3Rd Party Agreements	Carol Robinson, OR	11/28/2012	11/28/2012 ~SEIB
WSC Policy Procedure 2.5 - WSC P&P Onboarding Process with Addendum	Cassie McTaggart, CA	11/26/2012	11/28/2012 ~SEIB
WSC Policy Procedure 2.5 - WSC P&P Onboarding Process with Addendum	Carol Robinson, OR	11/28/2012	11/28/2012 ~SEIB
WSC Policy Procedure 2.6 - WSC P&P Onboarding Process with Addendum	Cassie McTaggart, CA	2/14/2013	2/15/2013
WSC Policy Procedure 2.6 - WSC P&P Onboarding Process with Addendum	Lisa Parker Christy Lorenzini-Riehm (interim reps), OR	2/14/2013	2/15/2013
WSC Policy Procedure 2.6 - WSC P&P Onboarding Process with Addendum	Paul Cartland, AK	2/14/2013	2/15/2013

WSC-P&P#1
Western States Consortium Governance Body

Subject: WSC Procedure for Policy and Procedure Change Process
Status: WSC-GB Approved
Policy #: 1
Date Approved: 10/30/2012
Version: 0.1
Pages: 4

I. Purpose

The Western States Consortium Governance Body (WSC Governance Body) has responsibility for developing, maintaining, repealing, amending and retaining the Policies and Procedures of the Western States Consortium. The purpose of this policy is to set forth the procedure by which the WSC will fulfill these responsibilities.

II. Policy

The WSC Governance Body shall establish and maintain Policy and Procedures for the Western States Consortium. WSC Policy and Procedures (WSC-P&P) are those documents that describe the management, operation, and participation in the Western States Consortium. As may become necessary for the proper functioning of the Western States Consortium, the WSC Governance Body may establish new WSC-P&P(s), or it may amend, repeal, and/or replace any existing WSC-P&P consistent with Article 4 Section 4 of the WSC Memorandum of Understanding.

III. Procedure

A. Retention, Maintenance and Dissemination of WSC-P&Ps

All WSC-P&Ps shall be maintained in an electronic form that can be accessed and printed if desired. The WSC Governance Body requests that Party States make copies of the WSC-P&Ps available in a location that is accessible to all stakeholders within their state in compliance with Article IV Section 5 of the WSC Memorandum of Understanding.

All current WSC-P&Ps as well as originals of all amended, repealed and replaced WSC-P&Ps shall be maintained for the duration of their usefulness as determined by the WSC Governance Body.

B. Submission of Proposed New, Amended, Repealed, or Replaced WSC-P&Ps

Any Party State may submit in writing to the WSC Governance Body a request for the development of a new WSC-P&P, or a request for the amendment or repeal of an existing WSC-P&P. Any Member of the WSC Governance Body may also bring forth any concern or question regarding WSC-P&Ps. All such requests shall identify (i) the WSC-P&P(s) that is the subject of the requested change (if any),

(ii) the type of WSC-P&Ps sought if it is a request to develop a new P&P, (iii) a thorough description of why the request is necessary, and (iv) an analysis of the expected impact of adopting the new WSC-P&P or modifying/repealing an existing WSC-P&P.

C. Consideration of Proposed New, Amended, Repealed, or Replaced P&Ps

The WSC Governance Body will consider any requests that meet the submission criteria set forth above at its next regularly scheduled meeting following receipt of such request or at a time to be scheduled and communicated to the Party States. If, after considering the request, the WSC Governance Body determines that the request does not have merit or lacks sufficient detail, it will communicate this determination to the requestor.

If after considering the request, the WSC Governance Body determines that the request has merit, it will forward the request to a Task Group designated by the WSC Governance Body to review the request and make a recommendation for action to the WSC Governance Body.

The WSC Governing Body will consider any Task Group recommendation for action (or for no action) and will conduct a vote on a recommended course of action for Party States and identify the timeframe to seek Party State approval of the recommended change.

When the WSC Governing Body informs the Party States of its recommendations for action on the WSC-P&Ps and seeks Party State approval for such action, the WSC Governing Body shall provide to following information to all Party States:

- a copy of the new, amended, repealed or replaced WSC-P&P;
- a thorough description as to the reasons for the implementation of the new WSC-P&P or amendment, repeal or replacement of an existing WSC-P&P and any foreseeable impact of the change;
- a projected effective date for the proposed changes; and
- the date by which each Party State must submit its approval or rejection of the proposed change to the WSC Governing Body.

D. Approval or Rejection of Proposed Changes to the WSC-P&P

Changes to the WSC-P&Ps must be approved by a consensus of all WSC Governance Body Members. If any Member rejects a proposed change, the Member must provide a rationale for such rejection. If any of the WSC Governance Body Members do not approve a change, the change is rejected and does not take effect.

If the requisite number of Members do approve a change, the WSC Governance Body will establish an effective date for the change and will provide all Party States with notice of the approval of a proposed change at least 30 days prior to the effective date of the change unless the Party States unanimously elect to have a shorter notice period.

Once a change takes effect, all Party States must comply with the changed WSC-P&P.

IV. Definitions

Member – currently synonymous with Party State, this term is used in anticipation of potential changes to membership in the WSC Governance Body, if decided by consensus of WSC Governance Body in the future.

Party State – Any state, territory or other similar entity that is a signatory to this MOU and participates in the Pilot according to the intentions of this MOU.

Task Group – Working groups of people identified by Party State Members that are tasked with evaluating request for new or changes to existing Policy and Procedures whose deliverable are a recommendation for consideration by the WSC Governance Body. Individuals working as part of a Task Group do not have to be representatives selected by the Party States that make up the WSC but are individuals selected by said representatives based on their qualifications to support the needs of the WSC Governance Body.

WSC Governance Body – the governance entity established by the WSC MOU established and responsible for governing the WSC including responsibility for developing, maintaining, repealing, amending and retaining the Policies and Procedures of the Western States Consortium.

All other capitalized terms, if not defined herein, shall have the same meaning as set forth in the WSC MOU.

V. References

Western States Consortium Memorandum of Understanding.

VI. Related Policies and Procedures

None.

VII. Version History

Version	Date	Author	Comment
1	10/09/2012	Aaron Seib	First Draft – adapted from eHealth Exchange Coordinating Committee implemented Policies and Procedures (see.www.healthewayinc.org)
2	10/09/2012	Aaron Seib	Updated footnote related to definition of member to include hint that we may want to consider allowing Core State Members to become participants of the governance model prior to signing a binding agreement to help ensure broad alignment.
3	10/31/2012	Aaron Seib	Updates following Governance Body Review

WSC-P&P#2.6
WESTERN STATES CONSORTIUM GOVERNANCE BODY

Subject: WSC-QE Onboarding Policy and Procedure.
Status: WSC-GB Approved
Policy #: 2
Date Approved: 2/14/2013 (10/31/2012)
Version: 0.6
Pages: 19

I. Purpose

The Western States Consortium Governance Body (WSC Governance Body) has responsibility for establishing uniform processes by which Party States can identify Western States Consortium Qualified Entities (WSC-QEs) from within their state (or area of authority) and to provide a mechanism by which such WSC-QEs can be added to the WSC-Pilot Trust Community. The purpose of this WSC-P&P is to define these uniform processes and establish the framework by which 'Party States' promote WSC-QEs into the WSC-Pilot Trust Community.

