RSA SECURITY®

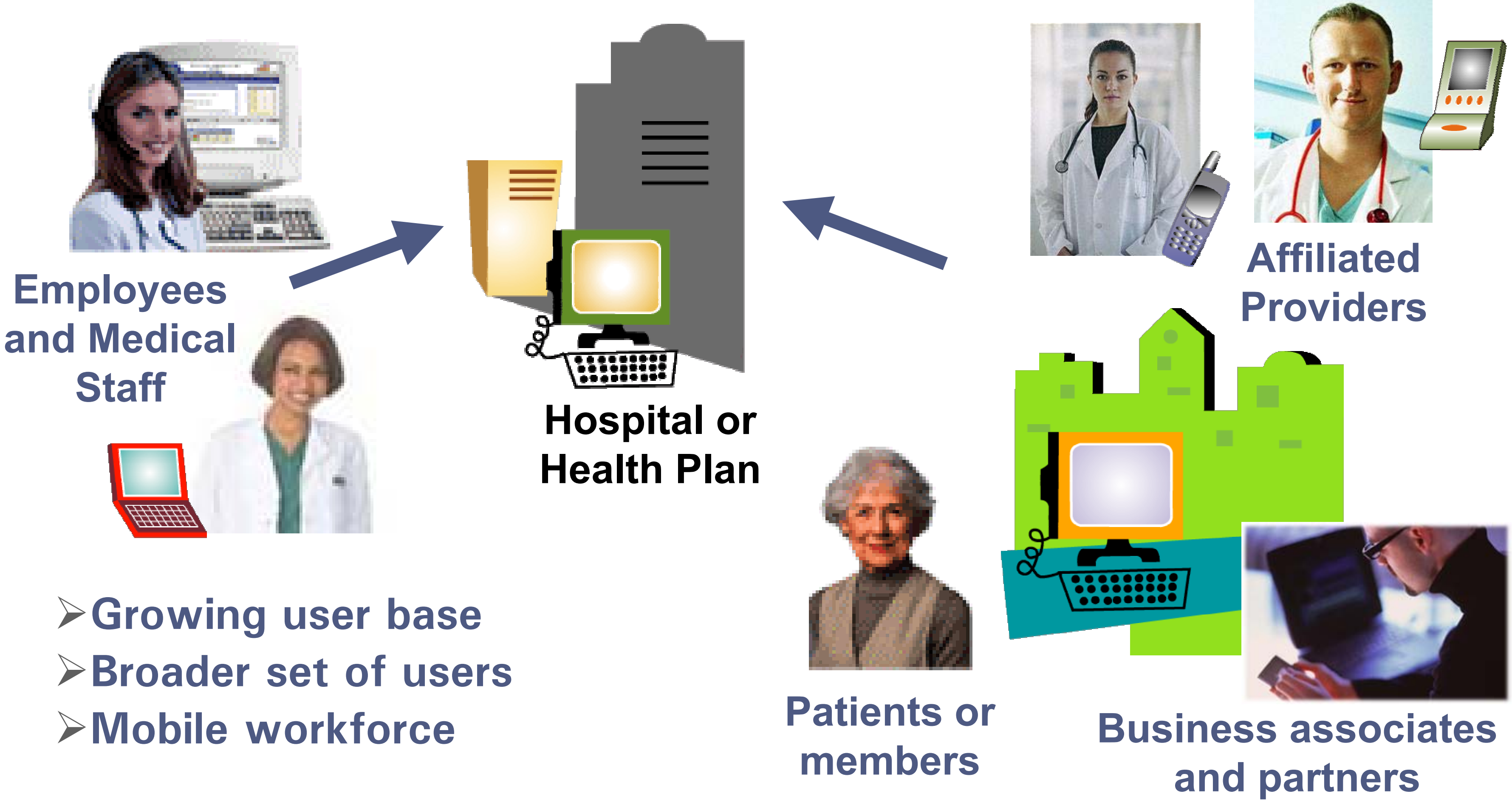
Case studies in Identity Management for Meeting HIPAA Privacy and Security Requirements

AUTHENTICATION ACCESS MANAGEMENT ENCRYPTION DIGITAL SIGNATURES

Agenda

- E-business trends in healthcare
- Challenges in Identity Management
- The Impact of HIPAA Privacy and Security Standards
- Meeting the standards: technology options
- Solutions in Identity Management
- Case studies

E-business trends in healthcare: Increased User Access



Employees and Medical Staff

Hospital or Health Plan

Affiliated Providers

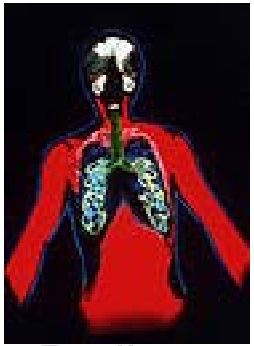
Patients or members

Business associates and partners

- Growing user base
- Broader set of users
- Mobile workforce

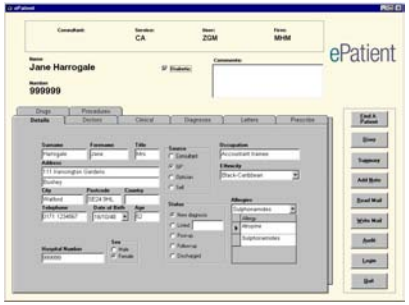
E-business trends in healthcare: Increased Application Exposure

