Security Considerations for Enabling State, Regional, and National-Level Trusted Health Information Exchange

Presented at the *Safeguarding Health Information: Building Assurance through HIPAA Security* Conference

By Eric Heflin, Dir of Standards and Interoperability, Medicity

Hosted by the HHS Office for Civil Rights (OCR) and the National Institute of Standards and Technology (NIST)

May 10, 2011

MEDICITY

Agenda for Cross-Gateway Security Considerations

- Speaker Intro
- Context
- Cross-Gateway HIPAA
- Detailed Case Study
- Gaps
- Lessons Learned
- Security Myths (Busted)
- Q&A

MEDICITY

Speaker Background

- Director of Standards and Interoperability, Medicity
- Chair of the Nationwide Health Information Network (NHIN/NwHIN) Exchange Specifications Factory Security and Privacy Workgroup
- Coauthor of eight 2010 NHIN production specifications
- Voting member of the IHE's Information Technology Infrastructure Workgroup, and Planning Committee
- Participated in former HITSP Security, Privacy, and Infrastructure Workgroup
- Architect of multiple state-wide and regional health information exchanges (HIEs)
- Direct Project/S&I Framework voting member
- Coauthor of state security, privacy, informing, and consent regulations
- Author of new CAQH CORE II Advanced Connectivity Rule security section
- **All thoughts are my own, and not necessary those of Medicity, the Nationwide Health Information Network workgroups, the IHE, etc. Should not be construed as legal advice.**

MEDICITY

Cross-Gateway HIPAA

- Pivotal question: "Can we build HIPAA-compliant federated trust systems for healthcare information exchange?"

- Today we're going to be discussing how HIPAA Security and Privacy protections work across organizational boundaries
- HIPAA/HITECH provided general guidance with intentional flexibility that can guide security and privacy protections across regional, state, federal, and even international healthcare exchanges
- Many technical capabilities for cross-gateway exchange supporting HIPAA will be discussed

MEDICITY

Terms Used

- **Cross-gateway:** Exchange (one way or bidirectional) between two distinct organizations, often called “cross-community”
- **Organization:** A legal entity with consistent policy, operating procedures, and subject to the same laws / regulations
- **HIPAA:** For this presentation, I use “HIPAA” as a reference to both to HIPAA and HITECH
- **Federated trust:** Ability to extend an organization’s internal trust model to other organizations

MEDICITY

The Challenge (From a Technical Security Perspective)

CONTEXT

MEDICITY

Overview - Context

- Securely exchanging healthcare-related data **inside** a single organization can be challenging:
  - Single sign on
  - Separation of control/responsibilities
  - Logging
  - User identity management
  - Roles
  - Access control
  - IT physical security

MEDICITY

Overview - Context

- Securely exchanging healthcare-related data **across** different organizational boundaries (states, regional HIEs, federal/private exchange, international exchange) can seem insurmountable:
  - Different legal jurisdictions
  - Conflicting requirements
  - Supporting consumer (patient) preferences
  - Desire to automate
  - Distributed architecture
  - Extending legacy systems
  - Mandate to be secure

MEDICITY

Overview - Is It Possible?

- Many are asking if it is even possible to securely exchange healthcare data across boundaries?
- The goal of my presentation today is to give you some factual information, and some personal perspectives, to help provide you with information to make an informed decision about IF, HOW, and WHEN you should consider exchange with other organizations, from a technical security perspective.
- Also will share some painful lessons learned in the trenches.

MEDICITY

What's Driving Cross-Gateway Trust?

- HHS/ONC vision
  - NHIN/NwHIN
  - Direct Project
  - S&I Framework Initiatives
- Congress
  - ARRA/Meaningful Use/HIPAA
- Desire for Better Outcomes
- Consumer (Patient) Demand
- Cost Pressures

MEDICITY

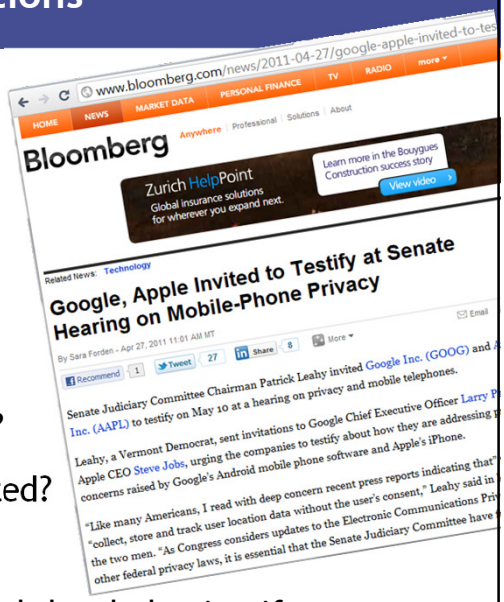
Show of Hands…

- Do you have an iPhone?
- Do you have an Android device?
- What is happening today in Congress related to these products and consumer privacy?

MEDICITY

Consumer (Patient) Trust Expectations

- Headlines from
  - Google
  - Sony
  - Apple
- Millions of HIT HHS breach notifications
- How many incidents remain unreported?
- How many weaknesses remain unexploited?



