SEMHIE Roadmap Comments, 4/3/15.

April 3, 2015.

SEMHIE (“Southeast Michigan Health Information Exchange) COMMENTS TO ONC ROADMAP ON ARCHITECTURE AND INFRASTRUCTURE AND A MODEL FOR “ACTIVE AUTHENTICATION” PREPARED BY MICHAEL (Mick) TALLEY, DIRECTOR & TREASURER, CO-PROJECT MANAGER.

SEMHIE supports to principles of the “Roadmap” drafted by ONC for the healthcare services industry to create a secure environment for data sharing involving an upgrade of the architectures and infrastructures currently in use in healthcare. To obtain interoperability, SEMHIE supports the use of standards in the healthcare industry and a combination of the volunteer standards bodies and the government standards bodies offer the best collaborative environment to involve the public and private sectors.

 SEMHIE is sharing with ONC an approach which was successful in July of 2012 to complete a contract with the Social Security Administration in which SEMHIE proposed a model, which can be duplicated at lost cost for HIEs, (“Health Information Exchanges”) to play a role for organizations large and small, with simple or sophisticated IT platforms for connectivity and secure data sharing with authentication for access control and the running of applications, involving expanded use of “APIs”.

SEMHIE notes that:

1. The healthcare industry needs to work collaboratively to discover whether or not an agreed upon “Governance” Framework, for public and private transactions to provide vendor neutral solutions, off a “Service Oriented Architecture”, (SOA) and access to applications either proprietary or “open source” can be stacked at the application level, to enhance the sharing of data for the generation of measurements of care for efficacy.
2. The healthcare services industry should embrace the use of “digital credentials” and the work of the “National Strategy of Trusted Identity in Cyber-space”, (NSTIC) and states other than Michigan should create solutions and electronic means for access involving “Consent Management” of who can see patient data with access for patients as to who has seen their data for what purpose.
3. SEMHIE supports the ONC requirement for testing and validation of solutions for increasing the comfort level of providers and payers in electronically sharing patient data to avoid breaches or mischief.
4. SEMHIE supports the first principle of “interoperability” noted by ONC in the Roadmap, with the view that “to the extent possible”, should be obtained by building on existing Health IT infrastructure, with the “model” being the “ATM, Debit, & Credit card” networks of financial institutions, which healthcare can leverage.

In the following comments and models, SEMHIE shares its technical approach, which was successful with the SSA, as a beginning point, as many of the aspects of the Roadmap are touched upon and discussed in the SEMHIE RFP to SSA.

SEMHIE as with the Roadmap, embraces the use of “Standards” and created a list below of the standards to be used to successfully complete the SSA contract in 2012. SEMHIE accepts as with the Roadmap, that an organization attempting to create a secure data sharing environment with access control of identity management has to have members who agree to comply with the use of those standards and if not in a near term state for compliance, must alert the other members of the group of this inability. This allows for other groups to make business decisions as to whether or not conduct certain types of transactions with a noted member of the collective. A list of the standards used by SEMHIE is contained below:

privacy standards development and deployment, and conducted work with the National Institute for Standards and Technology (NIST), with the American National Standards Institute (ANSI/ASC/X9), and with the Object Management Group (OMG). In the collaborative public/private environment of SEMHIE with OMG, multiple team members are familiar with implementation and deployment of the following list

of standards on the approved governance model and will adhere to those standards with the work of the RFP.

a. OASIS Security Assertion Markup Language(SAML) v2 b. OASIS standard, ITU-T x.1141(2).

c. HITSP TP20/SC109, (HL7 v3 RBAC, R!-2008, HL7 version 3 standard: role based access control, (RBAC) healthcare permissions catalog, release 1, Feb. 2008(1) --- HITSP C19/TP20/SC108 OASIS eXtensible Access Control Markup language (XACML), ITU-T Recommendations, X.1142, Feb. 2005

© 2009 Southeastern Michigan Health Information Exchange Association | 4-2



d. HITSP TP20/SC108, OASIS WS-Trust Version 1.3, March 2007

e. HITSP C19/TP20/SC108, OASIS Security Assertion Markup Language XACML ITU-T Recommendation X.1142, Feb. 2005 –OASIS Security Assertion Markup language (SAML) v2.0