II. Policy

Only Party States that have been approved for inclusion to the WSC Governance Body shall be able to promote WSC-QEs to the WSC-Pilot Trust Community. 'Party States' are responsible for vetting candidate WSC-QEs covered by their authority and shall attest to the candidate's satisfaction of the WSC Eligibility Criteria based on the 'Methods of Verification' established by the WSC Governance Body prior to promoting the WSC-QE to the WSC-Pilot Trust Community. Each Party State will be responsible for administering the addition and removal of WSC-QEs from the WSC Trust Community via the methods approved by the WSC Governance Body.

III. Procedure

A. Western States Consortium Eligibility Criteria for Service Offerings

The WSC Governance Body shall solely be responsible for defining and modifying the 'Eligibility Criteria' for inclusion in the service offerings of the WSC, including the WSC-Pilot Trust Community. The WSC Governance Body shall make available to Party States the criteria by which Party States are to evaluate candidate WSC-QEs for inclusion in each of the Service offerings of the Western States Consortium.

Service Offerings of the Western States Consortium[1]

1. The WSC-Pilot

   a) Eligibility Criteria for the WSC-Pilot.

      - The WSC Governance Body shall make available to Party States the criteria by which Party States are to evaluate candidate WSC-QEs.

        – For the Pilot the Eligibility Criteria are captured in a document to be called "WSC-P&P#2 – WSC-Pilot Eligibility Criteria Addendum".

      - The WSC Governance Body shall make changes to the Eligibility Criteria only once they are approved by following WSC- Procedure for Policy and Procedure Change Process (P&P #1).

        – Once changes have been approved by the WSC Governance Body the "WSC-P&P#2 – WSC-Pilot Eligibility Criteria Addendum" shall be updated and its history will reflect the date of the change.

      - These 'Eligibility Criteria' shall identify all of the requirements to be evaluated by Party States and for each requirement provide the following:

        – A description of the requirement
        – A rational for inclusion of the requirement
        – The method of verification to be employed by the Party State in evaluating the candidates satisfaction of the requirement to be performed by the Party State

   b) Party State Evaluation of Candidate WSC-QEs for the WSC-Pilot

      - Each Party State will be solely responsible for the evaluation of Candidates within its authority to evaluate.

        – Each Party State shall document its processes for conducting the evaluation of Candidate WSC-QEs.
        – Only WSC-QEs that have been evaluated according to the process shall be added to the WSC Trust Community

      - Only Candidates that satisfy all of the Eligibility Criteria will be added to the WSC Trust Community by the Party States. Party States shall:

        – Maintain a record of its evaluation of the Candidates satisfaction of the Eligibility Criteria.
        – Administer the addition of each WSC-QE by executing the process to add WSC-QEs to the Trust Community that has been approved by the WSC Governance Body.
        – In coordination with the WSC Governance Body update the record of each WSC-QE added to the WSC Trust Community as required if and when Eligibility Criteria are changed.
        – If the Party State learns of changes related to a WSC-QE that it promoted to the WSC Trust Community that disqualify the WSC-QE from being included in the WSC Trust Community that Party State shall execute the process to remove the WSC-QE from the

[1] Currently the WSC is constrained to the Pilot project as defined in the WSC-MOU. If, in the future the WSC expands to offer different service offerings that require independent eligibility criteria this procedure can be extended to include said here.

WSC Trust Community using the removal process approved by the WSC Governance Body.

c) Party State Administration of WSC-QEs for the WSC-Pilot.

- Party States shall only use procedures approved by the WSC Governance Body to add and remove WSC-QEs to the WSC Trust Community of the WSC-Pilot.
- The WSC Governance Body shall make available to Party States the approved procedure by which Party States may add and remove candidate WSC-QEs to (from) the WSC Trust Community.
  - For the Pilot the approved procedure will be captured in a document to be called "WSC-P&P#2 – WSC-Pilot Trust Community Administration Addendum".
- The WSC Governance Body shall make changes to the 'WSC Trust Community Administration Procedure' only once they are approved by following WSC-P&P#1.
  - Once changes have been approved by the WSC Governance Body the "WSC-P&P#2 – WSC-Pilot Trust Community Administration Addendum" shall be updated and its history will reflect the date of the change.

IV. Definitions

WSC-QE – An entity that has been vetted by a Party State and found to satisfy all of the Eligibility Criteria of the WSC Trust Community.

Party State – Any state, territory or other similar entity that is a signatory to this MOU and participates in the Pilot according to the intentions of this MOU.

Trust Community - A group of WSC-QEs that have been evaluated by a Party State to satisfy the conditions of the WSC Governance Body for participating in the exchange of health information between party states.

WSC Governance Body – the governance entity established by the WSC MOU established and responsible for governing the WSC including responsibility for developing, maintaining, repealing, amending and retaining the Policies and Procedures of the Western States Consortium.

WSC-Pilot – the limited set of services that are the subject of the WSC-MOU.

All other capitalized terms, if not defined herein, shall have the same meaning as set forth in the WSC MOU.

V. References

Western States Consortium Memorandum of Understanding.

VI. Related Policies and Procedures

To be developed: WSC-P&P to add Party States to the WSC Governance Body.

VII. Version History

Version	Date	Author	Comment
0.4	10/12/2012	Aaron Seib	First Draft
0.5	11/19/2012	Aaron Seib	Removed several typos

WSC-P&P#2 – WSC-PILOT ELIGIBILITY CRITERIA ADDENDUM

I. Purpose

This addendum defines the eligibility criteria for inclusion of a WSC Qualified Entity into the WSC-Pilot Trust Community to be evaluated by Party States.

II. Procedure: Eligibility Criteria of a WSC-QE

In this addendum the WSC-QE eligibility criteria are grouped into two sets.

- The first set are derived from the 'State HIE Implementation Guidelines for Direct Security and Trust' published by the ONC[1] (section A below).
- The second describes the Obligations of the Parties to the WSC-QE's Participant Agreement[2] (section B below).

A Party State shall confirm that candidate WSC-QEs satisfy each and all Eligibility Criteria of both sections prior to causing the WSC-QE to be added to the WSC-Pilot Trust Community.

A. WSC required Direct Project Security and Trust components

1. Conform to all of the Direct Project requirements

   - Specified in[3]:

     – Direct Project's Applicability Statement for Secure Health Transport version 1.1

Rational: The scope of the pilot is currently limited to the Direct Project mode of exchange.

Method of Verification: Currently there are no automated testing available to the Pilot to verify that the application WSC-QE conforms to the technical specifications. For the verification needs of the Pilot the WSC Governing Body will rely on self-attestation.

Noteworthy: NIST is currently working on test tools for this purpose that should become available to the initiative in the future.

2. Implements a Business Associate Agreement[4] as a component of contracting with their Participants

   - Verify that the applicant HISP implements a Business Associate Agreement as a component of their contract with a Participant

---

[1] See: http://statehieresources.org/wp-content/uploads/2012/07/State-HIE-Implementation-Guidelines-for-Direct-Security-and-Trust_7-2012.pdf

[2] Although the initial participants in the WSC-pilot are all third parties that provide DIRECT services on behalf of covered entities there is no reason assume that CEs that can comply with these eligibility criteria (including for example, Health Delivery Organizations) would not also qualify for participation in the WSC in the future. For CEs and similar entities a Participants Agreement would not exist. The CE's Local Policies would be a candidate for verification for satisfaction of the policy requirements

[3] See: http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__direct_project/3338

[4] If the candidate WSCV-QE is a Conduit model the Governance Body may elect to exempt the HISP from the requirement to implement a BAA. The WSC Governance Body will evaluate this consideration in the future if a WSC-QE that is a true Conduit model HISP is identified by a Party State.

