

March 2014

PHR Ignite Pilot National Association for Trusted Exchange ONC State Health Policy Project

Final Report

Prepared for

Office of the National Coordinator for Health Information Technology
US 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

This report was funded under
Contract No. HHSP23320095651WC,
Order No. HHSP23337007T_0002.
The contents of this report do not necessarily
reflect the opinions or policies of ONC.



[This page intentionally left blank.]

Contributing Authors

Alaska

Paul Cartland

State of Alaska Department of Health and Social Services

California

Ifetayo Freeman

California Office of Health Information Integrity

Rupinder Colby

California Office of Health Information Integrity

NATE

Aaron Seib

CEO, National Association for Trusted Exchange

Robert M. Cothren, PhD

CTO, National Association for Trusted Exchange

Oregon

Sharon Wentz, RN,

Business Development Coordinator, CareAccord

Lisa Parker

Director of HIT Policy Implementation and Program Design, CareAccord

RTI International

Jacqueline Bagwell

Stephanie Rizk

Edna Boone

ONC/RTI Consultant

John Hall

Krysora LLC

Mindy Montgomery

Krysora LLC

Humetrix

Christopher R. Burrow, MD

EVP Medical Affairs

Randy Ullrich

SVP Wireless Applications

Bettina Experton MD, MPH

President & CEO

No More Clipboard

Jeff Donnell

President, NoMoreClipboard

Microsoft HealthVault

Sean Nolan

Distinguished Engineer

Santa Cruz HIE (SCHIE)

Bill Beighe

CIO, SCHIE

Becky Shoemaker

Project Manager, SCHIE

San Diego Regional HIE (SDRHIE)

Cody Johansen

Technical Operations Manager

Dan Chavez

Executive Director

Ben Fox

Senior System Engineer

Briseña Petersen

Project Manager

UCSD

Edward Castillo, PhD, MPH

Assistant Adjunct Professor

Principal Investigator (PI)

James Killeen, MD

Clinical Professor of Emergency Medicine

Co-PI

The NATE PHR Ignite project team would like to thank the following for their contributions: Glen Crandall and Melissa Sands from the Veterans Administration for their participation in this and other NATE projects, Barbara Smith Ascendian Consulting for her project management support, Dr. Kenneth Carlson of Childhood Health Associates of Salem Oregon, and all of the providers and consumers that have taken part in this effort.

[This page intentionally left blank.]

Contents

Section	Page
Executive Summary	1
1. Introduction and Background	1-1
1.1 Background on the National Association of Trusted Exchange	1-1
1.2 PHR Ignite Pilot Project	1-1
1.3 NATE Governance Structure	1-4
1.4 NATE PHR Ignite Pilot Technical Infrastructure	1-6
1.5 Pilot Assumptions and Agreements	1-7
2. Pilot Planning, Implementation, and Implications	2-1
2.1 Piloting Use Case 1: Provider to Patient PHR	2-1
2.1.1 Policy Solutions and Implications.....	2-1
2.2 Piloting Use Case 2: Patient PHR to Provider	2-2
2.2.1 Policy Solutions and Implications.....	2-2
2.3 Technical Solution for Use Cases	2-4
2.3.1 Facilitate Trust Anchor Distribution Via Trust Bundles.....	2-4
2.4 Alaska Pilot: Alaska eHealth Network Bidirectional Exchange Pilot of Use Case 1 and Use Case 2	2-7
2.4.1 Alaska User Story.....	2-7
2.4.2 Alaska Key Challenges	2-8
2.4.3 Alaska Technical Solutions and Implications.....	2-8
2.5 California Humetrix Pilot: San Diego Health Connect and VA Transmit Medical Data to iBlueButton Mobile Application Pilot of Use Case 1	2-10
2.5.1 California Humetrix User Story	2-10
2.5.2 California Humetrix Key Challenges	2-11
2.5.3 California Humetrix Technical Solutions and Implications.....	2-11
2.5.4 California Humetrix Governance Solutions and Implications	2-14
2.6 California Santa Cruz Pilot: Santa Cruz HIE Bidirectional Exchange Pilot of Use Case 1 and Use Case 2	2-14
2.6.1 California Santa Cruz User Story	2-14
2.6.2 California Santa Cruz Key Challenges.....	2-15
2.6.3 California Santa Cruz Policy Solutions and Implications	2-15

2.6.4	California Santa Cruz Technical Solutions and Implications	2-15
2.6.5	California Santa Cruz Governance Solutions and Implications	2-16
2.7	California Pilot: University of California San Diego and San Diego Health Connect Pilot of Use Case 1 and Use Case 2	2-16
2.7.1	California USCD User Story	2-16
2.7.2	California USCD Key Challenges	2-17
2.7.3	California USCD Policy Solutions and Implications	2-17
2.7.4	California USCD Technical Solutions and Implications.....	2-18
2.8	Oregon Pilot: Oregon Health Authority Pilot of Bidirectional Exchange, Use Case 1 and Use Case 2	2-19
2.8.1	Oregon User Story.....	2-19
2.8.2	Oregon Key Challenges	2-19
2.8.3	Oregon Policy Solutions and Implications	2-19
2.8.4	Oregon Technical Solutions and Implications	2-20
2.8.5	Oregon Governance Solutions and Implications.....	2-20
3.	Lessons Learned	3-1
3.1	Process	3-1
3.1.1	Workflow.....	3-1
3.1.2	Trust Bundles	3-2
3.1.3	Communication.....	3-2
3.1.4	Direct Functionality Still Emerging	3-3
3.1.5	Improved Implementation of C-CDA Standards	3-4
3.2	Policy 3-4	
3.2.1	Onboarding and Monitoring Participant PHRs	3-4
4.	Recommendations	4-1
5.	Glossary	5-1
Appendices		
A	Policies	A-1
B	PHR Onboarding Form	B-1

Figures

Number	Page
1-1. NATE PHR Pilot Data Flow Diagram	1-3
2-1. HIO Population of Trust Store with Updated Trust Bundle	2-6
2-2. PHR Population of Trust Store with Updated Trust Bundle	2-7

Tables

Number	Page
2-1. Use Cases 1 and 2 Scenarios	2-1

EXECUTIVE SUMMARY

The National Association for Trusted Exchange (NATE) was officially incorporated in May 2013 with a vision to develop a scalable trust and policy framework to overcome barriers inhibiting the use of health information exchange (HIE). The group was originally formed as the Western States Consortium (WSC) with support from the State Health Policy Consortium (SHPC) project funded by the Office of the National Coordinator for Health IT (ONC) and received support from RTI International. The initial project focused on setting up the governance framework and policy requirements needed to allow providers to exchange information across State lines for treatment purposes using Direct Secure Messaging. By the end of the ONC-supported period of the WSC project, California and Oregon had officially signed a Memorandum of Understanding (MoU), and all eight participating States had approved a set of common policies for trusted exchange via Direct Secure Messaging (Direct). Since the completion of the initial project in 2012, 10 States have signed the MoU and additional States are indicating interest.

After its initial success, NATE sought to expand its framework and begin testing its ability to support other forms of exchange. Acknowledging the importance of consumer-mediated exchange, the NATE Personal Health Record (PHR) Ignite pilot aimed to reuse the provider-to-provider trust framework and test the ability to establish trusted relationships with untethered¹ PHRs. This pilot was a vehicle for patients to send and receive data bidirectionally with providers in the trust framework via Direct. This report highlights the basic structure of the project and its processes and outcomes.

NATE developed consumer-mediated exchange Use Cases as part of the PHR Ignite pilot project to inform privacy, security, and operational policies for patient access and exchange using PHRs and to guide deploying a trusted mechanism to enable exchange across multiple States using PHRs. The pilot considered two Use Cases for the bidirectional data exchange using PHRs:

1. **Use Case 1.** Recruited providers send structured data to patients who use a patient-subscribed, NATE-qualified PHR using Direct Secure Messaging/BlueButton+ specifications.
2. **Use Case 2.** Test patients send data from their PHRs to a second provider using Direct Secure Messaging/BlueButton+ specifications.

¹ For the purposes of this project, untethered PHRs were referred to as applications that were not tied to any particular electronic health record (EHR) system, but remained capable of accepting and storing a patient's health-related data from any source. Because they are not provided on behalf of a Health Insurance Portability and Accountability Act (HIPAA)-covered entity, often these untethered PHRs are not required to adhere to the regulations set forth in the HIPAA Privacy and Security rules regarding the use of protected health information (PHI) as they would be if they were a HIPAA-covered business associate (BA). Although untethered PHRs can provide privacy and security controls that are equivalent to HIPAA's, because they are not required to do so, additional thought is required to establish trust with these entities.

The participants recognized considerable barriers to completing Use Case 2, including how to convey data provenance so the receiving provider would be able to trust the content received as if it had been sent directly from the originating provider. Initial questions posed by participants included (1) whether provenance is an essential component of creating trust between a patient and the provider receiving data from a PHR; (2) whether provenance should be stored in the metadata of the record being sent or as a separate artifact sent with the content; (3) what other content would be necessary to share; and (4) how to differentiate patient-generated health data from information sent directly by a provider, to inform the receiving provider's workflow.

Patient generated health data (PGHD) has many clinical uses but is typically treated differently than the legal record of a Continuity of Care Document (CCD) sent by another care provider, and is also treated differently in providers' data handling policies. Provenance and associated metadata are essential to identify PGHD.

Pilot testing these exchanges allowed the team to establish requirements of the trust framework and answer practical workflow questions. These questions included if providers would receive the information prior to establishing the individual as a patient and when to determine whether the information could be integrated into the patient's record maintained on a provider's local EHR system.

Two distinct sets of policies and procedures for establishing trusted relationships were created for both Use Case 1 and Use Case 2. The policies supporting Use Case 1 established a Provider to PHR (P2PHR) trust bundle, and those supporting Use Case 2 established a PHR to Provider (PHR2P) trust bundle. The NATE governing body reviewed and approved these policies for use in the pilot activity. Providers and patients in the participating pilot States of California, Alaska, and Oregon were recruited, and pilot activity began. Each pilot had a fundamentally different set of stakeholders and processes, but all were governed by the common set of policies and procedures, with the explicit intent of demonstrating that they were sufficient to establish scalable trust among all NATE participants. Following the completion of the PHR Ignite pilot activities, the NATE governing body will receive a report from the pilot team with recommendations regarding the outcomes of the pilot. This report may either result in a recommendation for continued piloting or the adoption of a NATE policy for consideration by all NATE participating States.

Lessons learned from the pilot project include:

- A better understanding of process issues, such as workflow considerations, and the implementation of the trust bundles and the essential work related to stakeholder communication required to grow the consumer-mediated exchange. The pilot teams were particularly interested in testing ways to include provenance information in the metadata for the record, which would allow the receiving physician to make better choices about how to integrate the content received into their existing workflow.

- A number of technology barriers that must be overcome for widespread activity using PHRs for HIE were identified, including the inconsistent implementation of Direct functionality in both EHR and PHR systems and the inability of many systems to produce and consume CCD information. The use of the Consolidated Clinical Document Architecture (C-CDA), which provides CCD information in a standard format and is required by the Meaningful Use Stage 2 certification criteria, is implemented even less consistently.
- Information regarding the policies around onboarding and monitoring PHRs involved in the trust bundles was acquired, specifically the manner in which privacy- and security-related policies are documented and shared with both NATE and with patients using the various applications.

1. INTRODUCTION AND BACKGROUND

1.1 Background on the National Association of Trusted Exchange

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 information technology (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 cooperative agreement support to States and/or State-designated Entities to establish basic health information exchange (HIE) capacity among health care providers and hospitals, while the SHPC supports multistate initiatives to develop solutions to policy challenges specific to interstate HIE.

With support from the SHPC, the National Association for Trusted Exchange (NATE) PHR Ignite pilot project convened in September 2013. NATE emerged from a pilot project known as the Western States Consortium (WSC), previously supported by SHPC, to enable scalable trust for interstate exchange between Health Information Service Providers (HISPs), and was established as a not-for-profit incorporated in Washington, DC on May 1, 2013. NATE participants understand the variability in regulatory exchange policies across State lines and have agreed to a defined set of trust parameters to achieve success in an interstate pilot environment. All agreed-upon pilot solutions are based on a nonregulatory structure (i.e., are voluntary on the part of HISPs) because some States do not have statutory authority to set policies and standards for acceptable uses of Direct exchange with PHRs or to ensure organizations participating within a HISP would be required to meet certain criteria at this time.

Under the PHR Ignite pilot project, the members of NATE were asked to expand the current set of policies and procedures enabling provider-to-provider exchange using Direct by adding policies and procedures allowing them to onboard and promote exchange between providers and patients using Direct-enabled personal health records (PHRs).

