Securing Physician and Patient Portals for HIPAA Compliance

HIPAA Summit VIII

Session 2.04

1:00 – 2:00 pm

March 8

RSA SECURITY

Geisinger Health System

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**

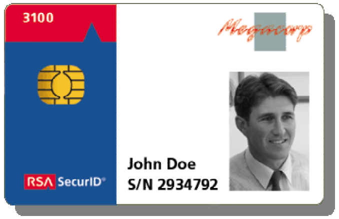
RSA SECURITY

Geisinger Health System

Authentication

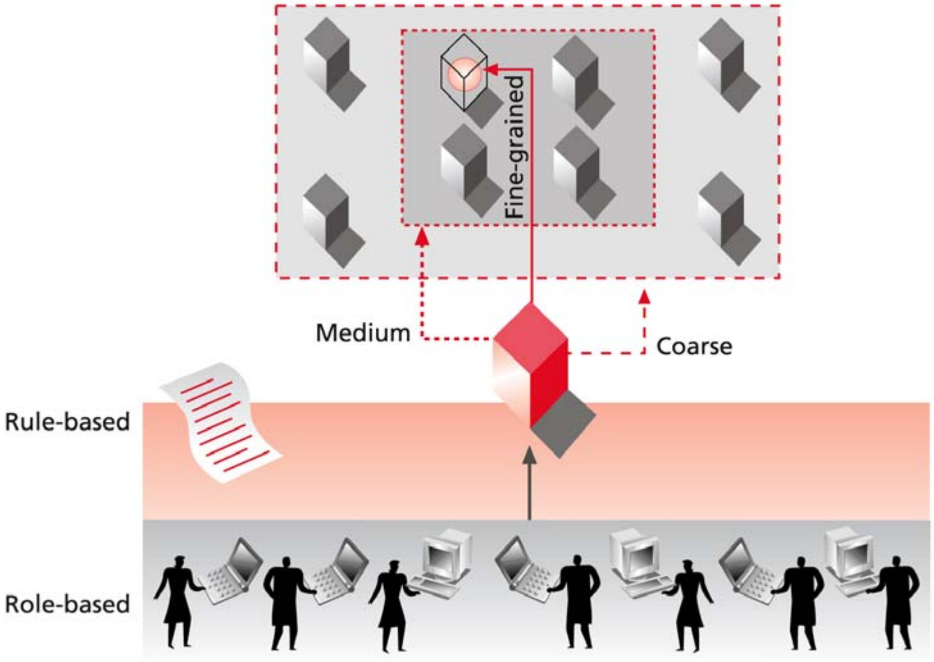
- Levels of authentication
  - Single factor versus multi-factor
- Diverse environments
  - On-site clinical versus on-site office
  - Web access for patients/members
  - Remote and web access for professionals
- Selection criteria
  - Strategic fit for users
  - Strategic fit in corporate/system
  - Total cost of ownership

Passwords



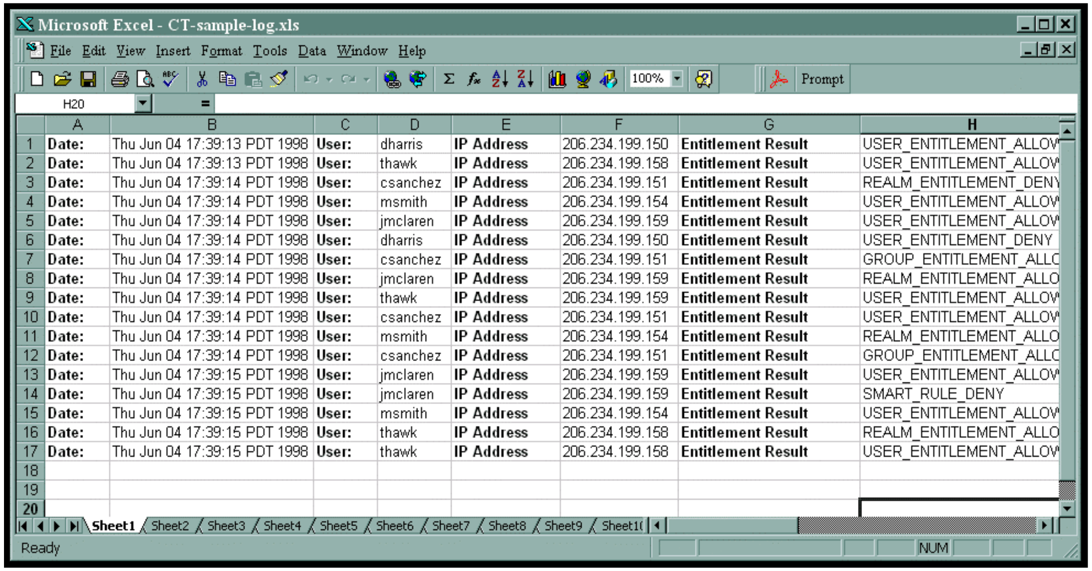
Access Control

- 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



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



Microsoft Excel - CT-sample-log.xls
File Edit View Insert Format Tools Data Window Help
100%
Prompt
H20
=
Sheet1 Sheet2 Sheet3 Sheet4 Sheet5 Sheet6 Sheet7 Sheet8 Sheet9 Sheet1(
Ready
NUM

	A	B	C	D	E	F	G	H
1	**Date:**	Thu Jun 04 17:39:13 PDT 1998	**User:**	dharris	**IP Address**	206.234.199.150	**Entitlement Result**	USER_ENTITLEMENT_ALLOW
2	**Date:**	Thu Jun 04 17:39:13 PDT 1998	**User:**	thawk	**IP Address**	206.234.199.158	**Entitlement Result**	USER_ENTITLEMENT_ALLOW
3	**Date:**	Thu Jun 04 17:39:14 PDT 1998	**User:**	csanchez	**IP Address**	206.234.199.151	**Entitlement Result**	REALM_ENTITLEMENT_DENY
4	**Date:**	Thu Jun 04 17:39:14 PDT 1998	**User:**	msmith	**IP Address**	206.234.199.154	**Entitlement Result**	USER_ENTITLEMENT_ALLOW
5	**Date:**	Thu Jun 04 17:39:14 PDT 1998	**User:**	jmclaren	**IP Address**	206.234.199.159	**Entitlement Result**	USER_ENTITLEMENT_ALLOW
6	**Date:**	Thu Jun 04 17:39:14 PDT 1998	**User:**	dharris	**IP Address**	206.234.199.150	**Entitlement Result**	USER_ENTITLEMENT_DENY
7	**Date:**	Thu Jun 04 17:39:14 PDT 1998	**User:**	csanchez	**IP Address**	206.234.199.151	**Entitlement Result**	GROUP_ENTITLEMENT_ALLO
8	**Date:**	Thu Jun 04 17:39:14 PDT 1998	**User:**	jmclaren	**IP Address**	206.234.199.159	**Entitlement Result**	REALM_ENTITLEMENT_ALLO
9	**Date:**	Thu Jun 04 17:39:14 PDT 1998	**User:**	thawk	**IP Address**	206.234.199.159	**Entitlement Result**	USER_ENTITLEMENT_ALLOW
10	**Date:**	Thu Jun 04 17:39:14 PDT 1998	**User:**	csanchez	**IP Address**	206.234.199.151	**Entitlement Result**	USER_ENTITLEMENT_ALLOW
11	**Date:**	Thu Jun 04 17:39:14 PDT 1998	**User:**	msmith	**IP Address**	206.234.199.154	**Entitlement Result**	REALM_ENTITLEMENT_ALLO
12	**Date:**	Thu Jun 04 17:39:14 PDT 1998	**User:**	csanchez	**IP Address**	206.234.199.151	**Entitlement Result**	GROUP_ENTITLEMENT_ALLO
13	**Date:**	Thu Jun 04 17:39:15 PDT 1998	**User:**	jmclaren	**IP Address**	206.234.199.159	**Entitlement Result**	USER_ENTITLEMENT_ALLOW
14	**Date:**	Thu Jun 04 17:39:15 PDT 1998	**User:**	jmclaren	**IP Address**	206.234.199.159	**Entitlement Result**	SMART_RULE_DENY
15	**Date:**	Thu Jun 04 17:39:15 PDT 1998	**User:**	msmith	**IP Address**	206.234.199.154	**Entitlement Result**	USER_ENTITLEMENT_ALLOW
16	**Date:**	Thu Jun 04 17:39:15 PDT 1998	**User:**	thawk	**IP Address**	206.234.199.158	**Entitlement Result**	REALM_ENTITLEMENT_ALLO
17	**Date:**	Thu Jun 04 17:39:15 PDT 1998	**User:**	thawk	**IP Address**	206.234.199.158	**Entitlement Result**	USER_ENTITLEMENT_ALLOW
18								
19								
20								