Rational: Required based on applicable law and evidentiary that the HISP holds itself to the provisions of the HIPAA Security Rule.

Method of Verification: Collect from HISP as component of Application Package.

Noteworthy: If the Applicant provides exchange services to any non-Covered Entities (such as Providers that operate on an all cash basis) the Applicant's Participant's Agreement must require that such Participants comply with the terms and conditions of HIPAA as if they were in fact a Covered Entity to be eligible to participate in the WSC.[5]

3. Have contractually binding legal agreements with their Participants

The Participants Agreement of a WSC Qualified-Entity should include all of the terms and conditions required in a Business Associates Agreement per item #2 above and the terms and conditions to effect the obligations identified in the subsection B below.

Rational: The obligations of the parties to a HISP's Participant Agreement are a critical component of a Trust Community. To be explored as part of conducting the Pilot.

Method of Verification: Collect from HISP as component of Application Package and verify that the obligations are satisfied contractually.

Noteworthy: The analysis to be performed by the Party State may require clarification with the candidate. Best practices in performing this verification need to be developed and may include guidelines in how to collaborate with the candidate to index the obligations against the HISP's Participant Agreement.

4. Demonstrate conformance with industry standard practices related to meeting privacy and security regulations in terms of both technical performance and business processes.

    - Through either availability of a written security audit report or formal third party accreditation provided by an established, independent third-party.

Rational: HISPs operate services on behalf of many participants and on a risk basis should provide sufficient evidence to justify trust.

Method of Verification: There is more to learn about the method that this component shall be verified and what evidence will suffice for a candidate WSC-QE to demonstrate conformance. Candidates include:

- formal accreditation provided by an established, independent third-party entity or
- availability of a written security audit report or
- completed EHNAC self-assessment tool.

[5] It is outside the scope of the current pilot is to determine a verification method to test the ability of an Applicant to selectively exclude non-Covered Entities from use of the Trust Bundle and Directory Services.

to be explored as part of conducting the Pilot.

Noteworthy:

- HISPs that manage private keys -- should perform specific risk assessment and risk mitigation to ensure that the private keys have the strongest protection from unauthorized use.
- HISPs that manage trust anchors on behalf of their customers should have well defined, publicly available policies that permit customers and other parties to evaluate the certificate issuance policies of those trust anchors.

5. Minimize data collection, use, retention and disclosure

The HISP should only collect the minimally required to meet the level of service required. To the extent that HISPs support multiple functions with different requirements for data use, they must separate those functions such that more extensive data use or disclosure is not required for more basic (direct) exchange models.

Rational: This component encompasses at least two obligations.

- That the HISP should only collect, use, retain or support the disclosure of the minimum data necessary based on the Purpose of Use; and
- If the HIO offers services in addition to its HISP service, when an Authorized User is using the Direct Project offering the functions of the HIO with regards to that use should be separated from those of other modes of exchange that may have more extensive disclosure requirements (such as query retrieve where the Patient's Data may be accessible by Authorized Users without the Decision of a Provider with an existing Patient relationship asserting that the disclosure is appropriate).

Method of Verification Attestation: Data received via Direct Project shall not be captured and made accessible by any party other than the one that the sender addressed the message to.

Noteworthy: —

6. HISP shall encrypt all edge protocol communications

- that enable "last mile" exchange between end-users' systems and an STA/HISP's Direct Project infrastructure by using SSL/TLS or similar industry standard.

Rational: For HISP that enable messages to be transported across the Internet on behalf of Participants that do not encrypt data content prior to transporting messages to the HISP the "pipe" between the Participant and the HISP must be secured.

Method of Verification: Self-attestation – HISP shall ensure data in motion and at rest is properly encrypted.

Noteworthy: In the future as evidence is acquired demonstrating that alternative technologies or methods satisfy the objectives of this component the WSC Governance Body may approve the new alternatives.

7. HISP shall have a process to identify Authorized End Users

The method of identifying Authorized End Users shall satisfy the following requirements:

Only facilitate Direct messages that utilize X509 v3 digital certificates which[6]:

- Conform to "medium" level of identity assurance for the selected certificate type[7].
- At a minimum the HISP will require proof of identity for an individual at the Participant's site (Participant's Authorized User Administrator) who will be responsible for identifying and maintaining the Authorized Users that the Participant permits to access the HISP's system.
- The HISP will obligate the Participant to safeguard the integrity of the Authorized User Maintenance Process.
- Do not have the non-repudiation flag set.[8]
- Conform to other requirements set forth in the Direct Project's Applicability Statement for Secure Health Transport.
- Have been issued to a health care related organization or more granular component of an organization (e.g., department, individual).

Rational: All WSC-QEs must meet or exceed this minimum in order to be part of the WSC-Pilot Trust Community. The WSC Governance Board has established this minimum.

Method of Verification: Self-attestation – Party State's shall document WSC-QE attestation.

Noteworthy: The WSC-Governance Body may modify this component as regulations change or new technologies emerge that are equivalent or exceed the protections of the method described.

8. Enable independent trust establishment by Authorized Users

Although included in the ONC's Guidance the WSC Team has determined that it will not support the ONC guidance that reads "Provide users with mechanisms to directly establish trust with another user (e.g., store the public key) to enable ad-hoc messaging even if the respective HISPs have not "white listed" each other." as the recommendation raised a number of issues regarding trust by participants in the WSC and numerous stakeholders.

9. Enable Direct Project's XDR and XDM for Direct Messaging

The WSC determined that the ONC recommendation that HISP "Enable Direct Project's XDR and XDM for Direct Messaging specifications in order to support Direct-ready EHR vendor implementations using this deployment pattern." will not be required for inclusion in the WSC Community of Trust at this time.

---

[6] The WSC removed the requirement that HISPs "Have been cross-certified to the Federal Bridge Certification Authority (FBCA)."

[7] See: FBCA documentation for definition of the term 'medium' for identity proofing. There are active discussions regarding the standards related to the FBCA and NIST LOAs that may influence this requirement in the future.

[8] Because the cert is at the Organization level the question of which individual actually signed the payload cannot be answered, therefore it is not sufficient to satisfy a digital signature legal requirement but it still ensures the integrity and privacy of the content.

B. Obligations of the Parties to the WSC-QEs Participant Agreement

The following section outlines the relationships between the parties and attempts to identify the "Obligations" or responsibilities of the parties to one another established by the WSC-QE's Participant Agreement that the WSC-Pilot Trust Community has identified to date as being instrumental to establishing trust for the Direct Mode of Exchange. It is expected that at least some of these "obligations" will be refined based on experience from running the pilot. It is the intention of the WSC Governance Body to refine the 'Eligibility Criteria' described in this section, updating the specifics that follow based on experience learned from running the pilot.

The Obligations described below are to be evidenced by the terms and conditions found in the Participants Agreement of the candidate WSC-QE. As there are many ways that the obligations of the parties to the Participant Agreement may be drafted in contract the description of obligations have been mapped to the hierarchical framework that follows to facilitate indexing of the WSC-QE's Participant Agreement to the obligations. The contract language and framework of specific WSC-QE's Participant Agreement addresses these obligations will vary. For example, some PAs may implement an End Users Agreement that all authorized users are required to sign as part of creating the Authorized End Users account which would simplify this identification by the Party State - while other Participant Agreements may require additional analysis to verify conformance of the 'Obligations of Authorized End Users'.