1.2 PHR Ignite Pilot Project

Empowering individuals to improve their health and health care through Health IT is one of ONC's strategic goals. With the growth in adoption of electronic records since the HITECH Act in 2009, data and systems to support patient empowerment through Health IT are becoming increasingly available and wide spread participation may soon be possible. Access to and use of this data enables patients to more actively participate in their own health care

decisions and serve as the central conduit for sharing their health information between providers who may use different electronic systems or are located in different geographic areas. This concept, often referred to as consumer-mediated exchange, not only allows patients to have more control of their health data, but also offers a simplified means of discovering patient privacy preferences.

The ONC Consumer eHealth initiative outlines objectives for patient engagement known as the "Three A's": Access, Action, and Attitudes, which include electronic access to health information, development of tools helping patients take appropriate action with their health information, and a shift in attitudes about the traditional roles of provider and patient empowered by the new information and tools. Under Stage 2 Meaningful Use criteria, certified EHRs are required to support the use of Direct Secure Messaging to enable the exchange of summary data for transitions of care. This functionality is intended to allow data to flow between health care providers, but also may be used to exchange information with the patient through Direct-enabled PHRs that could receive and collect information in a single location controlled by the consumer.

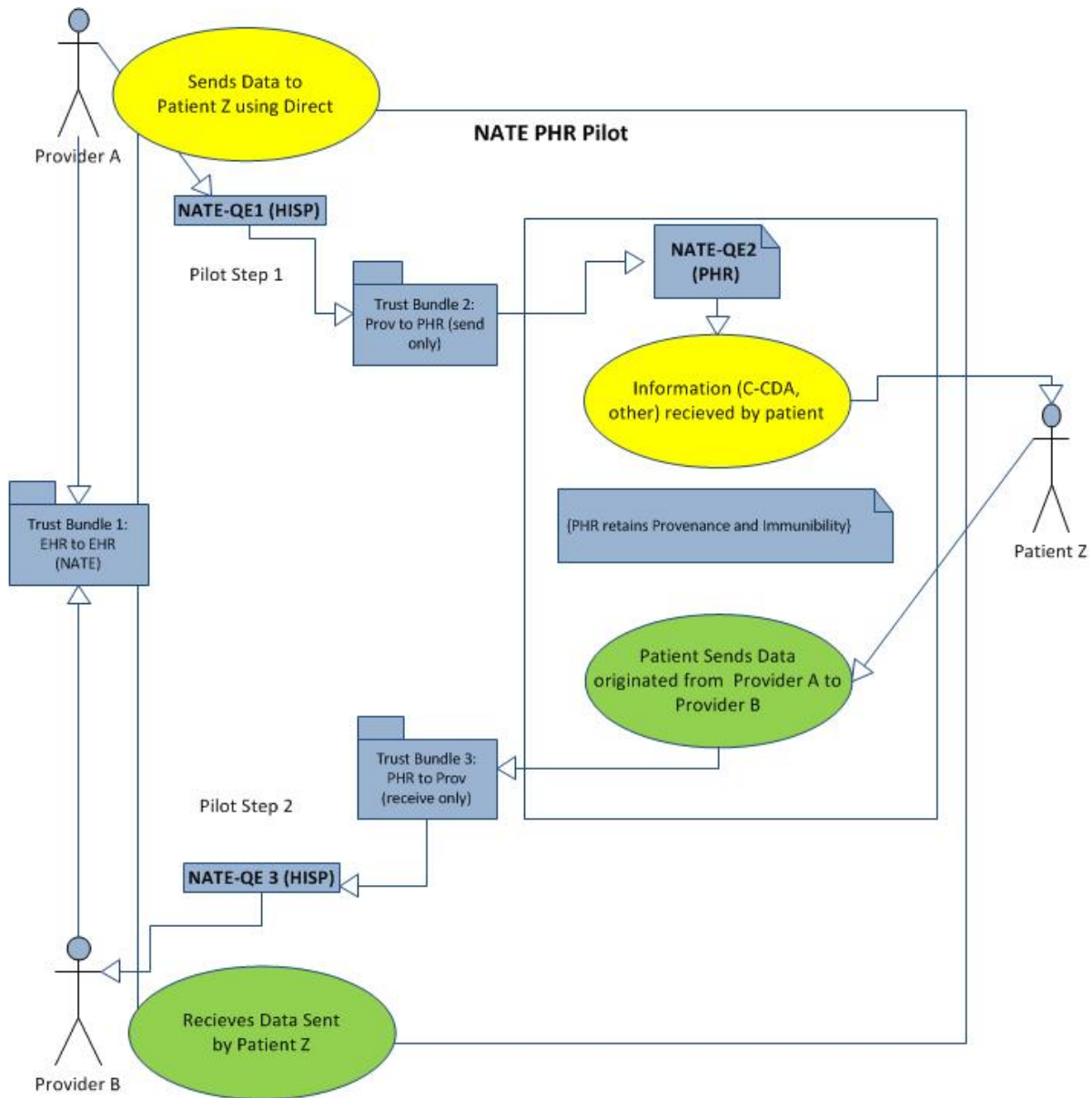
The purpose of the NATE PHR Ignite pilot project was to explore and implement Use Cases, data flows, and required mechanisms to facilitate the bidirectional sharing of data where (1) a provider is the originator and (2) where the PHR is the originator of data and the provider is the receiver of data. The pilot was also intended to outline policy, governance, and technical issues related to data exchange between end users of HISPs who are members of a NATE Trust Community and untethered PHRs used by patients. NATE member States Alaska, Oregon, and California participated in the pilot.

The pilot project aims were to enable wider use of PHRs to exchange data between patients and providers. The pilot considered two Use Cases for bidirectional data exchange involving PHRs:

1. Use Case 1: Recruited providers send structured data to a patient-subscribed NATE-qualified PHR using Direct Secure Messaging/BlueButton+ specifications.
2. Use Case 2: Test patients send patient data from their PHR to a second provider using Direct Secure Messaging/BlueButton+ specifications.

Figure 1-1 shows the pathways of exchange as conceived by members of the NATE project at the outset of the project. In the diagram, a provider attempts to send data to a patient through a HISP that has already been onboarded as a NATE-qualified entity (NATE-QE). The data are accepted via the NATE trust bundle to a PHR system that has also been onboarded using the PHR policies and procedures developed through the pilot. After receiving the structured data, the patient determines a need to send this information to a new provider, which is accomplished by sending a Direct message delivered via a HISP that has been onboarded as a NATE-QE.

Figure 1-1. NATE PHR Pilot Data Flow Diagram



The pilot was designed to:

- Develop a trust mechanism, known as a trust bundle, to facilitate determining trust on the part of NATE participants interested in exchanging data with a PHR source.
- Identify and establish minimum technical, security, and privacy requirements for untethered PHRs participating in the pilot and trust bundle(s).
- Identify and engage PHR vendors and providers as they provide consumers with access to their data via Direct-enabled exchange.
- Identify barriers to bidirectional patient information exchange.

The pilot established five participant groups:

- Alaska Pilot—The Alaska eHealth Network (AeHN) collaborated with Microsoft HealthVault and private providers to send clinical records from providers to the patient's HealthVault account, and with the Department of Veterans Affairs (VA) to use VA patients' HealthVault accounts to send clinical records from outside physicians to their VA providers who view the data via AeHN accounts created for the pilot.
- California Humetrix Pilot—Humetrix (<http://www.humetrix.com>) worked with San Diego Health Connect (<http://www.sdhealthconnect.org/>) and the VA using My HealthVet (MHV) PHR to transmit medical data to its iBlueButton (<http://www.ibluebutton.com/>) mobile application. Veterans receiving care through the VA or San Diego health care providers used their mobile phones to receive and manage health records from different providers.
- California Santa Cruz Pilot—The Santa Cruz HIE (SCHIE) (<http://www.santacruzhie.org/>) worked with three area provider organizations to deploy the NoMoreClipboard patient portal on behalf of 500 patients so they can exchange demographic and clinical data. The pilot project built on infrastructure for an HIE-wide patient portal.
- California University of California San Diego (UCSD) Pilot—UCSD and San Diego Health Connect collaborated with Microsoft HealthVault (<https://www.healthvault.com/us/en>), DELPHI, and CitiSense to make environmental data, including air quality and weather information, available to asthma patients.
- Oregon Pilot—The Oregon Health Authority (<http://www.oregon.gov/OHA/Pages/index.aspx>) facilitated a pilot to electronically exchange health information between a pediatric patient-centered primary care home and parents of chronically ill children using CareAccord® (<https://www.careaccord.org/>) and the patients' free PHR, Microsoft's HealthVault.

California's pilots were funded by American Recovery and Reinvestment (ARRA) funding allocated to California.

Each participant group became a member of the NATE trust community and installed the appropriate PHR trust bundle(s) to send and/or receive PHR data and the provider-to-provider trust bundle for treatment purposes. Each pilot organization populated its trust store with appropriate trust bundles.

The eligibility criteria for inclusion in NATE's PHR trust bundles were designed to engender trust among all parties, including providers on the patient care team who would need to trust the information sent to them from their patients' PHRs. NATE's work outlined in the policy section (Sections 2.1 and 2.2 of this report) demonstrates the development of a set of policies and procedures enabling PHR2P and P2PHR Direct exchange without requiring multiple business associate agreements (BAAs) between those HISPs in a pilot environment.

1.3 NATE Governance Structure

Over the past several years momentum has been building for the use of Direct to facilitate HIE between health care providers with known, trusted relationships. As Direct was

implemented across the country, it became clear that trusted relationships between HISPs had to be brokered by a neutral party—typically the State HIE program leaders. However, questions remained about scalable exchange and exchange between States, as each sought to develop “trust anchors” establishing a baseline of operational requirements specific to their State laws and HIE policies. NATE’s first SHPC-funded project, the WSC, developed a Governance Body and a set of policies and procedures. These policies and procedures generated the provider-to-provider for treatment purposes trust bundle (P2P4Tx) that allows HISPs in participating States to exchange Direct Secure Messages without proliferation of one-to-one BAAs.

The NATE Governance Body oversees NATE Party State² activities related to trust between HISPs and directory services. The NATE Governance Body consists of a designated representative from each of the member States; each State has committed, via a Memorandum of Understanding (MoU), to abide by the NATE-approved policies and procedures. The premise of the MoU between States is to ensure that before any HISP is allowed to participate in the trust community, the State where the HISP is operating must attest that the HISP meets the eligibility requirements as established in the policies and procedures.

In brief, the topics addressed by the NATE policies included requirements that a participating HISP must:

1. Conform to all Direct project requirements and specifications.
2. Implement a BAA³ to contract with their participants.
3. Have contractually binding legal agreements with their participants.
4. Demonstrate conformance with industry standard practices to meet privacy and security regulations for both technical performance and business processes.
5. Minimize data collection, use, retention, and disclosure.
6. Encrypt all edge protocol communications.⁴
7. Have a process to verify the identity of authorized end users.

² 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 described in the MoU.

³ 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 NATE Governance Body will evaluate this consideration in the future if a true conduit model HISP is identified by a member State.

⁴ The term “edge protocols” refers to the communications between a HISP that provides transport of Direct messages to other organizations, and the client—an e-mail client, Web portal, or EHR—used by a human authorized user to read and send messages.

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).

The Governance Body also indicated they preferred but did not require HISPs to enable Direct Project's External Data Representation Standard (XDR) and display manager (XDM) specifications for Direct exchange.⁵

Additional obligations applying to the participating HISP, their participating organizations, and the authorized users of their HISP services are spelled out in the NATE policies and procedures. These obligations are analogous to the requirements of participation agreements in many operational HISPs, 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.

This concept of governance is both distinct and complementary to other initiatives that broker trusted exchange for Direct, such as HISP accreditation. NATE facilitates a multistate governance structure that provides a review process to ensure that HISPs included in the larger trust bundle follow baseline requirements that ensure trusted exchange. In recognition of the variance in applicable State law, additional requirements beyond the baseline are allowable. In the case of Direct-based exchange, NATE attempts to reuse requirements between Use Cases as often as possible to make common criteria, such as transport requirements, consistent and create technical interoperability.

These common criteria are not unique to NATE's trust bundles and conformance from complementary efforts, such as Direct Trust, might be relied upon in future as validation that a given HISP satisfies some of the eligibility criteria for a NATE trust bundle. NATE would like to minimize the burden on HISPs to repeatedly prove compliance with common requirements. Although work remains to be done to support the reuse of accreditation from accrediting bodies such as EHNAC (Electronic Healthcare Network Accreditation Commission), member States should not need to revalidate a HISP's ability to meet or exceed the NATE criteria if they have demonstrated this capability as part of a previously received accreditation. They may need to demonstrate HISP compliance with additional criteria to enable exchange within the NATE trust bundle.