OASIS ITU –T X.1141 (2), OASIS WS Trust Version 1.3, March 2007

f. HITSP T15/T17/SC109. IHE ITI0RF Revision 4.0 or later, Audit Trail and Node Authentication

(ATNA) Integration Profile, Section 9.1 Authentication

g. IHE EUA , IETF RFC 4120 The Kerberos Network Authentication Service, (VS) July 2005

h. HITSP TP 30 IHE ITI-TF Revision 5.0 or Volume 2 Supplement 2007-2008 Cross Enterprise Document Sharing-b, (XDS.b), IHE ITI-TF Revision 5.0 or later, Enterprise User Authentication (EUA) profile

i. HITSP C19 IHE ITI-TF Volume 2 Supplement 2007-2008 Cross Enterprise User Assertion, (XUA) (3)

j. HITSP, C19, IHE, Registry Query, IHE XDS.b k. HITSP CAP143

l. HITSP TP30. Series

m. IHE Registry Query. Series

n. HITSP T16, IHE Consistent Time., Series o. HITSP Cap119

p. HITSP CAP 120

q. HIPAA Rules, Parts 160-164 r. HITSP T24/C25 C88

s. HITSP C87

t. IHE PWP, Series u. HITSP T64

v. HITSP C19

w. HITSP TP30, HITSP C26

x. IHE XDM/DSG/ATNA/BPPC

y. HITSP T33

Note: Part of SEMHIE’s architectural goal is to ensure that our providers have an easy way of communicating multi-formatted documents with each other. We have looked to the best practices in other industries to help solve this challenge. SEMHIE intends to explore the use of MDMI, a financial industry standard, to address some of the mapping challenges, and the use of a “Reference Index Model” or “Dictionary” provided by “Clinical Architecture”, however, our proposal is based on industry standard JavaCAPS transformation engine integration.

The MDMI open standard defines transaction data transformations or “maps”. These maps are computer readable and unambiguously define and preserve the business payload of any financial message regardless of its original protocol. MDMI has these four technical pillars:

1. Separation of data structures from business meaning – this assures repeatable maps.

2. Appropriate granularity for semantic interoperability – this assures reliable business information.

3. Hardened technology using Model Driven Architecture (MDA) – this assures openness.

4. Reuse and support of existing financial services and technical standards – this assures lowest adoption costs.

**4.2.2.4 Process all NHIN Standard Transactions (§B-1, §4.1.4)**

The Team SEMHIE system will process all NHIN standard transactions for electronic request for medical information, including the patient’s authorization to release information, within five (5) hours of receiving the electronic request. Figure 2 describes the flow of message traffic from the SSA, through the SEMHIE gateway and on to Oakwood Health System.

© 2009 Southeastern Michigan Health Information Exchange Association | 4-4





*Figure 2. Transaction Flow for SEMHIE/SSA Requests*

SSA’s CONNECT NHIN sends a message to SEMHIE NHIN, which routes a request to Oakwood’s Central Patient Index (CPI), which will match the demographic data from the SSA and generate a match profile percentage. Based on this percentage, the system will either automatically send back the patient CPI Identifier, or initiate a workflow for further validation of patient identity. Once the CPI Identifier has been correctly identified, the CPI will be sent back to the SSA via SEMHIE. The SSA will use this CPI identifier in all future correspondence. The SSA makes a request for an available documents list, at which time Oakwood generates a list and returns it via SEMHIE. At this point, when the SSA requests a specific document, the integration engine at SEMHIE will connect to one of five different Oakwood EMRs to collect the SSA required elements. The engine will transform the data into a CCD, validate the format and keep an auditable copy before sending it back to the SSA for processing.

**4.2.3.1.3 Acceptance of CCD**

SEMHIE will submit invoice for payment for the price item 001 upon acceptance of the CCD by SSA.