1. Obligations of the HISP

   i. Obligations of the HISP – WSC Facing

      The HISP shall commit to complying with all applicable federal and state laws and regulations in their Participants Agreement.

      - All Participants of the HISP that are given access to the WSC Offering will be required to be signatories to the HISP's Participants Agreement.
      - It is an obligation of the HISP to ensure that Participants that have been terminated are no longer able to use the services of the WSC.
      - HISP's shall not make PHI exchanged as part of this pilot accessible to anyone other than the specified recipient in the Direct message. For example:
        - The HISP shall not make it part of a portal that is accessible to other Participants
        - The HISP shall not de-identify the data and make it available
        - The HISP shall not allow the data to be used for marketing purposes.
      - Material Changes to HISP's Participants Agreement must be submitted to the Party-State. The State Party shall evaluate if the change would result in the HISP WSC Qualified HISP status being changed.
      - The HISP shall maintain appropriate auditing of its usage of the WSC service offerings.
      - The HISP shall use reasonable efforts to ensure that its connection to and use of the WSC offerings do not introduce 'malware' which will disrupt the proper operation of the WSC services or any part thereof.

- A HISP shall notify the State that approved it for inclusion in the WSC of a breach if the HISP (or one of its Participants) is required to make notification of a breach pursuant to applicable state and\or federal law.
- The HISP must continue to satisfy the requirements described in greater detail in section III.A of this document for the duration of their participation in the Pilot; and
- Acknowledge that the WSC Governance Body may modify these requirements as the needs of the WSC change and acknowledge that a condition of ongoing Qualified Entity Status may depend on submitting additional information or evidence that the HISP satisfies eligibility criteria of the WSC as approved by the governance body.
- Require that the HISP disclose to the Participant the Pilot nature of this program and that the service offered may be discontinued.
- Only Participants of the WSC-QE who have agreed to join the pilot should be able to utilize the offerings of the WSC (i.e., the WSC Digital Credential shouldn't be added to their direct messages and the non-recruited sites shouldn't be discoverable in Scenario 2).

ii. Obligations of the HISP – Participant Facing

- The Participant Agreement of the HISP must disclose how governance decisions are made to its Participants in its Participants Agreement regarding but not limited to:
  - Remedies of the Participant when changes to the Participants Agreement are approved
  - What are the types of parties that are eligible to use the service?
  - Dispute management process.
  - The process by which the HISP safeguards compliance of Participants to the terms of the Participants Agreement.
  - The process by which the HISP terminates Participants.
- The Participant Agreement of the HISP must have terms that survive beyond termination of the contract including:
  - Participant must continue to safeguard the Privacy and Security of Patient Data received even after termination of the PA.
  - Participant must continue to be responsible for the Conduct of Participant and its Authorized Users.
  - Those T&Cs that are required to survive of a Business Associates Agreement.
- HISP shall obligate the Participant to prohibit non-authorized users access to the system.
- HISP shall make appropriate training materials regarding Participants' rights and obligations and the proper access and use of the system available to each Participant.
- HISP shall make its monitoring of Participants transparent to the Participant.
- HISP shall have a process to terminate Participants who fail to satisfy the Participant obligations described below.

2. Obligations of the Participant

The Participant shall comply with all applicable federal and state laws and regulations.

- The Participant shall maintain sufficient safeguards and procedures to maintain the security and privacy of data received through the HISP.
- The Participant shall use best and reasonable efforts to ensure appropriate security measures are in place to protect PHI.

- Participant's Authorized Representative of the Participating Organization or his\her designee will be responsible for the accounts created for the Participants Authorized Users and ensuring that all of them meet the following criteria:
  - Participants will only create Authorized User Accounts for users permitted to handle PHI according to the local policy of the Organization.
  - Participant Organization will have a policy prohibiting the sharing of account information among permitted users.
  - Participant will not permit non-authorized users to access the HISP's system.
- The Participants shall use best and reasonable efforts to ensure that Authorized Users are trained in the secure and appropriate use of the HISP's System.
- A Participant shall notify its HISP of any breach notifications that the Participant must report to comply with applicable state or federal law.
- In the event of a termination of the Participants Agreement Participant shall use best and reasonable efforts to ensure that any Authorized User (in the role of sender or receiver) of the Participant's will no longer share or acquire data through the HISP.

3. Obligations of Authorized Users

i. In role of Data Recipient

The Authorized End User in the role of Data Receiver shall comply with all applicable federal and state laws and regulations.

- An Authorized End User in the role of Data Receiver shall use the HISP's service only for purposes of treatment, payment and operations as those terms are defined in HIPAA.
- An Authorized End User in the role of Data Receiver shall not provide data to third parties and shall only use data received by the system in the performance of its permitted purposes.
- An Authorized End User in the role of Data Receiver shall not use PHI received via the HISP in any manner prohibited by law.
- An Authorized End User in the role of Data Receiver shall not aggregate data to compare the performance or outcomes of Authorized Users not associated with the Participant.
- An Authorized End User in the role of Data Receiver shall limit its use and disclosure of Patient Data acquired through the HISP to the extent permitted by applicable law.
- An Authorized End User in the role of Data Receiver shall not disclose data that they receive via the HISP without appropriate authority.[9]

ii. In role of Data Sender

The Authorized End User in the role of Data Sender shall comply with all applicable federal and state laws and regulations.

- An Authorized End User in the role of Data Sender shall use the HISP's service only for purposes of treatment, payment and operations as those terms are defined in HIPAA.[10]

[9] This is to say if a consent is required to redisclose data that the Authorized End-User is obligated to have that consent in place prior to sharing data using the HISPs (or secondarily via the WSC offerings).

[10] For the purposes of the Pilot we are only permitting Authorized end-users from Participants that are a type = Provider so we don't anticipate that during the Pilot the system will be utilized for Payment Purposes.

- The Authorized End User in the role of Data Sender shall use the HISP's services to send only the amount of Patient Data that the data recipient is permitted to receive pursuant to applicable laws and regulations.[11]
- The Authorized End User in the role of Data Sender shall use reasonable care with respect to the accuracy and completeness of the data sent.
- The Authorized End User in the role of Data Sender is obligated to only send data that they have the authority to send (if consent required sender attest that they have it)
- The Authorized End User in the role of Data Sender grants right to use data sent to a receiver for the permitted purpose it was intended to be use in a fully-paid, non-exclusive royalty free right and license of the Patient Data released to the recipient.
- The Authorized End User in the role of Data Sender will use best and reasonable efforts to ensure that they will maintain all appropriate consent to disclose data as required by applicable federal and state law.[12]

III. Definitions

WSC-QE – An entity that has been vetted by a Party State and found to satisfy all of the Eligibility Criteria of the WSC Trust Community.

Party State – Any state, territory or other similar entity that is a signatory to this MOU and participates in the Pilot according to the intentions of this MOU.

Trust Community - A group of WSC-QEs that have been evaluated by a Party State to satisfy the conditions of the WSC Governance Body for participating in the exchange of health information between party states.

WSC Governance Body – the governance entity established by the WSC MOU established and responsible for governing the WSC including responsibility for developing, maintaining, repealing, amending and retaining the Policies and Procedures of the Western States Consortium.

WSC-Pilot – the limited set of services that are the subject of the WSC-MOU.
All other capitalized terms, if not defined herein, shall have the same meaning as set forth in the WSC MOU.

IV. References

To be determined.

V. Related Policies and Procedures

To be determined.