- HIPAA sets a floor for good practices, and thus helps justify consumer trust in healthcare data exchange

MEDICITY

Examples Demonstrating Secure Exchange

- NwHIN (Nationwide Health Information Network ONC/HHS project)
  - Based on IHE standards
  - In production
  - Detailed case study
- Direct Project (ONC/HHS project)
  - Based on IETF email, and an optional IHE standard
  - Pilot
- Many regional, several state, health information exchanges
  - Mostly based on NwHIN specifications
- epSOS (Smart Open Services for European Patients)
  - Based on IHE standards
  - Initiating phase

MEDICITY

A Few Basic Concepts

BASICS

MEDICITY

A Trust Hierarchy

- Ethical/Philosophical
- Legal
- Regulatory
- Policy
- Implementations
- Operating Procedures
- Iterative Evaluation and Improvement

Underpinnings

Aspirations

- Goal: Confidence in the trustworthiness in the system

MEDICITY

Types of Trust Models

Type	Multiple Applications	Multiple Security Domains	Multiple Organizations	Example
Monolithic	-	-	-	Large HIS app
Enterprise	Yes	Yes	-	EMR, small HIS, Admitting, LIS
Cross Enterprise (Federated Trust)	Yes	Yes	Yes	NwHIN
Hybrid	Yes	Yes	Yes	Several states

MEDICITY

Fundamental Trust Questions

- What entities trust other entities?
- What are you protecting the information from?
- What are the legal constraints?

MEDICITY

Key Trust Concepts

- Identity Proofing (levels of assurance)
- Relying Party
- Asserting Party
- PKI
- Hashing/Digital Signing
- Encryption
- Non-Repudiation of Action and Origin
- Reacting to compromised trust

MEDICITY

Requirements for Federated Trust

- Technical enforcement of applicable legislation and regulation
- Parties directly trust each other
  - Or
- At least one mutually trusted 3rd party
- Shared critical policies
- Technical interoperability (containers, keys encryption, services)
- Ability to identify participants in the chain of trust
- Ability to prove certain events occurred
- Expression and enforcement of organization local policy
- Expression and enforcement of consumer/patient preferences

MEDICITY

Cross-Gateway HIPAA Compliant Solutions Exist

- Capabilities exist and are in production today to:
  - Secure the communications channel
  - Identify both participants to an exchange with high assurance
  - Enable auditing of the users and/or computers involved
  - Purpose of the exchange
- Specifically:
  - TLS
  - 2-way-TLS
  - ATNA and SAML 2.0
  - SAML attributes

MEDICITY

Cross-Gateway Policy Solutions Exist

- Exchanges are in production now allowing:
  - Expression of basic computable policy
  - Links to non-computable advanced policy identifiers
  - Local policy enforcement across organization boundaries
- Specifically:
  - XSPA, XACML, BPPC
  - SAML

MEDICITY

Cross-Gateway Audit Logging Solutions Exist

- HIPAA Accounting requirements:
  - Proving certain actions
  - Logging
- Specifically:
  - 2-way-TLS node authentication
  - ATNA audit logging
  - Consistent Time (CT)

MEDICITY

Creating A Trust Fabric

- Adding the prior concepts together, along with variations such as multiple trusted 3rd parties, can result in the creation of a trust fabric
- All participants agree to
  - Use cases supported
  - Minimal common policy and practices
  - Agree to that which shall be trusted

MEDICITY

CROSS-GATEWAY HIPAA

MEDICITY

Crosswalk Between HIPAA and Technology

- The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the **confidentiality**, **integrity**, and **security** of electronic protected health information. – HHS
- A major goal of the Security Rule is to protect the **privacy** of individuals' health information while allowing covered entities to adopt new technologies to improve the quality and efficiency of patient care. - HHS
- HITECH, among other things, extends HIPAA to cross-gateway exchange in many cases
- The text of the final regulation can be found at 45 CFR Part 160 and Part 164, Subparts A and C

MEDICITY

How Can Security Be Enforced?

- SAML: Can ensure roles justify access to requested data. Responding gateway can inspect SAML attributes and decide to allow or deny the request.
- ATNA logging: Can ensure all cross-gateway requests and responses are memorialized.

MEDICITY

Crosswalk: HIPAA and Cross-Gateway Technology

- Below is a cross walk between some relevant HIPAA requirements and potentially applicable technical solutions (many from the IHE)
- **Confidentiality, Security, Privacy:** SAML, XACML, XSPA, ISO healthcare role, purpose of use attributes
- **Integrity:** Digital Signatures
- **Prevent Impermissible uses or disclosure:** SAML, ATNA logging, HPD
- **Audit control:** ATNA logging
- **Access control:** SAML, XUA, HPD, PWP
- **Transmission security:** 2-way-TLS

MEDICITY

Next

- Next, we'll quickly "inventory" the technical components available
- Then we'll do a detailed case study of how these technical components can be assembled into a cross-gateway solution supporting HIPAA

MEDICITY

Key Cross-Gateway Technologies

- SAML 2.0 – Security Assertion Markup Language
  - Can supply cross enterprise security information
  - Supports multiple models for end-user authentication
  - Supports system-level requests
  - Policy document links
  - Patient preferences document links
  - Roles (PurposeOfUse)
  - Basis for significant HIPAA cross-gateway functionality
  - And much more

