Securing Physician and Patient Portals for HIPAA Compliance

HIPAA Summit VIII

Session 2.04
1:00 – 2:00 pm
March 8
Agenda

• Identity and Access Management Technology and HIPAA Requirements
  – Bob Tahmaseb, Principal Systems Engineer, RSA Security, Inc.

• Securing Physician and Patient Portals for HIPAA Compliance
  – David Young, IT Program Director, Geisinger Health System

• Questions & Answers
Agenda

• Identity and Access Management Technology and HIPAA Requirements
  – Bob Tahmaseb, Principal Systems Engineer, RSA Security, Inc.

• Securing Physician and Patient Portals for HIPAA Compliance
  – David Young, IT Program Director, Geisinger Health System

• Questions & Answers
RSA Security

- Over two decades experience in information security
- Leader in industry research and standards
- Over 14,000 customers worldwide including leading healthcare organizations such as:

  ▪ Atlantic Health Systems
  ▪ Baylor Health Care System
  ▪ Bay Health Medical
  ▪ Blue Cross Blue Shield
  ▪ Boston Medical
  ▪ Cigna
  ▪ Geisinger Health System
  ▪ HCA
  ▪ Kaiser Foundation
  ▪ Oxford Health Plans Inc
  ▪ PacifiCare Health Systems
  ▪ Partners Healthcare System
  ▪ Providence Health System
  ▪ Scripps Health
  ▪ Sisters of Mercy Health System
  ▪ Trinity Health
  ▪ UPMC Health System
Definition of Identity and Access Management

The people, processes and technologies dedicated to creating, managing and revoking digital identities, as well as developing and enforcing policies governing authentication and access to information systems both inside and outside the enterprise.

- Authentication
- Access control
- Audit
Authentication

• Levels of authentication
  – Single factor versus multi-factor

• Diverse environments
  – On-site clinical versus on-site office
  – Web access for patients/members
  – Remote and web access for professionals

• Selection criteria
  – Strategic fit for users
  – Strategic fit in corporate/system
  – Total cost of ownership
Access Control

- Levels of access control
  - Resources
  - Actions
- Rule-based
  - Static and dynamic rules
- Role-based
  - Group users with similar access rights
  - Inheritance
  - Exceptions and exclusions
- Administration

---

[Image: RSA Security logo and Geisinger Health System logo]
Audit Controls

• Tracking and monitoring user access
  - User activity
  - Access privileges

• Level of detail
  - Type of event
  - Date and time
  - User ID
  - Function or command

• Storing and protection
Meeting the HIPAA Requirements

<table>
<thead>
<tr>
<th>Standard</th>
<th>Best practice</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIPAA Privacy</td>
<td>Role-based access control</td>
</tr>
<tr>
<td>Minimum Necessary</td>
<td></td>
</tr>
<tr>
<td>HIPAA Security Authentication</td>
<td>Strong authentication for remote access; possibly for internal access for some applications</td>
</tr>
<tr>
<td>HIPAA Security Access Control</td>
<td>Centralized user management and fine-grained access control</td>
</tr>
<tr>
<td>HIPAA Security Audit Controls</td>
<td>Logging and reporting mechanisms</td>
</tr>
</tbody>
</table>
Agenda

• Identity and Access Management Technology and HIPAA Requirements

• Securing Physician and Patient Portals for HIPAA Compliance
  – David Young, IT Program Director

• Questions & Answers
Securing Physician & Patient Portals for HIPAA Compliance

Case Study

• The Setting - Geisinger Health System
• The Challenge
• I&AM Planning & Deployment
• Our Patient Portal – “MyChart”
• Our Provider Portal – “GeisingerConnect”
• Portal Security Features
• Portal Status & Customer Feedback
Geisinger Health System


- Geisinger Health System, founded in 1915, serves a 31-county, largely rural area of north-central Pennsylvania.
- An integrated, healthcare delivery network
  - 52 clinic sites (42 Primary Care)
  - 2 inpatient facilities
  - 600+ employed physicians
  - 1,500,000 outpatient visits/year
  - Nearly 300,000 covered lives
  - 9,500 employees
Geisinger Service Region

Electronic Medical Record (EMR) Status

- All 600 physicians use the EMR (EpicCare) to:
  - View all results and records
  - Enter all orders
  - Document patient encounters
- All providers view results online
- Integrated appointment scheduling (Epic Cadence®)
- Implementation began 1997

EpicCare® and Cadence® are products provided by Epic Systems Corporation.
The Challenge

- GHS doctors (600+)
- Contracted doctors (4,000+)
- Referring doctors (10,000+)
- Patients (2,000,000+)
- Members (300,000+)
- Employees (8,500)
- Consumers (huge!)
- Employers
- Brokers
- Suppliers

SSO to Sensitive information
Geisinger Network
The Beginning: eAccess Task Force

- **Purpose** to scope out how entities access Geisinger’s electronic information in secure and confidential manner.
  - Formed Summer 2000

- **Membership**
  - Internal Audits, HIPAA officer, Information Security, Medical Records, IT Web, Desktop Services, Networks
eAccess Task Force

Outcomes

• Devised remote access policy
  – Identified 8 means of access
  – Identified 6 different role types
  – Mapped the acceptable means of access to each role type
  – Included the encryption and authentication requirements

• Recommendation to purchase I&AM software

• Recommendation to utilize RSA SecurID® tokens for stronger two-factor authentication, where required.