**4.2.3.2 Provide Set of Verification CCDs (§B-1, §4.2.2)**

Once the sample CCD has been completed and our systems have been modified to provide verification

CCDs, SEMHIE will generate up to 50 individual CCDs identified by SSA. Prior to submission,

SEMHIE will work with SSA to establish a secure means of providing the verification CCDs. Encryption and secure modes of data submission will be reviewed during this process. The verification CCDs will be generated from our health plans and submitted to SSA for review and acceptance. Our project plan includes a process similar to the sample CCD submission to iterate upon each CCD until we have acceptance of the verification CCDs.

***4.2.4 Task Area 3: NHIN Tasks (§B-1, §4.3)***

SEMHIE intends to use NHIN-CONNECT, an implementation of standards-based specifications for the exchange of health information between NHIN-compliant Health Information Exchanges (NHIEs) as illustrated in Figure 5. Sun technology was used by the Office of the National Coordinator (ONC) to develop the core software infrastructure and has been instrumental in leading the NHIN-CONNECT solution toward becoming a “reference implementation” of a Service Oriented Architecture (SOA) for the National Healthcare Information Exchange.

© 2009 Southeastern Michigan Health Information Exchange Association | 4-8





*Figure 5. NHIN-CONNECT is an implementation of standards-based specifications for the exchange of health information between NHIN-compliant Health Information Exchanges (NHIEs)*

**4.2.4.1 Provide Production NHIN Gateway Environment (§B-1, ¶4.3.1)**

The SEMHIE NHIN solution uses the NHIN CONNECT Gateway. The NHIN CONNECT Gateway was created using Sun technology and is fully supported. In addition, the SEMHIE Gateway will use new document-centric standards to provide security, privacy, proper identity and auditability of the information exchanged. The purpose of this design is to allow, over time, all of SEMHIE health care

providers to use the SEMHIE to electronically and consistently interact with the SSA for disability claims processing without requiring each of these health providers to implement and maintain their own

interface.

Figure 6 provides a high-level view of the proposed Team SEMHIE NHIN system. Each supported healthcare provider will use a standard CONNECT Gateway plus key Team SEMHIE services that will interact with the internal healthcare providers systems. These services will provide data transformation and CCD document processing, support security and privacy policies and service level assurance and auditability.

© 2009 Southeastern Michigan Health Information Exchange Association | 4-9





*Figure 6. Overview of the Proposed SEMHIE NHIN System*

***4.2.4.1.1 The Message Payload***

The mechanism for moving information through the NHIN network is web services. Within web services, documents are encoded as an XML document, and passed as an argument of the web service call. The documents that will move within the SEMHIE local NHIN Loop will be standard CCD documents but

will include a header block that will be used to handle the additional services of the proposed SAA / SEMHIE Service. The documents that will flow between SEMHIE and SSA will be standard CCD documents that can or will be compatible with the SSA systems. Figure 7 depicts the document payload.

© 2009 Southeastern Michigan Health Information Exchange Association | 4-10





*Figure 7. The Document Payload*

The SEMHIE Services Block is an additional XML document section that can support the following

Services:

(i) Efficient data mapping and creation of valid CCD documents (potentially using OMG’s MDMI

Standard and solution from “Clinical Architecture”.

(ii) Integrated identity management (Future-Later Phase)

(iv) Data-centric security and multi-level encryption (Future-Later Phase)

The SEMHIE services herein described envision an HIE infrastructure that provides services beyond the scope of this proposal. They are provided as background information only. The SEMHIE will adjust its overall HIE deployment project planning to accommodate the subset of services which are necessary for the deadlines and requirements of this proposal.

***4.2.4.1.2 CONNECT***

Sun’s technology is being used by the federal government for the NHIN-CONNECT implementation. The solution consists of two parts: Gateway and Adaptor Toolkit. Both parts use the technologies supported commercially as JavaCAPS. The components are Glassfish ESB, Sun’s Master Patient Index, Project Metro, MySQL, and Sun’s development environment, NetBeans.

CONNECT is the open source Gateway used to connect to the NHIN network. It is a rich and open technology that offers a wide range of services through APIs. Existing services can be replaced or modified and services can be added. The basic workflows for document transfer will be handled by CONNECT. Figure 8 illustrates the SEMHIE Gateway and Adaptor Toolkit.

