Enforcing Patient Privacy in Healthcare

HIMSS 2011 Annual Conference and Exhibit
February 20-24, 2011
Orange County Convention Center, Orlando, FL.

Mike Davis/VA
Duane DeCouteau
David Staggs

Richard Thoreson/SAMHSA
Enforcing Patient Privacy in Healthcare

Advanced technology demonstration of the President's Council of Advisors on Science and Technology (PCAST) recommendations for the use of tagged data in the enforcement of patient privacy and secure access to protected individually identifiable health information in Health Information Technology systems.

Protected information objects are tagged with security attributes ● Tagged objects provisioned to security system ● User makes authorized request for information ● System checks patient consent directive ● Information returned

Healthcare Scenarios

• Enforce patient privacy rules by using decision information tagged with patient privacy choices (e.g., HL7 confidentiality code, SNOMED-CT, identity, POU, role, location, decision, Opt-In).

• Enforce organizational privacy rules by using decision information tagged with data privacy attributes (e.g. HL7 confidentiality code groups, SNOMED-CT, identity, POU, roles, location, decision).
Demonstrate an attribute-based access control approach for the enforcement of organizational and patient-controlled privacy meeting the President’s HIT Report.*

- Use HL7 standard sensitivity vocabulary to “tag” electronic health record information objects with fine-grained attributes expressing patient privacy preferences.

- Use currently available commercial security products to create/enforce OASIS XACML standards-based policy rules

* HIT Report = PCAST Health Information Technology Report: http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-health-it-report.pdf

HL7  = Health Level Seven
OASIS = Organization for the Advancement of Structured Information Standards
XACML = eXtensible Access Control Markup Language
Privacy Enforcement Architecture

1. Apply and provision tagged objects
2. Apply patient privacy preferences
3. Get request and permissions
4. Decision/Response
Features


Security ● Efficiency ● Ease-of-use ● Confidence ● Increased privacy for individuals ● Greater choice ● Opportunities for innovation

Technical Features

- DHHS approved standards
- Standard Clinical Roles (ASTM, HL7)
- Standard Web-Service Protocols (SAML, XACML)
- Standard Information Models (HL7 Security and Privacy)
- Standard Reference Models (OASIS Cross-Enterprise Security and Privacy Access Control (XSPA))
Enforcing Patient Privacy in Healthcare

Advanced technology demonstration of the President’s Council of Advisors on Science and Technology (PCAST) recommendations for the use of tagged data in the enforcement of patient privacy and secure access to protected individually identifiable health information in Health Information Technology systems.

**Healthcare Scenarios**

- Enforce patient privacy rules by using decision information tagged with patient privacy choices (e.g., HL7 confidentiality code, SNOMED-CT, identity, POU, role, location, decision, Opt-In).
- Enforce organizational privacy rules by using decision information tagged with data privacy attributes (e.g. HL7 confidentiality code groups, SNOMED-CT, identity, POU, roles, location, decision).