RSA SECURITY

Geisinger Health System

Meeting the HIPAA Requirements

Standard	Best practice
HIPAA Privacy Minimum Necessary	Role-based access control
HIPAA Security Authentication	Strong authentication for remote access; possibly for internal access for some applications
HIPAA Security Access Control	Centralized user management and fine-grained access control
HIPAA Security Audit Controls	Logging and reporting mechanisms

RSA SECURITY

Geisinger Health System

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

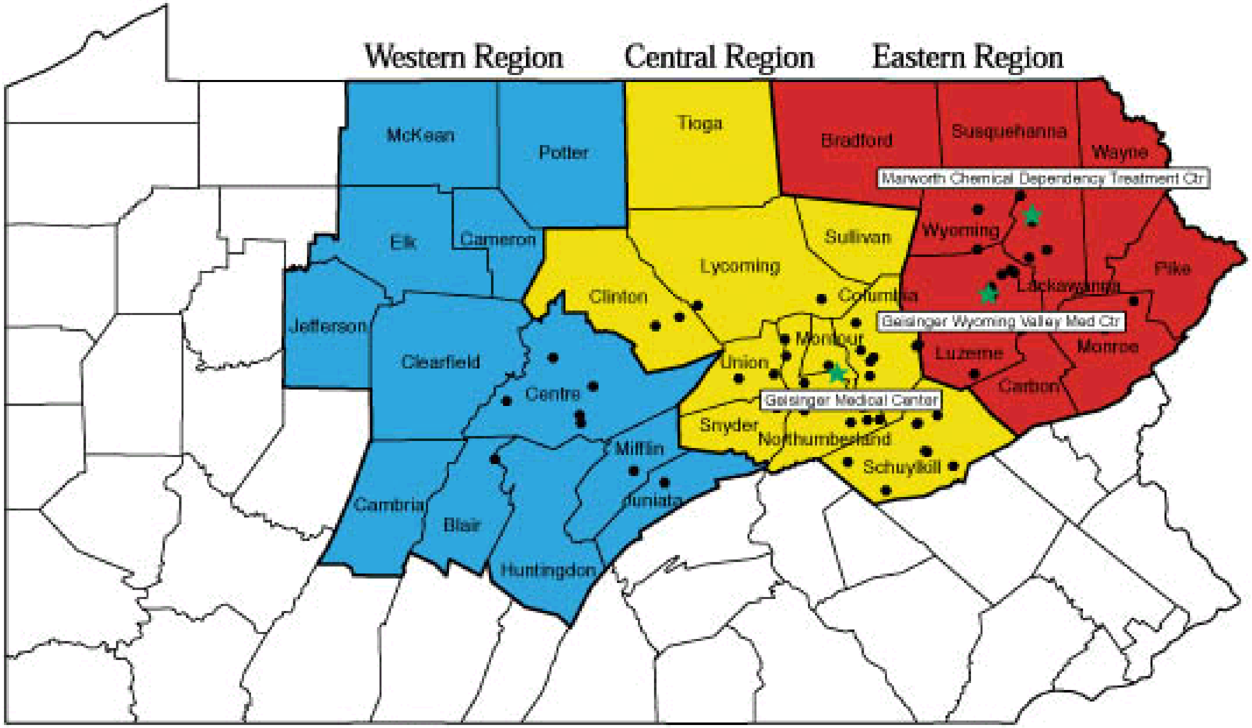
Geisinger Health System

Heal. Teach. Discover. Serve.

- 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

Heal. Teach. Discover. Serve.