© 2009 Southeastern Michigan Health Information Exchange Association | 4-11





*Figure 8. Gateway and Adaptor Toolkit*

***4.2.4.1.3 Component Description***

The next several sections describe the Sun components that make up the NHIN Gateway and Adaptor

Toolkit.

***Glassfish ESB***

Sun GlassFish Enterprise Services Bus (ESB) delivers a lightweight enterprise service bus and the tools necessary to rapidly build and deploy service-oriented architecture (SOA) components, providing flexibility and freedom from the dependencies that have traditionally locked enterprises into proprietary middleware software stacks. GlassfishESB is a platform for Business Integration, Enterprise Application Integration, and SOA.

 Provides a lightweight, modular architecture that enables agile service development, deployment and testing

 Allows users and vendors to plug and play through a pluggable architecture where components and services can be integrated in a vendor-independent way

 Leverages the transparent development and taps into innovation happening in the NHIN community

 Allows vertical and horizontal scalability through asynchronous and decoupled component architectures

 Provides flexibility with the choice of development language, tooling, topology and architecture style

(MOM, SOA, EJB, BPM, EDA, etc.)

© 2009 Southeastern Michigan Health Information Exchange Association | 4-12



***Master Patient Index***

Master Data Management solves data management problems and includes the following set of core components:

 Master Index Studio – Provides the capability to create any domain specific master index through the matching, de-duplication, merging, and cleansing of data from various data sources

 Data Integrator – Provides extract, transform, load capability and supports a wide variety of data sources

 Data Quality – Features matching, standardization, profiling, and cleansing capabilities

 Data Mashup – Server-side data mashup capability, having multiple forms including real-time views of information for master data consumers

 Data Migrator – Provides the ability to migrate database objects across database instances

***NetBeans***

The NHIN-CONNECT developers wanted an open source, flexible and easy to use development environment, so they selected NetBeans. Netbeans is an open-source Integrated Development Environment (IDE) for software developers, provides a rich client platform for application development support. It provides all the tools needed to create professional desktop, enterprise, web, and mobile applications with the Java language, C/C++. as well as dynamic languages such as PHP, JavaScript, Groovy, and Ruby. NetBeans IDE, straight out of the box, runs on many platforms including Windows, Linux, Mac OS X and Solaris.

***Project Metro***

Metro is a high-performance, extensible, easy-to-use web service stack. It is a one-stop shop for all your web service needs, from the simplest “hello world” web service to reliable, secured, and transacted web service that involves .NET services.

The two main components of Metro are:

 JAX-WS – The Core web services platform

 WSIT – Implementation of key WS-\* specs and interoperability with .NET 3.0

The Core web service that provides all the SOAP message functionality, including WS-Addressing and

MTOM, is available from JAX-WS.

***Open SSO***

Open SSO is the single solution for web access management, federation, and web services security and provides secure and centralized access control and single sign-on for all applications and web services, both within the enterprise and beyond.

For “Active Authentication”, SEMHIE and MiHIN created a “model”, which is noted below, to supplement the technology and standards selection for a working model, as SEMHIE is participating in the MiHIN, (“Michigan Healthcare Information Network”) “Federated Hub Pilot”, to work out the interoperability of different vendor solutions of digital credentials. SEMHIE and MiHIN have embraced the use of a “Bio-metric” in the model of “Two-Factor” authentication as described in “NIST 800-63-2”. Healthcare has a challenge in the deployment of digital credentials to automate the process of “Consent Management” and states other than Michigan should develop an approach. Michigan has an approved process for “consent” and this has to be tested and validated as a future phase. This supplement to the ONC Roadmap, as with use of the “Kantara Initiative” profile for “binding” permissions to a certificate or token has to be tested and validated and since the certificate will contain “policies”, relative to “governance”, that raises the question or the challenge as to how do you know that the policies you think are being deployed, are actually being deployed. As a future piece of the Roadmap, SEMHIE would recommend that a software solution to validate policies/permissions/authorizations is the ones the organization believes have been deployed. Sometimes people write the wrong code or there are “bugs”.