Hospital



Radiology

Pharmacy



CA ZGM MHM

ePatient

Jane Harrogale

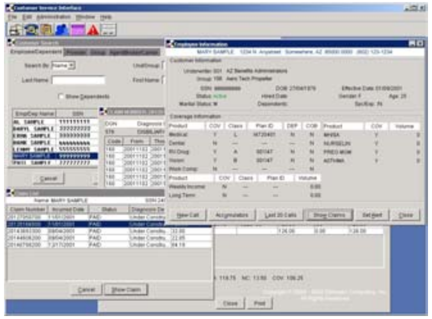
999999

Drugs | Procedures | Details | Doctors | Clinical | Diagnoses | Letters | Prescribe

Patient records

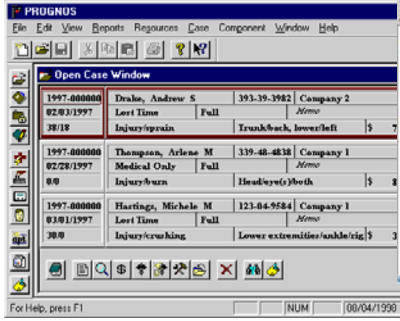
Laboratory

Health Plan



Eligibility

Accounts



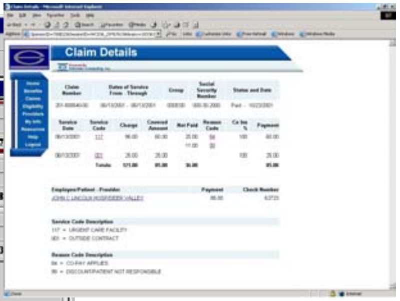
PROGNOS

File Edit View Reports Resources Case Component Window Help

Open Case Window

1997-000000	Drake, Andrew S	393-39-3982	Company 2
02/03/1997	Lost Time	Full	Memo
38/18	Injury/sprain	Trunk/back, lower/left	$
1997-000000	Thompson, Arlene M	339-48-4838	Company 1
02/28/1997	Medical Only	Full	Memo
0/0	Injury/burn	Head/eye(s)/both	$
1997-000000	Hastings, Michele M	123-04-9584	Company 1
03/01/1997	Lost Time	Full	Memo
30/0	Injury/crushing	Lower extremities/ankle/rig	$