1.4 NATE PHR Ignite Pilot Technical Infrastructure

The NATE PHR pilot scenarios were supported by a thin technical infrastructure which is robust enough to assure conformance to governance policies and enable secure and trusted exchange of health information between unaffiliated providers and organizations. This infrastructure comprises:

⁵ The XDR and XDM can be found at the Direct Project wiki:
<http://wiki.directproject.org/XDR+and+XDM+for+Direct+Messaging>

1. Secure transport—standards-based information exchange methods supporting provider needs and Use Cases.
2. Scalable trust—an approach to identifying exchange partners who meet criteria for trusted exchange established by NATE without requiring one-to-one agreements between each participating party, thus making a common set of trust principles scalable to a large number of parties.

Membership in the NATE trust community is established technically by a trust bundle—the collection of trust anchors for all entities that have been vetted and officially onboarded by a Party State to form a trust community. To enable communication with provider-centric HISPs participating in the pilot, NATE used the P2P4Tx trust bundle agreed upon by the NATE community.⁶ This bundle defines a process to manage and distribute the collection of trust anchors, which supports exchange between providers using NATE-qualified entities that have been onboarded by a Party State. 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 member HISP retrieves the trust bundle and installs its contents into its trust anchor store, enabling bidirectional exchange with all trust community members.

The NATE PHR Ignite pilot developed two additional trust bundles to enable communication with PHRs: the NATE Provider to PHR (P2PHR) bundle for PHRs capable of receiving data (PHR Receiver bundle) and the NATE PHR to Provider (PHR2P) bundle for PHRs capable of sending data (PHR Sender bundle).

1.5 Pilot Assumptions and Agreements

As NATE PHR pilot participants determined options to enable PHR Direct exchange, the group reviewed, expanded, and reaffirmed initial assumptions with all participants. This level of transparency was essential to ensure the group focused discussion and debate on unresolved issues.

One issue deemed out of scope for the project was an effort to suggest how providers use the data once received. Although the objective was to find solutions that would allow a provider to distinguish patient self-generated data from a record generated through another provider, the group recognized that each facility receiving content via Direct will have different data handling policies. Having the appropriate metadata to inform the interaction with the local EHR was essential, although it could be handled in different ways based on a receiving provider's workflow. For example, some data handling policies allow for inserting protected health information (PHI) generated by another provider into the medical record

⁶ For more information on the Provider to Provider for Treatment Purposes trust bundle, please reference the Western States Final report. Banger, A., Rizk, S. C., Bailey, R. F., Cartland, P., Mayer, L., Sommers, R. et al. (2013, September). *Western States Consortium ONC state health policy consortium project: Final report*. Prepared for Office of the National Coordinator for Health IT (ONC). <http://www.healthit.gov/sites/default/files/wscfinalreport.pdf>

associated with the patient, while patient-reported outcomes must be reviewed with the patient before they are inserted into the provider's EMR. The pilot sought to report on how improvements to metadata included in the record might affect provider workflow in the future, but did not seek to direct this interaction as part of the initial pilot phase.

The final project assumptions were as follows:

1. The PHR pilot will be conducted among NATE Party States that volunteer to participate, to inform recommendations for future expansion to all NATE Party States based on pilot experiences.
2. Individuals who release data (senders) are bound by the laws in the sender's State (e.g., consent requirements). Individuals who receive data (receivers) are bound by the receiver's State laws regarding access to and use of the data.
3. The pilot project is intended to explore and implement Use Cases, data flows, and required mechanisms to facilitate bidirectional data sharing where (1) a provider is the originator of data and the PHR is the receiver, and (2) where the PHR is the originator of data and the provider is the receiver. The pilot is also intended to outline policy, governance, and technical issues related to the exchange of data between end-users of HISPs that are members of a NATE trust community and non-HIPAA (untethered) PHRs.
4. Provenance information will be preserved at the level it was obtained by the individual PHRs in the pilot, recognizing that differences between PHRs exist regarding the level of granularity at which provenance is maintained. The pilot will research methods for representing these differences in a way that allows receiving providers to incorporate the incoming data into their existing work flow.
5. Participants will investigate adding an attachment to include provenance metadata about the content being sent. Participants will consider items that characterize the content as unchanged from the original author, annotated by the patient, or entirely generated by the patient. Additional items regarding workflow and use of the content by the receiving provider will also be considered.
6. The PHRs selected for the pilot will be untethered, or not controlled by a HIPAA-covered entity through a BAA.
 - a) The distinction between tethered and untethered is determined by whether the PHR is required to adhere to HIPAA Privacy and Security regulations (tethered) or not (untethered), not by whether the patient can add or import information from other sources.
 - b) For the purposes of the pilot, tethered PHRs are defined as those that only include data from the sponsoring covered entity. A HIPAA-covered entity can offer a PHR solution that accepts multiple data sources, such as NoMoreClipboard or Microsoft HealthVault, via a BAA. In this case, the issues of privacy, security, and trust are standardized because the PHR is bound to adhere to all requirements defined by HIPAA. To test the robustness of the policies under the trust bundle, the NATE PHR Ignite pilot will specifically focus on scenarios where the PHR application is untethered, and not subject to HIPAA requirements.
7. A PHR application will be created with onboarding requirements for all participating PHR vendors.

8. Providers will be responsible for binding direct addresses (creating the relationship between the patient's identity in their EMR and the Direct address of the patient associated with their PHR) to the individual before sending data to or receiving data from a patient. Participants will use recommendations for identity proofing provided in the Health IT Policy Committee Tiger Team.⁷
9. NATE will develop a trust bundle to facilitate the determination of trust on the part of NATE participants interested in exchanging information with a PHR source during the pilot.
10. Pilot participants will identify and establish minimum technical, security, and privacy requirements for untethered PHRs participating in the pilot and trust bundle.
11. Pilot participants (teams of health information organization [HIO] and PHR vendors) will recruit and support providers as they provide consumers using the participating PHRs with access to their data via Direct-enabled exchange.
12. Pilot participants will identify barriers to bidirectional patient information exchange.
13. Patients without established care relationships will not be included in the pilot.
14. Assumptions for the sending of data under Use Cases 1 and 2:
 - a) In Use Case 1, recruited providers will send structured data to a patient-subscribed, NATE-qualified PHR using Direct Secure Messaging/BlueButton+ specifications.
 - b) In Use Case 2, recruited providers will agree to receive structured data from a patient-subscribed, NATE-qualified PHR using Direct Secure Messaging/BlueButton+ specifications.
 - c) Patients⁸ have the right to access their information from all their treating providers and to send that information to others, including different providers.
 - d) NATE will enable exchange by establishing a trust bundle of participating PHRs, similar to that created under the BlueButton+ initiative, which satisfies the eligibility criteria established by the pilot participants.
 - e) The NATE trust bundle will require a unique outbound message address (i.e., once issued, Direct addresses must not be reused).

⁷ http://www.healthit.gov/facas/sites/faca/files/hitpc_transmittal_050313_pstt_recommendations.pdf

⁸ The eligibility of minors or other specially protected individuals was uncertain at the outset of the pilot and participants assumed that the pilot could be expanded to consider these patients' use cases as well, based on the providers recruited.

2. PILOT PLANNING, IMPLEMENTATION, AND IMPLICATIONS

Table 2-1. Use Cases 1 and 2 Scenarios

Use Case	Scenario
1	Recruited providers send structured data to a patient-subscribed, NATE-qualified PHR using Direct Secure Messaging/BlueButton+ specifications.
2	Test patients send data from their PHRs to a second provider using Direct Secure Messaging/BlueButton+ specifications.

2.1 Piloting Use Case 1: Provider to Patient PHR

2.1.1 Policy Solutions and Implications

The proposed policy solutions created a baseline set of policies that all pilot participants would use, test, and provide feedback on to improve and finalize them for wider use within the NATE participating States. These policies enable trust among all NATE participants and avoid requiring individual trust agreements between HISPs. This section summarizes the NATE pilot policy on Eligibility Criteria for P2PHR for NATE-QEs. The P2PHR policy used during the pilot activities is available in **Appendix A**.

Policies for Determining Eligibility for P2PHR Exchange

The purpose of the P2PHR policy was to define uniform processes and establish the framework by which Party States vet and promote a new NATE-QE that meets the definition of a PHR so that it may become a part of the NATE trust community. Once completed, this process would enable the flow of information from a NATE-QE already established as a trusted exchange partner under the existing P2P4Tx trust bundle (provider HISP) and a PHR, allowing participating providers to send PHI to patients using Direct-enabled PHRs.

Draft eligibility criteria of a NATE-QE for the P2PHR policy used under the pilot project included:

1. NATE-required Direct project security and trust components:
 - a) All NATE-QE (P2PHR) candidates must demonstrate adherence to the baseline requirements for the pilot.
2. Obligations of participating NATE-QE (P2P4Tx) for this Use Case:
 - a) HIOs participating in this pilot must be NATE-QE (P2P4Tx) entities.
3. Obligations of the NATE-QE (P2PHR) to patients:
 - a) The pilot will evaluate whether the PHR vendor discloses in its service agreement (including privacy notice and other artifacts) how governance decisions are made to users regarding but not limited to the following issues:

- i. Release of PHR data (personal data) for (1) marketing and advertising; (2) medical and pharmaceutical research; (3) reports about the company and customer activity; (4) the insurer and employer; and (5) the development of software applications.
 - ii. Release of PHR data (statistical data) for (1) marketing and advertising; (2) medical and pharmaceutical research; (3) reports about the company and customer activity; (4) the insurer and employer; and (5) the development of software applications.
 - iii. Whether limiting agreements that restrict what third parties can do with the personal data are required.
 - iv. Whether release of personal data is stopped if the PHR is closed or transferred.
 - v. How security measures are provided that are reasonable and appropriate to protect personal information, such as PHR data, in any form, from unauthorized access, disclosure, or use.
 - vi. Whether PHR data is stored in the United States only.
 - vii. Whether PHR data activity logs are kept for users to review.
 - viii. How the uniqueness of an assigned message address is ensured, and whether assurance is given that it will never be assigned to another user, even after an account is closed.
4. Obligations of the provider/entity sending the message to the patient upon their request:
- a) Provider to follow identity verification requirements for the individual requesting disclosure as defined locally and in compliance with HIPAA and State law.
 - i. The Privacy Rule requires covered entities to verify the identity and authority of a person requesting PHI, if not known to the covered entity. See 45 C.F.R. § 164.514(h).
 - ii. If the patient is known to the provider and a record of care is established, the verification of the requestor's identity is subject to local policy prior to the disclosure (e.g., request might be made in person, using photo ID).
5. Rights and responsibilities of the patient:
- a) In addition to capturing information about patients' rights and responsibilities, participants will document the constraints placed on patient recruitment for inclusion in this pilot and the related policy reasons for excluding any specially protected patients such as minor children or wards of the State.

2.2 Piloting Use Case 2: Patient PHR to Provider

2.2.1 Policy Solutions and Implications

Use Case 2 policy focused on capturing and providing details about the privacy and security functions of PHRs included in the trust bundle for patients, allowing them to make better informed decisions. However, the policy that would allow the PHI to flow back from the

patient's Direct-enabled PHR to a new provider created some questions that were not easy to answer before the pilot, including:

- **Provenance and immutability.** An advanced aspect of the pilot was to establish the mechanisms by which the provenance and immutability of content exchanged between a NATE-QE (PHR2P) untethered PHR solution and a NATE-QE (P2P4Tx) HIO could be operationalized. It was unknown at the outset whether this would involve obligations on part of the PHR or the HISP or a combination of both. A key objective of the pilot was to begin the process of discovery on how best to achieve this at the document level on behalf of a patient.
- **Onboarding process.** NATE attempted to determine if a single NATE-level evaluation process is acceptable to vet PHRs for inclusion in the trust bundle or if variance in applicable State law requires an alternate approach.

This section provides a summary of the NATE pilot policy on Eligibility Criteria for PHR2P for NATE-QEs. The P2PHR policy used during the pilot activities is available in its entirety in **Appendix A**.

Policies for Determining Eligibility for PHR2P Exchange

The purpose of the PHR2P policy was to define uniform processes and establish the framework by which Party States vet and promote NATE-QEs that meet the definition of a PHR into the NATE trust community, which would enable the flow of information from a PHR established as a NATE-QE to a trusted exchange partner under the P2P4Tx trust bundle. The PHR2P policy allows the loop of consumer-mediated exchange to be fulfilled in its entirety, allowing providers to not only receive PHI from their patients using Direct-enabled PHRs but that the content in a patient's PHR originating from another unaffiliated provider is trustworthy. This is essential for receiving providers to rely on the information as if it came directly from the original source (i.e., the provenance is known and the data from the PHR is unchanged since the patient received it from the unaffiliated provider).

