NORTHROP GRUMMAN

2nd NHIN Forum
Approaches to Provider Authentication and Authorization

Wendell Ocasio, M.D.
Principal Clinical Systems Architect, Health Solutions
Northrop Grumman

This document discusses an NHIN Architecture Prototype project made possible by a contract from the Office of the National Coordinator for Health Information Technology (ONC), DHHS. The content is solely the responsibility of the authors and does not necessarily represent the official view of ONC.

DEFINING THE FUTURE

NORTHROP GRUMMAN

Definitions

Term	Subject	Description	Comments	Examples
Authentication	User	Determine whether the end-user is actually the individual he/she claims to be	Usually lasts for the duration of session	Username + password Smart cards Biometrics
Authorization	Request	Determine whether a requested service should be provided or denied	Requester may not be the same as the end-user (e.g., office staff acting on behalf of physician)	Dr. Kildare is authorized to receive lab test results on patient John Smith
Assertion	Information about user or requester	Information passed between systems in support of authorization	The receiver of the assertion cannot independently validate (i.e. must trust) the truth of the assertion	Dr. Kildare's EHR asserts to a Data Location Service that Dr. Kildare is requesting lab results

NORTHROP GRUMMAN

Authentication options

User logs on into	Authentication done by	Implications	Pros	Cons
Edge system	Edge system	Edge system must assert identity of user	▪ Easy to implement ▪ Local control over account provisioning	▪ Trust required ▪ Identity matching across domains
Edge system	Health Information Network Authentication Service	Single-sign on across multiple edge applications	▪ Easier for users ▪ Larger identity domain	▪ Harder to implement ▪ Account provisioning
Health Information Network Service Portal	Health Information Network Service Portal	Portal can be considered another kind of edge system	▪ Allows access to users who do not have EHRs or other edge systems	▪ Account provisioning across organizations

NORTHROP GRUMMAN

Authorization options (not mutually exclusive)

Location where rules are applied	Implications	Pros	Cons
Requesting edge system	Authorization is asserted or implied by the request	▪ Simplest to implement (many edge applications already include authorization mechanisms)	▪ Requires full trust ▪ Patient consent can only be applied by on-the-spot assertion
Data provider edge system	Access control rules stored along with the data	▪ Data owners exert more direct control – less trust ▪ Good support for patient-specific rules	▪ Requestor identity must be asserted ▪ Patient preferences individually maintained at each data source
Health Information Network Service Provider	Decouples authorization rules from both data requestor and provider	▪ Patient preferences can be maintained in one place	▪ Requires discovery of service provider maintaining patient preferences (may differ from provider facilitating request transaction)

NORTHROP GRUMMAN

Types of Assertions

Information asserted	Implications	Pros	Cons

Identity of user, requester, or requester's organization	Authorization to be determined based on asserted identity	▪ Flexibility – authorization rules can be applied at multiple places
		▪ Supports provider-based access control
			▪ Requires shared understanding of identity. Options:
			  ▪ Shared directory
			  ▪ Unique identifier
			  ▪ Probabilistic matching

Role	Authorization to be determined based on asserted role	▪ Supports role-based access control, which can simplify authorization rules	▪ Does not support provider-based access control lists ▪ Requires role standardization
Authorization	Assertion can be explicitly included in message or implicit (assumed)	▪ Does not require shared identity or role standardization	▪ Requires highest degree of trust