MEDICITY

Key Cross-Gateway Technologies

- XCPD - Cross-Community Patient Discovery
  - Also NwHIN Patient Discovery spec
  - Method to determine existence of patients across gateways
  - Announce intentional side effect
  - Secured with SAML 2.0 (NwHIN), 2-way-TLS, ATNA logging, PKI
- XCA – Cross-Community Access
  - Also NwHIN Query for Document/Retrieve Documents
  - Method of listing and obtaining clinical content (and other types as well) across gateways
  - Secured with SAML 2.0 (NwHIN), 2-way-TLS, ATNA logging, PKI

MEDICITY

Key Cross-Gateway Technologies

- XACML – eXtensible Access Control Markup Language
  - Partially sufficient OASIS standard for expression of policy
  - Rule based
  - Probably needs additional constraints
- XSPA – Cross-Enterprise Security and Privacy Authorization
  - A structural container OASIS standard for expression of consumer preferences
  - Was created at the request of the NwHIN
  - Largely contains name=value pairs
  - Contents are essentially undefined

MEDICITY

Cross-Gateway Common Policies

- Legal and technical enrollment process
- Compliance certification process
- Adding, changing, removing systems and users within participating organizations
- Levels of identity proofing (low through high, see NSTIC)
- Types of user authentication
- User access control
- Trustworthy computing best IT practices
- Incident response
- Aggrieved party resolution

MEDICITY

Cross-Gateway HIPAA

- Combining the prior technologies (SAML, XCPD, etc.) with common policy can indeed result in a HIPAA-compliant cross-gateway system
- Next is a detailed case study employing these concepts

MEDICITY

NwHIN CASE STUDY

MEDICITY

Cross-Gateway Security in Action

- Now we'll take a detailed look at how the Nationwide Health Information Network (NHIN or NwHIN) employs many of the prior concepts to implementation HIPAA-compliant cross-gateway healthcare information exchange

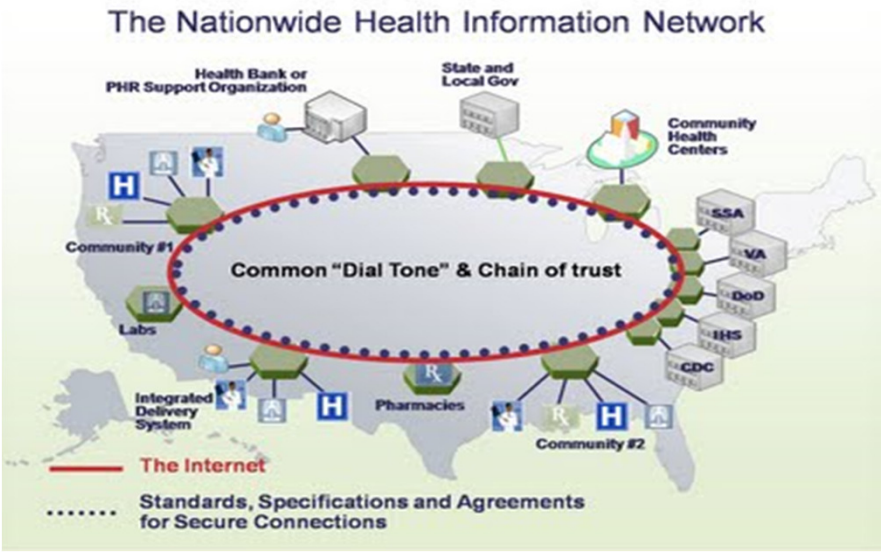
MEDICITY

NwHIN HIPAA Support

- Supports HIPAA via a combination of
  - Legal agreements (DURSA)
  - Operational support
  - Allowing for exchange of security information
  - Supporting local autonomy (roles, policy, access control)
  - Secure transport
  - Fine-grained auditing of all gateway activities (redundantly)
  - Extensible via registry, profiles, and layering of services

MEDICITY

NwHIN Vision



Source: ONC

MEDICITY

NwHIN Case Study

- Is fundamentally a “system level trust model”
- Strong gateway-to-gateway trust
- Heavily leverages Public Key Infrastructure (PKI)
- Employs a secure channel, with SOAP messages + SAML 2.0
- Uses an ONC-governed Certification Authority (CA)
- Has been reviewed using Threat/Risk Modeling
- By philosophy does not try to dictate that behind the Gateway
- A human user is only a “attribute” of Gateway communications
- All activities between gateways are securely logged
- Provides for automation and user-directed activities

MEDICITY

NwHIN Risk Mitigation

- Requires a mutual authentication encrypted channel (2-way-TLS)
  - NIST: This allows most threats to "fall away" by virtue of this design

Table 2-2. Threats Addressed by Current Web Service Standards

	Message Alteration	Loss of Confidentiality	Falsified Message	Man in the Middle	Principal Spoofing	Forged Claims	Replay of Message Parts	Replay of Message	Denial of Service
XML Encryption		X		X	X	X	X		
XML Signature	X		X		X	X	X	X	
WS-Security Tokens			X		X	X			
WS-Addressing								X	
SSL/TLS	X	X	X*	X	X*	X*	X		
SSL/TLS with client certificates	X	X	X	X	X	X	X		
HTTP Authentication			X		X	X			

* Threat mitigated only for provider messages to requester, not for requester messages to provider.