• Recommendation on use of 128-bit SSL server certificates
Requirements of I&AM System

- Need an effective solution to manage ALL access to secured web resources
- Ensure the “right” people are seeing the “right” information at the “right” time
- Enforce HIPAA Compliance for electronic PHI
- Integrate web security into existing infrastructure
- Single Sign-On (SSO)
- Flexible Security Administration

Solution: RSA ClearTrust

Geisinger Health System
Why RSA ClearTrust?

- Open Architecture – wide support for all platforms + Java
- Full Feature Set
  - Smart Rules: allow/deny access based on user properties & roles
  - Strong support for multiple authentication types and access control
  - Browser friendly, zero footprint
- Integration capabilities with our existing web infrastructure
- Performance and scalability
- Single Sign-On (SSO)
- Future Product Vision
Enhanced Security Model

Sensitive eHealth information

128-Bit SSL encryption

Firewall

Application security

Tokens, PKI, biometrics

RSA ClearTrust
Web access management
Geisinger Patient Portal

• “MyChart” Portal for Patients
  – Access into a selected “view” of Electronic Medical Record (EMR)
  – Secure Patient-Physician Internet messaging
  – Rx refill requests
  – Appointment request
  – Pediatric proxy access
  – Caregiver access
  – Free service to patients

MyChart® is a module of the EpicCare® EMR, provided by Epic Systems Corporation.
MyChart – Welcome Screen

Alerts
Proxy
Views
Messaging
Appointments
Administration
MyChart - Lab Results

Lab Tests

Results

Date     Test          Authorizing Provider       Status
10/29/1997 CREATININE       Test West, M.D.       Final result
09/26/1997 GLUCOSE            test; wyoming M.D.    Final result
09/08/1997 HDL                   Test West, M.D.       Final result
09/08/1997 LDL (DIRECT MEASURE)  Test West, M.D.       Final result
09/08/1997 TRIGLYCERIDES     Test West, M.D.       Final result
09/08/1997 PSA                   Test West, M.D.       Final result

Back to the previous page...
MyChart - Secure Messaging

PCP or last seen Physicians

Patient’s Communication Preference
MyChart Registration Process - Today

• Step 1 – Patient visits their physician office
  – Patient signs access request form
  – Patient given one-time use activation code

• Step 2 – Activate MyChart account on Geisinger.org
  – Identify themselves
  – Choose a UserID, Password, and Challenge Q/A
  – Accept the MyChart Terms & Conditions

• Step 3 – Login to MyChart with UserID and Password
Patient Registration
“Tell us who you are”
Patient Registration

“Choose your User ID & Password”
MyChart Registration - Tomorrow

- **Step 1** – Visit Geisinger.org and signup for Basic Portal (no PHI)
  - Identify yourself
  - Choose UserID, Password, and Challenge Q/A
  - Accepts T&Cs and then has immediate access to a Basic Patient portal
- **Step 2** – Request MyChart Access online
  - From Basic Patient portal, request enrollment to MyChart
  - MyChart activation code is US mailed to patient’s home address on file
- **Step 3** – Activate MyChart for Enhanced Portal (w/PHI) features
  - With activation code, logs into Basic Portal and activates MyChart
  - User accepts MyChart T&Cs and then can access their EMR via MyChart
  - Behind the scenes SSO between Basic and Enhanced Portal
Geisinger Affiliated Physician Portal

• “GeisingerConnect” features include:
  – Patient admissions & discharges with alerts
  – Insurance Information & discharge summaries
  – Outpatient office visits with clinic progress notes reporting
  – In/Outpatient transcribed documents
  – Access for Physicians and their office staff
  – EMRlink: temporary read-only access to their patients EMR
  – For our Open-Staff physicians, full access to EpicCare In-Patient EMR
  – SSO between systems handled by RSA ClearTrust
  – Two-factor authentication, where required, uses RSA SecurID tokens
GeisingerConnect Model

- EpicCare I/P EMR
  - Full EMR Access
- EMRlink
  - Read-only EMR Access
- GeisingerConnect Web Portal
  - Clinical Documents, Appts, ADT, Clinical Trials, CME

