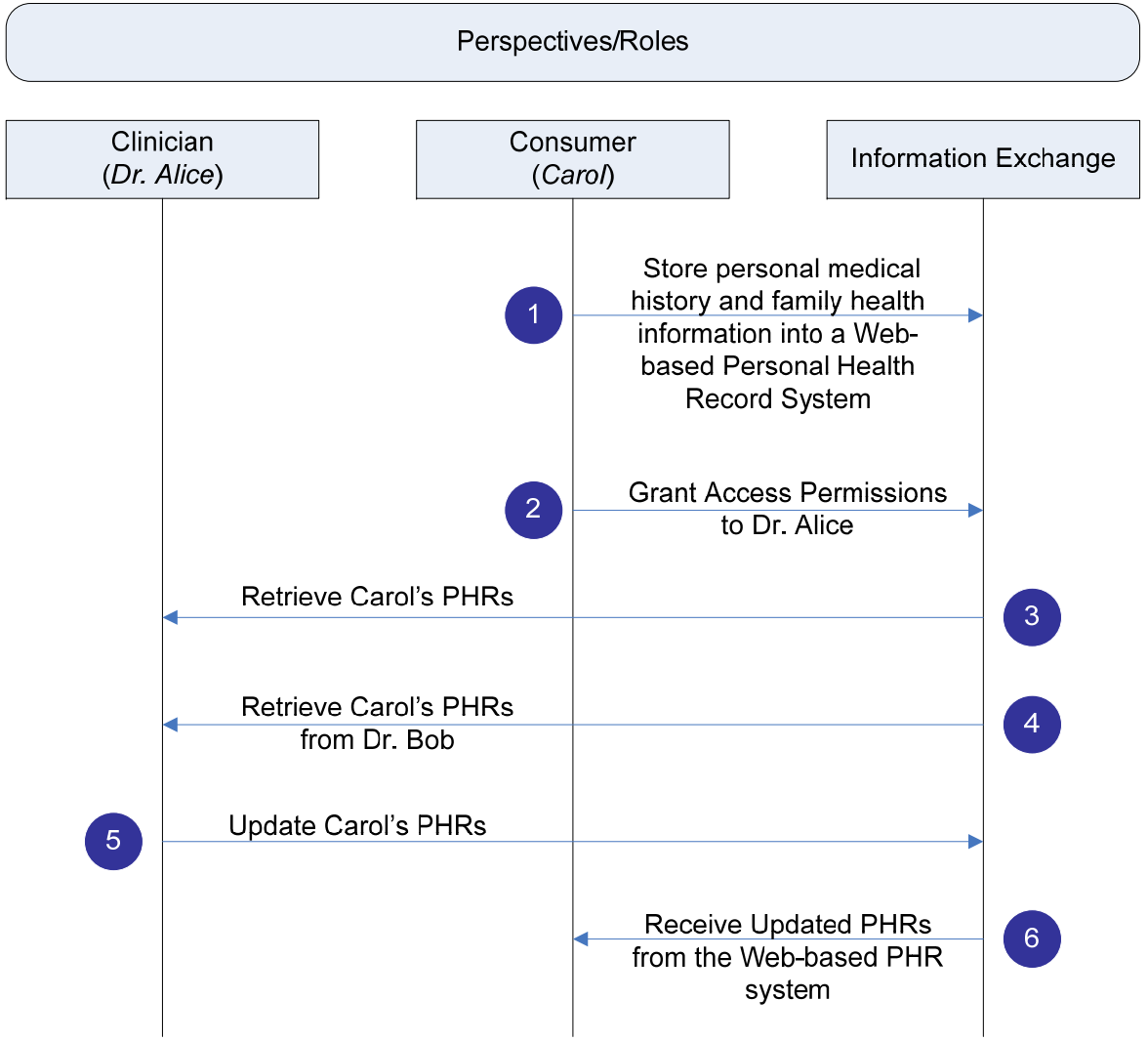
Architecting Measurable Security in Health Information Exchange Using SCAP