Source: NIST

MEDICITY

NwHIN Risk Mitigation

- Remaining threats are best solved by other mechanisms
- Replay attacks:
  - Mitigated by signed timestamps
- Denial of service:
  - Mitigated by perimeter systems

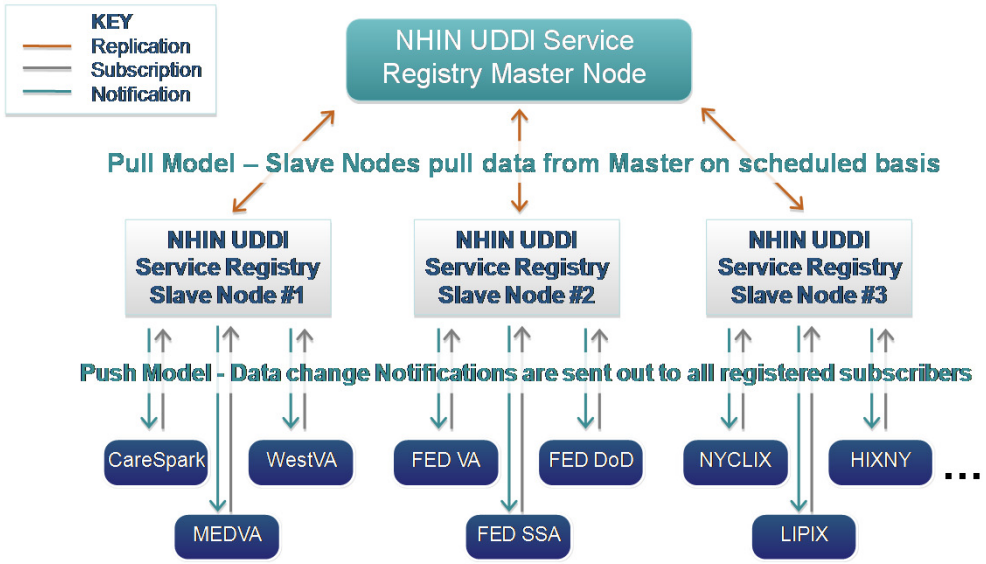
MEDICITY

NwHIN UDDI Use/Support

- UDDI - Universal Description and Discovery Interface
- UDDI OASIS Standard
- Can be thought of as a single, secure, and authoritative directory of critical NwHIN Gateway information
- Will likely be used in the future for version control
- Supports the HHS / HIPAA overarching objective of extensibility, and helps ensure correct identification of authorized exchange partners

MEDICITY

NwHIN UDDI



Source: ONC

MEDICITY

NwHIN UDDI Use/Support (Cont.)

- In 2009 the NwHIN Spec Factory completed the UDDI client specification
- In production use
- Specifies the optional use of the ONC-governed UDDI for:
  - Determining end points
  - Obtaining WSDLs
  - ~~Obtaining public keys~~ lesson learned!
  - Obtaining additional organization info (TBD versioning, capabilities)
  - New services support
- Goals:
  - Automation of some aspects of provisioning
  - Help support HIPAA via participant validation

MEDICITY

NwHIN Certification Authority

- The NwHIN issues its own x.509 certificates
- NwHIN uses certificates to:
  - Validate each endpoint
  - Encrypt communications channel
  - Digitally sign certain exchange security-related content
- NwHIN participants are required to frequently determine if a valid certificate has been revoked (due to compromise, organization changes, etc.)
- Revocation checking uses CRLs or OCSP Responders
  - Certificate Revocation Lists, Online Certificate Status Protocol

MEDICITY

NwHIN Certification Authority (Cont.)

- Initially the NwHIN was instructed to check X.509 certs in real time
- We quickly realized that was not realistic
- Policy is still under discussion but I anticipate it will be between 1 hr and 1 day
- Only NwHIN-CA issued certs will be trusted (or certificates “cross signed” from another trusted source such as the DoD)
- **Certificates are a vital and a viable mechanism to support HIPAA privacy and security requirements across gateways**

MEDICITY

NwHIN Certification Authority Status

- Status:
  - NwHIN has deployed a Certification Authority and a Certificate Revocation List (CRL) distribution point, and an Online Certificate Status Protocol (OCSP) responder network
  - Using a managed CA service from Entrust
  - In production use since mid 2010

MEDICITY

Non-Repudiation

- Non-repudiation is the inability of an organization to successfully deny that they performed some action
- NwHIN was asked by the ONC to support non-repudiation:
  - Of the authenticity and origin of the sender
  - Authenticity of the clinical content's esignature by a clinician?
- One expected use of XML-DSig was for non-repudiation
- But we have confirmation from the ONC that stronger SOAP level non-repudiation is not an active priority; it is in the pipeline but there is no current sponsor.