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®

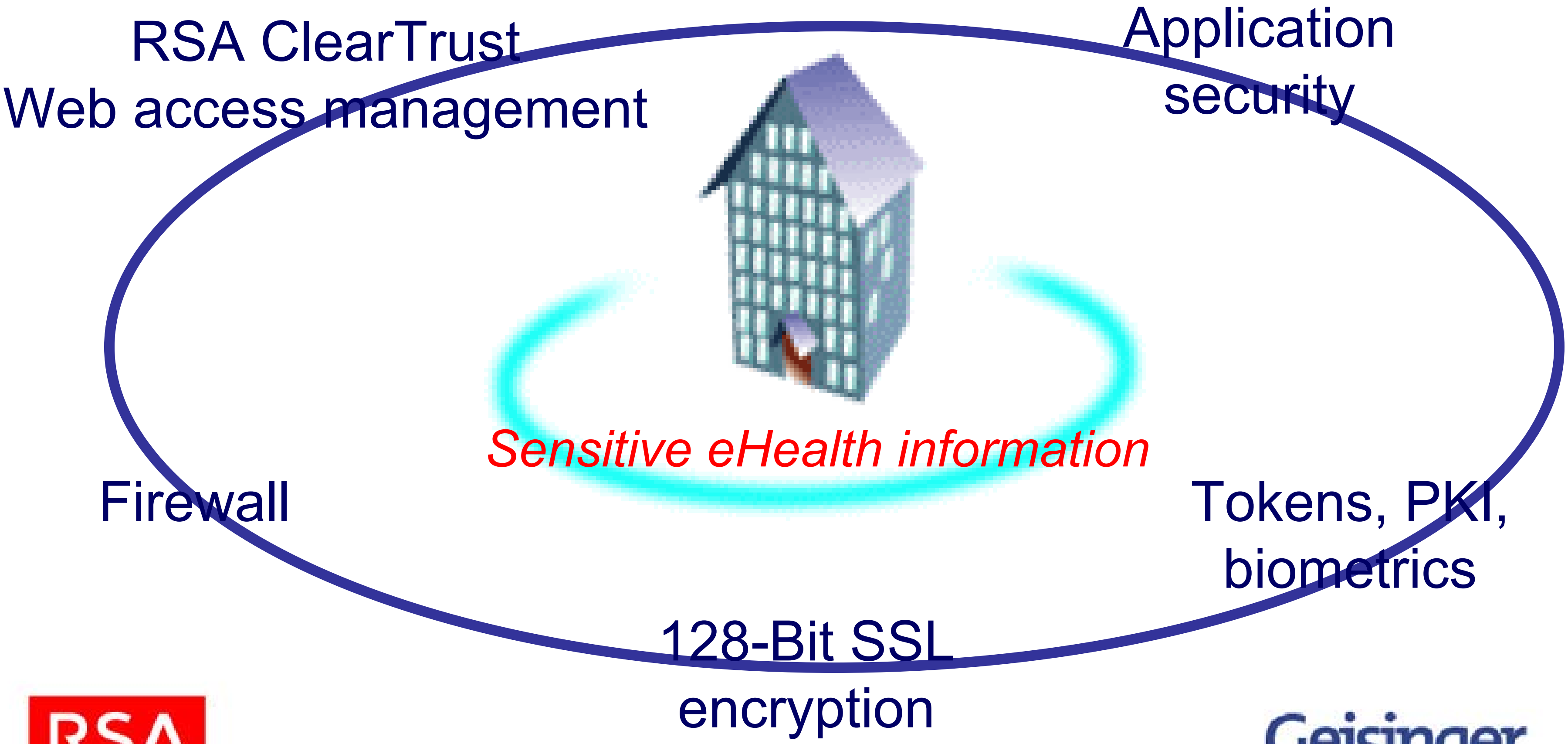
RSA SECURITY®

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



RSA ClearTrust
Web access management

Application
security

Sensitive eHealth information

Firewall

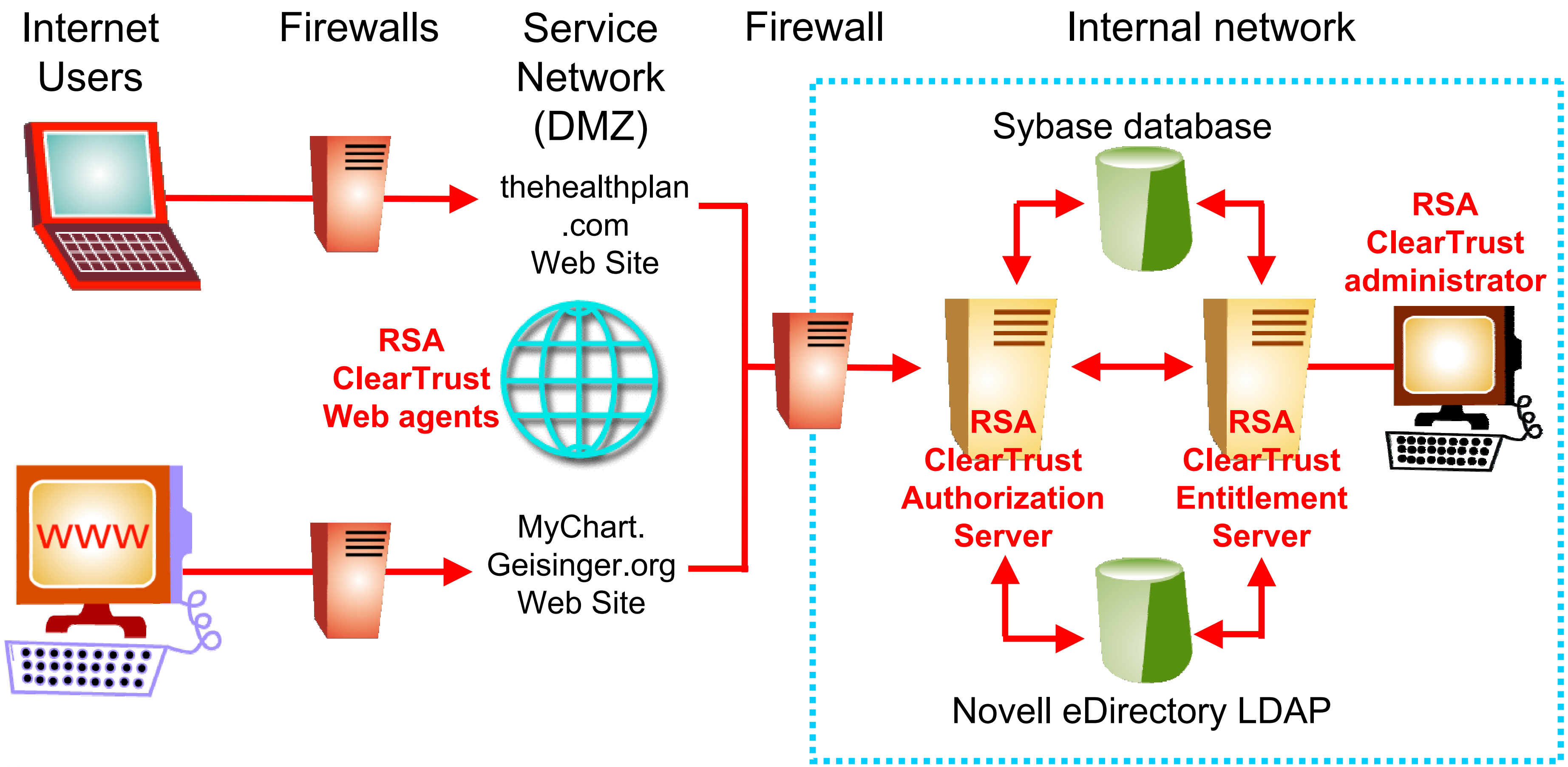
Tokens, PKI,
biometrics

128-Bit SSL
encryption

RSA SECURITY

Geisinger Health System

RSA ClearTrust Deployment


Internet Users
Firewalls
Service Network (DMZ)
Firewall
Internal network
thehealthplan .com Web Site
RSA ClearTrust Web agents
www
MyChart. Geisinger.org Web Site
Sybase database
RSA ClearTrust administrator
RSA ClearTrust Authorization Server
RSA ClearTrust Entitlement Server
Novell eDirectory LDAP

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.

RSA SECURITY

Geisinger Health System

MyChart – Welcome Screen

Alerts

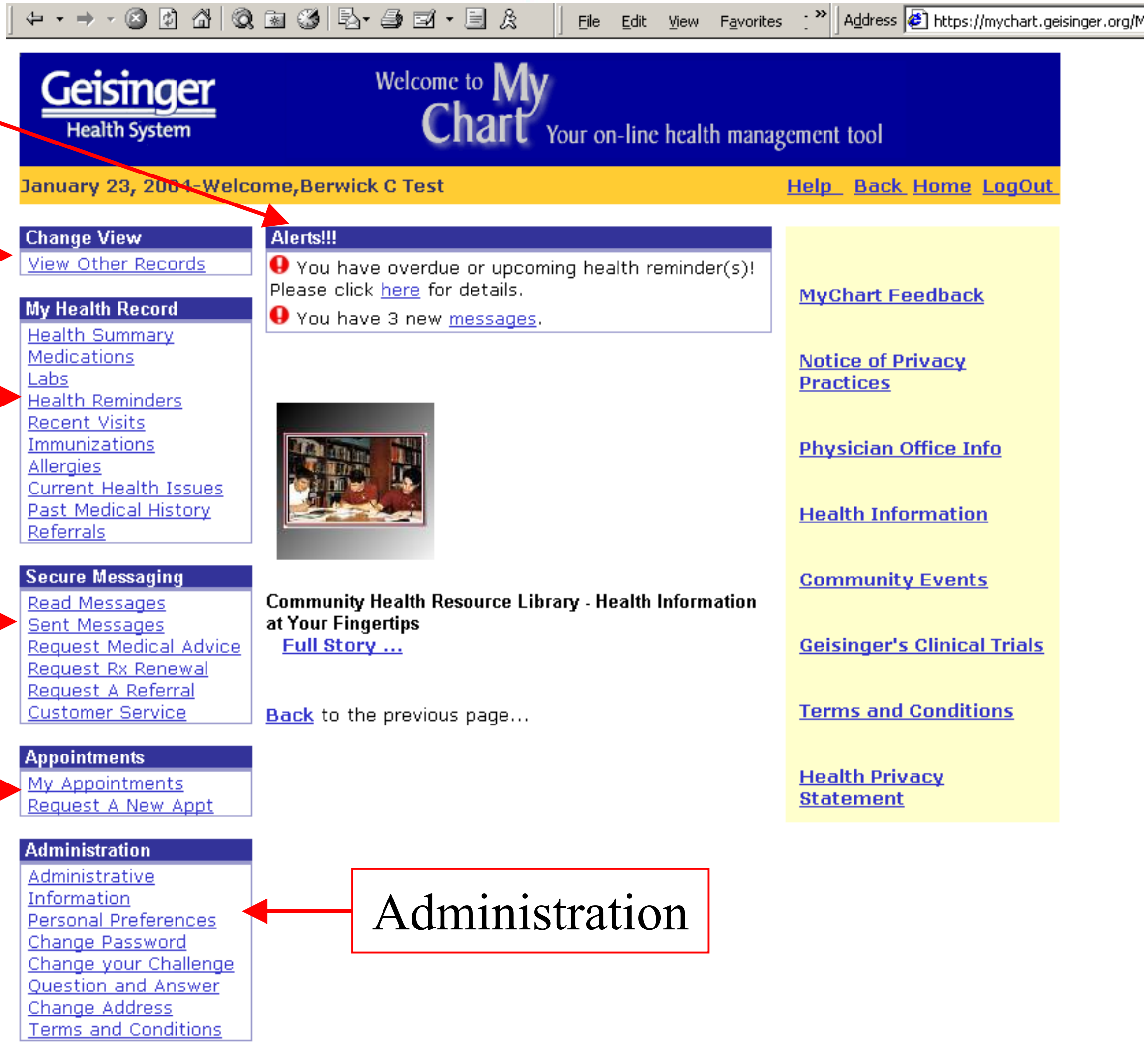
Proxy

Views

Messaging

Appointments

Administration



January 23, 2004-Welcome,Berwick C Test

Help Back Home LogOut

Change View
- View Other Records

My Health Record
- Health Summary
- Medications
- Labs
- Health Reminders
- Recent Visits
- Immunizations
- Allergies
- Current Health Issues
- Past Medical History
- Referrals

Secure Messaging
- Read Messages
- Sent Messages
- Request Medical Advice
- Request Rx Renewal
- Request A Referral
- Customer Service

Appointments
- My Appointments
- Request A New Appt

Administration
- Administrative Information
- Personal Preferences
- Change Password
- Change your Challenge Question and Answer
- Change Address
- Terms and Conditions

Alerts!!!