[11] For treatment purposes there are no minimum data use requirements. With regards to Payment and Operations there may be. It is the obligation of the Authorized user to decide if the data they are sending meets minimum data requirements when the intended receiver is for purposes of use related to Payment or Operations

[12] The consent requirements that apply are based on the state in which the sender provides care.

VI. Version History

Version	Date	Author	Comment
0.1	10/13/2012	Aaron Seib	First Draft
0.2	10/25/2012	Aaron Seib	Following review with NCHIN discovered typographic errors that were corrected in the version. Specifically, where the prior version listed out the subsections of Eligibility Criteria A in 'Obligations of the HISP – WSC Facing' of this Addendum in this version it has been restated without summarizing the subsections as they may change from time to time.
0.3	10/29/2012	Aaron Seib	Removed some legacy comments.
0.4	10/31/2012	Aaron Seib	Updated language to reflect feedback from WSC-Governance Body

WSC-P&P#2.6 – WSC-PILOT TRUST COMMUNITY ADMINISTRATION ADDENDUM

I. Purpose

This addendum defines the process for administering the WSC Trust Bundle to form the Trust Community of WSC Qualified Entities that participates in the pilot.

II. Procedure

This procedure comprises two parts:

1. The procedure for adding a new member to the Trust Community, and
2. The procedure for removing a member from the Trust Community.

The WSC Trust Bundle comprises the technical component of membership in the WSC Trust Community. Therefore, the procedures for adding members to and removing members from the Trust Community equates to the procedures for adding Trust Anchors to and removing Trust Anchors from the WSC Trust Bundle.

A Party State shall confirm that candidate WSC Qualified Entities satisfy the Eligibility Criteria and therefore qualify for addition to the Trust Community. A Party State shall likewise determine when a WSC Qualified Entity no longer satisfies the Eligibility Criteria and should be removed from the Trust Community.

A. Adding a Member to the Trust Community

The initial stages of the WSC pilot will include only a small number of HISPs as Qualified Entities. Therefore, the initial processes for adding members to the Trust Community are manual. The following process may be replaced by an automated process in the future.

1. The Party State identifies a single point of contact (POC) within the candidate Qualified Entity for all technical communications, along with an email address that is regularly monitored by the POC.

Rational: Notification of changes to the Trust Bundle will be communicated through email at least through the initial stages of the pilot. The name and contact information of the POC, including an email address, should be collected by the Party State as part of the application process of a candidate Qualified Entity.

2. The Party State determines that a candidate Qualified Entity has met the Eligibility Criteria and that the HISP should be added to the Trust Community.

Rational: The Party State has the sole authority to determine whether a candidate Qualified Entity meets the Eligibility Criteria.

3. The Party State contacts the Trust Bundle Coordinator by email instructing the Coordinator to add the Qualified Entity to the Trust Bundle, providing the contact information of the POC.

Rational: It is desirable for the WSC to define a single point of contact – the Trust Bundle Coordinator – to manage the process for Trust Community Administration.

Noteworthy: Members of the Direct Project have elected not to define a process or technical standard for alerting Trust Community members of changes to the Trust Bundle. The Governance Body has elected to create such a mechanism out of band for the purposes of the pilot.

4. The Trust Bundle Coordinator contacts the POC of the Qualified Entity HISP via email requesting that the HISP's Trust Anchor be provided by return email.

Rational: The presence of a HISP's Trust Anchor in the Trust Bundle is the sole technical indication of a Qualified Entity's membership in the WSC Trust Community.

Noteworthy: Since the Trust Anchor is a public key, strong security is not required to transport it.

5. The Trust Anchor is inspected by the Trust Bundle Coordinator to verify that it meets the criteria identified in the Eligibility Criteria, if any.

If defects are identified, the Trust Bundle Coordinator contacts the Party State to report the failure and contacts the POC to correct the defect and resubmit the Trust Anchor.

Rational: This may be the first technical check on meeting certificate requirements identified in the Certification Criteria, and issues should be reported to the Party State. It is desirable to correct any defects before proceeding to technical testing.

Noteworthy: A defect in the Trust Anchor may indicate a deviation from the Eligibility Criteria. The Party State should determine whether failure at this step indicates that Qualified Entity status should be revoked and this procedure should be halted.

6. The Trust Bundle Coordinator informs the POC of successful verification and places the verified Trust Anchor within the trust anchor store of the WSC Trust Community test HISP.
7. The Trust Bundle Coordinator sends the POC the Trust Anchor of the WSC Trust Community test HISP via email and arranges for a test of the Trust Anchor.

Noteworthy: This step requires that a HISP test site be established for testing the Trust Anchors of Qualified Entity HISPs. For the purposes of the pilot, the WSC Trust Bundle Coordinator will use the latest version of the Direct Reference Implementation to best ensure technical conformance with the Direct specifications.

8. The Trust Bundle Coordinator and POC conduct a test exchange of Direct messages between the WSC Trust Community test HISP and the Qualified Entity HISP.

If issues are identified, the Trust Bundle Coordinator reports them to the Party State. The issues are corrected, and the exchange retested until the test is successful.

Rational: This may be the second technical check on meeting certificate requirements identified in the Certification Criteria, and issues should be reported to the Party State. All issues with exchange with a Reference Implementation should be corrected before a Trust Anchor is added to the Trust Bundle.

Noteworthy: A defect in the Trust Anchor may indicate a deviation from the Eligibility Criteria. The Party State should determine whether failure at this step indicates that Qualified Entity status should be revoked and the procedure should be halted.

9. The Trust Bundle Coordinator informs the Party State of a successful test exchange, and adds the new Trust Anchor to ZIP compressed archive that comprises the Trust Bundle.

Rational: The Trust Bundle is defined as all Trust Anchors within a ZIP compressed archive. This step constitutes an update to the Trust Bundle.

Noteworthy: This step is an interim solution while standards for trust bundle distribution are being finalized. It will likely be replaced by adding a trust anchor to a PKCS7 container, and optionally signing that container.

10. The Trust Bundle Coordinator publishes the new Trust Bundle via a RESTful web service over HTTPS, removing the previously published Trust Bundle.

Rational: Use of HTTPS rather than HTTP establishes the identity and authority of the publisher and guarantees integrity of the Trust Bundle transfer.

Noteworthy: The use of RESTful web services over HTTP or HTTPS is an emerging standard for Trust Bundle distribution. The certificate used to secure HTTPS should not be self-signed in order to establish the identity of the publisher.

11. The Trust Bundle Coordinator sends an email to the Governance Entity and the POCs of all Qualified Entities and that are members of the Trust Community, including the newly added organization, alerting them that the Trust Bundle has been updated.

Rational: The emerging standard for Trust Bundle distribution does not call for any in-band or out-of-band notification of Trust Bundle changes, but instead places the responsibility for establishing the update schedule on the Trust Community member. Email will be used initially to contact the POCs to ensure that all Trust Community members update their trust stores promptly to enable the pilot to proceed.

Noteworthy: The Governance Entity is alerted simply so its members may monitor updates to the Trust Bundle. The Governance Entity might also alert Party States at its discretion.

12. The POCs of all Qualified Entities in the Trust Community download the updated Trust Bundle from the web service, and update the trust anchor stores in their HISP implementations.

Rational: This update adds the Trust Anchor of the new Qualified Entity to the local trust anchor store of each HISP, enabling trusted exchange and effectively adding the new organization to the Trust Community.

Noteworthy: This manual process may be replaced by a subscription service or push web service in the future to automate propagating updates to the Trust Bundle.

