

Testimony for HIT Policy Committee
Information Exchange Workgroup
Provider Directory Task Force
Panel 4 – Technical Requirements

Jeff Barnett
Symantec, Inc.
30 Sept 2010

Introduction

My name is Jeff Barnett, and I am Healthcare Industry Lead for Symantec's User Authentication group. I would like to thank the HIT Policy Committee for this opportunity to testify on the very important and challenging topic of Provider Directories and the importance of *trust* in provider directories as part of a sustainable Health Information Exchange (HIE) strategy. Symantec is a global leader in providing security, storage, and systems management solutions to help our customers – from consumers and small businesses to the largest global organizations – secure and manage their information against more risks at more points. These Symantec technologies and services are directly applicable to the challenges of providing HIEs and Provider Directories.

As HIEs develop, a number of process and technology challenges must be addressed in order to succeed, including:

- Planning for privacy, security and confidentiality
- Building trust among all parties involved
- Addressing more stringent compliance requirements
- Supporting issues unique to large medical files, such as specialized medical images
- Managing and storing a proliferation of data

While these challenges must be addressed as part of creating a sustainable and efficient HIE, my comments as part of this testimony will focus on *building trust amongst all parties involved* in the context of Provider Directories.

More than Security, Trust is the Fundamental Issue

Beyond security itself, building and maintaining trust is a fundamental concern for HIEs as trust is key enabler of sustainability. Aspects include maintaining privacy, security controls, reputation of users and organizations, reliability of information, level of assurance, common security policies, support for audits, compliance with applicable regulations, and interoperability of security technologies. As HIE information is created, stored, and shared, building healthcare professional and patient confidence in security leads to greater adoption and efficiency of HIE services. HIE Services can include exchange of care summary, lab results, electronic prescribing, and administrative transactions (claims & eligibility checking), and management of identity and digital credentials.

To address the myriad of challenges in protecting health information on a large scale across an inter-connected network, HIEs need to address the fundamental issues of knowing who is accessing HIE services, if the users and organizations they represent are trusted, and if the data can be trusted (particularly clinical data). By adopting a trust framework built on identity and authentication of users and organizations, HIEs can build a level of trust so that users feel their information is protected and shared in a manner that upholds the high degree of confidence required.

Addressing Trust Across a Range of Users

HIEs face a number of barriers related to adoption of HIE services; both from individual health care providers and states enabling HIEs. Provider directories facilitate health information exchange both within individual states and across the country, by providing core authentication services for users and organizations transacting on the HIE.

Users across HIEs typically fall into three categories:

- 1) Affiliated individuals (e.g. healthcare professionals, employees of corporations or government agencies)
- 2) Organizations (e.g. providers, payers, pharmacies, government agencies)
- 3) Patients/ Consumers

The types of transactions that these entities engage in include: remote access, purchases and other business transactions, credit card payments, e-mail, electronic signature, and virtual networking. The fundamental capability required to enable trust in these transactions is the ability to identify and authenticate (i.e. validate) the identity of the entities participating in the transactions. Additional security services required for trust in transactions include: confidentiality, integrity and non-repudiation.

Since security needs are not a one-size-fits-all problem, creating a trust framework that can address the myriad of existing requirements, while being flexible enough to support future enhancements to policy and technology provides the best approach.

Question 1: What are the core technical requirements that are needed to enable the establishment of provider directories?

Specific to the ability of a provider directory to enable identity and authentication components as part of the overall directory service, directories should employ a standards-based approach to uniquely identify both users and organizations, a digital identity to unique to them, and technology to authenticate (validate) each transaction. Technologies such as digital certificates (issued from a Public Key Infrastructure for both individuals and web servers) or one-time passwords (OTP) for strong (two-factor) authentication are examples of enabling technologies.

Question 2: What “trust framework” is needed for populating, maintaining and using provider directories?

Ensuring all parties in the trusted ecosystem of health information exchange is critical for building a trusted framework. Authentication enables users on either end of the exchange of health data to trust who the other person (or organization) is on each end.

Authentication of users and transactions vary by the level of assurance required

- Identity of the user or organization
- User’s role and level of access to sensitive information
- Credential associated with the user (e.g. user name and password only would be a low level of assurance)
- How the user is accessing the directory

To maintain interoperability, each participating organization and user must follow the same standards for authentication.



In support of a trusted provider directory, technical controls must work in conjunction with policies to address the following questions:

- 1) Is the information accurate?
- 2) Is the data up-to-date/ current?
- 3) What level of assurance is the information vetted? Does this meet the minimum requirements for the intended use?
- 4) What are the intended uses of the data contained in the provider directory?
- 5) Is the information authoritative?
- 6) Which users can access the information?
- 7) Is certain information only accessible to certain users?
- 8) What types of independent audits or certifications does the provider directory use to ensure compliance?
- 9) How is the individual or organization uniquely identified?
- 10) Does each participating organization within the *trust framework* recognize and accept the identity?
- 11) Is the provider directory interoperable with other directories?

Question 3: What should be the requirements on health information service providers (HISPs) for establishing directories for directed exchange? What are the broad brushes of the requirements?

Specific to authenticating identity for access to provider directories, each participating organization (business entity) and user as part of the directory should be identified electronically through a standard digital identity. As a baseline, NIST 800-63-1 establishes a policy and technology framework that outlines common sets of requirements and is already being explored by a number of healthcare organizations as part of the DEA's requirements on E-Prescribing of Controlled Substances. A substantial number of users (e.g. physicians) who would need to meet the E-Prescribing of Controlled Substances requirements would also be listed in provider directories.

Question 4: What would be the value of an open and standardized approach to directories in this context? Would this enable interoperability across directories? Would accreditation of HISPs be a good way to accomplish this? EHR certification?

Certain services that provider directories deliver, such as identity and authentication controls, have been standardized to provide a degree of interoperability. As a benefit to end users, an approach that reduces the number of duplicate processes (e.g. multiple registrations) and duplicate digital identities (e.g. certificates) across multiple directories would benefit the end users. For example, a single process to validate a user's identity and a single digital identity that is trusted across multiple organizations for multiple business purposes would provide real benefits to end users, which has been highlighted in the recent publication of the National Strategy for Trusted Identities in Cyberspace (NSTIC).