! You have overdue or upcoming health reminder(s)! Please click here for details.

! You have 3 new messages.

Community Health Resource Library - Health Information at Your Fingertips
Full Story ...

Back to the previous page...

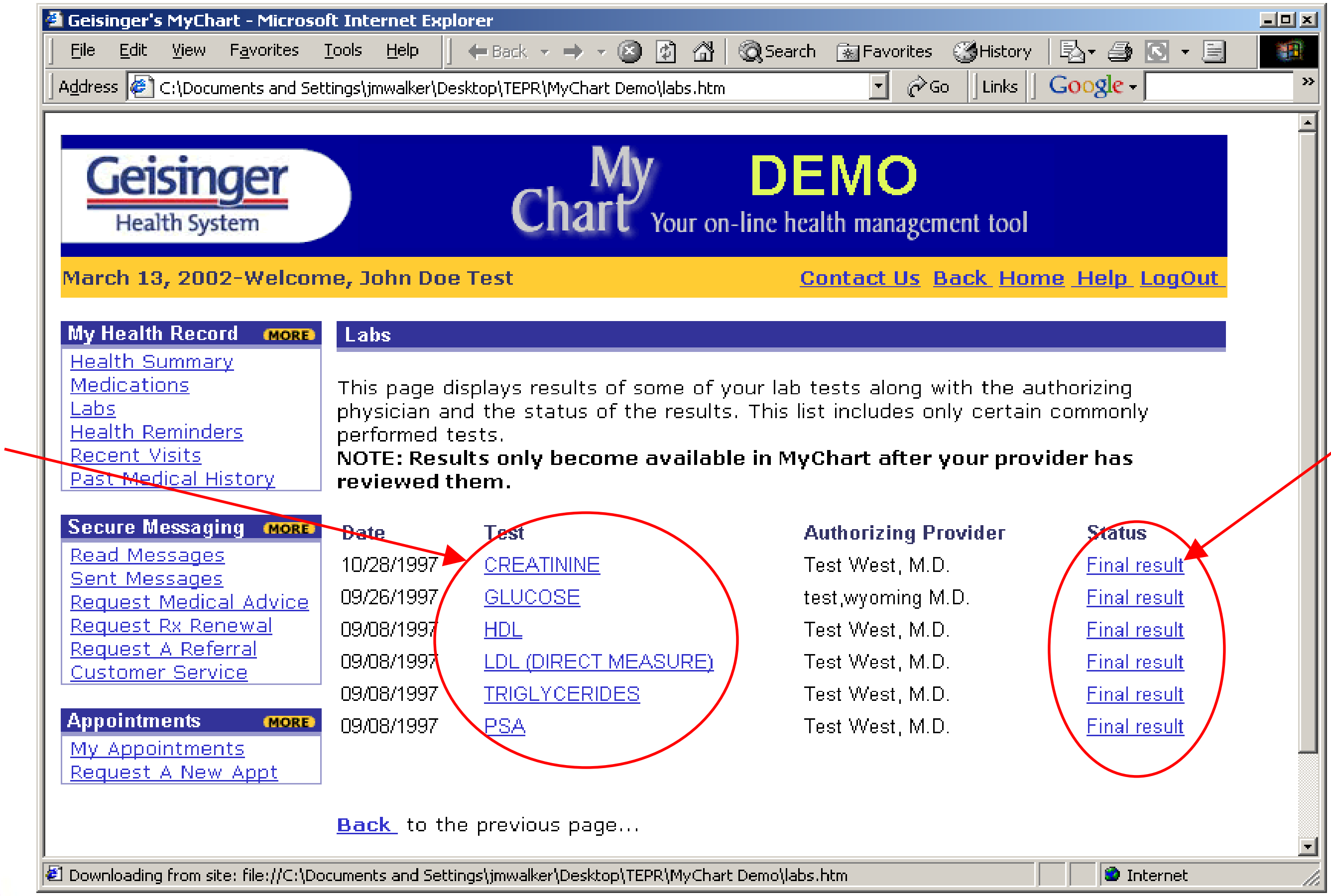
- MyChart Feedback
- Notice of Privacy Practices
- Physician Office Info
- Health Information
- Community Events
- Geisinger's Clinical Trials
- Terms and Conditions
- Health Privacy Statement

RSA SECURITY

Geisinger Health System

MyChart - Lab Results

Lab Tests



March 13, 2002-Welcome, John Doe Test

Labs

This page displays results of some of your lab tests along with the authorizing physician and the status of the results. This list includes only certain commonly performed tests.

NOTE: Results only become available in MyChart after your provider has reviewed them.

Date	Test	Authorizing Provider	Status
10/28/1997	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

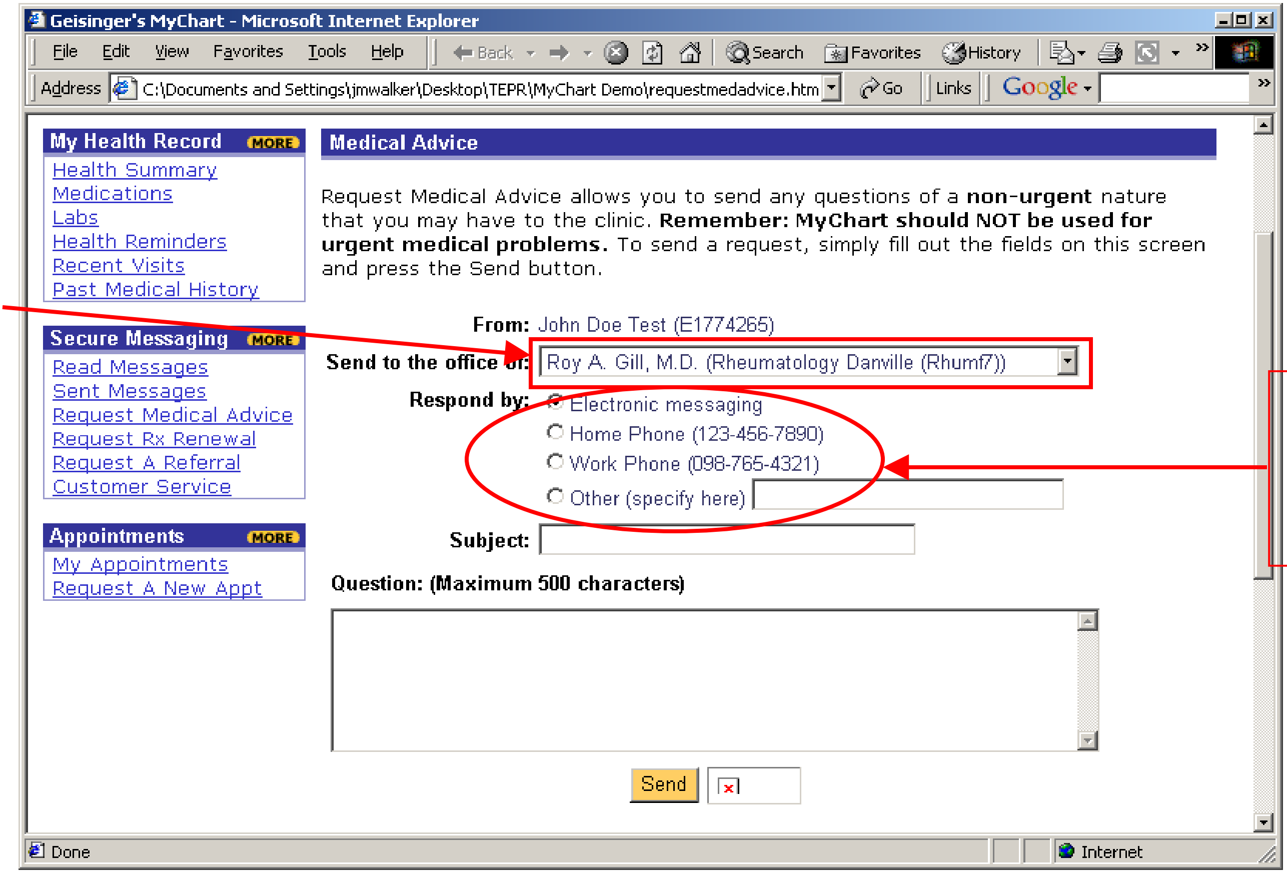
Back to the previous page...