MEDICITY

Non-Repudiation

- The Security and Privacy Subteam asserts that:
  - A NIST “moderate” level of non-repudiation of the SOAP message is achieved by:
    - NwHIN Policy / DURSA
    - ATNA logging
    - 2-way-SSL mutual authentication
  - A NIST “high” level of non-repudiation of esignature of the clinical content is achieved by:
    - HITSP C26 (document digital signature)
- No plans to modify NwHIN specs at this time for non-repudiation
- For those organizations seeking a “high” level of assurance, they should sponsor NwHIN spec changes or implement it via other methods such as XML-Encryption plus XML-Dsig
- Helps ensure consumer and provider confidence

MEDICITY

NwHIN Logging

- Each NwHIN gateway is required to log transactions
- Fined grained resolution (via SAML attributes)
- Consistent time
- IHE ATNA standard
- Forensic analysis and behavioral profiling
- **Helps support HIPAA accounting requirements**

MEDICITY

Other NwHIN HIPAA Issues

- The NwHIN conducted a risk analysis, and plans to periodically conduct additional analysis (**HIPAA risk mitigation**)
- Security personnel, workforce training, internal assessment are operations to be conducted by gateways (**HIPAA personnel**)
- Physical safeguards and workstation / device security are internal gateway operations (**HIPAA safeguards**)
- ONC-sponsored shared services (CA, UDDI) are operated using IT best practices (**HIPAA availability, safeguards, personnel**)

MEDICITY

NwHIN Future Security Direction

- Support for intermediaries is limited
  - Current specifications don't provide a mechanism for intermediaries to sign documents or SOAP messages
- Requires a secure channel with mutual authentication
  - Support for other protocols, such as SMTP will require a different mechanism such as XML-Encryption
  - Potential Direct Project integration
- Only provides NwHIN Gateway to NwHIN Gateway security
  - If we want security "behind" the gateways, also known as "end-to-end" security, then other approaches are needed such as use of XML-DSig / XML-Encryption of the SOAP Header and Body
- Lesson learned: Removed Audit Log Query Service

MEDICITY

The use of SAML in enforcing HIPAA privacy and security

SAML 2.0

MEDICITY

SAML 2.0 Drill Down

- As SAML 2.0 is a key technology used by many cross organizational healthcare information exchanges, it merits special consideration
- Why is SAML 2.0 so important for cross organizational exchange?
- Allows for a recipient (a “relying party”) to:
  - Inspect the reason the initiator (the “asserting party”) feels it should be granted access
  - Allows inspection of the “evidence” such as policy or other artifacts
  - Each request can be independently validated for authenticity
  - Is extensible to support private agreements
  - Supported widely by web services vendor “stacks”
- Thus, SAML 2.0 provides many of the essential building blocks necessary to establish cross-gateway federated trust

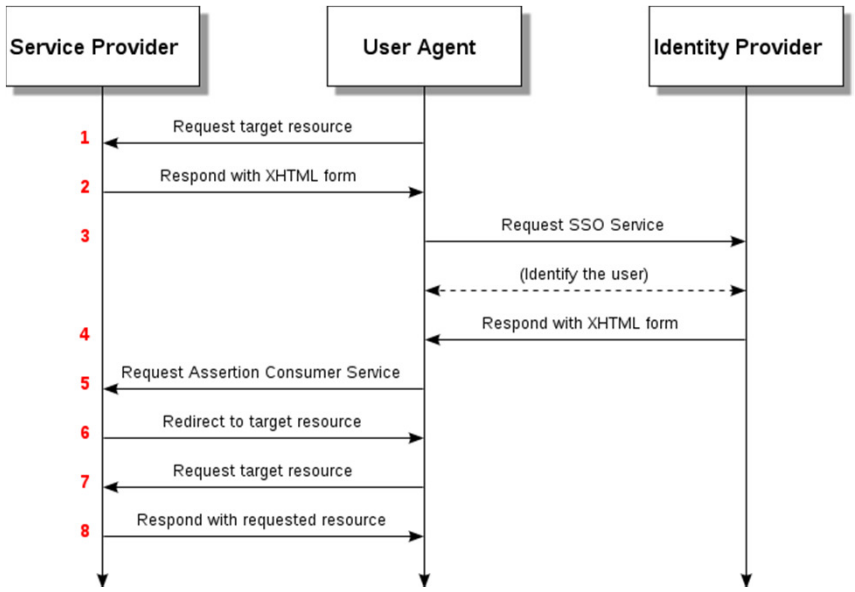
MEDICITY

SAML 2.0 – Two Modes

- Browser based interactive Single Sign On (SSO):
  - Applicable when human end-users are the trusted entities
  - Applications can call a 3rd party Identity Provider
  - Allows SSO across domains
- Backend security:
  - Applicable when gateways are the trusted entities
  - A human end-user may not be directly involved in the exchange
  - Allows complex multi-layer transitive trust such as a system vouching for another system vouching for a human end-user
  - Can carry end-user information, though, if needed