Ken Lin, Dan Steinberg
Baltimore, MD
10/27/09

Let’s start with a simple “shotgun” question

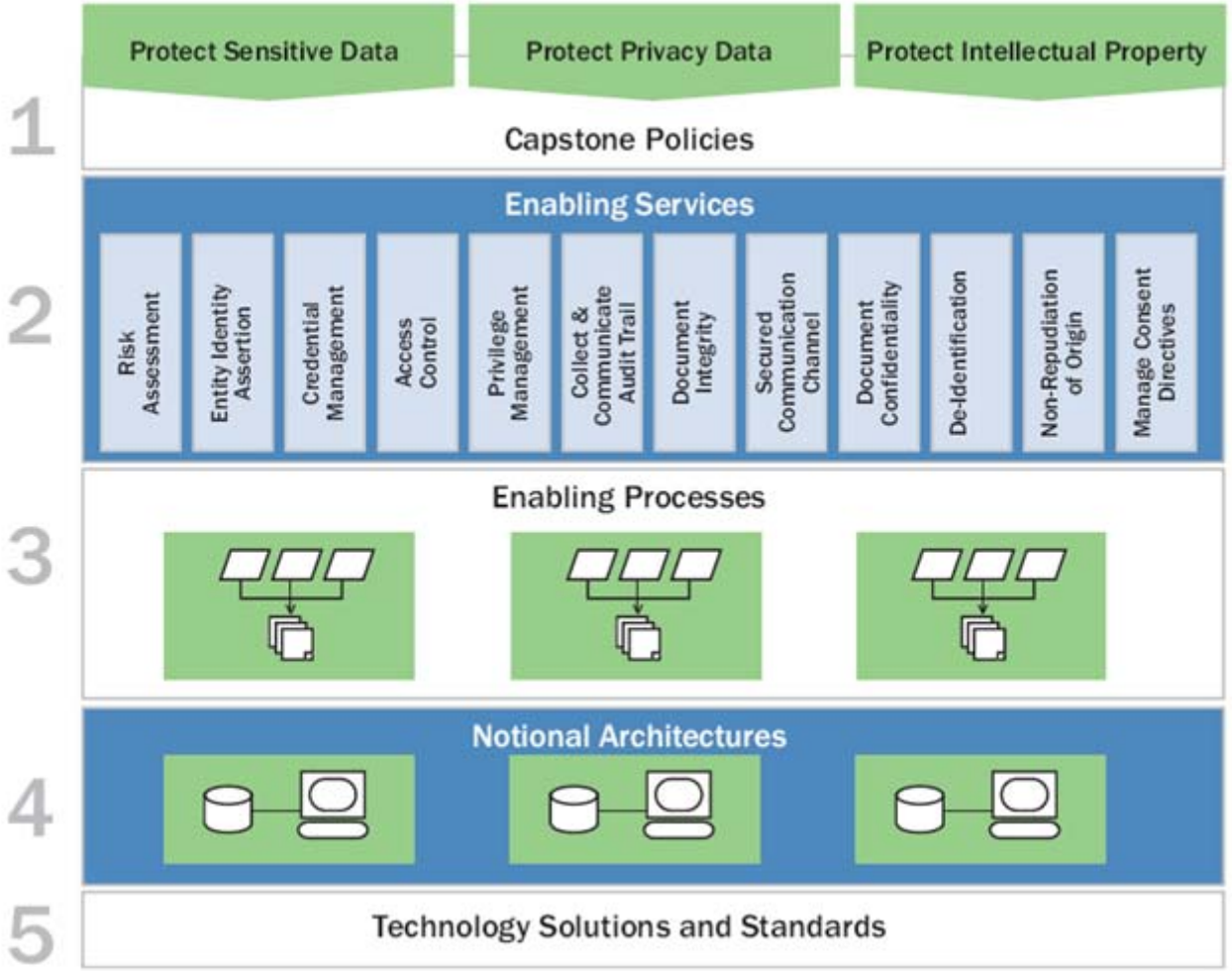
I own a shotgun. Am I secure?

