U.S. Department of Health and Human Services
Office of the National Coordinator for Health Information Technology

Privacy and Security Tiger Team

Health Information Technology Policy Committee

Consumer Choice Technology Hearing

June 29, 2010

Washington, D.C.

Department of Veterans Affairs
Veterans Health Administration Office of Health Information
Written Public Testimony
Duane DeCouteau

Introductions

Madam chair, and distinguished panel members. Thank you for inviting the Department of Veterans Affairs, Veterans Health Administration Office of Health Information, to participate in these demonstrations and report to you our ongoing efforts with regard to Consumer Choice Technologies being developed for use within health information exchanges (HIE).

The Department of Veterans Affairs is committed to the vision that consumer choice can be provided through open, mature, adaptable, service-based architectures and standards.

Road-to-Today

Today's presentation is about implementing advanced security and privacy in the Nationwide Health Information Network (NHIN) from a security practitioner's viewpoint. We demonstrate that the core technologies are themselves fundamentally practical, and that they can meet current and future security and privacy needs within the healthcare community without the need to replace existing electronic health record systems (EHR).

The VA currently participates in a number of standards development organizations as Co-chairs, including Health Level 7, the Organization for the Advancement of Structured Information Standards (OASIS), the American Society for Testing and Materials, the American National Standards Institute-International Committee for Information Technology Standards, the US Technical Advisory Group to the International Standards Organization and others. Health care standards and information models provide basic building blocks needed to respond to the security and privacy needs of our nation's Veterans.

Our road to Consumer Choice Technology has been one of strong collaboration. In addition to Federal partners, such as my distinguished colleague and co-presenter Captain Emory Fry, MD, from the Department of the Navy, we have enjoyed a special and close working relationship with the vendor community through our participation in OASIS. Our OASIS partners include IBM, Sun/Oracle, Jericho Systems, JBoss/Redhat, Axiomatics, Symlabs, Cisco, and others - all of whom share credit for the demonstration today.

We have led and participated in a number of multi-vendor OASIS and Health Information Technology Standards Panel (HITSP) sponsored interoperability demonstrations, including this one, depicting real-world security and privacy scenarios in health care. Other demonstrations include:

- RSA 2010, San Francisco, California (Protecting the Human Genome)
- HIMSS 2009, Chicago, Illinois (Advanced Security and Privacy in Healthcare)
- Ditton Manor 2008, London England (Extensions to Healthcare Security and Privacy Services)
- RSA 2008, San Francisco, California (Healthcare Security and Privacy as a Service)

We selected three illustrative healthcare use cases for demonstration today. This list is not all inclusive but simply representative of the technology and use of standards. These use cases include:

Use case #1 – Consumer chooses to limit access to certain portions of their healthcare record.
A patient being treated for depression has chosen to mask their medications record from outside requesting providers.

Use case #2 – Emergency Treatment Example of Organizational Policy
The health care organization has created policies requiring specific structured ASTM role, or specific HL7 Permissions in order to declare access by way of a purpose of use of “emergency.”

Use case #3 – Protecting the Human Genome
The use case demonstrates an adaptable security and privacy service layer. As medical knowledge advances, our ability to enforce patient choices should adapt to these advances.

I will now respond to the direct questions:

1) Regarding the aspect of how the technology implements the patient's consent and the granular choices given the patient. Health information systems capable of encoding their structured or semi-structured data using standard-based terminologies may use this system to provide varying degrees of access control to clinical data. The patient documents what information they do or do not want to share, under what circumstances they wish to share, and with whom using a patient friendly interface. Their choices are captured in an electronic consent directive that identifies their wishes using standard-based semantics, roles, and concept codes. This consent directive is consumed by the policy engine that ensures that any identified restrictions are applied to a patient's data at the time information is exchanged. Protection of consumer sensitive data is driven entirely by the consent directive that identifies the data to be removed, the context in which the decision should occur, the policy engine that applies the directive, and the redaction service that removes or enforces the patient's wishes. The resultant payload is then passed or denied, in full or in part, to the requesting entity that requested it.