MEDICITY

Interactive Session Based SAML 2.0



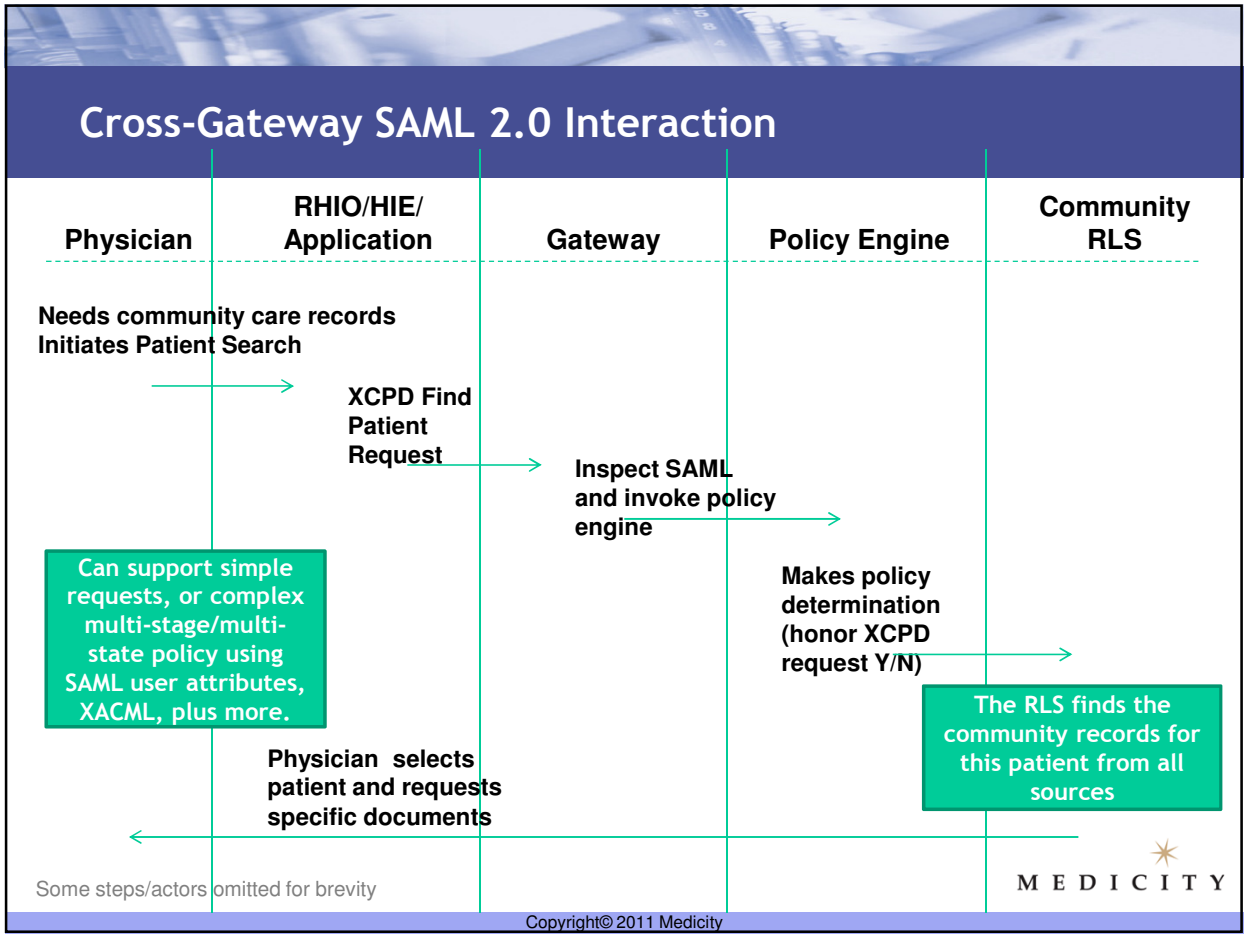
Source: OASIS

MEDICITY

Backend Gateway Based SAML 2.0

- Gateway to gateway transaction
- SAML 2.0 provided end-user attributes for dynamic access request determination
- Provided in the SOAP message security header
- Signed using XML-DSig
- Used extensively by the NwHIN Exchange, epSOS, others
- Attributes carried in the SAML header allow for
  - Fine grained audit logging
  - Policy enforcement
  - Access controls
- **Supports multiple HIPAA requirements across gateways**

MEDICITY


Cross-Gateway SAML 2.0 Interaction
Physician
RHIO/HIE/ Application
Gateway
Policy Engine
Community RLS
Needs community care records Initiates Patient Search
XCPD Find Patient Request
Inspect SAML and invoke policy engine
Makes policy determination (honor XCPD request Y/N)
Can support simple requests, or complex multi-stage/multi-state policy using SAML user attributes, XACML, plus more.
The RLS finds the community records for this patient from all sources
Physician selects patient and requests specific documents
Some steps/actors omitted for brevity
MEDICITY
Copyright© 2011 Medicity