Let’s look at a typical health information exchange scenario



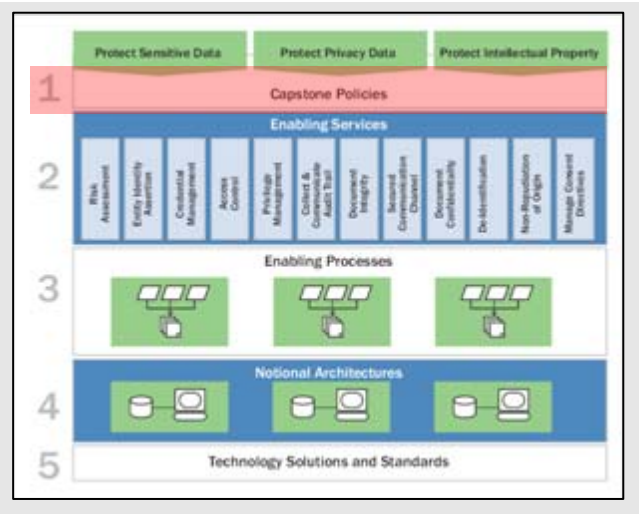
How to “implement” security in this scenario?

To avoid the “shotgun” approach, a multi-layer framework is needed



Source: NISTIR 7497

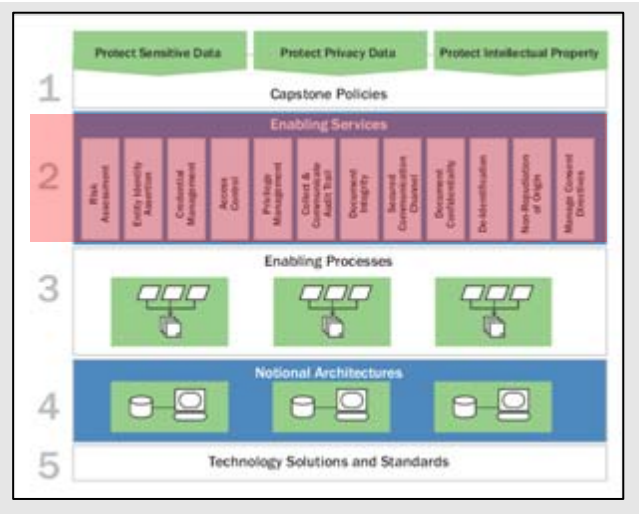
Step 1: Identify Capstone Policies

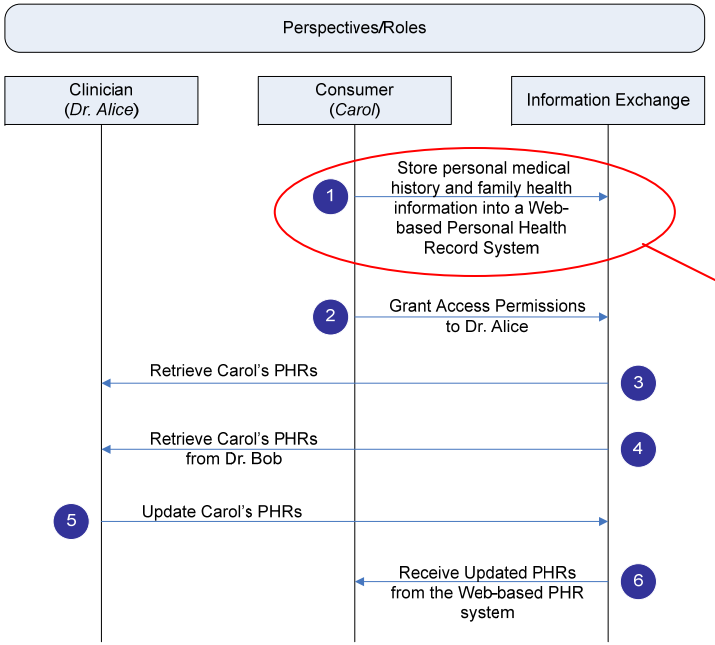


- National Regulations
  - HIPAA Privacy and Security Rules
- State and Local Regulations
  - Requires the disclosure of PHI to any healthcare provider at the patient's written request
  - Requires the provider to disclose to the patient or a patient's representative or guardian if there is a known or suspected breach of the patient's unencrypted information
- Organization (HIE Entity) Policies
  - Carol, and anyone to whom she grants access to her account, must log in using a username and ID
  - Passwords must have a minimum "strength," as described below
  - Carol, and anyone to whom she grants access to her account, must use a digital certificate to access her account
  - Carol, and anyone to whom she grants access to her account, must use a hardware token to assert their identity
  - Carol has unrestricted access to her own PHR
  - Carol has unlimited privileges to grant access and privileges to others, including privileges to read, write, and edit her account

