Identity Management: Securing Information in the HIPAA Environment

Mark Dixon
Chief Identity Officer
North American Software Line of Business
Sun Microsystems
Agenda

- Challenges we Face
- Identity and Access Management
- Consent Management
- How Sun Can Assist You
Agenda

- Challenges we Face
- Identity and Access Management
- Consent Management
- How Sun Can Assist You
Healthcare Industry's Increasing Reliance On Digital Patient Records

**Significant Challenges and Trends**

- Enhancing **security** and **privacy**.
- Increasing **cost efficiency**.
- Improving **quality of service**.
- **Complexity** factors:
  - Multi-enterprise environments.
  - Regional and national healthcare exchanges and healthcare information networks.
  - Wide diversity of healthcare IT systems.
The Impact of HIPAA/HITECH

“Security, Privacy and Confidentiality are foundational to the transformation of the healthcare environment.”

Robert Kolodner
Director of the Office National Coordinator
Department of Health and Human Services
Patient Consent

“Informed consent is more than simply getting a patient to sign a written consent form. It is a process of communication between a patient and physician that results in the patient's authorization or agreement to undergo a specific medical intervention.”

American Medical Association
Conflicting Challenges

Addressing Multiple Business Goals

- Increasing Efficiencies
- Web Services
- Extranets
- Portals
- Dynamic User Base
- Improve Access and Service
- Corporate Governance
- Privacy Demands
- Addressing Security & Compliance
- Risk Management
- Compliance Mandates
- Operations
- Help Desk
- Integration
- Development
Agenda

- Challenges we Face
- **Identity and Access Management**
- Consent Management
- How Sun Can Assist You
Identity and Access Management

Who has access to what, when?

DEFINE

ASSIGN

AUDIT

ENFORCE
Key IAM Enablers for HIPAA/HITECH

1. Assign and control user access rights.
2. Adjust user access rights when responsibilities change.
3. Revoke user access upon termination.
4. Manage allocation of user credentials.
5. Enforce segregation of duties (SOD) policies.
6. Provide uniform access policy.
7. Manage access based on business roles.
Key IAM Enablers for HIPAA/HITECH (cont.)

8. Enforce secure access policies.
10. Extend access control to business associates.
11. Verify access rights.
13. Provide automated reports.

It is all about securing applications, data, and users in order to protect the patient and provider.
ROI for Identity and Access Management

- **Reduce** risk of non-Compliance.
- **Cut** administration and help desk costs for users/identities.
- **Enhance** employee productivity.
- **Boost** security while enabling agility.
- **Lower** long-term Infrastructure costs.
- **Reduce** new application on-boarding costs.
- **Strategic** Support for new Revenue Opportunities.
  > Federation enabler.
  > Eases Acquisitions, mergers, expansions.
Agenda

- Challenges we Face
- Identity and Access Management
- Consent Management
- How Sun Can Assist You
Consent Management

- Essential to meet privacy/security requirements
- Data is typically dispersed among several organizations
- Many stakeholders
- Multiple jurisdictions
- Highly dependent on context/situation
Consent Management Challenges

• Privacy Legislation
  > Multiple jurisdictions
  > Who is able to perform the override without consent?

• Auditing requirements
  > Must provide an audit trail of who performed what action, whether the action was successful or not

• Privacy Officer within each Organization
  > Identifying their responsibilities and accountabilities associated to EHRs
  > Need for a business role within the Access Model
  > Depending on the implementation – can receive a near real time notification of an override without consent
Consent Management Concepts

• Override with consent
  > The patient (or their representative) has consented to allow the user access to the patients data.
  > The consent is realized through a keyword

• Override without consent (“break the glass”)
  > The user has either not obtained the consent or unable to obtain the consent of the patient and desires to access the patient's information
  > Patient arrives in an acute care facility unconscious is an example where the user is unable to obtain the consent of the patient.
Functionality: Identity and Roles

- Identity and Roles
  - Patients
  - Providers
  - Access Rights
  - Roles map business responsibilities to access rights

- Override Rights
  - Only users with specific roles can perform override without consent
Functionality: Consent Registry

- Consent Permissions
  - Patients
  - Organizations
  - Users
  - System-wide mask (everyone)
- Fine gained access
  - Include or exclude
  - Accommodate multiple jurisdictions
Functionality: Master Patient Index

• Enable correlation of patient data across multiple repositories
• Provide secure service to govern data access
Functionality: Administration

• Administrative Viewer
  > Supports only System Wide Mask (everyone)
  > Specific role enables distributed or centralized

• Service Governance
  > Has existing functionality to enforce
  > Can be enabled or disabled to utilize consent management testing
Consent Management Architecture

- **Patient Data Repository**
- **Identity and Role Repository**
- **Consent Management Registry**
- **Data Access Services**
- **Master Patient Index**
- **Web Portals**
- **Applications**

- Index to all patient records, regardless of location
- Patient records reside in many locations
- Patient and organization consent profiles
- Identities, roles, and access control credentials

Federated Data Access
British Columbia HIAL and IDAM

- Health Information Access + Service Provider
- Consent Management + Identity Management
Pragmatic Issues: Devil in the Details

- Legislative/policy driving implementation details
- Process adaptation resulting from policy changes
- Linking accountable persons to support staff
- Uniform understanding of roles across organizations
Agenda

- Challenges we Face
- Identity and Access Management
- Consent Management
- How Sun Can Assist You
Sun is committed to the sharing of information technology to power health information networks that provide secure, regulated access to patient data.
Sun Identity Management solves HIPAA/HITECH IT requirements:

> Enterprise security.
> Regulatory compliance and risk management.
> Operational efficiencies.

Addresses both HIPAA risk and compliance pain points:

> Automates access certification and re-certification process.
> Improves internal audit operational efficiencies.

Rated the market LEADER by Gartner and Forrester.

Directory Server EE
- High-performance Directory
- Virtual Directory Services
- Secure Store for Users and Authorization Policies

Identity Manager
- Automated User Provisioning
- Account and Password Sync
- Approvals and Workflows

OpenSSO Enterprise
- Web Single Sign-On
- Federation
- Web Services Security

Role Manager
- Role Management
- Access Certification
- Identity Auditing
Why Sun IAM for HIPAA Compliance?

Product Strategy and Expertise

Simple
- Sun IAM solutions are 100% Java™ technology and easy to deploy, configure, and use.
- Web browser-based access to all functionality.

Open
- Open architecture makes applying Sun IAM solutions to multiple networked resources faster and simpler.
- Open source, transparency.

Proven
- Sun manages billions of user identities, and its solutions have received positive recognition from industry analysts and experts.
- Minimizes risk and compliance violations.
Identity Management is a journey, not a project or event.

Assess where you are in the process. Outline a strategy that fits your organization.
Sun IAM Healthcare Customers

Simple
Open
Proven
More Information, and Downloads

• Sun HIPAA/HITECH Compliance Whitepaper
  https://www.sun.com/offers/details/identity_access_management.xml

• Sun Identity and Access Management
  http://www.sun.com/software/identity/index.jsp

• Sun Identity Manager

• Sun Role Manager
  http://www.sun.com/software/products/rolemanager/index.xml

• Sun OpenSSO Enterprise
  http://www.sun.com/openssso

• Sun Directory Server Enterprise Edition
  http://www.sun.com/dsee
Identity Management: Securing Information in the HIPAA Environment

Mark Dixon
mark.g.dixon@sun.com
www.discoveringidentity.com