For Help, press F1 NUM 08/04/1998 09:18 AM



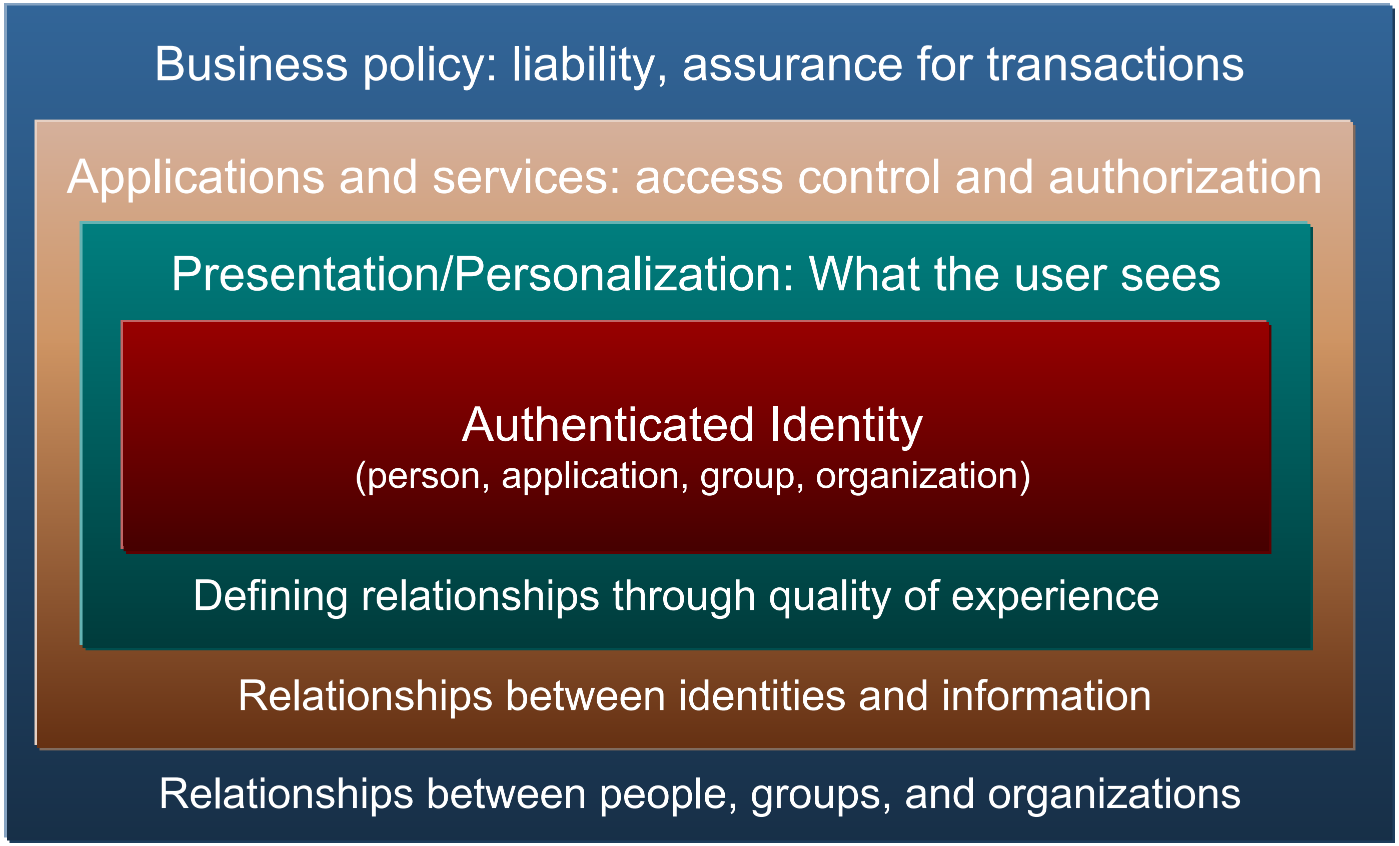
Claim Details

Claims

Referrals and Authorizations

- External access
- Mission critical applications

Defining Identity Management



Business policy: liability, assurance for transactions

Applications and services: access control and authorization

Presentation/Personalization: What the user sees

Authenticated Identity
(person, application, group, organization)

Defining relationships through quality of experience

Relationships between identities and information

Relationships between people, groups, and organizations

Source: Burton Group, October, 2002

Challenges in Identity Management

- User base is diverse, dynamic, and demanding
- Stronger authentication required for more applications
- Consistent enforcement of security policy across entire enterprise
- Increased Exposure to Risk

The Impact of HIPAA Privacy and Security

Privacy and Security Work Together

- **The Privacy Rule covers what information is to be protected, the uses and disclosures of information, and patients' privacy rights**
  - Finalized with a compliance date of April 14, 2003
- **Security covers what safeguards must be in place to protect information from unauthorized access, alteration, deletion, or transmission.**
  - Finalized with a compliance date of April 21, 2005
  - April 14, 2003 is also relevant since security measures must be in place to meet the Privacy Regulation

HIPAA Privacy Standards

- Mostly organizational, procedural
  - Inform patients of privacy rights
  - Provide notice of privacy practices
  - Appoint a privacy officer
- Requires Role-based Access Control
  - Based on “Minimum necessary” provisions
    - Must provide workers access to only the minimum necessary information needed to perform their work
    - Must develop policies and procedures and implement security measures to comply with minimum necessary provisions

HIPAA Security Standards

- General requirements
  - Ensure the confidentiality, integrity, and availability of all electronic protected health information
  - Protect against any reasonably anticipated threats or hazards, or uses or disclosures
- Flexible Approach
  - Use security measures that *reasonably and appropriately* implement the standards based on *risk analysis*
  - Technology-neutral
- Administrative, Physical, and Technical Safeguards

Meeting the Standards

Security Technical Safeguards	**Technology options**
Authentication	Passwords, Two-factor authentication, Digital Certificates, Smartcards, Biometrics
Access Control	ACLs, Web access management system, Encryption/Decryption
Data Integrity	Checksum, Digital signatures
Transmission Security	Encryption
Audit Controls	Logging and reporting mechanisms
Privacy RBAC Requirement	Web access management system

Authentication:
Time-synchronous two-factor

- Users authenticated through the use of an authenticator (token or smart card) by providing the token code (something the user *has*) and PIN (something the user *knows*)
- OR
- User authenticated through the use of existing mobile phones and PDAs by receiving a one-time access code as an SMS or text message

Authentication: Digital Certificates

- Data files containing information about the user and digitally signed by the issuing organization
  - Tied to corresponding public/private key pair
- Certificate management system issues and manages digital certificates
- Relative strength depends on protection of private key
  - Password governed by policy
  - Time-synchronous token
  - Smartcard

Access Control: Web Access Management

RSA SECURITY

- Centrally manages user privileges
  - Secures applications, Web sites, and other Web-based resources via intranets, extranets, and B2B and B2C infrastructures
  - Ensures only authorized users get access to specific resources
  - Provides fine-grained control over who can access what
  - Designed to flexibly integrate into environment
  - Transparent Web single sign-on
  - Delegated user management