Direct and Indirect Access

External Physician affiliation with Geisinger

HIPAA Traffic Control

RSA Security

Geisinger Health System
### Geisinger Connect – Patient List

#### Patient List

<table>
<thead>
<tr>
<th>Patient Name</th>
<th>Age</th>
<th>Gen</th>
<th>Visit Date</th>
<th>Visit Type</th>
<th>Department</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ford, Sally</td>
<td>37</td>
<td>F</td>
<td>11/30/03</td>
<td>Office Visit</td>
<td>Rheumatology F7</td>
</tr>
<tr>
<td>Williams, Chris</td>
<td>4</td>
<td>M</td>
<td>11/28/03</td>
<td>Inpatient (I)</td>
<td>GWW-PED</td>
</tr>
<tr>
<td>Johnson, Elizabeth</td>
<td>15</td>
<td>F</td>
<td>11/28/03</td>
<td>Inpatient (I)</td>
<td>GWW-PED</td>
</tr>
<tr>
<td>Gates, Bill</td>
<td>48</td>
<td>M</td>
<td>11/27/03</td>
<td>Inpatient (I)</td>
<td>GWW-MED</td>
</tr>
<tr>
<td>Trump, Donald</td>
<td>70</td>
<td>M</td>
<td>11/27/03</td>
<td>Inpatient (I)</td>
<td>GWW-HRT</td>
</tr>
<tr>
<td>Brown, Alan</td>
<td>26</td>
<td>M</td>
<td>11/27/03</td>
<td>Inpatient (I)</td>
<td>GMC-CVM</td>
</tr>
<tr>
<td>Jones, Madison</td>
<td>23 mths</td>
<td>F</td>
<td>11/24/03</td>
<td>Inpatient (I)</td>
<td>GMC-FHS</td>
</tr>
<tr>
<td>West, Brandi</td>
<td>59</td>
<td>F</td>
<td>11/17/03</td>
<td>Inpatient (I)</td>
<td>GWW-MED</td>
</tr>
</tbody>
</table>

#### Referral Form

#### EMR Access

---

**RSA Security**
Geisinger Portals: Security was Job 1

1. * Role-Based Access: For Patients, Physicians, Employees, Members, Office Staff, Medical Students, and others
2. * Two-factor Authentication with UserID/Password and RSA SecurID hardware tokens
3. * User and administrator activity audit logging
4. * Intrusion detection with event triggers
5. * Session and inactivity timeouts
6. * Password expiration periods
7. * Strong password formulation and enforcement rules
8. * Self-service utilizing a challenge question and answer for forgotten passwords
9. * Uniform policy management and enforcement across all web servers and user roles.
10. Out-of-band process for first time registrants
11. 128-Bit Secure Socket Layer (SSL) Encryption
12. HTTPS-based Secure Messaging with “You’ve got mail” alerts

* RSA ClearTrust supported security features
Role-based Access: Implementation

Web Resources

Web Server
Role-based Access: Smart Rules

Web Resource

Smart Rules

User Properties

How To...
- Understand Smart Rules
- Add Smart Rules
- Edit Smart Rules
- Delete Smart Rules
- Understand Security Policy

Smart Rules - 2. Manage Smart Rules

1. Select Application
2. Manage Smart Rules
3. Add Smart Rule

Manage existing Smart Rules or add new Smart Rules to control access to this application.

Add New

Smart Rules for Resource: /members/
Application: Health Plan Portal

<table>
<thead>
<tr>
<th>Smart Rule</th>
<th>Access</th>
<th>Edit</th>
<th>Remove</th>
</tr>
</thead>
<tbody>
<tr>
<td>HEALTH_PLAN_MEMBER is true</td>
<td>Allow</td>
<td>Edit</td>
<td>Remove</td>
</tr>
<tr>
<td>HEALTH_PLAN_EMPLOYEE is true</td>
<td>Allow</td>
<td>Edit</td>
<td>Remove</td>
</tr>
</tbody>
</table>
Current Portal Status

- 25,000+ users are provisioned by RSA ClearTrust
  - 9,500 employees
  - 10,000 patients (projected to be 85,000 by September 2004)
    - less than 1% of all patients
    - 10-20 new registrations/day
    - Generating ~15 helpdesk call per week
  - 500 external physician and office staff users
  - 3,000 Health Plan members (100 new registrations/month)
- Six secured portals and two domains protected by RSA ClearTrust
- 50% of those patients given activation codes follow through and register on the site
- 1 FTE dedicated to RSA ClearTrust development/support
Customer Feedback

- “Other things equal, I would prefer to go to a doctor who provides MyChart.” 85
- “I would recommend MyChart to a friend.” 91
- “I can manage my health better by using MyChart.” 75
- “I am worried about someone seeing my MyChart information without my permission.” 29
- “It is easy to find the information I need using MyChart.” 85
- “I feel comfortable using a computer and the internet.” 91
- “I would like to have more of my lab results available online.” 92
- “I am likely to use MyChart in the future.” 92
- From one physician’s office using GeisingerConnect: “This will save us a 100 phone calls per day to Geisinger!”
Agenda

• Identity and Access Management Technology and HIPAA Requirements
  – Bob Tahmaseb, Principal Systems Engineer, RSA Security, Inc.

• Securing Physician and Patient Portals for HIPAA Compliance
  – David Young, IT Program Director, Geisinger Health System

• Questions & Answers