28 June 2006

Office of the National Coordinator for
Health Information Technology

Nationwide Health Information Network Forum

Session Number: 2.6

Session Name: Security

Facilitator: Matt Scholl, National Institute of Standards and Technology (NIST)

Discussant: Johnathan Coleman, SecurityRiskSolutions, LLC

U.S. Department of Health and Human Services

Agenda

Introduction
- Process for the Breakout Discussion
- Description of Content Area

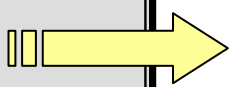
Discussion
- Specific Areas of Variation or Need
- Identification of New Issues
- Architecture Differences
- Requirements Gaps
- Defining Minimal
- Questions to Consortia

Introduction - Session Process

- Please use microphones during discussions – sessions are being audio recorded
- Handouts
  - Functional Requirements .xls spreadsheet
  - Requirements Input Form
- Focus discussion on this functional category
- Not a review of individual requirements
- Requirements with policy implications will be noted and sent to appropriate process for discussion (e.g, HIT Policy Council, etc.)

Introduction - Session Overview

Session Number	Title
2.1	Data Content
2.2	Data Transactions
2.3	Data Transformation
2.4	Information Location and Data Storage
2.5	System Qualities
2.6	Security



Functional Categories to be discussed

Security

- Authentication
- Authorization
- Confidentiality
- Credentialing

Introduction-
Entity Definitions Brief Review

Entity	Definition
Authentication	The ability to uniquely identify and validate (to a reasonable degree) the identity of an entity. These requirements are applicable to systems, services, and organizational actors.
Authorization	The ability to determine and grant access to systems, services and data based on prescribed parameters (instantiated authorization/access policies). For example, the process of granting authority or delegation to specified actors.
Confidentiality	The ability to ensure that data are not disclosed (e.g., viewed, obtained or made known) to unauthorized individuals per organizational policies. Functionality to provide privacy, de-identification, anonymization and re-linking would be included in the confidentiality category.
Credentialing	The process of validating or confirming the qualifications of licensed professionals, e.g., clinical provider. These functional requirements are distinct from authentication and authorization.

Discussion – Quick Review of Identified Issues

- What NHIN services are necessary to support (direct or indirect) identity proofing, authentication, and data to patient mapping in consumer systems?
- What services are needed to support identity proofing, authentication, credentialing, role-based access controls and updates for providers of care?
- There are many policy issues that need to be resolved for consumer management of health data. When these policies develop, what services will be necessary to enable consumer “blocking” of certain data? Consumer management of different levels of data sensitivity?
- From a technical perspective, at what level and by whom are security services most easily handled (i.e., individual provider, care delivery organization, network service provider)?
- Are there special technical services that need to exist to support a variety of consumer roles; care giver, healthcare proxy, legal guardian?
- Is it possible to have a provider authentication approach that is not as weak as the weakest authentication practices at a particular care delivery site?
- How can NHIN components limit the impact of security failures in care delivery organizations?

Discussion – Quick Review of Identified Issues

- If using authentication at provider organizations to access NHIN services, how do users without electronic health records authenticate?
- How can “opt out” be implemented? Is it possible to have “opt out” status that does not have to be protected at every encounter?
- What are the architecture and technology considerations associated with fine-grained “opt-out” or “opt-in” controls (e.g., controlling distribution of specific classes or instances of data or controlling distribution to specific individuals or roles)?
- What NHIN services are necessary if two factor authentication becomes a policy?
- Are there different considerations for authorizations of user roles other than consumers and care providers (e.g., care managers, researchers, public health officials, quality organizations?)
- What policy issues in confidentially and security need to be resolved to advance NHIN functioning?
- Is there a conflict between reasonable requirements for audit and potential requirements not to persist certain patient data within the NHIN? Are there established architectural approaches and technologies for dealing with such a conflict?

Discussion – New Issues

What other issues are there that have not been identified?

Discussion – Specific Areas of Variation or Need

- What NHIN services are necessary to support (direct or indirect) identity proofing, authentication, and data to patient mapping in consumer systems?

Discussion – Specific Areas of Variation or Need

- What services are needed to support identity proofing, authentication, credentialing, role-based access controls and updates for providers of care?

Discussion – Specific Areas of Variation or Need

- There are many policy issues that need to be resolved for consumer management of health data. When these policies develop, what services will be necessary to enable consumer “blocking” of certain data? Consumer management of different levels of data sensitivity?

Discussion – Specific Areas of Variation or Need

- From a technical perspective, at what level and by whom are security services most easily handled (i.e., individual provider, care delivery organization, network service provider)?

Discussion – Specific Areas of Variation or Need

- Are there special technical services that need to exist to support a variety of consumer roles; care giver, healthcare proxy, legal guardian?

Discussion – Specific Areas of Variation or Need

- Is it possible to have a provider authentication approach that is not as weak as the weakest authentication practices at a particular care delivery site?

Discussion – Specific Areas of Variation or Need

- How can NHIN components limit the impact of security failures in care delivery organizations?

Discussion – Specific Areas of Variation or Need

- If using authentication at provider organizations to access NHIN services, how do users without electronic health records authenticate?

Discussion – Specific Areas of Variation or Need

- How can “opt out” be implemented? Is it possible to have “opt out” status that does not have to be protected at every encounter?

Discussion – Specific Areas of Variation or Need

- What are the architecture and technology considerations associated with fine-grained “opt-out” or “opt-in” controls (e.g., controlling distribution of specific classes or instances of data or controlling distribution to specific individuals or roles)?

Discussion – Specific Areas of Variation or Need

- What NHIN services are necessary if two factor authentication becomes a policy?

Discussion – Specific Areas of Variation or Need

- Are there different considerations for authorizations of user roles other than consumers and care providers (e.g., care managers, researchers, public health officials, quality organizations?)

Discussion – Specific Areas of Variation or Need

- What policy issues in confidentially and security need to be resolved to advance NHIN functioning?

Discussion – Specific Areas of Variation or Need

- Is there a conflict between reasonable requirements for audit and potential requirements not to persist certain patient data within the NHIN? Are there established architectural approaches and technologies for dealing with such a conflict?

Discussion of New Issues Identified

- New Issues

Discussion - Architectural Differences

- Are there significant architectural differences?
- How many different architectural approaches are actually represented in this breakout area?
- What are they?

Discussion - Requirements Gaps

What are the areas where there are requirements gaps for this functional category?

Discussion – Defining Minimal

NCVHS needs to eventually refine the >1100 requirements to a “minimal”, but inclusive list. What is the best approach to having “minimal” requirements in this functional category?

Discussion - Questions to Consortia

What questions or issues would you like to ask of the consortia relative to this functional category?

Agenda Review

Wednesday, June 28 Afternoon

1:30- 3:00 pm	Entity Break Out Sessions
3:00- 3:15 pm	Break
3:15- 4:45 pm	Functional Category Breakout Sessions
4:45 pm	Adjourn

Thursday, June 29 Morning

8:00- 9:00 am	Use Case and NHIN Infrastructure Breakout Sessions
9:00- 9:15 am	Break
9:15- 10:15 am	Plenary Session- NHIN Consortia Architecture Response
10:15- 10:30 am	Break
10:30- 12:30 am	Closing Plenary Presentations to NCVHS and Public Comment

Documents for Reference

General

Functionality Requirements XLS

NHIN Requirements Approach

Session Specific

Session 2.6 Specific

Please note: To access embedded documents, please press “esc” key to exit presentation mode