Access Control: Encryption/Decryption

- Digital certificates
  - Encrypt document or message using public key
  - Access is limited only to those who can decrypt the data with private key
  - Provides a system to retrieve encryption keys in case of loss
- Encryption/compression utility
  - Utility for encrypting and compressing desktop files and e-mail attachments
    - Incorporates ZIP technology
  - Supports both password and certificate-based encryption

Data Integrity: Digital Signatures

- Digital certificates
  - Used for digitally signing web-based forms and e-mail messages
  - Digital signature process protects data integrity
    - Uses cryptographic techniques
    - Applications that have been digital signature-enabled can automatically verify signature and determine if the data that was signed has been altered

Transmission Security: Encryption

- Encryption technology should support strong encryption up to 2048 bits (asymmetric) and 128 bits (symmetric)
- Digital certificates for secure e-mail
- SSL server certificates for secure web communications
- Encryption/compression utility for files in transit

Audit Controls: Logging and reporting

- Authentication and access control systems should provide logging and reporting mechanisms for monitoring and analyzing users' access to resources, applications and files
- Should allow administrator to trace actions to individual users
- Logs should be configurable (e.g. what events, when, to where), time-stamped and strictly limited to system administrators

RBAC: Web access management

- Rights and permissions are granted to roles rather than individual users
  - Users are logically combined into *Groups* (role category) and *Sub-groups* (role sub-category)
  - Individuals and sub-groups inherit rights of group
  - Create exceptions for individuals using policy-based rules
    - Rules based on static and dynamic attributes

Are passwords good enough for HIPAA Compliance?

- Standard does not prescribe authentication method
- Do risk analysis and select *appropriate and reasonable* method
  - Look at security best practices in the industry
- For some applications, best practices require more than passwords
  - E.g. "Remote access requires two-factor authentication."*
- For others, current best practices say passwords okay
  - E.g. For patient or member access to web sites**
- For many applications, will depend on organization
- Best practices evolving

***HIPAA Security: the latest and best practices*, Tom Walsh, CISSP, HIMSS, 2003

**Gartner

Solutions in Identity Management

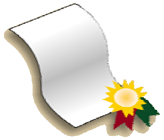
Providers: Strong authentication for remote access

Physicians

Future for on-site

Staff

Today



Future for on-site

Welcome To Geisinger Health System - Microsoft Internet Explorer

Geisinger Health System

TAKE CONTROL of YOUR HEALTH

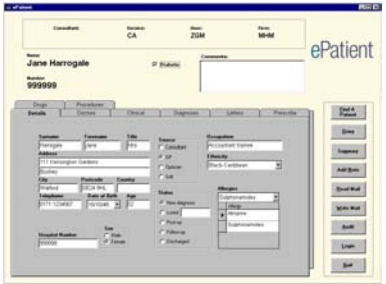
Insurances we accept...
Geisinger Health System participates in a wide variety of medical insurances and health plans. See a complete listing here.

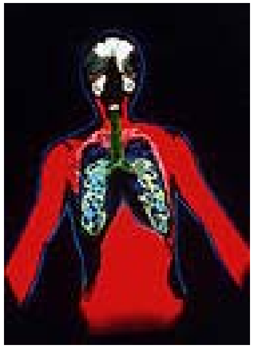
Learn more about philanthropy and giving opportunities at Geisinger here

WHAT'S NEW at Geisinger

HEALTH CARE in the news

Patient records, test results, lab results, pharmacy orders

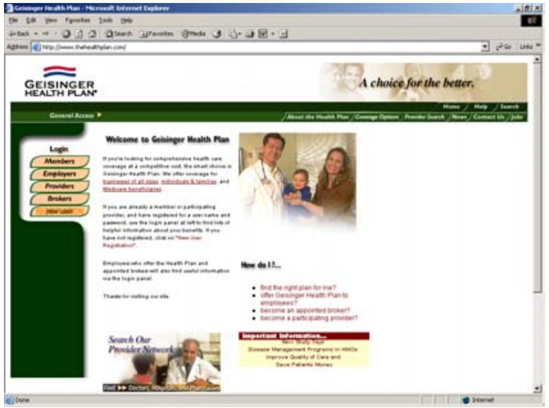




Payers: Strong authentication for remote and on-site access

Employees

Affiliated Providers


Geisinger Health Plan - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.thehealthplan.com/
Go Links
GEISINGER HEALTH PLAN
A choice for the better.
Home Help Search
General Access
About the Health Plan Coverage Options Provider Search News Contact Us Jobs
Login
Members
Employers
Providers
Brokers
New User
Search Our Provider Network
Done
Internet

Welcome to Geisinger Health Plan

If you're looking for comprehensive health care coverage at a competitive cost, the smart choice is Geisinger Health Plan. We offer coverage for businesses of all sizes, individuals & families, and Medicare beneficiaries.