Draft eligibility criteria of a NATE-QE for the P2PHR policy used under the pilot project included:

1. NATE required Direct project security and trust components:
 - a) All NATE-QE (PHR2P) candidates must demonstrate adherence to the baseline requirements for the pilot.
2. Obligations of participating NATE-QE (P2P4Tx) for this Use Case:
 - a) HIOs participating in this pilot must be NATE-QE (P2P4Tx) entities.
3. Obligations of the NATE-QE (PHR2P) to patients:
 - a) The pilot will evaluate if the PHR's service agreement (with Privacy Notice) must disclose how governance decisions are made to its participants in its participant agreement regarding but not limited to the following issues:
 - i. Release of PHR data (personal data) for (1) marketing and advertising; (2) medical and pharmaceutical research; (3) reports about the company

- and customer activity; (4) the insurer and employer; and (5) the development of software applications.
 - ii. Release of PHR data (statistical data) for (1) marketing and advertising; (2) medical and pharmaceutical research; (3) reports about the company and customer activity; (4) the insurer and employer; and (5) the development of software applications.
 - iii. Whether limiting agreements⁹ that restrict what third parties can do with the personal data are required.
 - iv. Whether release of personal data is stopped if the PHR is closed or transferred.
 - v. How security measures are provided that are reasonable and appropriate to protect personal information, such as PHR data, in any form, from unauthorized access, disclosure, or use.
 - vi. Whether PHR data is stored in the United States only.
 - vii. Whether PHR data activity logs are kept for users to review.
 - viii. How the uniqueness of an assigned message address is ensured, and whether assurance is given that it will never be assigned to another user, even after an account is closed
4. Obligations of the provider/entity receiving the message from the PHR upon the patient's request:
- a) What, if any, functional acknowledgement back to the PHR should be supported? How can it be supported with existing technologies? What are the barriers if any?

2.3 Technical Solution for Use Cases

The technical solutions for the pilots focused on mechanisms to overcome one-off trust agreements and trust anchor exchange for consumer-mediated exchange via untethered PHRs. The technical solutions proposed for both Use Case 1 and Use Case 2 focus on the creation of trust bundles as described below.

2.3.1 Facilitate Trust Anchor Distribution Via Trust Bundles

A trust bundle is a collection of trust anchors for each HISP that is onboarded to NATE. This bundle can be retrieved by all HISPs that have completed onboarding. It is used to distribute the trust anchors of all onboarded and participating HISPs, as additional HISPs onboard to or are removed from the NATE trust community and trust profile, or to update their certificates. This enables trust between the various HISPs without requiring trust anchor exchanges between any two individual participants. Trust anchor exchange between each participant leads to the creation of an exponential number of one-to-one agreements,

⁹ Limiting agreements are legally binding agreements that prohibit certain third parties, which are not the PHR company's service providers, from releasing a patient's personal data or re-identifying individuals. Third parties can include advertisers, researchers, and others who receive PHR data.

which is not scalable for widespread Direct adoption. NATE has adopted the new Implementation Guide for Trust Bundle Content and Distribution to distribute all trust anchors through trust bundles, and participated in the pilot for that new standard.

The process of implementing trust bundles in Use Case 1 follows the steps listed below:




















1. A HISP supplying Direct Secure Messaging services to a provider is included in the P2P4Tx trust bundle, which originally established scalable trust between providers to exchange information.
2. Under the P2PHR or “PHR Receiver” Bundle, a separate trust bundle established for this pilot, the participating PHR system’s trust anchor is added.
3. The HISP in step 1 loads the P2PHR trust bundle, trusting its anchors for sending.
4. The PHR installs the P2P4Tx trust bundle, trusting its anchors for receiving.
5. Trusted exchange from a HISP to a PHR is established for all parties included in the trust bundle.

While Use Case 1 establishes the mechanism to support a “push” of information to the patient’s PHR, Use Case 2 establishes the foundation for trusted, scalable bi-directional exchange in which the consumer mediates the movement of data from one provider to another. The implementation process follows the steps listed below:

1. A HISP supplying Direct Secure Messaging services to a provider is included in the P2P4Tx trust bundle, which originally established scalable trust between providers to exchange information.
2. Under the PHR2P or “PHR Sender” Bundle, a separate trust bundle established for this pilot, the participating PHR system’s trust anchor is added.
3. The HISP in step 1 loads the PHR2P trust bundle, trusting its anchors for receiving data from a PHR.
4. The PHR installs the P2P4Tx trust bundle, trusting its anchors for sending.
5. Trusted exchange from a PHR system to a HISP is established for all parties included in the trust bundle.















Figures 2-1 and 2-2 provide a visual representation of how these trust bundles can be used to create scalable exchange across state borders, with the entities involved in the NATE PHR Ignite pilot project serving as examples. In Figure 2-1, each checkmark indicates a trust bundle that must be successfully loaded by the pilot HIO entity to enable the receipt of information from all entities included in the trust bundle. The cloud icon indicates that the entity is included as a member of the trust bundle itself. In this scenario, AeHIN (Alaska), CareAccord (Oregon), SCHIE (California) and SDRHIE (California) can all share information bi-directionally using Direct from provider to provider, as shown in column one. By loading both the P2PHR and the PHR2P trust bundles as shown in columns two and three, their providers are now able to send information to PHR systems in the trust bundles, and receive information as well.

Figure 2-1. HIO Population of Trust Store with Updated Trust Bundle

Entity	1  P2P4Tx	2  P2PHR "Receiver"	3  PHR2P "Sender"
 AeHN	 Bundle Member Bundle Loaded	 Bundle Loaded	 Bundle Loaded
 Care Accord	 Bundle Member Bundle Loaded	 Bundle Loaded	 Bundle Loaded
 SCHIE	 Bundle Member Bundle Loaded	 Bundle Loaded	 Bundle Loaded
 SDRHIE	 Bundle Member Bundle Loaded	 Bundle Loaded	 Bundle Loaded

In Figure 2-2, each PHR system included in the pilot (Humetrix, NoMoreClipboard, and HealthVault) is able to receive information from participating HIOs after a) loading the P2P4Tx trust bundle as shown in column one which provides indication of which HIOs are trusted by NATE, and b) being added to the NATE P2PHR trust bundle, as shown in column two, indicated by the cloud icon. Both NoMoreClipboard and HealthVault are able to participate in the sending of data back to the providers associated with the HIO since they are part of the PHR2P trust bundle as shown in column three. Humetrix is not included in the P2PHR trust bundle at this time because they have not implemented functionality through their application to submit data to outside sources. Both the receipt and sending back of data to an HIO from a trusted PHR is predicated on the assumption that the P2PHR and PHR2P trust bundles have been loaded by the participating HIOs as shown in Figure 2-3.

Figure 2-2. PHR Population of Trust Store with Updated Trust Bundle

Entity	1  P2P4Tx	2  P2PHR "Receiver"	3  PHR2P "Sender"
 Humetrix	 Bundle Loaded	 Bundle Member	
 NoMore Clipboard	 Bundle Loaded	 Bundle Member	 Bundle Member
 HealthVault	 Bundle Loaded	 Bundle Member	 Bundle Member

2.4 Alaska Pilot: Alaska eHealth Network Bidirectional Exchange Pilot of Use Case 1 and Use Case 2

2.4.1 Alaska User Story

The State of Alaska and the Alaska eHealth Network (AeHN) executed a pilot of consumer-mediated exchange using the Microsoft HealthVault PHR.

Two Use Cases were tested:

1. Sending CCDs from provider to PHR—Managed by AeHN
2. Sending CCDs from provider to PHR and PHR to receiving provider—Managed by Health IT coordinator

The following entities participated:

- Alaska eHealth Network—HIE and Direct HISP
- Microsoft HealthVault—PHR vendor
- LaTouche Pediatrics—Use Case 1 sending provider to participant’s PHR using Allscripts Professional version 13 and the AeHN Direct Secure Messaging portal
- Full Spectrum Pediatrics—Use Case 1 sending provider to participant’s PHR using e-MD version 7.2 and the AeHN Direct Secure Messaging portal

- Allergy, Asthma, and Immunology Center of Alaska—Use Case 2 sending provider to participant’s PHR using Allscripts Professional version 9.2.2 and the AeHN Direct Secure Messaging portal
- Veterans Administration—Use Case 2 receiving provider receiving CCD from the participant’s PHR using the AeHN Direct Secure Messaging portal
- Various urban pediatric patients recruited by AeHN—Using Microsoft HealthVault

2.4.2 Alaska Key Challenges

1. No providers were able to access the AeHN Direct solution from within their EHRs. The sending providers had to export the document to their desktops then attach it to the message in the AeHN Direct Secure Messaging portal.
2. The LaTouche Pediatrics EHR encrypted the file when it was exported to the desktop; however, no key for decryption was initially provided to Microsoft HealthVault, rendering the file unusable at the PHR. Further conversation with the EHR vendor revealed the ability to decrypt the file and send it using the Direct Secure Messaging portal. The CDA from this method was imported successfully.
3. Microsoft HealthVault could not use the CDA exported from the full spectrum EHR without editing to conform to the C-CDA specification. The patient was unwilling to grant permission for someone to manually edit the file, and it was not imported.
4. The original Allergy, Asthma, and Immunology Center’s EHR version sent a Continuity of Care Record (CCR) that Microsoft HealthVault could not use without editing to conform to the CCD specification. A manually edited version was successfully provided and used. Subsequently, the provider upgraded to Allscripts Professional version 13 and sent a CCD that HealthVault could use.
5. The VA did not have its own Direct solution and used the AeHN Direct Secure Messaging portal.

2.4.3 Alaska Technical Solutions and Implications

Use Case 1: AeHN Comments

Mothers at LaTouche Pediatrics participating in Use Case 1 were well versed in technology and browsers and had no trouble accessing the Web, HealthVault, and Direct. However, LaTouche physicians were less savvy. In both cases, even though staff from AeHN had spent time previously training physicians, they had to retrain the physician office staff. In one office, the physician had a staff person who was previously trained on Direct but left. AeHN trained the new staff member. In the other case, the staff knew how to use the system but the physician did not.

The technical functionality available in the EHR systems used in the pilot was also problematic. Both EHRs in the pilot were able to send CCDs. However, neither CCD was in the standard C-CDA format. The Allscripts file was encrypted, which required a key to open it. Pilot project staff successfully sent two records to HealthVault after Allscripts was upgraded and the staff were shown how to send an unencrypted C-CDA. This process was

not straightforward, however, and required many calls and e-mails to Allscripts and Microsoft during a 1-month period.

The Alaska pilot project staff were never able to import the CCD exported from the eMDs EHR system because of additional problems with the software version used at the physician's office. The physician's office was reluctant to upgrade or make changes at this time. AeHN staff continue to work with the physician and plan to assist with further tests.

Use Case 2

The Health IT coordinator in Alaska was used as the test case to pilot Use Case 2. The coordinator had previously downloaded BlueButton information from the VA system using MyHealthVet and sent to his HealthVault account in 2011, 2012, and 2013 using an AeHN Direct mailbox. He also sent a MyHealthVet CCD file to his HealthVault record. His HealthVault record also included some self-entered information. As part of the pilot Alaska Allergy sent both a CCR and a CCD to the Health IT coordinator's HealthVault account. The coordinator used the HealthVault functionality to send a CCD and HTML version of the CCD from HealthVault to a VA provider. The HealthVault data was not filtered using any of the filters Microsoft provides in the application. The coordinator also sent the Alaska Allergy CCR and a PDF version of the CCR to the VA provider using Direct. The coordinator reviewed the documents with the VA provider in a face-to-face meeting. Since the VA EHR cannot import a CCD, the review was accomplished by the VA printing out the human-readable versions of the HealthVault and Alaska Allergy CCDs.

VA Comments

The VA noted that the CCD data from the HealthVault account was of little value because (1) it included too much information, and (2) it did not contain provenance. Regarding the amount of information, the practitioner at the VA stated, "The consolidated HIE view of the integrated record is what is needed. Getting bits and pieces is very difficult to interpret. Even if the allergy CCR information was succinct and easy to read, collecting and integrating that information from several CCRs at the same time will be very difficult and could potentially lead to error in and of itself." Regarding provenance, the VA felt that they needed to know the source of the data in the C-CDA (i.e., which information was patient-generated, lab-generated, from an in-home monitoring device, or from another provider).

The VA further noted that the CCR provided from Alaska Allergy was more valuable because it was from a known source and it contained less irrelevant data. The VA indicated that the relevant information from Alaska Allergy was the medication list and the problem list.

Health IT Coordinator Comments

The Health IT coordinator commented that most of the information in the HealthVault CCD that was of little value came from the VA in the various BlueButton files that had been

previously downloaded. This issue may have resulted from the quality of the information in early versions of the VA BlueButton file. The HealthVault account holder can filter CCD information to include/exclude information types (immunizations, lab test results, etc.) or by a date range. The amount of data returned could potentially be mitigated in the following ways:

1. Veterans could be directed and shown how to limit the queries to the information that the VA would like to receive.
2. HealthVault could allow the ability to filter the CCD created to exclude certain data sources.
3. HealthVault could provide a VA-specific CCD that would exclude VA-originated information.