B. Removing a Member from the Trust Community

The initial stages of the WSC pilot will include only a small number of HISPs as Qualified Entities. Therefore, like the process for adding members, the initial processes for removing members from the Trust Community are manual. The following process may be replaced by an automated process in the future.

1. The Party State determines that a previously Qualified Entity no longer meets the Eligibility Criteria or, for some other reason, should be removed from the Trust Community.

Rational: The Party State has the sole authority to determine whether an organization should be removed from the Trust Community.

2. The Party State contacts the Trust Bundle Coordinator by email instructing the Coordinator to remove the organization from the Trust Bundle.

Rational: It is desirable for the WSC to define a single point of contact – the Trust Bundle Coordinator – to manage the process for Trust Community Administration.

Noteworthy: Members of the Direct Project have elected not to define a process or technical standard for alerting Trust Community members of changes to the Trust Bundle. Since the pilot includes a small number of organizations, removal of an organization is not anticipated as a frequent event. However, the Governance Body has elected to create such a mechanism out of band for the purposes of the pilot.

3. The Trust Bundle Coordinator removes the Trust Anchor for the removed organization from the ZIP compressed archive designated to hold the Trust Bundle.

Rational: This step constitutes an update to the Trust Bundle.

4. The Trust Bundle Coordinator publishes the new Trust Bundle via a RESTful web service over HTTPS, removing the previously published Trust Bundle.
5. The Trust Bundle Coordinator sends an email to the Governance Entity and the POCs of all remaining Qualified Entities and that are members of the Trust Community alerting them that the Trust Bundle has been updated.

Rational: Email will be used initially to contact the POCs.

Noteworthy: The Governance Entity is alerted simply so its members may monitor updates to the Trust Bundle. The Governance Entity might also alert Party States at its discretion.

6. The POCs of all Qualified Entities in the Trust Community download the updated Trust Bundle from the web service, and update the trust anchor stores in their HISP implementations.

Rational: This update removes the Trust Anchor of the removed organization from the local trust anchor store of each HISP, disabling exchange and effectively removing the organization to the Trust Community.

Noteworthy: This manual process may be replaced by a subscription service or push web service in the future to automate propagating updates to the Trust Bundle, especially for removal operations. This process does not bypass the any requirement to monitor certificate revocation that may be part of the Direct specifications.

III. Definitions

Certificate Authority (CA) – An organization that issues digital certificates. A CA has a published identity assurance, authentication, security, and (perhaps) other policies.

Health Information Service Provider (HISP) – An organization that provides secure transport for directed exchange in compliance with technical specifications for the Direct Project. For the WSC Pilot, a HISP must conform to the requirements of the Eligibility Criteria of a WSC Qualified Entity.

Trust Anchor – The public key of a digital certificate for the CA used to sign a HISP's certificates. All Direct endpoints signed by a CA agree to abide by its identity assurance, authentication, security, and other policies.

Trust Community – A group of organizations that elect to follow a set of policies and processes, and therefore agree to share protected health information. For the WSC Pilot, all members of the Trust Community have been evaluated by a Party State to satisfy the Eligibility Criteria of a WSC Qualified Entity.

Trust Bundle – A collection of trust anchors for members of a Trust Community that elect to follow a minimum set of policies and processes, perhaps for a specific health information exchange use case. The WSC Trust Bundle comprises WSC Pilot participants that agree to abide by the Eligibility Criteria of a WSC Qualified Entity for the defined pilot use case.

IV. References

The Direct Project Trust Bundle Subworkgroup, with records at http://wiki.directproject.org/Trust+Bundle+Sub+Work+Group, was convened to create an implementation guide for Trust Bundle packaging and distribution. The current schedule calls for consensus agreement on a draft guide in February or March, and for pilot implementation in April. That document should be referenced when complete.

V. Related Policies and Procedures

To be determined.

VI. Version History

Version	Date	Author	Comment
1	16 Oct 2012	Robert Cothren	First draft
2	7 Feb 2013	Robert Cothren	Edited to conform to emerging standard for Trust Bundle distribution.

WSC-P&P#3 – COMMUNICATIONS POLICY
WESTERN STATES CONSORTIUM GOVERNANCE BODY

Subject: WSC Communication Policy
Status: WSC-GB Approved
Policy #: 3
Date Approved: 10/30/2012
Version: 0.3
Pages: 3

I. Purpose

The purpose of this policy is to define the Western States Consortium (WSC) Party States' responsibilities when communicating with other Party States or other non-Trust entities and to define the WSC Governance Body's responsibility to review and approve of the content of Party States' communication in certain circumstances. This policy also defines the WSC Governance Body's responsibility to develop a Communication Plan for the WSC Party States.

II. Policy

The WSC Party States will follow basic communication standards as described in the WSC Communication Plan when making statements (either oral or written) about the WSC either on its own behalf or on behalf of the WSC. The WSC Governance Body shall review and approve Party States' formal communication and statements when speaking on behalf of the WSC. The WSC Governance Body shall develop and maintain a Communication Plan for the WSC.

III. Procedure

A. Basic Communication Guidelines for Party States

1) There may be various occasions when Party States must communicate with other non-Trust entities or make public statements regarding the status of the WSC activities. In these situations, if the Party State is speaking on its own behalf, it will follow the basic policies established below.

   a. Any oral or written statements made by the Party State will represent its own position and will not represent the WSC unless approved by the WSC Governance Board through the procedure described below.
   b. The Party State will not make public statements that reveal information the WSC or the WSC Governance Board has not approved for public knowledge.
   c. If the Party State is unsure of any public statements it is to make, the WSC Governance Board will provide review of the content to facilitate consistent messaging about the WSC.

2) When an individual Party State or a group of Party States are requested to communicate or make a formal, public statement on behalf of the WSC, the Party State is to request approval to make the public statement from the WSC Governance Board and shall also obtain the Governance Board's approval of the statement contents.

a. The Party State will submit the following background information to all members of the WSC Governance Board. The request shall be made at least 5 business days in advance of the date the public statement is to be made or an interview is scheduled to the Governance Board.

i. Description of the circumstances for which a public statement is to be made, i.e., public event, newspaper or journal, or television interview
ii. Date the Party State is requested to make or provide the statement
iii. Date the statement is to be made public
iv. Date by which the WSC Governance Board is to respond to the Party State
v. Draft copy of the content of the public statement

B. WSC Governance Body's Review Process

1) The individual Party State or a group of Party States who are requesting to make a public statement on behalf of the WSC shall submit their request and the information as described in items III.A.(2)(a)(i) through (v) above to two designated WSC Governance Body members (WSCGB reviewers[1]) for review. Upon receipt of the request and background information, the two designated members will notify the rest of the WSC Governance Body members of the receipt of the request and a brief summary of the nature of the request. If the Party State member making the request is one of the WSCGB reviewers, then another WSCGB member will be called upon to review the request.
2) The two designated WSCGB reviewers will review the Party State's request within 5 working days of receipt of the request. The criteria to be used for determining whether the request and statement content is to be approved or not will be at a minimum those described in items III.A.(2)(b) through (d) above. The WSCGB reviewers will either approve, approve with amendments, or disapprove the statement contents.
3) Once the WSCGB reviewers have made a decision, they will send their recommendation to the Party State and the rest of the WSC Governance Body for notification.

C. Communication Plan Development

The WSC Governance Body will develop and maintain a WSC Communication Plan to be followed by the WSC Party States. The plan will describe the modes of communication, the frequency of communication, provide guidelines on in-person or teleconference meetings. The WSC Governance Body may amend the Communication Plan consistent with the process described in the WSC Procedure for Policy and Procedure Change Process (Policy #1).

