June 25, 2012

TO: Office of the National Coordinator for Health Information Technology (ONC), Department of Health and Human Services, Request for Information

FROM: Randy Vanderhoof, Executive Director, Smart Card Alliance

SUBJECT: Smart Card Alliance Response to Office of the National Coordinator for Health Information Technology (ONC), Department of Health and Human Services, Request for Information (RFI), **"**Nationwide Health Information Network: Conditions for Trusted Exchange," 45 CFR Part 171

The Smart Card Alliance Healthcare Council reviewed the Office of the National Coordinator for Health Information Technology (ONC), Department of Health and Human Services, Request for Information (RFI), **"**Nationwide Health Information Network: Conditions for Trusted Exchange," 45 CFR Part 171, published in the Federal Register, Vol. 77, No. 94, Tues., May 15, 2012.

We offer the attached responses to several of the questions posed in the RFI.

The Smart Card Alliance Healthcare Council appreciates the opportunity to provide input to the ONC on the trust framework for the Nationwide Health Information Network (NwHIN). We would be happy to work with ONC on further defining and specifying the framework, policies, best practices and technologies for identity management and authentication for the NwHIN.

If you have questions on these responses, please contact our Healthcare Council Chair, Michael Magrath, Gemalto (Michael.Magrath@gemalto.com) or me (rvanderhoof@smartcardalliance.org, 1-800-556-6828).

Sincerely,

Randy Vanderhoof

Executive Director

Smart Card Alliance

Smart Card Alliance Response to ONC Request for Information: Nationwide Health Information Network: Conditions for Trusted Exchange, 45 CFR Part 171

The Smart Card Alliance Healthcare Council is pleased to submit our response to the Office of the National Coordinator for Health Information Technology (ONC), Department of Health and Human Services (HHS), Request for Information (RFI), **"**Nationwide Health Information Network: Conditions for Trusted Exchange," 45 CFR Part 171.

Although several of the questions in the RFI are outside of the expertise of the smart card industry, we offer the responses below to several that pertain to identity, authentication, patient matching and digital certificates that are within our area of expertise.

Question 24: What is the most appropriate level of assurance that an Nationwide Health Information Network Validated Entities (NVE) should look to achieve in directly authenticating and authorizing a party for which it facilitates electronic exchange?

The Privacy and Security Framework Requirements and Guidance for the State Health Information Exchange Cooperative Agreement Program,[1] released by ONC on March 22, 2012, recommend NIST Level of Assurance 3[2] for states and State Designated Entities (SDEs). The document states, "HIE entities should establish strong identity proofing and authentication policies for user access to electronic health information systems. Recipients should indicate the assurance level they are using in their privacy and security frameworks, using NIST 800-63 version 1.0.23 as a guide and resource. The recommended assurance level is Level 3."

The Smart Card Alliance agrees that, at a minimum, Level 3 should be required not only to authenticate into HIEs, but also for the entire Nationwide Health Information Network (NwHIN). To reduce fraud, protect patient privacy and secure access to the NwHIN, it is imperative that Level 3 assurance, at a minimum, be required. Recommending a minimum of Level 3 and not mandating it opens the door to fraud and identity theft. In our opinion, the ONC needs to assert its authority and require strong authentication.

To provide the utmost security and protection of Americans' most personal and sensitive information – citizens' health information, the Smart Card Alliance strongly believes that ONC should also mention and endorse NIST Level 4 assurance in the form of the Personal Identity Verification-Interoperable (PIV-I) credential – the same identity and authentication technology used in the HHS employee ID.

PIV-I is the credential being deployed as the First Responder Authentication Credential (FRAC) by several state and local governments because it is standards-based, non-proprietary, trusted by the federal government, and able to be used for multiple purposes. The first responder population encompasses approximately 20 million people in the U.S. A significant portion of this population is every physician, nurse and emergency medical technician (EMT). By putting a FRAC in the hands of the medical community, local authorities will be able to rapidly grant access only to qualified individuals during emergency situations like Hurricane Katrina.

Given the federal initiatives impacting the U.S. healthcare system, it is clear that healthcare organizations and providers will need to strengthen their identity and authentication methods and obtain digital identity

[1] "Privacy and Security Framework Requirements and Guidance for the State Health Information Exchange Cooperative Agreement Program," ONC-HIE-PIN-003 March 22, 2012, http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_0_5545_1488_17157_43/http%3B/wci-pubcontent/publish/onc/public_communities/_content/files/onc_hie_pin_003_final.pdf

[2] "Electronic Authentication Guideline," NIST Special Publication 800-63, http://csrc.nist.gov/publications/PubsSPs.html

credentials. During these harsh economic times, organizations are conscious of expenses and are looking for a return on their investment while minimally impacting provider workflow. The last thing providers want is to carry yet another ID badge or token. To minimize impact, a single credential should meet or exceed all of the identity and authentication requirements affecting the healthcare industry.