Source: NISTIR 7497

Step 2: Identify Enabling Services

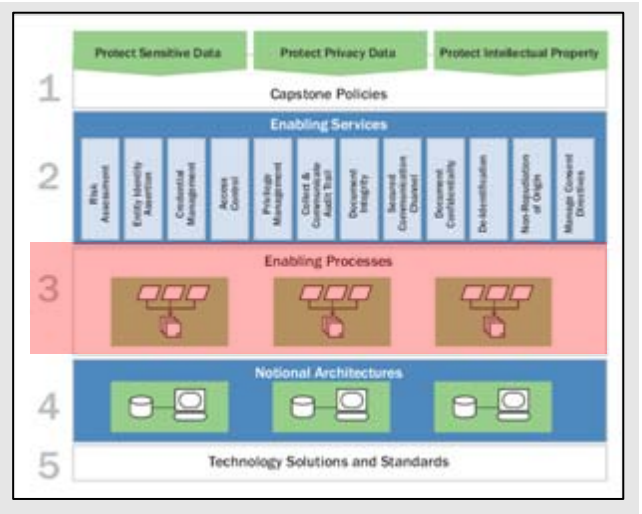




HIE #	HIE Description	Enabling Services	Enabling Services Description
1	Carol stores her and her family's health information into a Web-based Personal Health Record (PHR) system	Risk Assessment	Risk assessment is used to analyze the business risks of compromising the security and privacy of the health information exchanged.
		Entity Identity Assertion	The Web-based PHR requires Carol to identify herself using a registered credential every time she logs in.
		Access Control	The Web-based PHR grants access permissions based on privileges an authenticated individual has.
		Credential Management	The Web-based PHR that Carol selects will require Carol to use certain types of credentials to register.
		Privilege Management	Carol has full access permissions to her PHR and she can assign access permissions to her doctors.
		Audit Trail	All accesses to Carol's Web-based PHR will be logged. Suspicious accesses will trigger warning messages that will be sent to Carol.
		Secure Communication Channel	All information transmitted is secured between Carol's terminal and the Web-based PHR.