Downloading from site: file://C:\Documents and Settings\jmwalker\Desktop\TEPR\MyChart Demo\labs.htm

Results

MyChart - Secure Messaging

PCP or last seen Physicians



Medical Advice

Request Medical Advice allows you to send any questions of a **non-urgent** nature that you may have to the clinic. **Remember: MyChart should NOT be used for urgent medical problems.** To send a request, simply fill out the fields on this screen and press the Send button.

From: John Doe Test (E1774265)

Send to the office of: Roy A. Gill, M.D. (Rheumatology Danville (Rhumf7))

Respond by:
● Electronic messaging
○ Home Phone (123-456-7890)
○ Work Phone (098-765-4321)
○ Other (specify here)

Subject:

Question: (Maximum 500 characters)

Patient's Communication Preference

RSA SECURITY

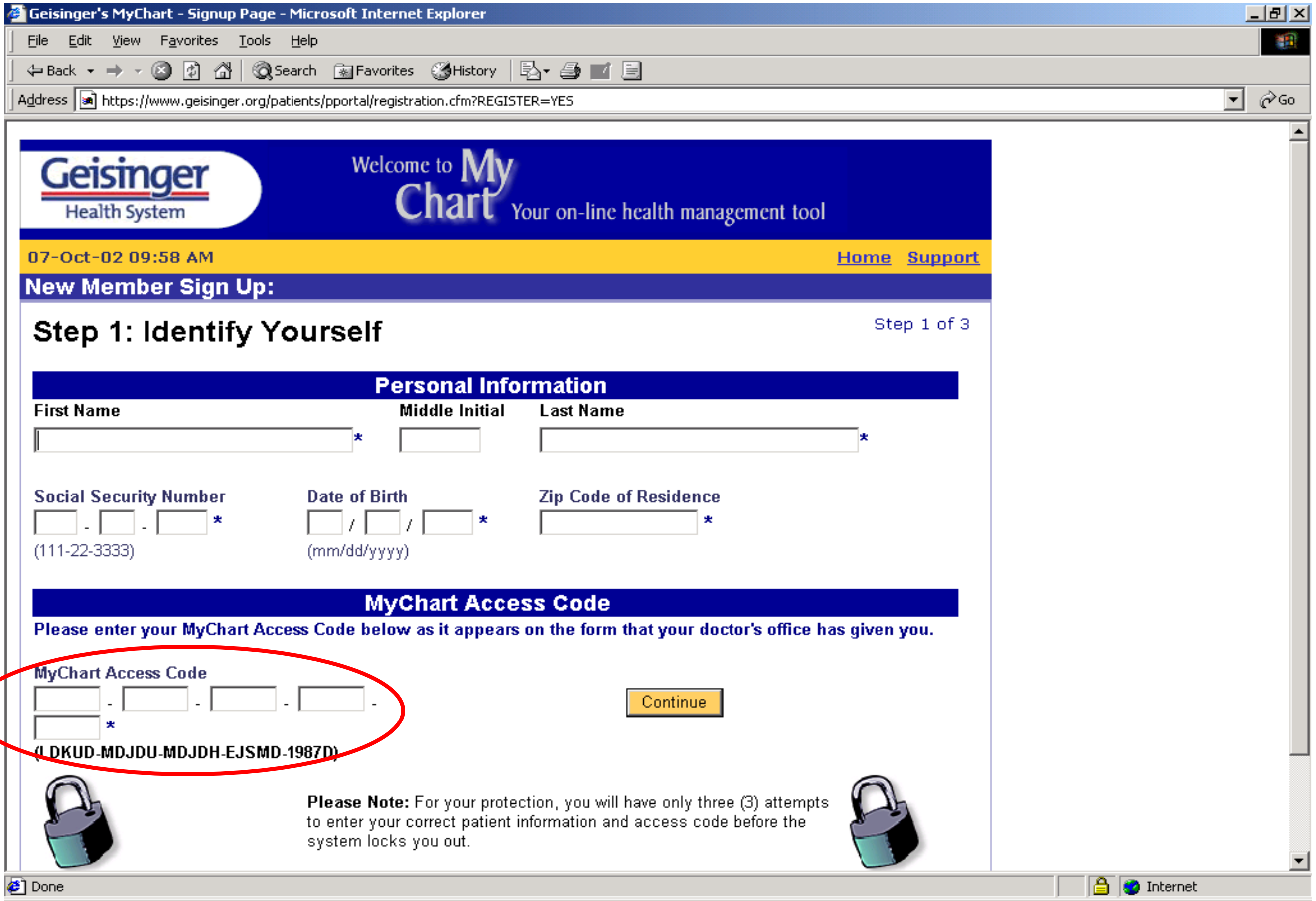
Geisinger Health System

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"



Geisinger's MyChart - Signup Page - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address https://www.geisinger.org/patients/pportal/registration.cfm?REGISTER=YES
Go
Geisinger Health System
Welcome to My Chart Your on-line health management tool
Home Support
Done
Internet

07-Oct-02 09:58 AM

New Member Sign Up:

Step 1: Identify Yourself

Step 1 of 3

Personal Information

First Name * Middle Initial Last Name *

Social Security Number * (111-22-3333)

Date of Birth * (mm/dd/yyyy)

Zip Code of Residence *

MyChart Access Code

Please enter your MyChart Access Code below as it appears on the form that your doctor's office has given you.

MyChart Access Code *

(LDKUD-MDJDU-MDJDH-EJSMD-1987D)

Continue

Please Note: For your protection, you will have only three (3) attempts to enter your correct patient information and access code before the system locks you out.