The issue of provenance needs further exploration, as this pilot was unable to determine a viable solution for storing and maintaining that information in the file metadata. The outcome of this Use Case revealed more insights about why the VA is currently unable to receive consolidated information through this method. This Use Case failed because (1) the VA's EHR was unable to use a CCD and (2) the data could not be filtered to remove information that the receiving provider originally created.

2.5 California Humetrix Pilot: San Diego Health Connect and VA Transmit Medical Data to iBlueButton Mobile Application Pilot of Use Case 1

2.5.1 California Humetrix User Story

Humetrix worked with San Diego Health Connect (SDHC) and the VA to explore Use Cases, data flows, and required mechanisms to facilitate sharing data in one direction, where the provider is a data originator and the PHR/iBlueButton iPhone application is the data receiver. This pilot tested the Use Case using two different transmissions:

- Use Case 1a: Transmit BlueButton C-CDA to the iBlueButton application. SDHC participating providers at the UCSD Health System sent patient data in a structured format (a C-CDA XML file) from the UCSD EPIC EMR system to the patient iBlueButton application using the Mirth Mail service (the HISP), demonstrating that providers could send a transition of care (ToC) C-CDA file to iBlueButton using Direct.
- Use Case 1b: Transmit a Blue Button VA C32-CCD from MHV to the patient iBlueButton application using the new "transmit" function of the MHV portal that uses the Direct protocol. As described below, this could only be done using sample data in a test environment as the MHV portal is not yet live.

2.5.2 California Humetrix Key Challenges

The Humetrix team working with UCSD encountered the following challenges:

- The CCDs produced by MHV and by the EPIC EMR system at UCSD do not presently fully conform to the HL7 C-CDA standard and differ significantly.
- The UCSD EPIC EMR system does not allow a physician to produce a CCD for a patient and export it to the physician's desktop, nor does it enable a physician to use Direct to transmit a CCD to a patient-specified endpoint such as the one provided by the iBlueButton application.
- The MHV Direct service has not yet moved beyond a test environment preventing live patient testing as planned.
- Humetrix determined that there was no single X.509 root certificate acceptable to the Department of Defense (DoD), VA, NATE, and the BlueButton+ trust bundle because of current DoD policies that require the use of an external certification authority (ECA) component certificate that chains back to a DoD root certificate.
- Defining a mutually acceptable BAA between Humetrix and SDHC recognizing that Humetrix is not a covered entity under the HIPAA omnibus rule.

2.5.3 California Humetrix Technical Solutions and Implications

The iBlueButton application was customized to use the new BlueButton+ standards to enable users to receive C-CDAs sent via the Direct protocol directly on their mobile devices for Use Cases 1a and 1b. The pilot study analyzed technical barriers in configuring the data originator and data receiver systems for Direct exchange and successfully completed test exchanges for both Use Cases. Pilot test accomplishments are described below.

Humetrix and SDHC successfully tested transmitting a sample C-CDA CCD from SDHC Mirth mail service to the iBlueButton application after both Humetrix and SDHC/Mirth mail systems were provisioned with NATE P2P4Tx and NATE P2PHR trust bundles, respectively.

Humetrix recruited a UCSD physician and patient volunteers (including a veteran receiving care at both the San Diego VA and UCSD Health Systems) to successfully conduct a live pilot of transmitting patient data (a C-CDA CCD) produced by the UCSD Health System EPIC EMR system to the iBlueButton application.

This live pilot was successfully completed on January 15, 2014. In this pilot, the recruited patient downloaded to her iPhone a pre-release build of the Humetrix iBlueButton application made available exclusively to her for this pilot. This version of the iBlueButton application enables a user to create multiple accounts (one for each family member who gave permission). During this visit with her UCSD physician (who also cares for her husband and for whom the patient has documented health care power of attorney in the UCSD EMR system), the following steps were completed:

1. The patient and the physician together logged into the UCSD EPIC MyChart patient portal.

2. They downloaded her C-CDA summary medical record and the C-CDA summary record for her husband, a veteran also receiving care at the San Diego VA Health System.
3. The UCSD physician successfully logged in to the assigned Mirth mail account used for this pilot.
4. The physician attached the patient's C-CDA, and sent the C-CDA to the patient's Direct address (previously assigned to the patient by the iBlueButton application).
5. The C-CDA was successfully delivered to the patient's iBlueButton application under her profile, and properly displayed using the style sheet Humetrix had prepared for this Use Case.
6. The physician sent her husband's C-CDA using Mirth mail and the husband's Direct e-mail address, also provisioned by the iBlueButton application under a separate profile created for her husband.
7. The record successfully arrived under the correct profile in the patient's iBlueButton application, and displayed as expected.
8. The patient used the iBlueButton application to successfully download, parse, and display her own Medicare BlueButton record.

Humetrix and the VA successfully tested transmission of a MHV sample CCD from the VA Direct test environment to the iBlueButton application after manual exchange of X509 certificates to provision Humetrix and the VA Direct implementations. For this test exchange, Humetrix provided the VA with the iBlueButton certificate in the BlueButton+ production patient trust bundle. When the VA can provide an operational MHV pre-production testing environment (now scheduled for February 2014), Humetrix and the VA will test the iBlueButton application first using sample CCDs to be followed by testing with live patient data (with this patient's husband along with other veterans).

Humetrix also successfully conducted a test exchange of Tricare Online (TOL) CCDs after provisioning the Humetrix Direct Server with a DoD certificate provided for this test. For this test (conducted with Booz Allen Hamilton, TOL contractors), Humetrix acquired and installed an Operational Research Consultants (ORC) ECA component certificate required by the DoD and successfully received and displayed a sample CCD from TOL preproduction DoD/VA Direct as a service using the same Humetrix-optimized style sheet for display of C-CDAs in the iBlueButton application.

Solutions to each of the key challenges enumerated in Section 2.5.2 are described below.

- **The CCDs produced by MHV and by the EPIC EMR system at UCSD do not presently fully conform to the HL7 C-CDA standard and differ significantly.** Humetrix optimized two separate style sheets for mobile display of these respective records, which are automatically launched by the iBlueButton application when the files are received so that CCDs produced by MHV, EPIC, Cerner, WebChartMD, and TOL systems are all properly displayed in human-readable form when transmitted by Direct to the patient's smartphone iBlueButton application. Humetrix also developed

a new iBlueButton application summary record view that aggregates medications, conditions, allergies, and immunization data from the Medicare BlueButton record and from parsed C-CDA/CCD produced by MHV, the UCSD EPIC EMR system, as well as C-CDA CCDs, which conform to the HL7 standard (EMERGE and Cerner C-CDAs obtained from https://github.com/chb/sample_ccdas).

- **The UCSD EPIC EMR system does not allow a physician to produce a CCD for a patient and export it to the physician’s desktop, nor does it enable a physician to use Direct to transmit a CCD to a patient-specified endpoint such as the one provided by the iBlueButton application.** As a result, live testing during this pilot required that the physician and patient together access the MyChart EPIC patient portal using the patient’s login credentials, export a zip file to the physician’s desktop, and then select a CCD and attach it to a Direct message using the web-based SDHC Mirth mail service to transmit the file by the Direct Protocol to the patient’s iBlueButton application.
- **The MHV Direct service has not yet moved beyond a test environment preventing live patient testing as planned.** Humetrix has continued to work with the VA beyond the term of this pilot and at the time of this writing has successfully tested the iBlueButton application as a receiver of CCDs transmitted by Direct from the MHV pre-production environment, which will be demonstrated at the February 2014 Health Information Management Systems Society (HIMSS) annual conference interoperability showcase.
- **Humetrix determined that there was no single X.509 root certificate acceptable to DoD, VA, NATE, and the BlueButton+ trust bundle because of current DoD policies that require the use of an ECA component certificate that chains back to a DoD root certificate.** After consultation with TOL, Humetrix acquired the DoD required ECA component certificate from ORC, a U.S. Government ECA. Humetrix then successfully conducted testing of transmitting a TOL CCD to the iBlueButton application once manual exchange of certificates with TOL Direct server was put in place.
- **Defining a mutually acceptable BAA between Humetrix and SDHC recognizing that Humetrix is not a covered entity under the HIPAA omnibus rule.** Overcoming this challenge required negotiation with SDHC, which is obligated under its own rules to sign a BAA with every entity with which it exchanges PHI. This was ultimately resolved by crafting language for a BAA that made it clear that Humetrix, as a nontethered PHR, was not a business associate of SDHC and not a HIPAA-covered entity as defined by the HIPAA omnibus rule.

The results of this pilot demonstrate that this customized iBlueButton application can give veterans a mobile application with a robust consumer-mediated exchange solution for patients receiving care from both the VA health system and from private health systems. The iBlueButton application allows veterans to securely receive, display, store, and transmit MHV and Medicare BlueButton records as well as C-CDA CCDs generated by EMR systems (including the EPIC EMR system used at many U.S. private hospital systems). Beyond this specific Use Case, the pilot also demonstrates that iBlueButton-enabled exchange can be either implemented directly by providers participating in a regional HIE that provides access to a Direct mail service, such as Mirth mail, or through making available to patients a

Meaningful Use Stage 2 certified patient portal with view/download/transmit (VDT) functionality.

2.5.4 California Humetrix Governance Solutions and Implications

Humetrix reviewed the California Medical Information Act (CMIA: Cal. Civ. Code § 56.06(a)) and the 2014 CMIA updated law (Cal. Civ. Code § 56.06(b)), which imposes the same restrictions on PHRs that exist for health care providers with regard to maintaining the confidentiality of PHI and prevents the unauthorized use of PHI without the express consent of the individual concerned. Humetrix's legal counsel, a recognized expert on HIPAA requirements, conducted this review to ensure that the iBlueButton application was in compliance with this law. Humetrix attested to compliance with all applicable Federal and State laws to PHRS in the NATE onboarding form which can be found in Appendix A, Section A.1.

The California NATE board approval of the inclusion of the iBlueButton application certificate in the NATE P2PHR Trust bundle should help facilitate other HIEs and provider organizations in California enable patients and caregivers to use the iBlueButton to receive, store, and manage their health records once iBlueButton has been released for public use (scheduled for February 2014) through iTunes and Google Play application stores.

2.6 California Santa Cruz Pilot: Santa Cruz HIE Bidirectional Exchange Pilot of Use Case 1 and Use Case 2

2.6.1 California Santa Cruz User Story

The objective of this pilot was to identify and attempt to overcome technical and policy challenges of bidirectional transport of patient health data between end users of HISPs that are members of a NATE trust community and patient-owned PHRs. The PHR used for the pilot was connected to the HIE, allowing access to various sources of clinical data to the patients in the HIE system.

Operationally, the participants needed to establish a production HISP-to-HISP connection between SCHIE and NoMoreClipboard to enable Direct transactions. This connection was based on BlueButton+ guidelines. The pilot also developed and implemented the policies, workflow processes, and education required to support electronic exchange between participants using the patient portal and participating providers.

SCHIE and Orange County Partnership Regional Health Information Organization (OCPRHIO) worked together to onboard three or more OCPRHIO end users for request and delivery of patient health information to patients from Santa Cruz. SCHIE plans to expand the pilot to onboard 10 or more licensed clinical users and 100–12,500 patients (maximum permitted under this license) in the near future to test the full functionality of the PHR/HIE connection.

Using Direct functionality provided through NoMoreClipboard.com allowed information to flow from the PHR system to the locations selected.

The PHR enables patients and others to use the cc: Me module. This module allows users to create a unique cc: Me web address where physicians and other providers can post CCDs that the PHR can use. Patients can use the embedded FroozHIE¹⁰ data comparison and reconciliation tool to selectively import properly formatted C-CDA data into the PHR. Patients also have the option of auto-reconciling incoming CCD data so that new data automatically populates the PHR account.

2.6.2 California Santa Cruz Key Challenges

The following were seen as the biggest challenges for implementing both Use Cases in the Santa Cruz pilot:

1. Defining the requirements of NATE policies for trusted exchange and how to technically implement those policies.
2. Defining how health information is exchanged from PHR to EHR while safeguarding the integrity of the health information.
3. Integration challenges for PIX PDQ delivery to PHR from HIE.

2.6.3 California Santa Cruz Policy Solutions and Implications

SCHIE has comprehensive security policies and processes in place as part of their HIE operation. SCHIE is compliant with Federal and local laws on electronic HIE and adheres to the principles of HIE for the demonstration projects.