Source: NISTIR 7497

Step 3: Develop Enabling Processes



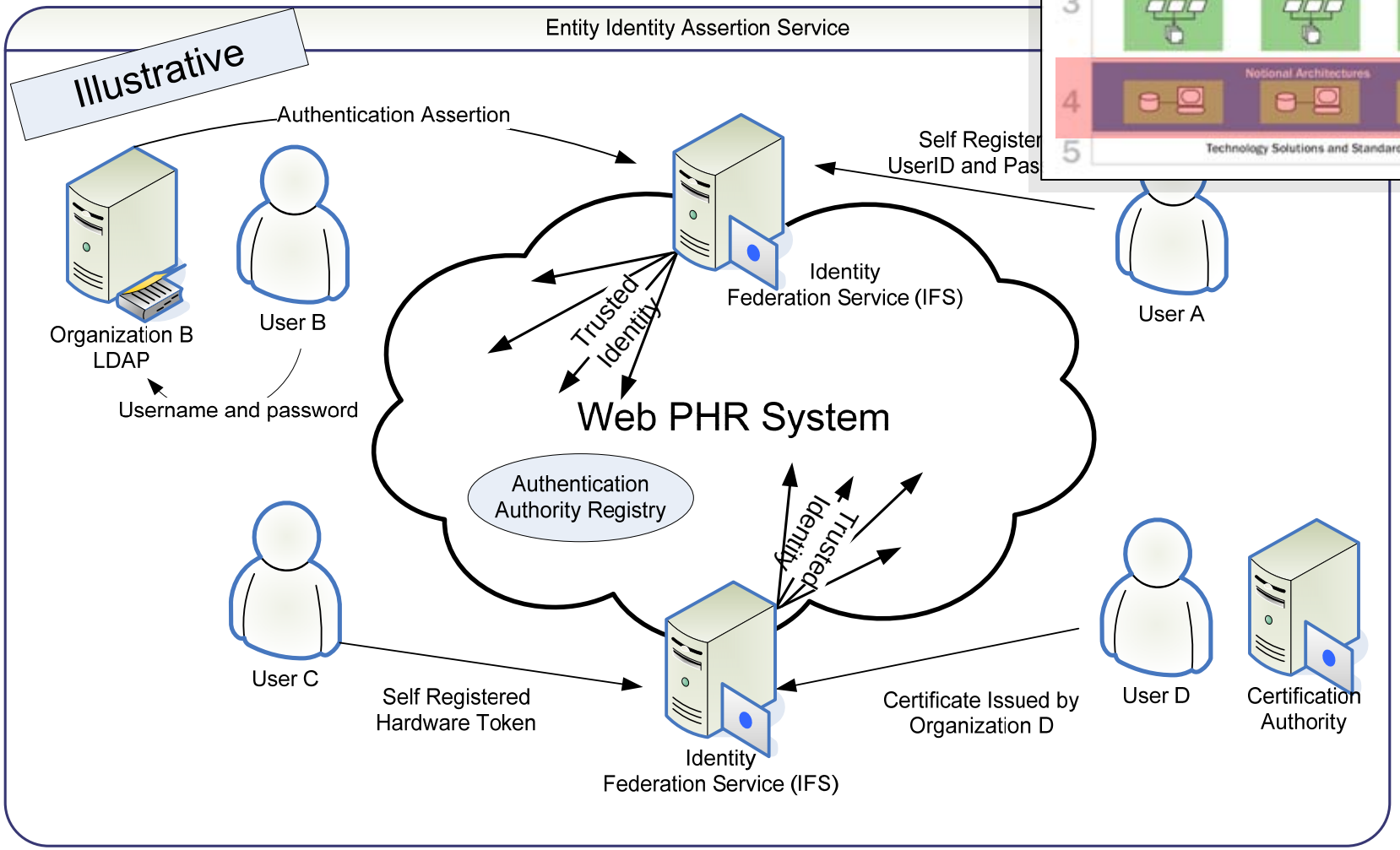
- The Entity Identity Assertion service of the Web-based PHR system has the following requirements:

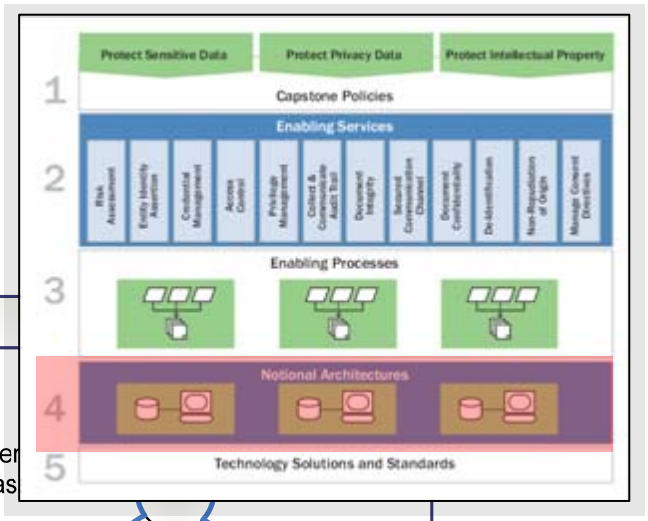
- The system shall accept three types of credentials to authenticate users (including service providers, consumers, and any others):
  - User created ID with Strong password;
  - Digital certificates; and
  - Hardware tokens.
- The system shall authenticate every transaction.
- The system shall accept credentials (any of the three types) issued from trusted third parties.

Credentials	Processes
User ID and Password	• Passwords must be stored in irreversible encrypted form and the password file cannot be viewed in unencrypted form. • A password must not be displayed on the data entry/display device. • Passwords must be at least eight characters long. • Passwords must be composed of at least three of the following: English uppercase letters, English lowercase letters, numeric characters, and special characters. • Password lifetime will not exceed 60 days. • Users cannot use the previous six passwords. • The system will give the user a choice of alternative passwords from which to chose. • Passwords must be changed by the user after initial logon.
Digital Certificates	• The certificate must be an X.509v3 certificate. • The certificate must be within the valid period. • The certificate must be verified and validated through authentication. • The system will not issue digital certificates. Users will present trusted third party issued certificates that are valid and verifiable by the system.
Hardware Tokens	• The system will accept and support pre-approved types of hardware tokens as authentication credentials.