The PIV-I credential is a multi-purpose electronic identity credential, built on international and domestic standards and available today from several manufacturers.

For more information about PIV-I please visit http://www.idmanagement.gov/.

Question 25: Would an indirect approach to satisfy this Condition for Trusted Exchange (CTE) reduce the potential trust that an NVE could provide? More specifically, should we consider proposing specific requirements that would need to be met in order for indirect authentication and authorization processes to be implemented consistently across NVEs?

As stated in our response to Question #24, the Smart Card Alliance recommends that ONC mandate a minimum of Level 3 assurance to access electronic health records (EHRs) on the entire NwHIN. In addition, ONC should suggest that healthcare organizations consider the highest of assurance – Level 4 – to reduce fraud, protect patient privacy and secure access to the NwHIN.

Question 44: Are there circumstances where a provider should be allowed access through the NVE to the health information of one or more individuals with whom it does not have a treatment relationship for the purpose of treating one of its patients?

Definitely. In the event of natural disaster or other catastrophic event, first responders should be allowed access through the NVE in order to treat patients. It is critical that the FRAC be able to be used to access the NwHIN to facilitate treatment in emergency situations.

Question 46: If a secure ''RESTful'' transport specification is developed during the course of this rulemaking, should we also propose it as a way of demonstrating compliance with this CTE?

Condition [I–2]: An NVE must follow required standards for establishing and discovering digital certificates.

We strongly recommend that if digital certificates are used, they follow the policies of the Federal Bridge Certificate Authority.

Question 48: Should this CTE require all participants engaged in planned electronic exchange to obtain an organizational (or group) digital certificate consistent with the policies of the Federal Bridge?

- **Condition [I–3]: An NVE must have the ability to verify and match the subject of a message, including the ability to locate a potential source of available information for a specific subject**

Yes. Any organization communicating with the Federal government should have its root with and follow the policies of the Federal Bridge so that systems can be trusted.

Question 49: Should we adopt a CTE that requires NVEs to employ matching algorithms that meet a specific accuracy level or a CTE that limits false positives to certain minimum ratio? What should the required levels be?

It is clear that "unassisted" automated demographic matching cannot be used to achieve the goals of the NwHIN. This is true for two reasons. First, it is unlikely that any Enterprise/Electronic Master Patient Index (EMPI) can achieve sustained performance at the accuracy indicated – a specificity of 99.9% and a sensitivity of 95%. Second, even if that accuracy can be achieved, it will not meet the needs of the NwHIN.

The experience of Harris County, Texas is informative here[3]. The EMPI system has 12 years of data on 3.4 million patients. Within this system:

- 249,213 patients have the same first and last name.
- There are 76,354 instances where at least five individuals share the same first and last names.
- There are 69,807 situations where at least two people have the same first and last names and the same birth date.
- The database contains 2,488 patients named "Maria Garcia." 231 of those "Maria Garcia's" have the same birth date.

No matter how sophisticated the demographic matching algorithm might be, no EMPI could be expected to achieve a specificity of 99.9% when dealing with the population of Harris County, Texas. The eventual population being managed by the NwHIN will be roughly 100 times as large as Harris County. Since the accuracy of demographic matching must decrease as the size of the population increases, there is simply no hope that the overall accuracy of patient matching across the NwHIN could be anywhere near the 99.9% specificity and 95% sensitivity indicated as a target by the Power Team. Other factors such as siblings, twins, foreign names, and hyphenated names represent additional situations that further degrade the accuracy of demographic matching as a means to patient identification.

Second, even assuming that it was possible to achieve 99.9% specificity and 95% sensitivity, these levels of accuracy are not sufficient to make operation of the NwHIN feasible. The following table looks at potential daily frequencies of EMPI matching across the NwHIN.

Daily number of EMPI matches	Number of false positives	Number of false negatives
10,000	10	500
100,000	100	5,000
1,000,000	1,000	50,000
10,000,000	10,000	500,000

The error rates indicated in this table are simply not sustainable for the operation of the NwHIN. None of the readers of this analysis would be willing to use an ATM card to make a deposit if there were a 5% chance that their cash would be lost. The NwHIN will be handling medical information that in many cases is more valuable than money. It does not have the human or technical resources to resolve thousands of indeterminate matches each day. Nor does it have the financial reserves necessary to contend with the inevitable set of lawsuits that may arise due to matching errors.