IV. Definitions

Party State – Any state, territory or other similar entity that is a signatory to this MOU and participates in the Pilot according to the intentions of this MOU.

WSC Governance Body – the governance entity established by the WSC MOU established and responsible for governing the WSC including responsibility for developing, maintaining, repealing, amending and retaining the Policies and Procedures of the Western States Consortium.

[1] The WSC Member may elect to designate a person to stand in for them in this role.

V. References

None

VI. Related Policies and Procedures

WSC Procedure for Policy and Procedure Change Process (Policy #1)

VII. Version History

Draft	Date	Version Number	Author	Comment
1	10/15/2012	0.1	Susan Kinoshita	First Draft
2	10/17/2012	0.2	Susan Kinoshita	Draft 2
3	10/17/2012	0.3	Aaron Seib	Draft 3 – update to standardize formatting across P&P manual.

WSC-GB POLICY LOG 1
STATEMENT OF AUTHORITY

On 11/19/2012 the WSC-GB met telephonically to discuss the intent and purpose of the "Statement of Authority" artifact and the intent of its use in determining who may become members of the WSC-GB.

The question that was initially brought to the WSC-GB: Is statutory authority a requirement for new states to sign the WSC MOU and pursue onboarding to the WSC-GB?

The WSC-GB discussed the details of requiring a "Statement of Authority" artifact from entities that were interested in becoming Party State's to the MOU. Several questions were posed about the specific authority that would be expected by signatories of these documents; would the signatories be required to have statutory authority, could a State Designated Entity be designated as the states representative and signatory or does the signatory have to be an "agent of the state"? During the discussion all WSC-GB representatives agreed to the following:

- The intent of the 'Statement of Authority' was to establish documentation to be evaluated by the WSC-GB when considering if the applicant Party State was the appropriate entity to be representing a given jurisdiction
- The WSC-GB recognizes that not all State's Legislatures have established in statute an Agency Role or that if such an authority were granted that it every case would the State Agency necessarily be the best entity to fulfill the role of a Representative on the WSC-Governance body.
- The intent was to ensure that the WSC-GB had recognized the sovereign status of each state and worked with the entity that would be the best fit for the WSC-GB representative.
- To this end the WSC-GB has decided that a letter from a given State's HIT Coordinator (as indicated in the ONC Cooperative Agreement for State HIE Programs) describing that State's approach to HIE Governance is implemented could appropriately indicate that a State Designated Entity that is not a State Agency is the best State Party Representative.
- While drafting the "Statement of Authority" Letter the State HIT Coordinator drafting should consider Party State responsibilities as described in the MOU.

    1. Each Party state shall:

        a. Identify the authority and process for administering this MOU within its state;
        b. Appoint a Party State representative who shall become a member of the WSC Governance Body, as described in Article IV below.

    2. Continue to collaboratively participate in and execute the duties of the WSC Governance Body.
    3. Determine Candidate WSC-QEs that meet the requirements for inclusion in the WSC developed by the WSC Governance Body pursuant to this MOU.
    4. Evaluate entities for inclusion in the Trust Community and take the technical steps necessary to enable the Trust Community to exchange information between the party states.
    5. Provide an appropriate notice to Participants in each party state about the Trust Community.

- The entity identified by the State should be responsible for fulfilling the responsibilities of items 4 & 5 above impartially.

Essentially, the intent of the WSC is to ensure that the WSC-GB is working with the appropriate entity for a given state and to optimize the governance process by working with the entity or entities that are most familiar with the local policy requirements of the given state and its HIE market needs.

WSC-GB POLICY LOG 2

On 11/19/2012 the WSC-GB met telephonically to discuss whether or not the WSC-GB had the authority under the current MOU to enter into agreements with third parties.

The question that was initially brought to the WSC-GB: Can the WSC-GB sign a MOU with DirectTrust – an independent organization established to provide accreditation services – on behalf of the WSC.

The discussion clarified that under the language of the existing MOU the WSC-GB is not expressly given the authority to enter into any agreements on behalf of the Consortium.

At this time WSC-GB does not anticipate entering into any agreements with any parties as this is not consistent with the Purposes, Responsibilities or Duties of the WSC-GB as described in the WSC-MOU. Further discussion with the full WSC member states on modifying the MOU to permit the WSC-GB to enter into formal agreements may modify this decision in the future.

Appendix F—Western States Consortium Memorandum of Understanding

Western States Consortium
Memorandum of Understanding

RECITALS:

WHEREAS, the Party States desire to enter into this agreement in order to ensure the continuation of the pilot program initiated as part of ONC's State Health Policy Consortium to facilitate interstate exchange of health information between Western States Consortium Qualified-Entities. By signing this agreement each Party State is acknowledging that it has the authority to enter into the agreement.

WHEREAS, a condition of transacting information with other Western States Consortium Qualified Entities, each Western States Consortium Qualified Entity (WSC-QE) must acknowledge and agree to participate in the pilot by executing an Agreement with the appropriate Party State;

WHEREAS, the Party States recognize that nothing in this agreement is meant to or shall interfere with a Party State's authority to regulate the exchange of electronic health information in their state. Rather, the Party States enter into this Agreement to enable their voluntary participation in a common Trust Community, as set forth below;

NOW, THEREFORE, for and in consideration of the mutual covenants herein contained, the Participants hereto mutually agree as follows:

ARTICLE I. DEFINITIONS

In this MOU, unless the context clearly requires otherwise:

Definitions:

Participant – An individual or entity that signs a participant agreement with a Party State's WSC-QE in order to participate in the electronic exchange of protected health information.

Party States – Any state, territory or other similar entity that is a signatory to this MOU and participates in the Pilot according to the intentions of this MOU.

Pilot – The subject of this MOU wherein Party States voluntarily participate in a series of activities, the primary purpose of which is to test and evaluate policies, procedures and technologies for secure interstate exchange of health information and the Governance processes thereof.

Trust Community – A group of WSC-QEs that have been evaluated by a Party State to satisfy the conditions of the WSC Governance Body for participating in the exchange of health information between party states.

Western States Consortium Qualified Entities (WSC-QE) – Entities that maintain a Provider Directory or like capabilities and support the trusted exchange of electronic health information between Participants in the health care community.

ARTICLE II. PURPOSES

The purposes of this MOU are to:

1. Ensure that the Pilot in which the Party States are currently engaged in continues.
2. Establish a Governance Body to be known as the 'Western States Consortium Governance Body' (WSC Governance Body) for the Pilot to develop eligibility criteria and to define the operating policies and procedures for participation in the Western States Consortium.
3. Require each Party State and their approved 'WSC-QE' to adhere to the policy and procedures established by the WSC Governance Body.

ARTICLE III. RESPONSIBILITIES OF PARTIES

Party State responsibilities.

1. Each Party State shall:

    a. Identify the authority and process for administering this MOU within its state;
    b. Appoint a Party State representative who shall become a member of the WSC Governance Body, as described in Article IV below.

2. Continue to collaboratively participate in and execute the duties of the WSC Governance Body.
3. Determine Candidate WSC-QEs that meet the requirements for inclusion in the WSC developed by the WSC Governance Body pursuant to this MOU.
4. Evaluate entities for inclusion in the Trust Community and take the technical steps necessary to enable the Trust Community to exchange information between the party states.
5. Provide an appropriate notice to Participants in each Party State about the Trust Community.