If you are already a member or participating provider, and have registered for a user name and password, use the login panel at left to find lots of helpful information about your benefits. If you have not registered, click on "New User Registration".

Employers who offer the Health Plan and appointed brokers will also find useful information via the login panel.

Thanks for visiting our site.

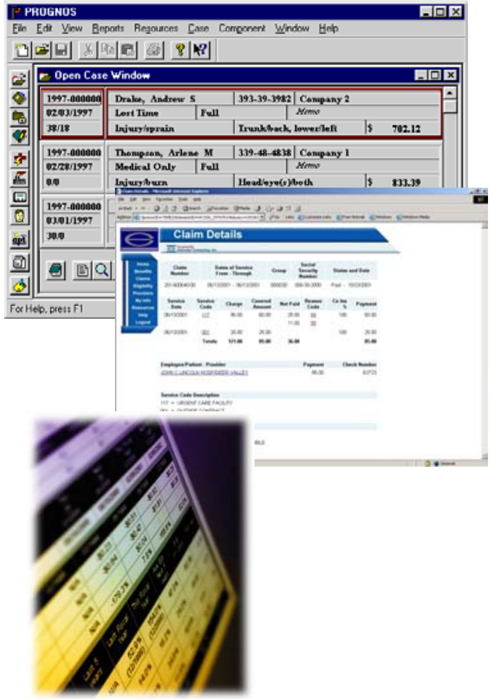
How do I?...

- find the right plan for me?
- offer Geisinger Health Plan to employees?
- become an appointed broker?
- become a participating provider?

Important Information...
New Study Says
Disease Management Programs in HMOs
Improve Quality of Care and
Save Patients Money

Brokers

Claims, referrals, accounts



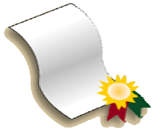
1997-000000	Drake, Andrew S	393-39-3982	Company 2	
02/03/1997	Lost Time	Full	Memo	
38/18	Injury/sprain	Trunk/back, lower/left	$	702.12
1997-000000	Thompson, Arlene M	339-48-4838	Company 1	
02/28/1997	Medical Only	Full	Memo	
0.0	Injury/burn	Head/eye(s)/both	$	833.39
1997-000000				
03/01/1997				
30.0				

Providers and Payers: Password authentication for remote access

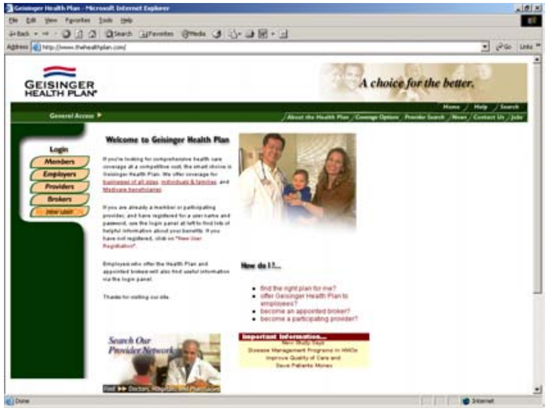
Patient or Member

Password

2003



? > 2003


Geisinger Health Plan - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.thehealthplan.com/
Go Links
Home Help Search
General Access
About the Health Plan Coverage Options Provider Search News Contact Us Jobs
Login
Members
Employers
Providers
Brokers
New User
Done
Internet

GEISINGER HEALTH PLAN

A choice for the better.

Welcome to Geisinger Health Plan

If you're looking for comprehensive health care coverage at a competitive cost, the smart choice is Geisinger Health Plan. We offer coverage for businesses of all sizes, individuals & families, and Medicare beneficiaries.

If you are already a member or participating provider, and have registered for a user name and password, use the login panel at left to find lots of helpful information about your benefits. If you have not registered, click on "New User Registration".

Employers who offer the Health Plan and appointed brokers will also find useful information via the login panel.

Thanks for visiting our site.

Search Our Provider Network

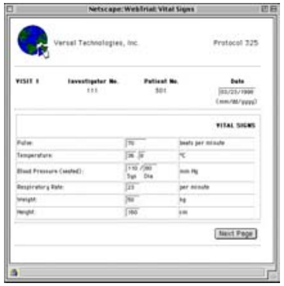
Find ▶▶ Doctors, Hospitals and Pharmacies

How do I?...

- find the right plan for me?
- offer Geisinger Health Plan to employees?
- become an appointed broker?
- become a participating provider?

Important Information...

New Study Says Disease Management Programs in HMOs Improve Quality of Care and Save Patients Money



Versal Technologies, Inc.