2.6.4 California Santa Cruz Technical Solutions and Implications

SCHIE worked with OCPRHIO and NoMoreClipboard to establish a HISP-to-HISP connection enabling providers and patients to exchange health information bidirectionally for the California Office of Health Information Integrity (CalOHII) pilot. SCHIE and NoMoreClipboard are active participants in Direct exchange and production-level deployment of BlueButton+. The pilot set up a SCHIE patient portal for the Santa Cruz area with linkages to NoMoreClipboard.

- SCHIE and NoMoreClipboard successfully tested and transmitted Direct messages from SCHIE Mirth Mail Service to the NoMoreClipboard PHR cc: Me using Direct protocol after both systems were provisioned with NATE trust bundles.
- SCHIE has recruited three organizations and 10+ providers. SCHIE and NoMoreClipboard have provided organizations with demonstrations that show the NoMoreClipboard functionality and module options, providing demos from physician

¹⁰ Information about FroozHIE can be found on the NoMoreClipboard wiki: https://www.nomoreclipboard.com/wiki/Main_Page

experience using dashboards and work lists as well as patients' view of NoMoreClipboard PHR (demonstrations are still occurring and training is ongoing).

- SCHIE is conducting a live pilot of transmission of patient data (C-CDA) produced by EHR to NoMoreClipboard PHR. Testing was completed in January 2014 and production is ongoing.
- SCHIE is also testing patient data C-CDA produced by HIE to NoMoreClipboard PHR.
- Pilot participants will recruit three patients from each organization.
- SCHIE will be testing PHR functionality on iPad mobile devices (testing is now underway with current NoMoreClipboard format; however, NoMoreClipboard is developing display configurations for mobile devices).
- SCHIE is working with participants to setup kiosks in the participants' waiting room. Staff will be able to assist patients with their NoMoreClipboard PHR registration process. Providers will send C-CDA to patients' NoMoreClipboard cc:Me using Direct e-mail protocol. Patients can then be shown how to view and consume the C-CD and to prepopulate their NoMoreClipboard health record. Patients can verify information, make edits, and submit. Patients will also learn how to submit and/or reply to their physician from their PHR account.

2.6.5 California Santa Cruz Governance Solutions and Implications

SCHIE complied with NATE onboarding requirements and regulations. NoMoreClipboard onboarded with NATE, and also complies with California laws and regulations, including laws for minors. SCHIE also complies with all State and Federal regulations, including laws for minors and updated law requirements for PHRs.

2.7 California Pilot: University of California San Diego and San Diego Health Connect Pilot of Use Case 1 and Use Case 2

2.7.1 California UCSD User Story

UCSD worked with SDHC to test and demonstrate secure and reliable bidirectional transport of patient data between end-users of NATE community HISPs and patient-owned PHRs using information from asthma patients. Patients with uncontrolled asthma often require acute treatment with multidose inhalers (MDI). Many times these patients go to the emergency department because of acute exacerbations. UCSD developed the following story line to guide the pilot test of exchange.

A UCSD Health System patient sees her medical provider because of asthma complications. The patient's provider recommends two new devices that may help her control her asthma. One device is the commercially available Propeller Health (previously Asthmopolis) MDI counter, to monitor her rescue inhaler usage. The other is an environmental air quality monitor developed by UCSD called CitiSense to continually monitor the patient's surrounding air quality. The EMR used by the provider has a tethered PHR but it does not currently accept device data from outside sources. Therefore, the provider also recommends

the patient register for a Microsoft HealthVault account, which has device data integration capability.

A CCD of the patient's medical record is created for her and exported to her HealthVault account. She uses the devices for the following month. Initially, she finds the devices interesting and often checks on the information available to her, but soon becomes distracted and uses them less often. During this period, her asthma is uncontrolled and she uses her rescue inhaler often.

Because the patient's asthma continues to be a problem, she makes another appointment with her primary care provider. Prior to the appointment, she sends the device data to her provider through her HealthVault account. The provider and patient review the summaries that incorporate both environmental air quality data and MDI usage information to identify any patterns. They find that the air quality at a coffee shop she frequents near her workplace is not optimal for an asthmatic. The air quality is also less than optimal at the frequently visited home of a friend who smokes. MDI data show that the inhaler is used more often when she visits these locations. With this new information, the patient decides to find a new coffee shop for her morning coffee. Her friend tries to quit smoking and makes sure to smoke outside, away from the patient, when she does smoke. Thereafter, realizing how these data can help improve her asthma control, she continually checks the data available to her so she can take control of her own health.

2.7.2 California USCD Key Challenges

The key challenges in the UCSD pilot centered on system and data interoperability as well as data aggregation and visualization of MDI utilization and environmental data (geohealth data) in a way that is meaningful. The initial plan included full integration of MDI count data from the Propeller Health device for a seamless patient experience. However, because of competing company priorities, this could not be accomplished during the pilot period. Therefore, patient data entry was required to include these data elements. Also, interoperability between the CitiSense data server and the Microsoft Azure cloud posed several unexpected issues such as standardizing exchange messages and aggregating the exchange messages into the Azure cloud. Finally, developing a meaningful visual summary incorporating environmental data and MDI utilization data was also challenging.

2.7.3 California USCD Policy Solutions and Implications

The UCSD pilot project did not directly deal with policy solutions or implications because it used commercially available applications. Our subjects signed individual agreements with HealthVault and Propeller Health. As active patients within the UCSD Health System, they had existing tethered PHR (UCSD MyChart) accounts and their medical records were readily available for the pilot. Also, because the UCSD Health System is a participating member of SDHC, the providers have active Direct accounts. The environmental air quality data was

not considered PHI and therefore exempt from HIPAA regulations. Lastly, our institutional review board (IRB) deemed this a quality improvement project exempt from IRB review.

2.7.4 California USCD Technical Solutions and Implications

The technical solutions used for this project were all existing technologies and services that were not integrated.

EPIC was the EMR used to construct the patient CCD that was imported into HealthVault, which was the patient's PHR. The CCD included the patient's medications, allergies, problem list, and encounter data. HealthVault consumed and displayed the CCD data in a patient-friendly format. Using HealthVault, a Direct account (<http://directproject.org>) was established for the patient and connected with the provider's Direct account within SDHC, the regional HIE. An initial "hello" message was used for verification between the two accounts.

The mobile devices included CitiSense environmental sensor and Propeller Health's MDI counter. CitiSense was developed at UCSD to track specific environmental air quality data. Data are acquired every 6 seconds and uploaded to a server for aggregation and export. Propeller Health's MDI counter is an independent, commercially available acute asthma monitoring device (<http://propellerhealth.com>). Patients accessed their Propeller Health data on their proprietary Web page, which was also made available to the patient's provider. The summary of MDI utilization included the number of times it was used and the geolocation. Both the CitiSense and Propeller Health devices transmit data independently via Bluetooth to the patient's smartphone.

Environmental data from the CitiSense server was exported to SDHC's Microsoft Azure cloud via XML using an automated process. Patients manually entered their MDI usage from the Propeller Health summary report into their HealthVault account. These data were aggregated and displayed on a Microsoft Bing map. The summarized data were transformed into a JPG and sent to the patient's HealthVault account based on patient preferences. The message from the Microsoft Azure cloud to Microsoft HealthVault was sent as both an XML message and later as a Direct message. Once in HealthVault, the summary was available to be pushed from the HealthVault account to the provider via a Direct message from the patient.

This pilot demonstrated the ability for a user to send messages to their provider that incorporate device and environmental data in a secure platform using Direct messaging. This was accomplished using existing applications such as EPIC, HealthVault, SDHC, and commercially available environmental air quality tracking and health monitoring devices.

2.8 Oregon Pilot: Oregon Health Authority Pilot of Bidirectional Exchange, Use Case 1 and Use Case 2

2.8.1 Oregon User Story

The Oregon Health Authority worked with a small pediatric practice to identify an individual patient to test receiving and sending of health information using Microsoft HealthVault. The patient is being treated for *Osteogenesis imperfecta* (OI), sometimes known as brittle bone disease, or Lobstein syndrome, a congenital bone disorder characterized by brittle bones that are prone to fracture. People with OI are born with defective connective tissue, or without the ability to make it, usually because of a deficiency of Type-I collagen.

The patient used in the pilot also sees a specialist in Nebraska and frequently sees another physician in the same practice. The patient uses e-mail at least monthly to communicate with the pediatric case manager for the practice via the tethered portal, to update the clinic about any changes in prescribed medications made by the specialist in Nebraska and to request a referral. In addition, the patient is seen for normal well-child visits. The patient's mother wanted the appointment and referral documentation sent to HealthVault, and to be able to exchange X-rays and other images with both providers.

2.8.2 Oregon Key Challenges

The key challenges in the Oregon pilot centered on system and data interoperability. Initially, the EHR system-created CCD/C-CDA was not in a format that could be imported seamlessly into the patient's PHR record. This was brought to the attention of the EHR vendor who directed the provider to open a "defect ticket" and create an official record of the issue so the EHR vendor's technology team could work on a solution. The short-term solution was for the PHR vendor to fix the CCD/C-CDA by manually modifying the output of the XML document once received to conform with the standard to allow the document to be imported into the patient's PHR record. Although this solution works on a small-scale, short-term basis, the longer-term solution is for all parties to align with the CCD/C-CDA standard. The EHR vendor's ability to implement a solution during the pilot is uncertain. Interoperability between the HISP used by the provider and the HISP used by the patient's PHR was straightforward and was achieved seamlessly.

2.8.3 Oregon Policy Solutions and Implications

Policy issues were not addressed specifically in the Oregon pilot. Because Oregon's consent model is "opt out at the point of encounter," all patients and caregivers are given the opportunity to allow electronic transmission of their data at each encounter. The Oregon pilot scenario was demonstrated in a pediatric patient-centered medical home (PCMH) model of care delivery so the issues and barriers of patient access to information and providers have been removed thanks to the certification requirements for PCMHs (<http://www.ncqa.org/Programs/Recognition/PatientCenteredMedicalHomePCMH.aspx>).

Oregon's pilot was limited to a primary site that is certified as a PCMH; therefore, policy examination and development may be needed to address concerns of patient access and exchange of data in other care settings.

2.8.4 Oregon Technical Solutions and Implications

The technical components of the Oregon HIE used for the pilot are based on established and emerging national standards. The primary components are as follows:

- EHR System—Allscripts
- PHR System—Microsoft HealthVault
- Transport Standard—Direct (SMTP/SMIME) using Mirth mail
- Provider directory (not a primary focus of the user story)—Mirth provider directory with Health Provider Directory Plus (HPD+) support

These technical solutions will allow for consumer-mediated bidirectional exchange of information between a patient/care giver and that patient's care team.

During the procurement, implementation, and operational phases of the Oregon HIE system, the focus has been on providing solutions that adhere to established national standards and support emerging and new standards as they are adopted. This forward-compatibility approach will serve Oregon's health care constituents for many years to come.

2.8.5 Oregon Governance Solutions and Implications

Oregon's HIE and Health IT governance is provided by a government-led, public/private partnership through the Oregon Health Authority for both policy and operations, with a contracted vendor (Harris Corporation) for the CareAccord Program. The initial decision was to fully use the State Cooperative Agreement funding provided by ONC to maximize the potential of Medicaid funding (Oregon Health Authority is the Medicaid Agency for Oregon) and enhance the likelihood of coordination between the HIE efforts and the Medicaid EHR Incentive Payment programs. The Health Information Technology Council (HITOC) coordinates Oregon's public and private statewide efforts in Health IT. HITOC is supported by the Office of Health Information Technology (OHIT). The HITOC recommended Oregon designate a public/private, nonprofit entity to take on statewide HIE governance and operational duties at a future time. Currently, Oregon participates as a member State of NATE, and the CareAccord HIE solution is Direct Trusted Agent Accreditation Program (DTAAP) accredited.

3. LESSONS LEARNED

The goal of the NATE PHR Ignite pilot project was to enable the wider use of PHRs as a vehicle for patients to bi-directionally exchange health data with their providers and inform privacy and security policies as well as operational policies to scale the growth of trusted exchange with patients across the nation. This chapter describes lessons learned throughout the project by participants. These lessons are categorized under major headings of process and policy.