Personal Info

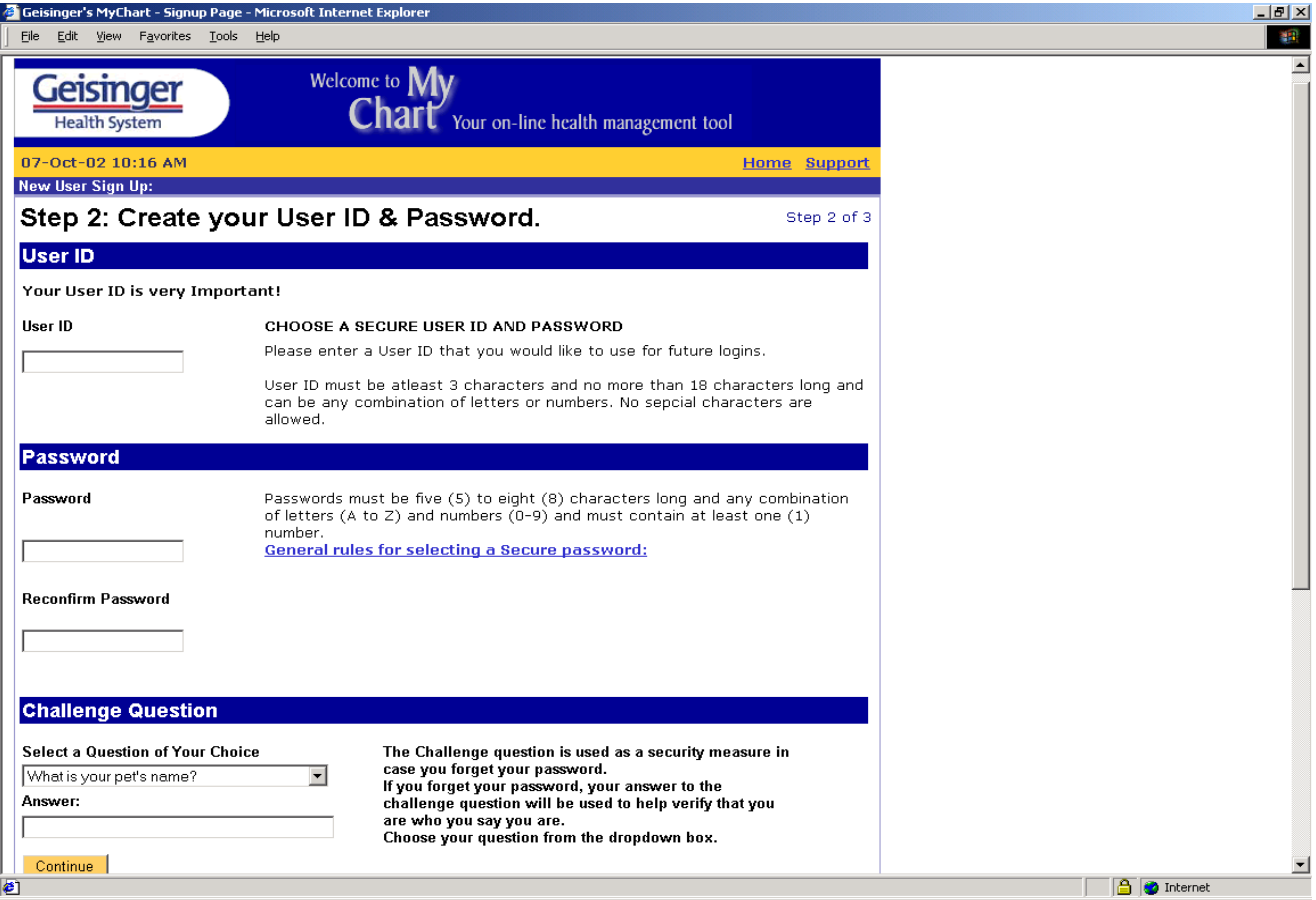
One-time use access code

Patient Registration
“Choose your User ID & Password”

Select UserID

Select Password

Select Challenge Q&A


Geisinger's MyChart - Signup Page - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Geisinger Health System
Welcome to My Chart Your on-line health management tool
Home Support
Internet

07-Oct-02 10:16 AM

New User Sign Up:

Step 2: Create your User ID & Password. Step 2 of 3

User ID

Your User ID is very Important!

User ID

CHOOSE A SECURE USER ID AND PASSWORD

Please enter a User ID that you would like to use for future logins.

User ID must be atleast 3 characters and no more than 18 characters long and can be any combination of letters or numbers. No sepcial characters are allowed.

Password

Password

Passwords must be five (5) to eight (8) characters long and any combination of letters (A to Z) and numbers (0-9) and must contain at least one (1) number.

General rules for selecting a Secure password:

Reconfirm Password

Challenge Question

Select a Question of Your Choice

What is your pet's name?

Answer:

The Challenge question is used as a security measure in case you forget your password.
If you forget your password, your answer to the challenge question will be used to help verify that you are who you say you are.
Choose your question from the dropdown box.

Continue

RSA SECURITY

Geisinger Health System

MyChart Registration - Tomorrow

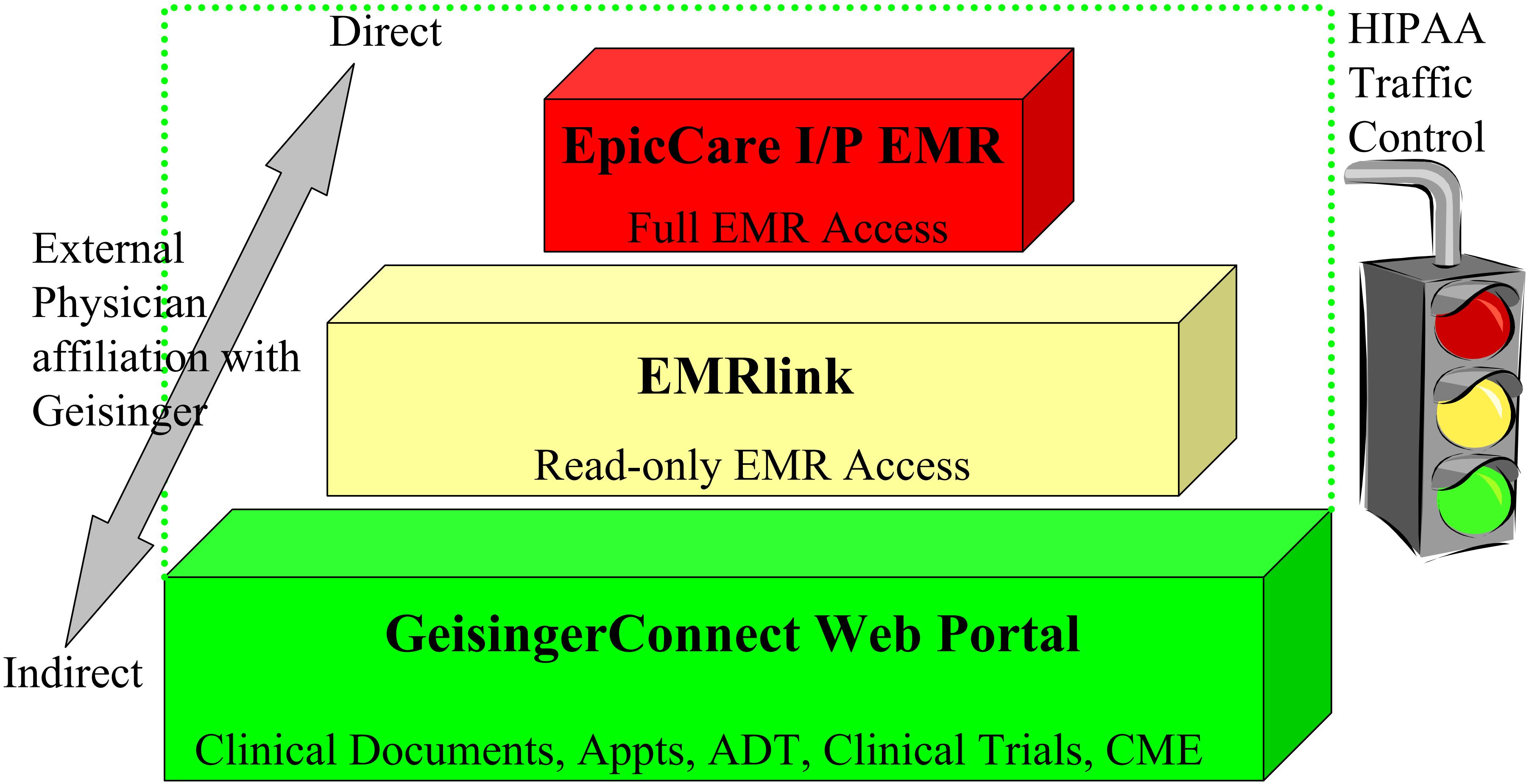
- Step 1 – Visit Geisinger.org and signup for Basic Portal (no PHI)
  - Identify yourself
  - Choose UserID, Password, and Challenge Q/A
  - Accepts T&Cs and then has immediate access to a Basic Patient portal
- Step 2 – Request MyChart Access online
  - From Basic Patient portal, request enrollment 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 has been developed exclusively by Geisinger for use by its external, physician partners.