Protocol 325

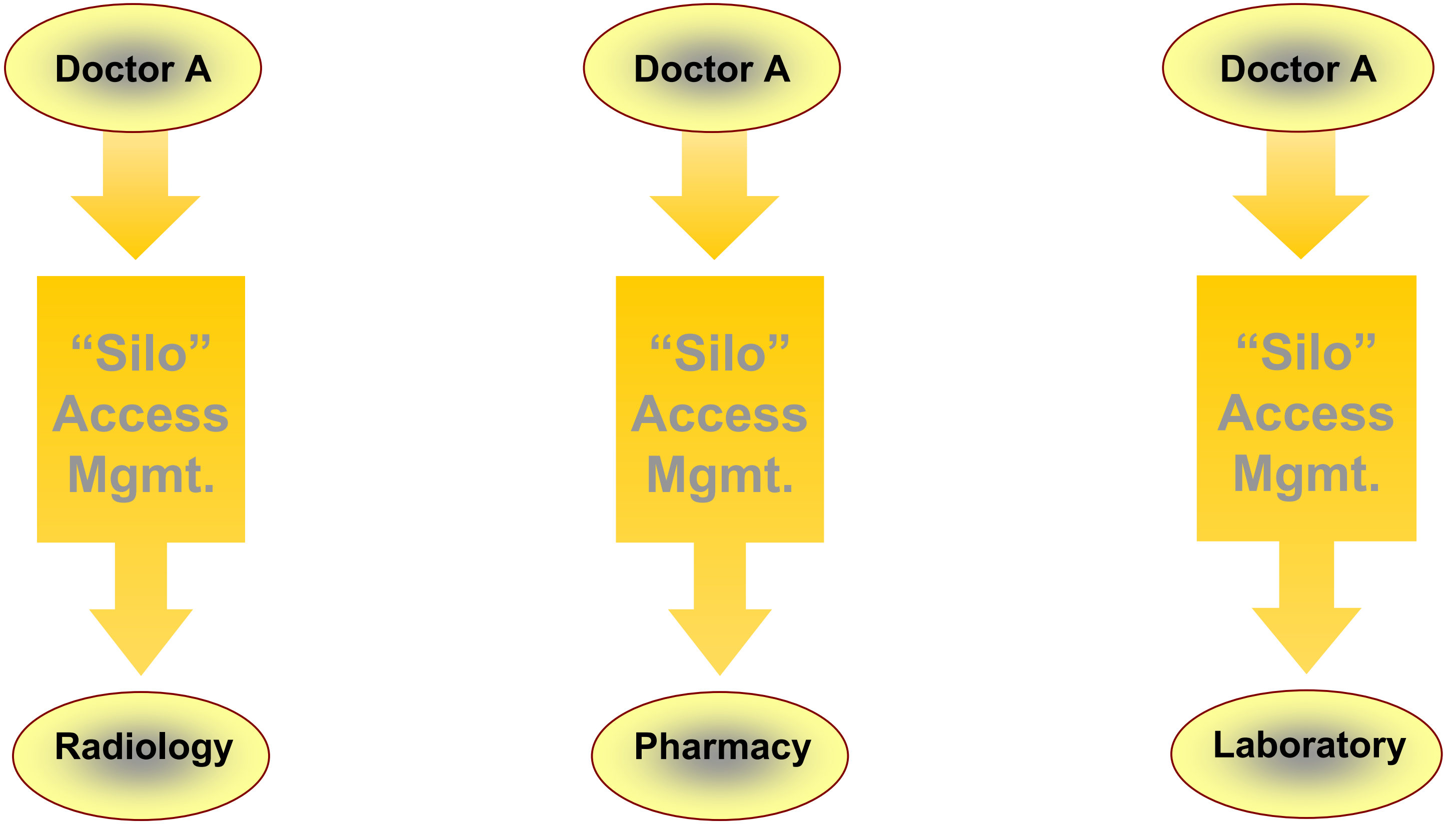
VISIT 1	Investigator No.	Patient No.	Date
	111	501	[illegible] (mm/dd/yyyy)