3.1 Process

3.1.1 Workflow

Considerable workflow issues were encountered, which should be expected when piloting a Use Case new to the domain. For the purposes of the pilot, customized short-term workarounds to enable the exchange were needed to facilitate execution of the pilot's Use Case. Two key areas where NATE needed to establish guidance around workflows were (1) information receipt by providers and (2) workarounds related to processing the C-CDA-like content received by the PHRs. Major workflow issues included:

- Provenance: By and large, the pilot projects confirmed that provenance of data is important to providers receiving data from external PHR systems or providers. Each of the pilot participants who worked with participating practices reported that because the receipt of data from patients via this mode was new to the practice, updates to data receipt policies were required. Practice staff wanted to be readily able to differentiate incoming messages containing content unmodified from another provider versus patient-annotated or patient-created data since existing data receipt workflows were driven by this differentiation. Although methods of signaling the source of the data would facilitate workflow, it was noted that no EMRs in place today would be able to automatically process incoming messages based on it.
 - *Lesson learned*—There is a need to establish metadata standards to integrate patient-mediated data with provider's operational workflows.
- Data format: Most EHR systems deployed today are not producing C-CDAs formatted in accordance with the standard as C-CDAs were not part of the certification criteria for the version of EHRs encountered during the pilot. Additional work needs to be done in this area to prevent the additional workflow steps participants need to understand if PHRs are to be widely used.
 - *Lesson learned*—The market is still migrating to content standards that can be used interoperably, but the expectation is that as legacy systems are replaced with certified solutions this issue will dwindle.
- Patient identity management: Providers participating in the pilot were comfortable associating a patient with their Direct address and relying upon the Level of Assurance (LOA) established by the PHR selected by the patient.
 - *Lesson learned*—Providers are accustomed to their role in establishing the identity of their patient and comfortable binding the patient's chosen Direct address within their EMR, but providers assume that patients who select PHRs

have made informed decisions about the security and privacy provisions of selected PHRs. There is a role to be played in the community to ensure that patients understand the pros and cons associated with different security and privacy alternatives available in the market.

3.1.2 Trust Bundles

- **Implementation:** No problems were reported with the distribution or implementation of the trust bundles themselves, further validating the ability for trust bundles to support a framework for governing scalable trust and widespread HIE functionality using Direct Secure Messaging for this Use Case.
 - *Lesson learned*—Trust bundles can support scalable trust for a Use Case where the trust community agrees to the policy representations made by the bundle.
- **Reported advantage of bidirectional exchange:** Providers reported that there was perceived benefit in both directions when the patient was able to make disclosure decisions on his or her own behalf. When the patient pushed data to other providers independent of the practice, providers felt this allowed each patient to determine what was sensitive from their perspective, relieving them of a complex responsibility. They also reported that when receiving data originally generated by another provider from a patient, the receiving provider had fewer concerns about whether disclosure of sensitive data was authorized by the patient.
 - *Lesson learned*—Patient-mediated exchange may be especially instrumental in overcoming barriers to exchanging sensitive data in the typical provider-to-provider world. This advantage is only realizable when trustworthy EMRs and trustworthy PHRs can exchange bidirectionally via a mechanism such as a trust bundle.

3.1.3 Communication

- **Educational materials:** Educational materials are needed for both patients and providers to accelerate the realization of patient-mediated exchange. A common myth among providers is that enabling bidirectional exchange with patients will generate significant volumes of unwanted messages, while patients are unclear about how their caregivers will use the information they share with them.
 - *Lesson learned*—
 - Both providers and patients could benefit from additional explanatory material about what to expect and how best to use this new option for engaging with one another. We believe that the following will prove valuable to the experience of both providers and patients that leverage this capability in the future:
 - Address the gap in metadata standards related to patient reported data (see recommendations).
 - Support providers in the development of data receipt policies to include electronically reported data originating from Direct-enabled PHRs.
- Encouraging practices to share this policy with the patient. **Value to providers:** Stakeholders must be kept informed and must be engaged with exchange and interoperability activities, especially those that set policy on the care delivery side. A driving force behind the pilot was to enable Use Cases that demonstrate the value

that consumer-mediated exchange has for the future of HIE for both the patient and the provider community.

- *Lesson learned*—The pilot helped establish a small but growing pool of physicians and patients who can speak to the benefits of patient-mediated exchange to help inform the public, providers, and policy makers about this critical HIE vehicle.
- Patient safety value: Patients' interest in obtaining and managing their own health data in electronic format is expected to increase rapidly as use of EHRs become standard. Although projects such as this one can provide a technical and policy framework that enables patients to play a central role in managing health data, it is imperative to find Use Cases of value to providers so at the point of care they will encourage patients to participate in consumer-mediated exchange. It is also imperative to inform the public of the patient safety benefits of consumer-mediated exchange to accelerate adoption, provider acceptance and participation.
 - *Lesson learned*—Although providers are still warming to the idea of implementing patient-mediated exchange in their practices and are looking for information to make an informed decision, patients also need to be made aware of their rights and the tools available to them to access and exchange their health information. When a consumer is able to produce verified health record information for a treating physician who may not have a pre-established exchange relationship with other providers caring for the patient, the treating provider has more accurate and complete information on which to base a treatment decision. They are better able to avoid adverse drug reactions, reduce duplicate tests, and make more informed assessments based on previous diagnoses or treatments. A message delivered by some of the providers to consumers about the safety benefits to their children was effective. When parents saw this exchange as a safety benefit for their children, they were motivated to act.

3.1.4 Direct Functionality Still Emerging

- Direct functionality still emerging: In many cases, pilot participants were unfamiliar with using Direct secure transport functionalities, or they needed to upgrade their EHR systems to gain Direct functionality. Protocols and solutions for using Direct are still not widely available or in practice within the Health IT industry. However, since this technology helps providers meet Meaningful Use Stage 2 certification for EHR systems, it will likely be more widely used in the near future.
 - *Lesson learned*—There is an opportunity to refine policies and procedures related to patient-mediated exchange so that as Direct capability become more ubiquitous, common approaches and expectations developed in these early stages are encouraged as best practices at the provider level.
- Technologists are still learning to implement Direct: Some providers that recently adopted Direct as a mode of exchange followed encryption practices that made the data deliverable but inaccessible to the PHR receiving the data. This occurred when content was encrypted with a key not associated with the Direct Account of the sender before it was transmitted. During the pilot the vendor was educated on how to modify their procedures to align with the Direct method of exchange so that the receiving PHR could access the content where appropriate.
 - *Lesson learned*—Certification of Direct capabilities for EHRs should ensure that content being delivered can be accessed by receiving system.

3.1.5 Improved Implementation of C-CDA Standards

- Interoperable content still wanted: The production of and ability to consume a standard C-CDA is immature in many EHR and PHR systems. The PHR applications used in this pilot are considered quite advanced and are all capable of receiving and parsing well-formatted C-CDA data; nevertheless, certain technical barriers emerged, some of which the pilot participants were not able to overcome. From the EHR side, a number of issues occurred because EHR system-created contents were not in a standard format that could be imported seamlessly into the patient's PHR.
 - *Lesson learned*—Simply being able to make content from one system accessible to another is not sufficient to enable interoperability.
- Content validators would help: There is a need for a validator implementation of C-CDA standards as well as any future content standards that may develop over time to fit specific clinical needs (such as prenatal care).
 - *Lesson learned*—Sincere best efforts to comply with the content standard are not sufficient to support interoperability and a validator is important to both the generator and potential consumer of exchanged content.

3.2 Policy

3.2.1 Onboarding and Monitoring Participant PHRs

- Model privacy notice is a good start: Although the onboarding processes for the pilot PHRs worked well, considerable communication is needed about the expectations related to privacy and security, particularly with untethered, non-HIPAA-covered PHRs. The project team determined that NATE's responsibility is not to dictate which PHR systems are "more secure" than others; patients have the right to choose which PHR best suits their needs. However, the privacy and security policies of any PHR systems included in the NATE trust bundle must be clearly stated, published, and maintained so that both patients and providers have an easy-to-understand reference for this information. The ONC Model Privacy Notice served as a starting point for discussions about which items should be captured and published, although it quickly became clear that additional considerations were needed, especially for bidirectional exchange to occur.
 - *Lesson learned*—There is a demand for a trust bundle that meets the practical needs of the patient and industry that the pilot's policies inform, but additional input from a broader group of stakeholders is required before expectations of common reliance is achieved.
- Taxonomy wanted: It is important to agree to a common terminology to have successful discussions about implementation, especially related to policy and legal issues.
 - *Lesson learned*—There is further need to contribute to a common taxonomy in this emerging domain to facilitate broader acceptance and contributions from across the community.

4. RECOMMENDATIONS

NATE member States support and look forward to continuing their multistate governance approach to increase interoperability, decrease the cost and complexity of Direct exchange, increase trust among participants, foster consumer-mediated exchange, and mobilize exchange to support patient care.

Considerable work must be done to reinforce and build on the work that NATE has accomplished. Member States will benefit from repeated testing and deployment as more HISPs become engaged in PHR-to-EHR exchange and as more providers begin to use Direct exchange services across different State environments.

The list of potential issues for NATE's future attention with respect to PHR exchange includes the following:

1. **Improve PHR and EHR vendors' implementations of Direct and support both providers and patients in using the functionality for improved patient-mediated exchange.**

Although the expansion of Direct secure transport has not yet achieved critical mass with providers, it seems certain to do so in the near future, as Meaningful Use Stage 2-compliant systems continue to roll out over the next year. An important confluence of work that mutually benefits PHR and EHR vendors would focus on a standard that conveyed provenance of data from PHRs to EHRs. NATE is continually open to including new EHR and PHR vendors in future phases of this work.

2. **Improve the ability of providers and patients to use exchanged data by supporting standards that improve workflow.** The ability to send and receive data is only useful to the recipients if the information is easy to understand and use. Improving these functionalities in the EHR and PHR systems alone will not solve the problem. As these pilots indicated, considerable workflow issues remain that often require manual or short-term workarounds to make data useful. We recommend that a concerted activity dedicated to establishing the metadata standards be leveraged to include both EHR and PHR vendors. The pilot participants intend to continue to collaborate and inform the requirements in relation to metadata produced by PHRs regarding provenance.

3. **Support the creation of standards and a 'validator' system for the ability to parse data in C-CDAs.** The current NIST template within certification is not robust enough to enable the degree of interoperability needed to support patient-mediated exchange.

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 NATE strategies for PHR Direct exchange fit within the context of other HIE methods currently in practice around the country. Although collaboration is often challenging for States because of time demands and staff shortages, ONC or other convening organizations may consider a mechanism, such as a series of in-person meetings or Webinars, to highlight programs and other multistate projects similar to NATE to support shared learning of these lessons.

5. GLOSSARY

CCD—Continuity of Care Document. Establishes a rich set of templates representing the typical sections of a summary record, and expresses these templates as constraints on Clinical Document Architecture (CDA) using an implementation guide for sharing Continuity of Care Record (CCR) patient summary data using the HL7 version 3 CDA, Release 2.

CDA—Clinical Document Architecture. A document markup standard that specifies the structure and semantics of "clinical documents" for the purpose of exchange between health care providers and patients. Typical CDA documents would be a Discharge Summary, Imaging Report, Admission & Physical, Pathology Report, and more.

C-CDA—Consolidated CDA. Defined by HL7 as a single source for implementing the multiple CDA documents, including CCD, discharge summary, and many others. Provides a common architecture, coding, semantic framework, and markup language for the creation of electronic clinical documents. CDA documents are coded in Extensible Markup Language (XML).

CA—Certificate Authority. 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, it 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.¹¹

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

PHI—Personal health information

PKI—Public key infrastructure, aka PKI certificates

Push model—A model of HIE where data are sent from one provider to another provider upon request, rather than through a query submitted to a larger network.

Query-retrieve model (aka "pull" model)—A model of HIE 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.

¹¹ <http://wiki.directproject.org/file/view/DirectProjectOverview.pdf>

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—A 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 CA's identity assurance, authentication, security) established by an umbrella governance organization that 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:
POLICIES**



Subject: NATE-QE Eligibility Criteria for: Provider to PHR (P2PHR)		Policy #: 3.c.3	
Status: Pilot Profile Pending Pilot States Approval		Approved/Authorized By: WORKING DOCUMENT	
Date Approved:	Effective Date:	Version: 0.2	Pages:

I. Purpose

The National Association for Trusted Exchange (NATE) has responsibility for establishing uniform processes by which Party States may evaluate entities within their state (such as HIOs or PHRs) to determine if they satisfy the eligibility criteria to be recognized as NATE Qualified Entities (NATE-QEs). NATE provides mechanisms by which such NATE-QEs may be added to the NATE Trust Community thus enabling trusted exchange across states where states accept the criteria and agree to rely on the evaluations performed by other member states. The purpose of this NATE-P&P is to define uniform processes and establish the framework by which ‘Party States’ vet and promote NATE-QEs that meet the definition of a Personal Health Record (PHR) into the NATE Trust Community in order to enable the flow of information from a NATE –QE (P2P4Tx) to a NATE–QE (P2PHR), allowing relying Providers to send PHI to their patients utilizing Direct-enabled PHRs.