GeisingerConnect Model



Direct

External Physician affiliation with Geisinger

Indirect

EpicCare I/P EMR

Full EMR Access

EMRlink

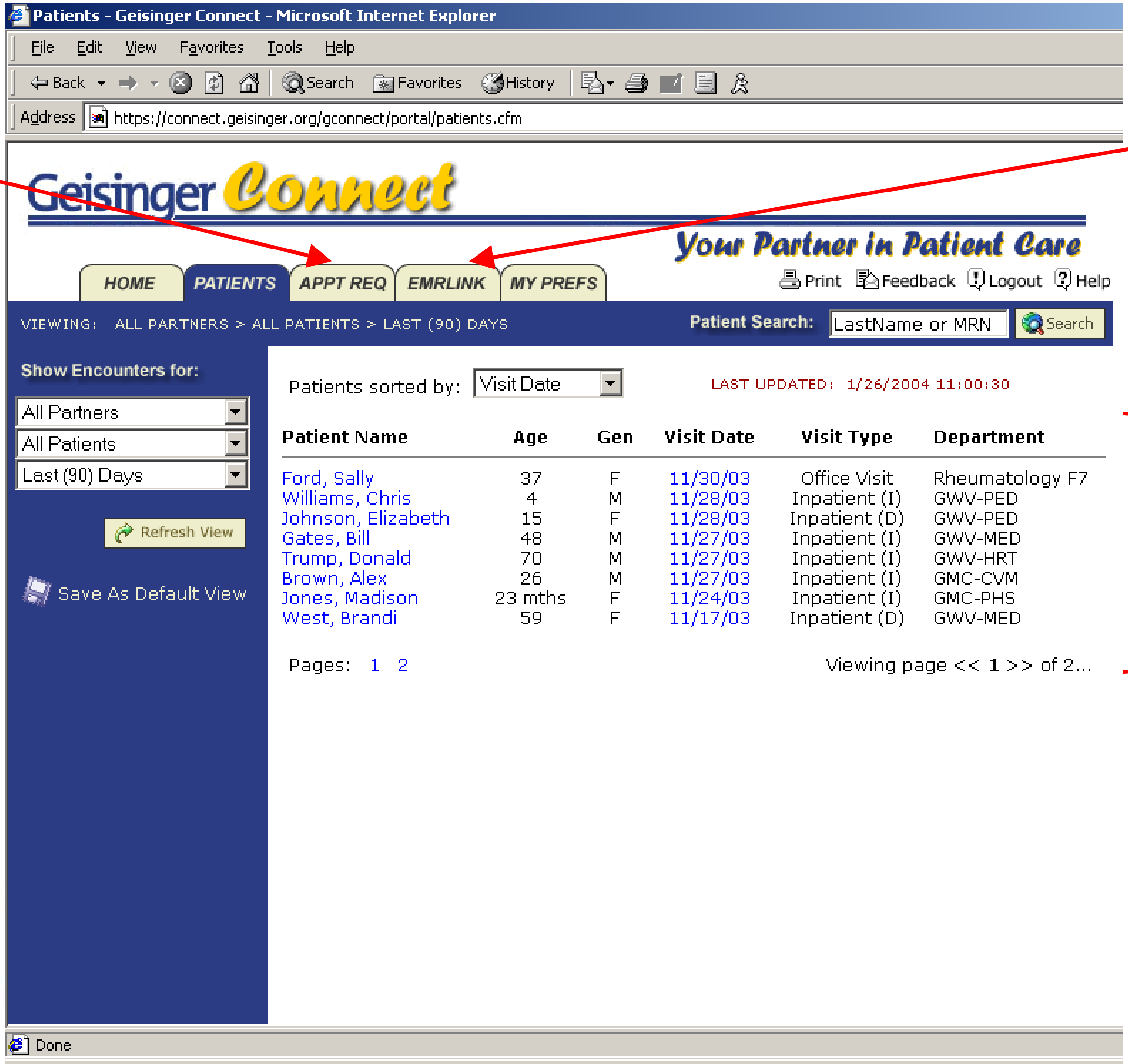
Read-only EMR Access

GeisingerConnect Web Portal

Clinical Documents, Appts, ADT, Clinical Trials, CME

HIPAA Traffic Control

Geisinger Connect – Patient List


Patients - Geisinger Connect - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address https://connect.geisinger.org/gconnect/portal/patients.cfm
Geisinger Connect
Your Partner in Patient Care
HOME PATIENTS APPT REQ EMRLINK MY PREFS
Print Feedback Logout Help
Patient Search: LastName or MRN Search
Refresh View
Save As Default View
Done

VIEWING: ALL PARTNERS > ALL PATIENTS > LAST (90) DAYS

Show Encounters for:

All Partners

All Patients

Last (90) Days

Patients sorted by: Visit Date

LAST UPDATED: 1/26/2004 11:00:30

Patient Name	Age	Gen	Visit Date	Visit Type	Department
Ford, Sally	37	F	11/30/03	Office Visit	Rheumatology F7
Williams, Chris	4	M	11/28/03	Inpatient (I)	GWV-PED
Johnson, Elizabeth	15	F	11/28/03	Inpatient (D)	GWV-PED
Gates, Bill	48	M	11/27/03	Inpatient (I)	GWV-MED
Trump, Donald	70	M	11/27/03	Inpatient (I)	GWV-HRT
Brown, Alex	26	M	11/27/03	Inpatient (I)	GMC-CVM
Jones, Madison	23 mths	F	11/24/03	Inpatient (I)	GMC-PHS
West, Brandi	59	F	11/17/03	Inpatient (D)	GWV-MED

Pages: 1 2

Viewing page << 1 >> of 2...