The addition of a unique patient healthcare identifier, whether voluntary or mandatory, would enable the matching performance of the NwHIN to approach an error rate of zero for both false positive and false negative matching errors for patients who are equipped with such an identifier. This capability can be incorporated as an increment to the existing EMPI systems deployed within HIEs. It makes possible a significant increment in the privacy management of clinical information. It can also be combined with biometrics, security certificates, smart cards and a wide range of other methodologies to achieve enhanced authentication for specific healthcare functions.

Errors are inevitable in any system that involves humans and the use of a unique identifier enables graceful recovery from episodes of identity error, theft and fraud. With a unique identifier, break-the-glass capabilities can be supported for situations where emergency care may necessitate overriding normal patient privacy restrictions and, in addition, there are straightforward techniques for subsequently recovering patient privacy after a break-the-glass episode has ended. Finally, the use of a unique

[3] Houston Chronicle, 4/5/11, http://www.chron.com/news/houston-texas/article/Harris-County-Hospital-District-tries-new-kind-of-1689057.php

identifier enables anonymized result reporting for activities such as research, education, and public health that wish to deal with large amounts of data that should never be traceable back to the individual who is the source of the information.

It seems ill-advised to propose an initial implementation of the NwHIN governance structure where it can be proven that the system will fail. Additional thought and planning around the need for extremely accurate nationwide patient identification appears warranted.

Question 50: What core data elements should be included for patient matching queries?

Accurate patient identification through EMPI-mediated demographic data element matching will continue to be a core requirement for operation of the NwHIN even though it, by itself, is not adequate to achieve the identification accuracy the NwHIN needs. Choice of the appropriate core data elements represents a tradeoff. In order to achieve the maximum discriminating power, one should include the most data elements possible. On the other hand, more data elements mean more time required for data capture, more opportunities for error, and increased likelihood that data elements will be unknown or left missing.

The following table represents experience from two different studies on which data elements should be included in demographic matching.

Data Element	Study 1[4]	Study 2[5]
Globally unique identifier	X	
Last name	X	X
First name	X	X
Middle name	X	X
Date of birth	X	X
Gender	X	X
Address	X	
City	X	
State	X	
Zip code	X	
Phone number	X	
SSN*		X
SSN (last 4 digits)**		
Other data elements***		

*The Social Security Number is often precluded due to privacy concerns.

**The last 4 SSN digits is seen as a privacy-preserving compromise.

***There are many options including: ethnicity, guarantor, insurance number, driver's license number, and mother's maiden name.

These sets of data elements can provide reasonable accuracy for 'normal' demographic matching but are still subject to unreasonable error rates in circumstances such as:

- Twins, where many of the elements will be similar
- Foreign names, where misspelling is frequent and names may not follow the standard first, middle, last name paradigm
- Hyphenated names, where it is not clear whether to use the first, the second, or both names

[4] Robert Wood Johnson Pioneer Foundation research grant on reliable patient identification, 2010-11.
[5] Patient Identity Integrity, a white paper by the HIMSS Patient Identity Integrity Work Group, Dec. 2009.

- Situations where a system does not collect all of the data elements or places restrictions (e.g., no hyphens, length limits) on the characters that can be entered
- Persons who are homeless, move frequently, have compromised mental function, or have a reason to want to conceal their identity

Only the addition of another capability such as a biometric or a globally unique personal identifier can reliably account for these problematic circumstances.

Protecting the privacy of any patient personal information is critical; patient data should be encrypted and accessed only by authorized parties. The use of smart card technology is critical to both protect personal information and enable secure, authenticated access to the data by authorized healthcare providers.

Question 51: What standards should we consider for patient matching queries?

If the patient matching query has the potential to include a unique identifier then the applicable standards would include:

- E 1714, Standard Guide for Properties of a Universal Healthcare Identifier (UHID), ASTM International, http://www.astm.org/Standard/index.shtml
- E 2553 , Standard Guide for the Implementation of a Voluntary National Healthcare Identification System, ASTM International, http://www.astm.org/Standard/index.shtml

About the Smart Card Alliance

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use, and widespread application of smart card technology. Through specific projects such as education programs, market research, advocacy, industry relations, and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the United States and Latin America. For more information please visit http://www.smartcardalliance.org.

About the Smart Card Alliance Healthcare Council

The Smart Card Alliance Healthcare Council brings together payers, providers, and technologists to promote the adoption of smart cards in U.S. healthcare organizations. The Healthcare Council provides a forum where all stakeholders can collaborate to educate the market on how smart cards can be used and to work on issues inhibiting the industry.