Key Goals of Pilot

- Finalize and pilot the eligibility criteria for inclusion of PHRs in the P2PHR trust bundle. Working with Pilot Implementers, the team will:
 1. Evaluate changes required, if any, to *NATE Policy 3.c: Policy for Trust Profiles using Direct*—determine if there are differences in how clinically-focused HISP’s comply with the requirements of the Direct mode of exchange versus PHRs that implement Direct.
 2. Determine if the Pilot premise that being a current NATE-QE (P2P4Tx) is sufficient to support data flow from a Participating Provider to a PHR and evaluate the benefit of such an intermediary supporting providers (i.e., the HISP) in the use case from a policy and trust perspective. If additional eligibility criteria are warranted for consideration by the NATE BoD, the pilot will document same.
 3. Working with Pilot Implementers to document obligations of the NATE—QE (P2PHR). Our approach will be to work with the implementers to evaluate the sufficiency of the existing Blue Button+ (BB+) Receive Policy for this profile’s mono-directional exchange from the Provider to the Patient, where the Patient has requested to receive information from the Provider and where the Provider has done in-person identity proofing of the Patient).
 4. Document obligations of the Provider—in addition to the Provider performing the in-person identity proofing proposed by the pilot, we will work with implementers to determine if any additional obligations must be established for this use case.

5. Document Rights and Responsibilities of the Patient – we will work with implementers of the pilots to identify and contribute to a common set of knowledge of what the Patient’s rights and responsibilities are, indicating any exceptions that may be established to exclude specially protected populations from the pilot (if determined necessary).
- Verify the technical approach is capable of supporting the communities’ expectations with regards to trustworthy exchange of PHI between NATE-QE (P2P4Tx) HIOs and NATE-QE (P2PHR) PHR solutions.
 - Establish and vet common definitions for terms used to communicate about the use case, including the definition of PHRs as used in the context of this profile.
 - Gather information to inform next steps regarding NATE’s ongoing activities in support of patient mediated exchange.
 - Ascertain the policy needs, if any, for individual states to further qualify NATE-QEs (P2PHR) for the use case if formally vetted by another state or NATE.

II. Applicability of Policies

This profile applies to the following:

- Member states responsible for promoting PHRs that implement Direct in their state that satisfies the criteria of the P2PHR profile.
- The NATE Trust Bundle Coordinator and others involved in related functions.

III. Policy

NATE-QE (P2PHR) eligibility criteria are grouped into two sets:

- The first set are derived from *NATE Policy #3.c: Policy for Trust Profiles using Direct* [The pilot will determine if there are exceptions to this profile component and document same]; and
- The second, detailed below, describes the Eligibility Criteria of a NATE-QE’s (P2PHR) to be evaluated as part of this pilot.

A Member State shall confirm that candidate NATE-QEs satisfy each and all Eligibility Criteria of both prior to causing the NATE-QE (P2PHR) to be added to the NATE Trust Profile following Procedure 3.d.1.

Eligibility Criteria of a NATE—QE (P2PHR)

- A. NATE-required Direct Project security and trust components
 - i. All NATE-QE (P2PHR) candidates must demonstrate adherence to the baseline requirements for the pilot.

Rationale—see NATE Policy #3.c.1

Method of verification—see NATE Policy #3.c.1

B. Obligations of participating NATE-QE (P2P4Tx) for this Use Case.

- i. HIOs participating in this Pilot must be NATE-QE (P2P4Tx) entities.

Rationale—The sending party must have demonstrated its adherence to the eligibility criteria of NATE’s P2P4Tx in order to participate in the piloting of this Trust Bundle.

Method of verification—presence of HIO in NATE P2P4Tx Trust Bundle.

C. Obligations of the NATE—QE (P2PHR) to patients

- i. The pilot will evaluate if the PHR’s Service Agreement (including Privacy notice and other artifacts) must disclose how governance decisions are made to its participants in its participant agreement regarding but not limited to the following issues:
- a. Release of PHR data (personal data) for (1) marketing and advertising; (2) medical and pharmaceutical research; (3) reports about the company and customer activity; (4) the insurer and employer; and (5) the development of software applications.
 - b. Release of PHR data (statistical data) for (1) marketing and advertising; (2) medical and pharmaceutical research; (3) reports about the company and customer activity; (4) the insurer and employer; and (5) the development of software applications.
 - c. Whether limiting agreements that restrict what third parties can do with the personal data are required.
 - d. Whether release of personal data is stopped if the PHR is closed or transferred.
 - e. How security measures are provided that are reasonable and appropriate to protect personal information, such as PHR data, in any form, from unauthorized access, disclosure, or use.
 - f. Whether PHR data is stored in the United States only.
 - g. Whether PHR data activity logs are kept for users to review.
 - h. How the uniqueness of an assigned message address is ensured, and whether assurance is given that it will never be assigned to another user, even after an account is closed.

Rationale—[ONC Personal Health Record \(PHR\) Model Privacy Notice](#)

Method of verification—Each Candidate PHR fills out a checklist that is publicly available and published on the web. The checklist is reviewed by the designated NATE Party State to ensure verification of the policies.

D. Obligations of the Provider/Entity sending the message to the patient upon their request:

- i. Provider to follow identity verification requirements for the individual requesting disclosure as defined locally and in compliance with HIPAA and State law.
- a. The Privacy Rule requires covered entities to verify the identity and authority of a person requesting PHI, if not known to the covered entity. See 45 C.F.R. § 164.514(h).

- b. If the patient is known to the provider and a record of care is established, the verification of the requestor's identity is subject to local policy prior to the disclosure (e.g., request might be made in person, using photo ID).

Rationale—TBD—MU2/MU3/HIPAA requirement

Method of verification—TBD—Pilot may rely on attestation of Participating providers for purposes of inclusion in Pilot.

E. Rights and responsibilities of the patient

- a. In addition to capturing information about patients' rights and responsibilities, participants will document the constraints placed on patient recruitment for inclusion in this pilot and the related policy reasons for excluding any specially protected patients such as minor children or wards of the State.

Rationale—TBD—MU2/MU3/HIPAA requirement

Method of verification—TBD

IV. Related Procedures

Policies for Trust Profiles using Direct (3.c)

Procedure for Onboarding to a Trust Profile (3.d.1)

**APPENDIX B:
PHR ONBOARDING FORM**

[This page intentionally left blank.]

PHR ONBOARDING APPLICATION

Main Point of Contact	
Name:	Organization:
Telephone Number:	Mobile:
Email:	
Physical Address:	
Trust Bundles Submitting For:	
<input type="checkbox"/> PHR "Receiver" <input type="checkbox"/> PHR "Sender" <input type="checkbox"/> Both	

Overview of Document

This document lays out the criteria for a PHR's inclusion in one or more of the National Association for Trusted Exchange's (NATE) PHR Trust Bundle(s) for the purposes of the PHR Ignite Pilot Project. All PHRs must complete this form and supply the necessary attestation information and proof to be considered for inclusion into the NATE PHR Trust Bundle.

Throughout the pilot, this document will be reviewed and as a result of the pilot there may be significant changes to this document and subsequently criteria for remaining in the bundle. If and when these or similar PHR Trust Bundles move from a Pilot state to a Production state, each PHR will be required to resubmit the final version of this form and the associated attestation and proof for inclusion in the Production Trust Bundle.

For the purposes of this pilot, trusted sources of data shall be limited to those found in the NATE-P2P4Tx Trust Bundles, the Pilot Trust Bundles (P2PHR and PHR2P) and those other trusted data sources designated by Pilot Participants (such as DELPHI, CitiSense, MyHealthVet) in their proposals. Additional sources of data will not be considered for the purposes of the study report and are deemed outside the scope of the pilot.

Once your application has been approved by the NATE PHR Pilot Steering Team (consisting of NATE Member State Representatives participating in the pilot) you will be required to forward the following information to bundles@hiecosystem.net:

-
1. The technical point of contact (name and email address) for the person responsible for managing updates to trust anchors in the trust store.
 2. The technical point of contact (name and email address) for the person responsible for transport (not content) testing, should it be different from (1) above.
 3. The trust anchor certificate for the Direct HISP.

Certificates can be provided in any format. However, some formats and extensions are identified as a potential security threat by our email servers. Therefore, either (1) include the certificate in a ZIP file archive, or (2) change the extension to something harmless (such as "txt") and includes in the body of the email the correct format/extension.

See NATE's [Procedure for Onboarding to a Trust Profile](#) for additional context.

Questions regarding this form, onboarding processes, and attestation can be directed to Aaron Seib, NATE CEO, aaron.seib@23eleven.net

A. General Obligations of the PHR

Obligation	Method of Attestation	Please provide a description of how your application or service satisfies this Obligation and attach any additional documentation or evidence as necessary
1. The PHR shall comply with all applicable state and federal laws and regulations.	<input type="checkbox"/> Self-Attestation alone	<Applicant> expects to remain compliant with all applicable laws and regulations within the states in which we are conducting the pilot; including the following:
2. The PHR shall display their Privacy Notice in an easily accessible location prior to sign up or use. Must include language on the PHR's data practices, including those areas addressed by the ONC Personal Health Record (PHR) Privacy Notice .	<input type="checkbox"/> Self-Attestation with supporting materials submitted	Applicant should include links to their published privacy notices and link to home page of PHR service. For those applicants that offer smart phone applications only, text of their privacy policies or instructions on how a user is presented their privacy policy are sufficient alternatives. Applicant should also include a narrative response on their compliance with ONC Personal Health Record (PHR) Privacy Notice.
3. The PHR shall notify its users and consumers of changes to its Privacy Notice per applicable law; when PHR is required to notify its users NATE shall be notified as well.	<input type="checkbox"/> Self-Attestation alone	Applicant should provide a narrative response on how their users are notified of changes and updates to the Privacy Notice. Applicant should describe how NATE is to be notified of updates to privacy policies.
4. The PHR shall conform to industry-accepted practices and at a minimum maintain necessary safeguards for ensuring the privacy and security of personally identifiable health information.	<input type="checkbox"/> Self-Attestation alone <input type="checkbox"/> Self-Attestation with supporting materials submitted <input type="checkbox"/> Other	Applicant should provide a narrative description of how their PHR offering meets these practices.

B. Obligations of the PHR in the Role of Data Sender

Obligation	Method of Attestation	Please provide a description of how your organization satisfies this Obligation and attach any additional documentation or evidence as necessary
1. The PHR shall transmit data as approved by the consumer.	<input type="checkbox"/> Self-Attestation alone <input type="checkbox"/> Self-Attestation with supporting materials submitted	Applicant should supply a statement of attestation and/or inclusion of reference to the applicable policy or policy section.
2. When and where industry-accepted data formats and standards allow, PHRs must include and convey data provenance information (specify method at later date)	<input type="checkbox"/> Self-Attestation alone <input type="checkbox"/> Self-Attestation with supporting materials. <input type="checkbox"/> Other	<p>Applicant should indicate how provenance of sent data and/or documents is indicated. Copies of CCDs/CCDAs/other documents, screen shots, or descriptions of where and how provenance is indicated are acceptable.</p> <p>For those applicants that are demonstrating the pilot-defined provenance using "Request.txt" or similar mechanism, please include an example once available.</p>

C. Specific Eligibility Criteria for Direct

Obligation	Method of Attestation	Please provide a description of how your organization satisfies this Obligation and attach any additional documentation or evidence as necessary
1. Conform to Direct Project's <i>Applicability Statement for Secure Health Transport, version 1.1.</i>	<input type="checkbox"/> Self-Attestation alone <input type="checkbox"/> Self-Attestation with supporting materials. <input type="checkbox"/> Other	Applicant should provide attestation and/or narrative description of their compliance with the Applicability Statement.
2. Encrypt all edge protocol communications (last mile exchange).	<input type="checkbox"/> Self-Attestation alone <input type="checkbox"/> Self-Attestation with supporting materials.	Applicant should provide a description of how edge protocols are secured.

Obligation	Method of Attestation	Please provide a description of how your organization satisfies this Obligation and attach any additional documentation or evidence as necessary
3. Where applicable, have a documented process for the provisioning and management of digital certificates	<input type="checkbox"/> Self-Attestation alone <input type="checkbox"/> Self-Attestation with supporting materials.	Applicant should include a copy of applicable certificate policy or supply the rationale for why this item is not applicable.
4. The PHR shall notify the Trust Bundle Coordinator when trust anchors/public keys should be removed or replaced due to any reason (including expiration or trust anchors) and supply new trust anchors in a timely fashion.	<input type="checkbox"/> Self-Attestation alone <input type="checkbox"/> Self-Attestation with supporting materials. <input type="checkbox"/> Other	Applicant should provide attestation of compliance, including the name and title of who is responsible for notifications and certificate management.
5. Ensure that at a given time, only unique Direct addresses are active. Once a Direct address is inactivated, a period of at least three (3) years must pass before a given address can be reissued.	<input type="checkbox"/> Self-Attestation alone	Applicant should provide written attestation of compliance.

My signature below affirms that the above information is true, complete and accurate, and that I am authorized to execute this PHR Onboarding Form on behalf of the designated organization. I understand that Pilot Participants' self-attestation to the Obligations may or may not be further verified by NATE for purposes of the Pilot.

Printed Name

Title and Organization

Signature

Date