Office of the National Coordinator for Health Information Technology

Health IT Standards Committee

Privacy and Security Workgroup

Hearing On

The National Strategy for Trusted Identities in Cyberspace

March 12, 2014

Prepared remarks

Of

Kaiser Permanente

The following prepared testimony is submitted by Kaiser Permanente, to the Office of the National Coordinator, the Health IT Standards Committee and the Privacy and Security Workgroup in connection with a hearing on the National Strategy for Trusted Identities in Cyberspace (NSTIC)

Kaiser Permanente appreciates the opportunity to provide comments and recommendations to the Health IT Standards Committee and Privacy and Security Workgroup regarding the National Strategy for Trusted Identities in Cyberspace.

The Kaiser Permanente Medical Care Program in the largest private integrated healthcare delivery system in the U.S, delivering health care to over 9 million members in eight states and the District of Columbia[1] Kaiser Permanente is committed to delivering high quality healthcare by fostering cooperation and collaboration among providers, hospitals, health plan, and our purchasers.

My name is Tim McKay. I am a Principal Solutions Consultant with Kaiser Permanente's Digital Technologies and Operations department.

A key strength of Kaiser Permanente's integrated health system is its ability to connect with our members through digital channels. For example, in any given month, there will be 5.5 million sign ons to our secure patient portal, with 1.5 million secure emails exchanged between patients and providers, and patients will review online over 5 million lab test results. Fully one third of our patient portal access is now coming through mobile devices. Kaiser Permanente

[1] Kaiser Permanente comprises Kaiser Foundation Health Plan, Inc., the nation's largest not-for-profit health plan, and its health plan subsidiaries outside California and Hawaii; the not –for –profit Kaiser Foundation Hospitals, which operates 38 hospitals and over 550 medical offices; and the Permanente Medical Groups, independent physician group practices that contract with Kaiser Foundation Health Plan to meet the health needs of Kaiser Permanente's member's. Kaiser Permanente also includes the Permanente Dental Associates, a multispecialty dental group, in the Northwest.

members access all of their digital services through their channel of choice using one set of secure identity credentials. We understand the benefits inherent in a unified identity system.

From Kaiser Permanente's point of view, NSTIC is a welcome initiative.

Having NSTIC identities broadly used within healthcare would be very desirable. For example, a single patient NSTIC identity could allow access to multiple patient portals across healthcare organizations and provide easier enrollment for health insurance through state and federal exchanges. NISTIC identities for health care providers would allow more seamless use of EHR platforms, and simplify protocols for the release and reception of medical information. With a NISTIC identity, an emergency responder could get needed medical information from multiple medical institutions quickly which would save lives and enhance patient safety.

That being said, adoption of NSTIC identities within the healthcare community is possible, but would be complex. The use cases for why a strong, portable identity is needed within healthcare differ by role (provider, emergency responder, patient, patient caregiver), and point to at least some degree of difference in core standards by role for:

Credential provisioning
Credential maintenance

- Status/role updates
- Forgot User ID/password
- Biometric enrollment/reenrollment
- Credential de-provisioning (status changes, relationship changes, death)

Proxy extensions of a provisioned identity, and
Metadata accompanying credentials for identity matching between disparate systems

A key differentiator between medical and general commercial identities involves a concept of relative versus pinpoint identity. For many commercial uses of identity credentials, it is possible for people to self-provision an identity with minimal information, and as long as a person can use their credentials to reliably authenticate against them, the same identity can be used in multiple situations with relatively low risk. When a relative identity is used in a fraudulent manner in commercial situations, the losses are more often than not monetary, and the systems which accept, for example, the use of credit cards for online purchases, build into their business models some margin for loss. While for individual consumers, fraudulent use of such identity credentials can have broader impact to such things such as credit scores, there are methods, albeit difficult, to largely remedy identified problems.

However, if an identity is used to inappropriately access pre-existing medical information, the costs, for both a patient and the provider organization can be substantial and non-recoverable. Once medical information is released "into the wild" you can't undo the damage. And you must know exactly who is requesting a release of medical information and their legitimate relationship to the patient before doing so through any automated system.

Medical providers and emergency responders need pinpoint identities in order for requests for information, both in-house and between institutions, to be validly evaluated and made actionable. Fraudulent use of identities by persons in these roles could easily be used to cull patient information to promote medical fraud and create substantial dangers to patients (e.g., accidentally or maliciously changing medication doses in EHR systems).

Within the patient realm, reasonable first steps for moving toward NSTIC identities would be to establish "gold" standards and workflows for identity provisioning and the establishment of necessary metadata which could allow for identity federation between patient portals provided by insurance carriers and health systems as well as health care exchanges. It is important to note that these standards must address exception paths as rigorously as standard provisioning workflows. For example, if a "gold standard" pinpoint-type identity is established, the validity of the identity can be undermined by weak standards for resetting account passwords. Ideally, for an NSTIC type patient identity to be truly and consistently portable, there would need to be a commitment by all participating organizations to the perpetual maintenance of the identities which they establish, or, alternatively, outsource all identity functions to a trusted third party. However, what would be a viable financial model for outsourcing NSTIC medical identity functions without compromising the use of patient metadata for commercial purposes, and what would happen to the validity of established identities if the 3rd party identity organization closes or is sold?

Rather than forming a complete NSTIC health-identity ecosystem, in the near term it may be more viable to use NSTIC health-industry supported standards in a limited way to provision identities within a given system to an agreed-upon standard, such that a receiving system can initially accept a claimed identity as valid. In turn, the receiving system would provision that same identity within its own system and in so doing accept responsibilities for its maintenance—in effect, establishing protocols to facilitate "gold-standard" provisioned identities to be daisy-chained, with identity maintenance functions passing from organization to organization as the need for an identity sunsets, rather than being centrally and perpetually maintained by the initial issuing organization.

Note that while "commercial" and "health" identities would not inherently need to be separate NSTIC identities, designing a general ecosystem to accommodate both would be difficult and could slow the broader commercial use of NSTIC identities. Moreover, internal research at Kaiser Permanente suggests that patients prefer their identity credentials to be separate from other roles. For example, Brokers and Employers who have online access to Kaiser Permanente programs and services do not, by in large, want to use these same credentials to access our patient portal and consumer mobile properties. To that end, Kaiser Permanente retains separate identity repositories for "patient" and "business" roles.

In terms of patient identity standards, including identity provisioning and sign on procedures, sensitivity to population characteristics is necessary. Security controls should be usability tested with those who actually use them, including the elderly and people with limited education. In

line with NSTIC principles, credentialing procedures and security controls should not widen the current “digital divide” due to their complexity or cost.

In closing, the management of medical identity credentials is not trivial in terms of both money and time. While identity management is not the core competence of health care organizations, out of necessity, this competence has been developed, and substantial changes to existing identity management systems, standards and procedures should allow for a migration path from “old” to “new”. With the advent of NSTIC, a reassessment of the role of health care organizations in provisioning and maintaining medical identities seems prudent. That being said, deep participation by the health care industry is highly recommended, with NSTIC soliciting and including both individual health care organizations and health standards organizations, such as HL7 and WEDI, into NSTIC committees and programs.