The SEMHIE/MiHIN model is noted below in “Figure 1”.

**Figure 1: Southeast Michigan Healthcare Information Exchange (SEMHIE) generic model for defining enforce- ment points for active authentication.**

There are four actors requiring active authentication within this use case.

1. The doctor in Clinic A or the medical personnel in Clinic B requesting access to a patient’s Electronic

Health Record (EHR).



5

**SEMHIE/MiHIN NIST-NSTIC Proposal**

Project Name: SEMHIE MIHIN NIST-NSTIC Proposal

2013-NIST-NSTIC-02: Trusted Online Credentials for Accessing Government Services Cooperative Agreement Program

2. Government entities requesting access to patient records for public health reporting, research and sur- veillance of communicable diseases.

3. A patient utilizing a computing device to access EHR over a public or secure private network.

4. A medical personnel acting on behalf of the users keying in the opt-in and opt-out selections.

There are a few entry points in the systems that require active authentication. The actors in the use case would use the more generally accepted biometric schemes like retina scans, palm print, voice and finger print, whenever a request is made to access the patient’s HER. These biometric modes would be embedded into the devices where the actual authentication would take place.

Currently, there are various modes of opt-in / opt-out models to consider

 Allow all authorized provider organizations involved in providing medical care to access critical patient da- ta information across disparate networks.

 Authorize temporary access to a default set of patient information by a licensed practitioner only in the case of an emergency or unanticipated event.

 Authorize data access if and only if the patient has the ability to request what data and whom the data is being shared with.

 Government entities require access to patient records for public health reporting, research and surveil- lance of communicable diseases.

Figure 1, defines the points of active authentication from enrollment of a patient with a healthcare entity, (Doctor’s Office, Healthcare Information Exchange, (HIE), or Clinic.) to the use of the HL7 “Continuity of Care Document”, (CCD) for secure data sharing across networks. The approach is one of being “data-centric” and SEMHIE/MiHIN intends to encrypt the data and at the SEMHIE/MiHIN node generate and populate the CCD with the authorized encrypted data allowed under the consent management patient document. The requestor of the data, which

could be a person with a mobile device, a program, or a machine can then de-crypt the data con- tained in the CCD, with authorization.

The attributes of the end-user or requestor are “bound” or “binded” to the digital credential which shall also contain the relevant state and federal laws and policies appropriate to the trans- actions. The approach facilitates automation of the process and is repeatable across domains, networks, and industries. For example, the insurance industry in multiple venues, such as the “Standards and Interoperability Framework”, (S & I Framework sponsored by the “Office of the National Coordinator”, (ONC) has embraced the use of the CCD as a repeatable method of se- curely sharing data across networks between the provider and the insurance agency or payer.

The intent of SEMHIE/MiHIN is to facilitate requests between the “Qualified Organizations”,

(QOs) and MiHIN. SEMHIE is a QO of the MiHIN effort.



***Glassfish Enterprise Server***

The Sun GlassFish Enterprise Java EE 5 based Server (formerly Sun Java System Application Server) is the leading platform for building and deploying next-generation applications and services.

***MySQL***

MySQL is the database of choice for NHIN-CONNECT. MySQL offers fast performance, high reliability, ease of use, and dramatic cost savings. The combination of MySQL’s popularity and Sun’s offerings for scalable infrastructure make Sun and MySQL the platform of choice for NHIN-CONNECT.

***Additional NHIN-CONNECT Code***

In addition to the infrastructure software, the available CONNECT code has a number of applications that will be used, where appropriate, to support the implementation of the SEMHIE services. Examples of the available applications are:

 Patient Index Cross system (PIX) – Unique identifier of patient across systems per community

 Patient Demographics (PDQ) – Single patient view and demographic information on the patient

 Cross Enterprise Document Sharing (XDS.b) (Registry and Repository) – Register of documents available on a patient and keeps track of where they are stored (repository)

 Cross Community Access (XCA) – Ability to exchange docs across health entities