LOCAL POLICY SUPPORT

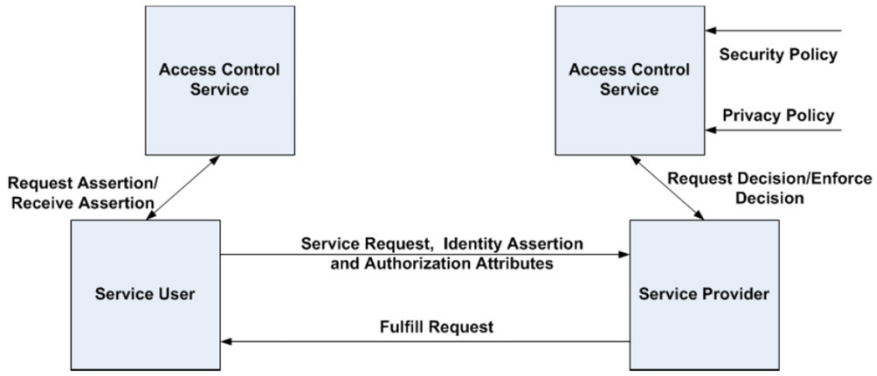
MEDICITY

XSPA / XACML Support

- NwHIN participants recognized a gap existed in terms of standards
- OASIS created XSPA at the NHIN's request
- XSPA – Cross Enterprise Security and Privacy Authorization
- Gateways can leverage:
  - XSPA attribute objects
  - XACML rules
- Both of these standards are very flexible
- But need definition of specific content and/or rules to be expressed and the associated business logic

MEDICITY

Consent Directives Enforcement

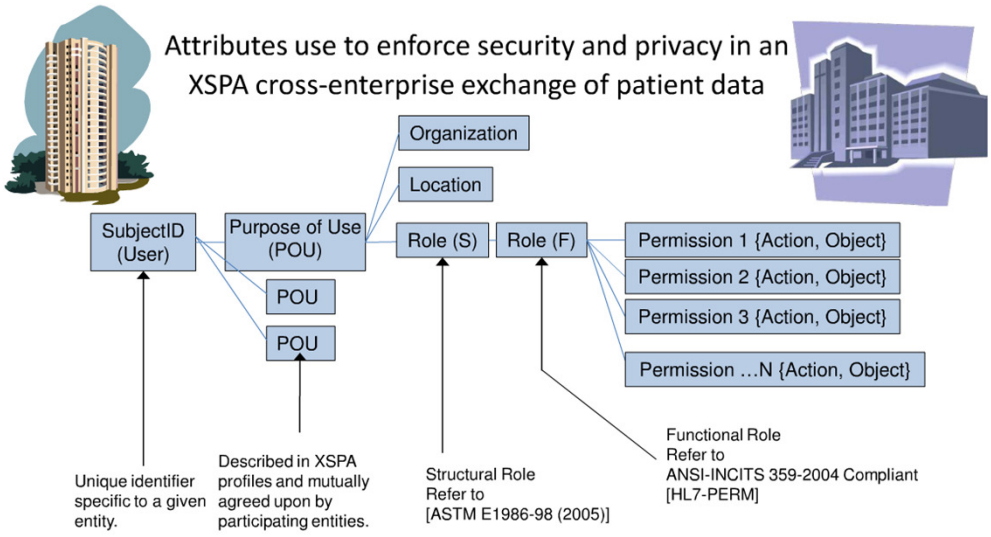


HITSP TP20 Access Control, TP30 Manage Consent Directives, OASIS XSPA SAML, WS-TRUST

Source: VA

MEDICITY

Security and Privacy Enforcement



Source: VA

MEDICITY

HIPAA Cross-Gateway Access Control Support

- Together, SAML 2.0, XSPA, XACML, and BPPC can enable support for consumer-expressed restrictions
- Can also help ensure access is limited to authorized people

MEDICITY

TWO OTHER BRIEF EXAMPLES

MEDICITY

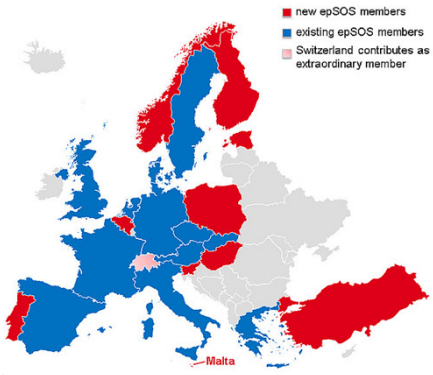
What about the Direct Project?

- Direct is promising, as it represents a type of "push"
- It is secure
- The methods of establishing that security are largely either:
  - Participants are part of a HISP
    - Or
  - Participants must manually establish the trust
- I'm hopeful that the Direct Project will:
  - Be merged into the NwHIN Exchange
  - That it will leverage a provider directory
    - Reduce risk of inadvertent disclosure
    - Can store x.509 keys in the directory more automation
  - Support more HIPAA aspects in the future such as accounting

MEDICITY

epSOS Project

- 23 different European countries: 20 EU member states and 3 non-EU member states
- In a first phase:
  - Patient Summary: access to important medical data for patient treatment
  - Cross-border use of electronic prescripti ("ePrescription" - or "eMedication" systems)
- In a second phase:
  - Integration of the 112 emergency services
  - Integration of the European Health Insurance Card (EHIC)
  - Patient access to data