ARTICLE IV. ESTABLISHMENT OF A WSC GOVERNANCE BODY

1. Establishment.

    This MOU establishes a "WSC Governance Body" that shall develop policies and procedures that govern the creation and use of the Western States Consortium.

2. Organization.

    a. Membership. The WSC Governance Body shall be composed of one member from each Party State.
    b. Officers. When the WSC Governance Body exceeds two members the Membership shall appoint a Chair of the WSC Governance Body who shall be responsible for calling meetings, setting the agenda for meetings, and undertaking other responsibilities to ensure the WSC Governance Body is accomplishing the purposes of this MOU.

3. Meetings.

   The WSC Governance Body shall meet as needed by phone, videoconference, in person, or by other means, and shall hold its first meeting as soon as practicable after the first two Party States have signed this MOU.

4. Duties.

   The WSC Governance body shall:

   - Approve the ongoing operation of the Pilot, and monitor its operations through data collection requirements.
   - Draft and approve data collection requirements from the operation of the Pilot to include metrics of WSC-QE of the services of the WSC.
   - Establish criteria for inclusion in the Trust Community.
   - Establish a process for developing a Policies and Procedures Manual for the operations of the WSC.
   - Develop and periodically review and revise the Policies and Procedures Manual for the operations of the WSC. The Manual shall include but is not limited to:
     - Policy and Procedures for selecting and modifying the eligibility criteria of WSC-QEs and the Trust Community;
     - Trust Community Management Policy and Procedures; and
     - WSC Communications coordination Policy and Procedures.
   - Collect data of the WSC operations from WSC-QE usage;
   - Oversee membership of Party States;
   - Advance the goals of the Western States Consortium

5. Transparency

   The WSC Governance Body shall make available for public inspection its agendas and approved policies and procedures. Each state will be responsible for determining how to satisfy the requirements of transparency based on their State's applicable state law.

ARTICLE V. EFFECTIVE DATE OF MOU

1. Effective Date.

   This MOU shall take effect upon being entered into by two or more Party States. If and when additional states enter into this MOU it shall become effective among those states and each Party State that has previously signed it.

2. Counterparts.

   With respect to the first two Party States to this Agreement, the Effective Date shall be the date on which the second Party State executes this Agreement. For all Party States thereafter, the Effective Date shall be the date that the specific Party State executes this Agreement. This Agreement may be executed in any number of counterparts, each of which shall be deemed an original as against the Party State

whose signature appears thereon, but all of which taken together shall constitute but one and the same instrument.

ARTICLE VI. TERMINATION OF MOU

1. In general.

   The WSC Governance Body shall continue in existence as long as this MOU remains in effect to be reviewed periodically by the Governance Body but not less than once every Calendar year.

2. Effect.

   Any termination of this MOU by a Party State shall become effective 10 days after written notice of termination is provided by the Party State to each other Party State.

ARTICLE VII. ADJUDICATION OF DISPUTES

1. In general.

   The WSC Governance Body shall:

   a. Have initial authority to make determinations with respect to any dispute regarding:

      i. Interpretation of this MOU;
      ii. Any Policies or Procedures established by the WSC Governance Body pursuant to Article IV; and
      iii. Any dispute or controversy between any parties to this MOU.

   b. Review any dispute described in paragraph (1) at a regularly scheduled meeting of the WSC Governing Body and only render a decision based upon a majority vote of the members of the council. Such decision shall be published by each Party State pursuant to the requirements of Article IV(5).

ARTICLE VIII. AUTHORIZED RECORD DISCLOSURES

1. Record Disclosure.

   Any record obtained under this MOU may be used only for the official purposes for which the record was requested. Each Party State shall establish procedures, consistent with the applicable law of its State and the Policies and Procedures, established by the WSC Governance Body under Article IV(5); and shall ensure that records obtained under this MOU are used only by authorized officials for authorized purposes.

ARTICLE IX. MISCELLANEOUS PROVISIONS

1. No authority for nonappropriated expenditures. Nothing in this MOU shall require the Party States to obligate or expend funds.
2. Nothing in this MOU shall diminish or lessen the obligations, responsibilities, and authorities of any state, whether a Party State or a nonparty state, or of HIO/HISP or other subdivision or component thereof, including the rules and procedures promulgated by the WSC Governance Body under Article VI, regarding the use and dissemination of health information.
3. **NON-BINDING**. This MOU is not intended to be legally binding and does not create any contractual or other legal obligations on any Party, nor will the Parties be subject to any legal liability resulting from non-performance of any provisions of this MOU. This MOU does not create a partnership, joint venture, or other type of legal entity, nor shall it be construed to interfere with or supersede other agreements the Parties may pursue. Neither Party may represent, or operate on behalf of, or bind the other Party without the other Party's written consent by a duly authorized agent, nor use the marks or logos of the other Party without that Party's consent. While not binding, the Parties undertake to act in good faith with respect to each other, and to adopt reasonable measures to ensure the realization of the objectives of this MOU. The Parties agree not to create any financial or other obligations, make any commitments, take any positions on behalf of the other Party, or use the name or logo of that Party without that Party's specific, written consent by an individual duly authorized to bind the organization.

ARTICLE X. SEVERABILITY

The provisions of this MOU shall be severable, and if any phrase, clause, sentence, or provision of this MOU is declared to be contrary to the laws of any participating state, or to the Constitution of the United States, or the applicability thereof to any Party State, or circumstance is held invalid, the validity of the remainder of this MOU and the applicability thereof to any Party State shall not be affected thereby. If a portion of this MOU is held contrary to the laws of any Party State, all other portions of this MOU shall remain in full force and effect as to the remaining Party States and in full force and effect as to the Party State affected, as to all other provisions.

Western State Consortium
Memorandum of Understanding
Signature Page

[fill in State] Representative

By: _____
Signature

Its: _____
State Representative Name and Title

_____
Office/State Department

_____
Street address

_____
City, State and Zip

Date: _____

Appendix G—Oregon Statement of Authority

Statement of Authority: Western States Consortium Pilot Project

413.255 Cooperative research and demonstration projects for health and health care purposes. In addition to its other powers, the Oregon Health Authority may:

1) Enter into agreements with, join with or accept grants from the federal government for cooperative research and demonstration projects for health and health care purposes, including, but not limited to, any project that:

   (a) Improves the lifelong health of Oregonians.
   (b) Aids in effecting coordination of planning between private and public health and health care agencies of the state.
   (c) Improves the administration and effectiveness of programs carried on or assisted by the authority.

2) With the cooperation and the financial assistance of the federal government, train personnel employed or preparing for employment by the authority. The training may be carried out in any manner, including but not limited to:

   (a) Directly by the authority.
   (b) Indirectly through grants to public or other nonprofit institutions of learning or through grants of fellowships.
   (c) Any other manner for which federal aid in support of the training is available.

3) Subject to the allotment system provided for in ORS 291.234 to 291.260, expend the sums required to be expended for the programs and projects described in subsections (1) and (2) of this section. [2011 c.720 §47]

Appendix H—California Statement of Authority

California Statement of Authority to Enter into MOU

As stated in the California Health & Safety Code, §130251 (d), California Health and Human Services Agency (CHHS) or state-designated entity:

> shall execute tasks related to accessing federal stimulus funds made available through ARRA, and facilitate and expand the use and disclosure of health information electronically among organizations according to nationally recognized standards and implementation specifications while protecting, to the greatest extent possible, individual privacy and the confidentiality of electronic medical records.

Through statutory authority, CHHS shall participate in the Western States Consortium as described in the Western States Consortium Memorandum of Understand.