VITAL SIGNS

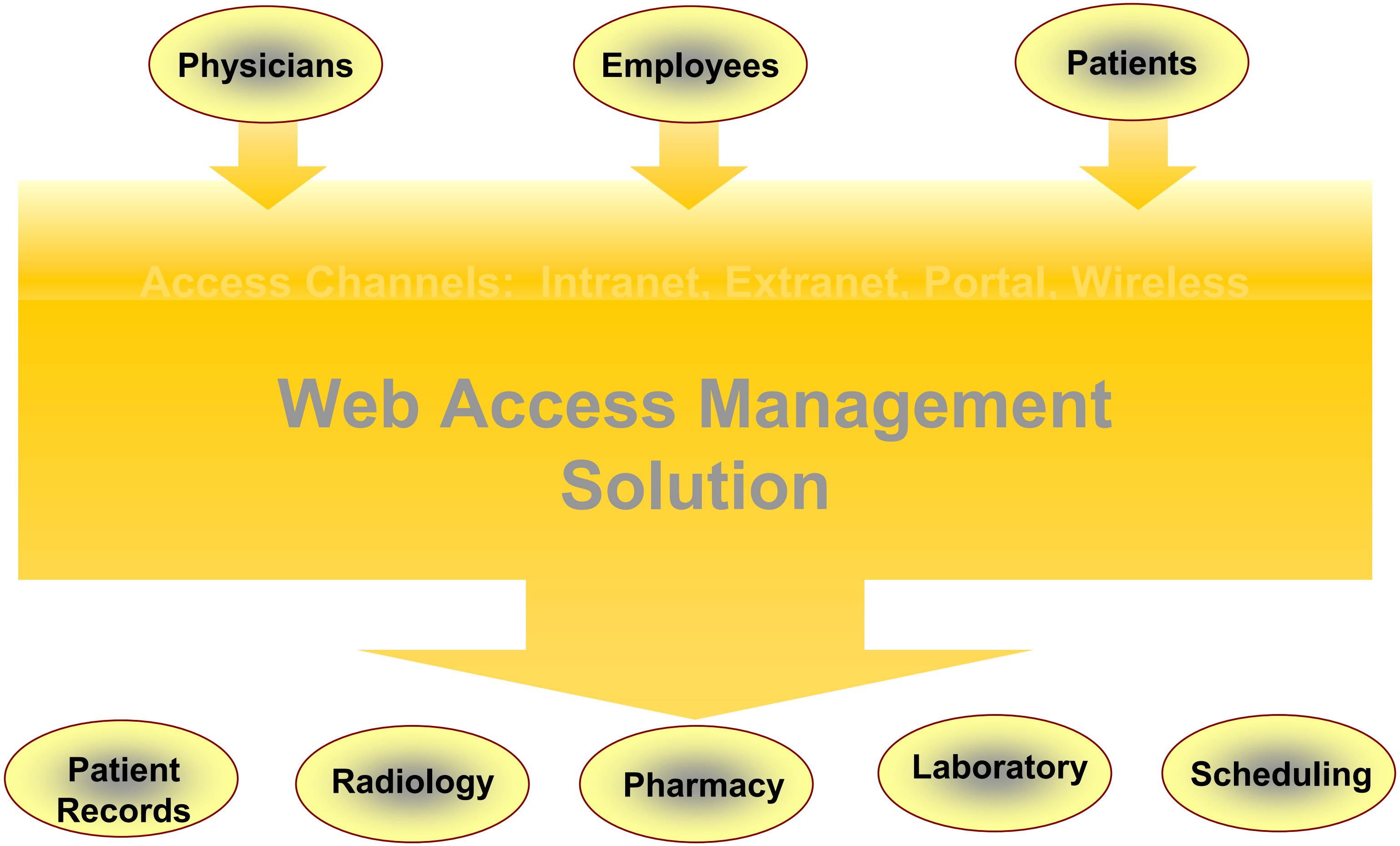
Pulse:	70	beats per minute
Temperature:	36 . 8	°C
Blood Pressure (seated):	110 / 80 Sys Dia	mm Hg
Respiratory Rate:	23	per minute
Weight:	50	kg
Height:	160	cm

Access controlled by web access management system to ensure that patient/ member can only view (and not edit) their own medical records (and not others)

Moving from application-specific access control…



…to centralized access control


Physicians
Employees
Patients
Access Channels: Intranet, Extranet, Portal, Wireless
Web Access Management Solution
Patient Records
Radiology
Pharmacy
Laboratory
Scheduling

Case studies

Blue Cross Blue Shield of Kansas

- Independent member of BCBS Association
  - 700,000 members and 2,000 employees
  - $940 M underwritten business and $2.1 B Medicare claims
- Objectives
  - Manage access to information on Web site and intranet
  - Provide different users with access to different views (RBAC)
  - Ensure only authorized users access confidential health information
  - Provide SSO to multiple Web-based applications
  - Monitor user activity: audit trails
  - Save time on security administration
  - Scalable infrastructure
  - Meet HIPAA requirements

Blue Cross Blue Shield of Kansas

- **Solution:**
  - Web Access Management and Two-factor Authentication
  - 25,000 users
- **Key factors**
  - Graded authentication
    - Remote employees, remote-hospital nurses and in-house IT administrators use two-factor authentication
    - Patients use passwords
  - Policy-based rules using dynamic attributes
  - Ability to provide RBAC
  - Ease of install
  - Delegated administrative model
  - Fine-grained access control

BlueCross BlueShield Association

Large U.S. Health Plan

- National healthcare and benefits organization
  - Millions of members
  - Tens of thousands of employees
- Objectives
  - Decrease costs for remote access
  - Develop security framework for web-based applications
  - Strengthen user authentication practices
  - Meet HIPAA requirements

Large U.S. Health Plan

RSA SECURITY

- Solution
  - Digital certificate management infrastructure
  - Employee user authentication (20,000+ users)
    - Remote access and on-site access
- Key factors
  - Reduced costs by moving from dial-up to VPN
  - Implemented stronger authentication
  - Scalable to handle large user base
  - Foundation for secure web communications (deployed SSL server certificates), secure e-mail (in process) and digital signing (future)