Source: NISTIR 7497

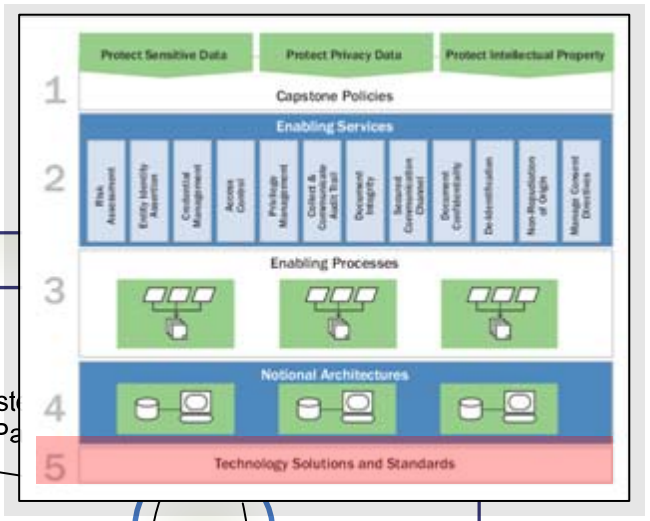
Step 4: Develop Notional Architecture





Source: NISTIR 7497

Step 5: Select Technical Solutions



Illustrative

Entity Identity Assertion Service

Single Sign On Portal

Authentication Assertion

OpenSAML

Self Regist
UserID and Pa

Organization B
LDAP

User B

Username and password

Trusted
Identity

Identity
Federation Service (IFS)

User A

Web PHR System

Authentication
Authority Registry

Trusted
Identity

User C

Self Registered
Hardware Token

Identity
Federation Service (IFS)

Certificate Issued by
Organization D

User D

Certification
Authority

Hardware Token

X.509 Certificate

Source: NISTIR 7497

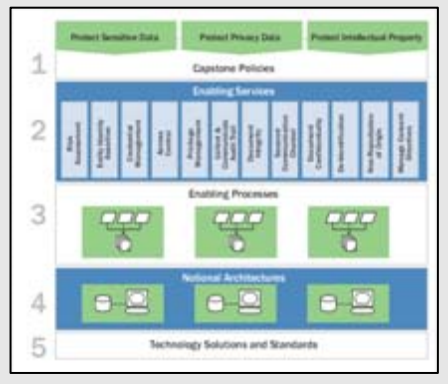
The “Information Exchange” part has been secured based on policies, but to create a “Trust Fabric”, operations assurance are required

- In order for HIE entities to “Trust” each other, certain level of operations assurance at the “End Points” needs to be established:
  - How often does an entity scan their systems for vulnerabilities?
  - How does an entity mitigate security flaws?
  - Does an entity harden their platform and perform regular configuration management?
- SCAP can automate these tasks and establish the basic “Trust Fabric”
- To build “Measurable” Trust Fabric between Health Information Exchange entities:
  - “Measurable” needs to be defined in the context of information exchange (i.e., Risk profiles) and accepted by the participating entities
  - Define agreed-upon risk levels between HIE entities
  - “Certified” XCCDFs and OVALs for each product involved in the transaction
  - Each participating organization performs their due diligence on SCAP

As the adoption of Health Information Technology increases, operations assurance will have an impact on information exchange and an organization's security posture