Referral Form

EMR Access

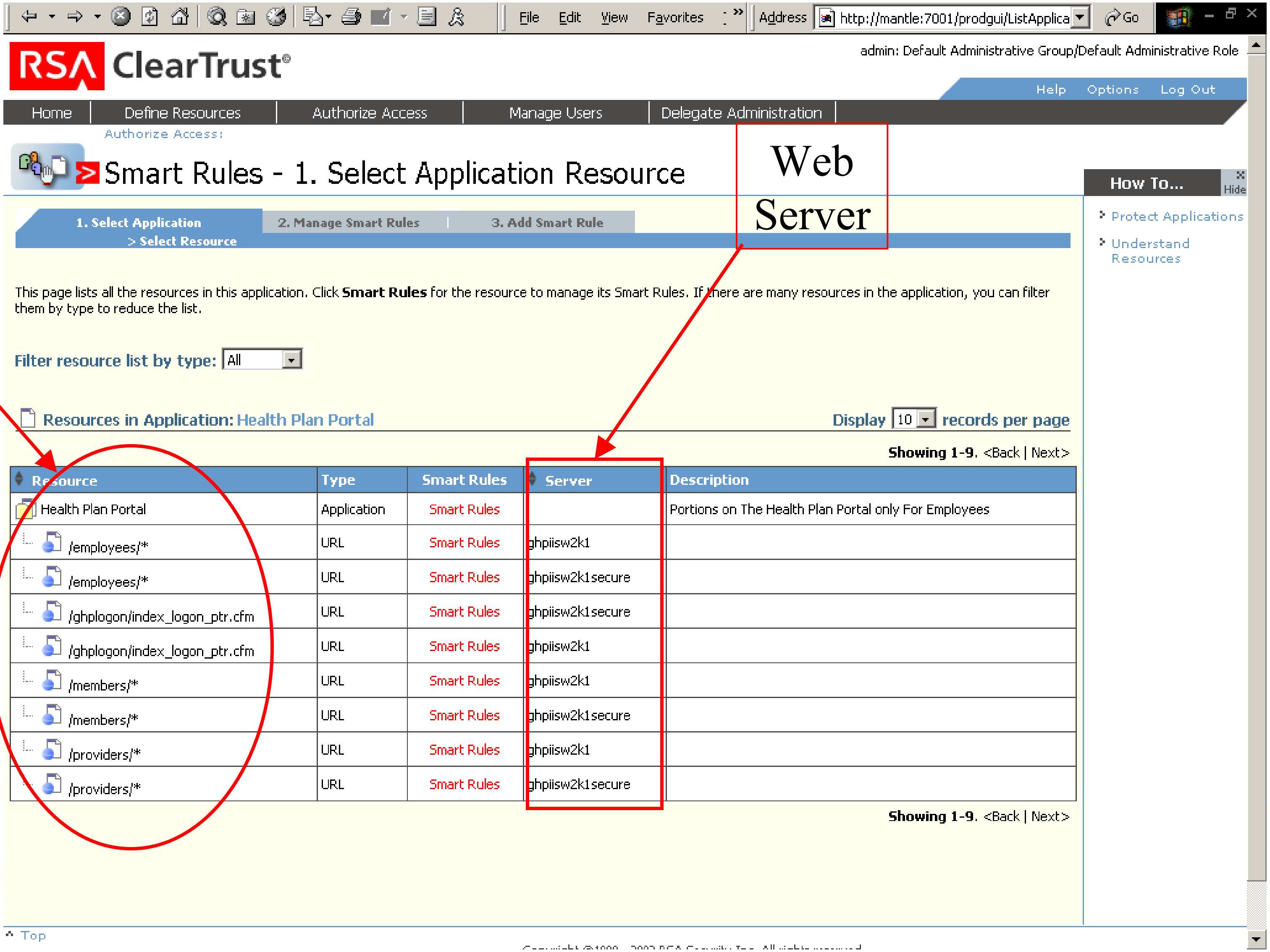
Patient List

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



File Edit View Favorites Address http://mantle:7001/prodgui/ListApplica Go
RSA ClearTrust®
admin: Default Administrative Group/Default Administrative Role
Help Options Log Out
Home Define Resources Authorize Access Manage Users Delegate Administration
Authorize Access:
How To... Hide
Protect Applications
Understand Resources
1. Select Application > Select Resource
2. Manage Smart Rules
3. Add Smart Rule
Web Server

Smart Rules - 1. Select Application Resource

This page lists all the resources in this application. Click **Smart Rules** for the resource to manage its Smart Rules. If there are many resources in the application, you can filter them by type to reduce the list.

Filter resource list by type: All

Resources in Application: Health Plan Portal

Display 10 records per page

Showing 1-9. <Back | Next>

Resource	Type	Smart Rules	Server	Description
Health Plan Portal	Application	Smart Rules		Portions on The Health Plan Portal only For Employees
/employees/*	URL	Smart Rules	ghpiisw2k1	
/employees/*	URL	Smart Rules	ghpiisw2k1secure	
/ghplogon/index_logon_ptr.cfm	URL	Smart Rules	ghpiisw2k1secure	
/ghplogon/index_logon_ptr.cfm	URL	Smart Rules	ghpiisw2k1	
/members/*	URL	Smart Rules	ghpiisw2k1	
/members/*	URL	Smart Rules	ghpiisw2k1secure	
/providers/*	URL	Smart Rules	ghpiisw2k1	
/providers/*	URL	Smart Rules	ghpiisw2k1secure	

Showing 1-9. <Back | Next>

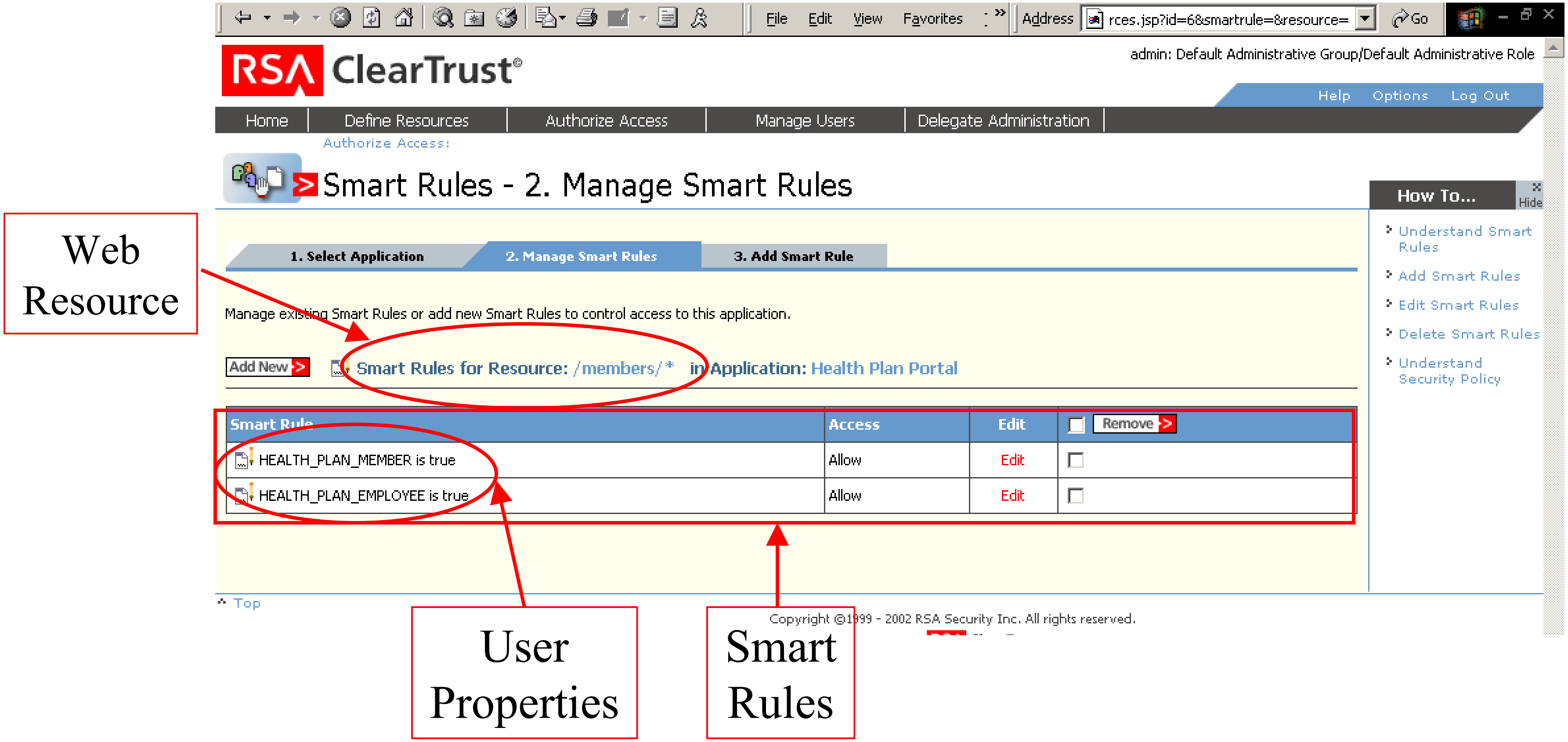
Top

Copyright ©1999 - 2002 RSA Security Inc. All rights reserved.

Web Resources

RSA SECURITY®

Role-based Access: Smart Rules



RSA ClearTrust®

admin: Default Administrative Group/Default Administrative Role

Help Options Log Out
Home | Define Resources | Authorize Access | Manage Users | Delegate Administration
Authorize Access:

Smart Rules - 2. Manage Smart Rules

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

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

Smart Rule	Access	Edit	☐ Remove
HEALTH_PLAN_MEMBER is true	Allow	Edit	☐
HEALTH_PLAN_EMPLOYEE is true	Allow	Edit	☐

Copyright ©1999 - 2002 RSA Security Inc. All rights reserved.

Web Resource

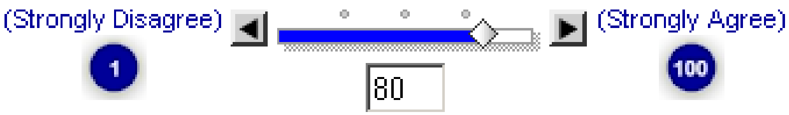
User Properties

Smart Rules

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