   Put another way, the technology implements the patient's consent by fully and seamlessly managing consent as sets of rules and attributes to be integrated into the existing jurisdictional and organizational security and privacy enforcement system. Our implementation uses and applies the model expressed in HITSP's TP20 Access Control and specified standards of OASIS and their profiles, as well as attributes value sets from HL7, ASTM, SNOMED CT, or LOINC or others. Hence the approach is fully interoperable and capable of sharing its policies, including consumer policies with other health care organizations.

2) In terms of addressing the maturity of the technology, we acknowledge that access control in health care is much less mature than identity and authentication, confidentiality, and data integrity. At the same time, major components exist currently in commercial products from top ranking vendors, which is a key point made in all of our technology demonstrations. Where gaps exist, they are primarily in the underlying information systems and the EHR's inability to specify data attributes (e.g., the sensitivity of a protected information object). While the technology we describe can enforce rules regarding defined sensitivities, it is not the security system's role to define sensitivity, rather which is a function best left to clinical experts and consumers themselves. Major components of the system are currently planned for deployment and are nearing operational status in Kaiser Permanente/VA NHIN and Virtual Lifetime Electronic Health Record (VLER) pilots in San Diego, California. Further expansion of the pilots is planned, with major capabilities expected to be operational in early 2011. For DoD and VA, the system is currently capable of enforcing fine grained consent directives for well defined domains like medications, diagnoses, and laboratory tests. Finally, there is still significant research that needs to be done in identifying the best way to mange access in rapidly changing medical domains.

3) The system has significant advantages in that it is entirely standards based, fine grained, and driven by commodity hardware/software that makes it applicable to ANY healthcare system capable of applying semantic constraint to its data. It can be implemented without wholesale replacement of legacy systems. It employs standards and models already approved by the Office of the National Coordinator. Crucial components of this solution, such as the core policy decision point technology, including 12 proven base security policies are available today at no cost from NHIN CONNECT.

4) We absolutely believe that this technology is scalable so that small and medium-sized providers could implement it. The emphasis on standards and commodity infrastructure allows us to implement the system using a completely open source stack or using proprietary vendor solutions. These implementations can be "black boxed" into consumer-grade appliances that would be easy to install and maintain either on site or in a "software as a service" environment.

5) Regarding interoperability, the system is entirely standards based and thus interoperable at the semantic level. As implemented in the NHIN and VLER demonstrations where data structure is also standardized, the system allows for fully automated, auditable, patient-driven access control. The patient consent directive is exchangeable including as an HL7 CDA R2 Consent Directive, as is the content and format of the computable policy, which is now an OASIS standard. The extent to which this standard can be applied to the data structures at a given organization is variable.

6) The system is inherently designed to be interoperable, and fundamentally there are no overt barriers to interoperability from the HIE perspective. What is missing, however, is a consistent patient policy view across organizations. Patients currently need to negotiate their choices with each provider. Lack of interoperability for consumer choice places significant burden on consumers that leaves them dependent upon health care organizations that see little benefit in restricting the essentially unfettered access they currently enjoy.

7) Resources necessary to implement the consent system in its current form include a consumer preference editor, an organizational policy editor, capability to vet consumer policy against organizational policy, automated acceptance of policy, manual process for policy exceptions, a policy engine, a redaction service, and an HL7 canonical model that enforces system semantics. New work projects in OASIS/HL7 include the development of ontology that would simplify the consumer expression of their choices and possibly improve the efficiency and speed of the policy decision engines.

8) Currently, the system is in a limited production pilot in San Diego, California, with less than 300 patients of a 1,200 shared patient population base between VA and Kaiser Permanente. The next iteration, a DoD/VA pilot in Hampton, Virginia, should add a few thousand more. When fully operational the system will be capable of

serving the entire population of Veterans actively seeking care (about 6 million at any time), plus all patients with registered consumer choices but who are not currently active (meaning that few requests would be expected for their information). The system is expected to easily scale horizontally to support the needs of shared DoD and VA patient populations.

Conclusion

Thank you again for the opportunity to participate in this important hearing on consumer choice and technology options.

We believe that core consumer choice standards are in place. New standards are under development to meet gaps. Multiple vendors have demonstrated the ability to implement consumer choice technology with shipping products. Significant gains in consumer choice can be made without change to or replacement of legacy EHR systems. Key policy decision point solutions exist and are available at no cost. EHR systems need to be able to define and identify sensitive data if security systems are to enforce consumer choice regarding data sensitivity and other aspects under the control of the EHR.