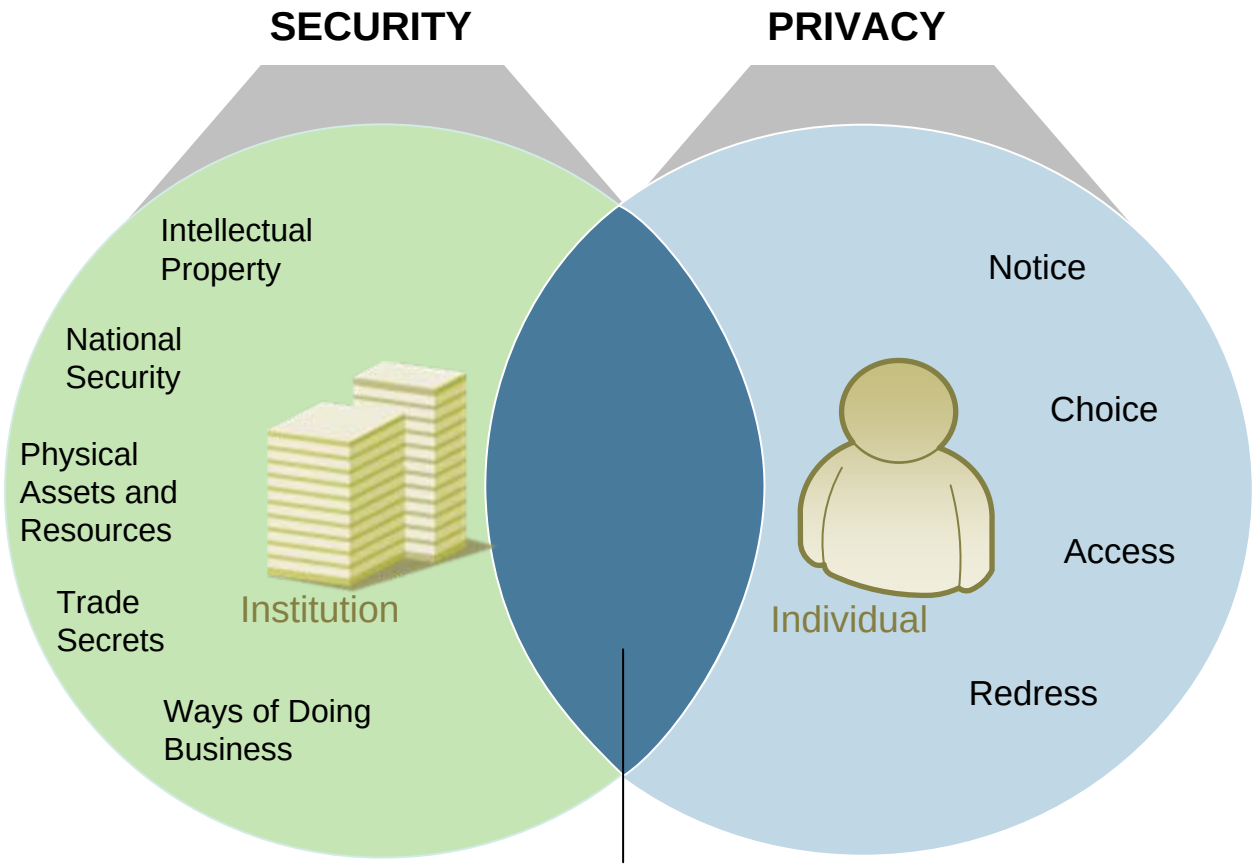
- SCAP has the potential to help an organization implement automatic security management (e.g., patch management, and vulnerability management) and increase operations assurance consistently

- As a precedent, however, health care organizations must ensure they have developed their health privacy and security architectures consistently with requirements and business needs
  - Laws
  - Regulations
  - Policies
  - Standards
  - Institutional Requirements



- Don't forget the security framework! Look at all the layers as an integral piece. NISTIR 7497 has the whole story

SCAP may also assist in addressing privacy concerns, particularly those that intersect with security concerns



Safeguarding a individual's personally identifiable information

Privacy and Security are distinct but related disciplines that share an interest in a number of topics.

SCAP has definite relevance in this area of overlap.

Future uses for SCAP in healthcare environments may involve expanding its use to protecting privacy

- Adoption of EHRs/Meaningful Use
  - ONC HIT Policy Committee Meaningful use matrix requires users to “Ensure adequate privacy and security protections for personal health information”
  - Specific 2011 “meaningful use” standards include “Compliance with HIPAA Privacy and Security Rules and state laws” and “Compliance with fair data sharing practices set forth in the Nationwide Privacy and Security Framework”
- SCAP can help with the protection of private information, notably Protected Health Information (PHI) under the HIPAA Security Rule
  - Risk analysis (especially assessment of vulnerabilities)
  - Information system activity review
  - Evaluation (periodic technical assessment)
  - Audit controls
- Applications of SCAP can assist with other automated, electronic approaches to protecting privacy
  - Privacy engineering
  - Consent tracking
  - Training and education
  - Web-enabled privacy

Questions/Discussion