MEDICITY

GAPS

MEDICITY

Current Challenges

- Expression of consumer preferences and organizational policy in a computable manner, and availability of such when and where needed
- Expression for local, regional, state, federal, and international legs/regs
- Huge variations in law
- Automated conflict detection and resolution
- Un-implementable statue (one state, for example, has incorrect codified test code result values subject to privacy in current statute)
- Human workflow (patients, providers)
- Technology “whitespace” areas
- Balancing conflicting needs for stability and responsiveness
  - Stable law in a dynamic security environment
- Workflow across domains

MEDICITY

Other Industry Challenges

- Key management is probably one of the most problematic areas
  - How do end-users get x.509 keys installed in their local applications?
  - How will documents that are encrypted or signed be accessed and validated 50 years from now when the keys have long expired?
  - How can organizations effectively escrow keys in cross-enterprise scenarios?
  - How can revoked keys be quickly acted on?
- Will an intermediary "hub" or HISP always be required to make key management practical?
- Technical implementations are not correct (yet) especially related to SAML 2.0 support by vendor "stacks" and require work-arounds.

MEDICITY

LESSONS LEARNED

MEDICITY

Architectural Considerations

- Security of a system depends on the security of all components
- Security can be enhanced by ensuring each component is optimally secured ('right' permissioned, tamper detection, isolated)
- Provider directories will likely reduce inadvertent disclosure risks
- Focus on early semantic interoperability
- Clearly define what entities will trust what other entities, including transitive trust
- How will you express policy?
- Where will you inspect and enforce policy?

MEDICITY

Cross-Organizational Exchange Best Practices

- Risk assessment and mitigation (required by § 164.308(a)(1)(ii)(A))
- Software development best security practices (OWASP, others)
- Operational procedures
- Comprehensive, implementable, policy (consistent, or at least compatible)
- Adopt NIST guidelines (SP 800-*, more)
- Don't forget the human workforce aspect
- Documented
- Involve cross-domain counterparts early and over communicate
- Conduct internal and third party audits
- Ensure legal and technical groups inside an organization possess a deep understanding of each others issues, and reach consensus
- Consider HIPAA to be a floor
- Leverage NIST guidelines and toolkits even if you are not required to

MEDICITY

Cross-Gateway Risk Mitigation

- Model some specific threats of interest to your stakeholders, and as per HIPAA
- Inference attacks
- Statistical outliers
- Correlation across multiple sources
- Consider pseudonymization and de-identifying
- State-sponsored hacking (e.g. “Titian Rain”)
- Mobile devices
- People – strong authentication (2FA)
- Disasters

MEDICITY

SUCCESS FACTORS

MEDICITY

Success Checklist for Federated Trust

- Are components exactly necessary and sufficient to support approved use cases?
- Are the trusted entities clearly understood?
- Is the federated trust technically correct?

MEDICITY

Policy/Operational Checklist

- Is security governed by organization policy?
  - Design considerations
  - Solution development (coding)
  - Operational
  - Change management
- Is the organizational policy periodically reviewed?
- Does the organization fully understand the above for each of their HIE trading partners?
- Are operational procedures understood, comprehensive, and documented?
- Realistic and implementable breach detection and response?

MEDICITY

SECURITY MYTHS (BUSTED)

MEDICITY

Policy/Operational Checklist

Myth	True/False	Comments
The NwHIN uses SAML 1.x	False	The NwHIN uses SAML 2.0
SAML 2.0 is complex for implementers	?	Most web services vendor stacks support SAML 2.0 comprehensively, but some older stacks are flawed
The NwHIN doesn't support end-user logins	False	End-users log in to their native systems and SAML can carry their unique attributes
The Direct Project is insecure	False	Direct requires use of TLS or PKI
Cross-gateway exchange can't support HIPAA	False	Many applicable HIPAA requirements are supported with today's technology

MEDICITY

CONCLUSION

MEDICITY

Conclusion

- I started this presentation asking the question "Can we build HIPAA-compliant federated trust systems for healthcare information exchange?"
- The answer, I believe, is "Yes, we can build secure, HIPAA-compliant, federated trust across organizational, state, and even national boundaries using existing technologies."
- Challenges remain, but are being overcome both in the USA and abroad
- You can help! Evaluate the cross-gateway environment for your organization and provide feedback and volunteer time to standards groups to help close gaps identified.

MEDICITY

FOR MORE INFORMATION

MEDICITY

For More Information

- OASIS SAML 2.0, XSPA, XACML
  - http://www.oasis-open.org/
- Nationwide Health Information Network Exchange Wiki
  - http://exchange-specifications.wikispaces.com/home
- Department of Health and Human Services Published Nationwide Health Information Network 2010 Production Specs and Tools
  - http://healthit.hhs.gov/portal/server.pt?open=512&objID=1142&parentname=CommunityPage&parentid=4&mode=2
- HHS HIPAA Guidance
  - http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html
- Integrating the Healthcare Enterprise (IHE)
  - http://www.ihe.net
- NIST Publications, available at
  - http://csrc.nist.gov/publications/PubsSPs.html
- HHS Breach notification site

  http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html

MEDICITY

Q&A

Please let me know your questions….

The speaker may be reached at

eheflin –at- medicity.com

or the NwHIN workgroups

http://exchange-specifications.wikispaces.com

or the IHE workgroups

http://wiki.ihe.net/index.php?title=IT_Infrastructure

Thank you!!

MEDICITY