Boston Medical Center

- **Private, not for profit, 547-licensed bed AMC**
  - Provides full spectrum of pediatric and adult care services
  - 800,000 patient visits and 25,000 admissions annually
- **Objectives**
  - Provide secure remote access for doctors and other staff to key clinical applications
    - Sunrise Clinical Manager, CPOE for in-patient care
    - Logician from G.E. Med, EPR for outpatient and ambulatory care
  - Provide SSO to multiple Web-based applications
  - Centralize administrative control of user access privileges
  - Ensure only authorized medical staff have access to PHI
  - Implement role-based access control
  - Meet HIPAA requirements

Boston Medical Center

RSA SECURITY

- Solution
  - Web Access Management and Two-factor Authentication
  - 4,000 users
- Key factors
  - Provides right balance between end-user convenience and security for sensitive patient records
  - Ease of integration
  - Web Single Sign-on: reducing the number of passwords
  - Centralized management of Web access privileges

BOSTON MEDICAL CENTER

Geisinger Health System

- Physician-led healthcare system
  - Serves more than two million people
  - In 38 counties in Pennsylvania
- Objectives
  - Rollout secure Web applications
    - Portals for affiliated providers and patients
  - Integrate with existing systems
    - Epic System’s MyChart, Novell’s LDAP-compliant eDirectory,™ Sybase databases and Macromedia’s ColdFusion application development software
  - Provide a high level of security
  - Meet HIPAA requirements

Geisinger Health System

Heal. Teach. Discover. Serve.

Geisinger Health System

- **Solution**
  - Web Access Management and Two-factor Authentication
  - 10,000 users currently and growing (8,500 employees and 1,500 external users)
- **Key factors**
  - Graded authentication
    - Access to certain information requires two-factor authentication
  - Fine-grained access control
  - Role-based access control
  - Ability to monitoring user activity with detailed audit trails

Geisinger Health System

Heal. Teach. Discover. Serve.

Providence Health System

RSA SECURITY

- Comprehensive array of services across a four-state area
  - Including 20 acute care hospitals, 9 long-term care facilities, and a network of physician organizations
  - Sponsors health plans covering more than 850,000 members
- Objectives
  - Deliver critical information to doctors wherever they are
    - Lab results, X-Ray reports, billing information, ECG, X-ray images and medication information
  - Integrate with Citrix MetaFrame XP
  - Ensure personal medical information remains confidential
  - Security solution fail-safe and easy for the clinicians to manage
  - Meet HIPAA requirements

Providence | Health System

Providence Health System

- **Solution**
  - Two-factor Authentication
  - 2,000 users
- **Key factors**
  - Convenient and easy to use for doctors
  - Keeps patient information confidential
  - Reduces operating costs
  - Easily deployed
  - Seamless interoperability with Citrix MetaFrame

Catholic Health System

- Large provider in upstate New York
  - 8,000 employees and 1,200 physicians
  - Serves over 200,000 patients through network of hospitals, centers and facilities (total of 40 sites)
- Goals
  - Reduce costs and complexity of remote access
  - Allow medical staff to have fast, easy, and secure access to patient data from external clinics or home
    - Deliver applications with strong encryption and strong authentication
  - Protect privacy of patient data
  - Meet the requirements of HIPAA

Catholic Health System
Medical excellence with a tradition of caring.

Catholic Health System

- Solution
  - Two-factor authentication
  - Users use same authentication method to sign-on to multiple applications
  - Physicians get secure access to patient data from any location at any time
- Key factors
  - Reduced cost of installation and on-going support
  - Medical staff can quickly, securely, and easily access central resources
  - Integration with Neoteris Instant Virtual Extranet (SSL VPN gateway)

Catholic Health System
Medical excellence with a tradition of caring.

North Shore Long Island Jewish Health System

- Located in Great Neck, N.Y
  - 18 hospitals and 30,000 employees
- Objectives
  - For remote access to the intranet by physicians and contractors
  - Compatible with environment which includes wireless LANs, LDAP-based directories
  - Meet HIPAA privacy and security rules
  - Use audit and access controls to protect patient data
  - Implement "industry best practices"

North Shore Long Island Jewish Health System

- Solution
  - Two-factor authentication with time synchronous tokens and Mobile two-factor authentication using phones/PDAs for remote access
  - Digital certificates for patient bedside-registration system (planned)
    - A digital signature will be applied to every use of electronic patient record
  - Digital certificates for encrypting and digitally signing e-mail (planned)
- Key factors
  - Integration with Cisco-based VPN
  - Integration with Novell eDirectory (metadirectory for patient information) and Microsoft Active Directory (directory service)
  - Comprehensive audit trail of changes and non-repudiation

NORTH SHORE
LONG ISLAND JEWISH
HEALTH SYSTEM

Siemens Medical Solutions Health Services Corporation

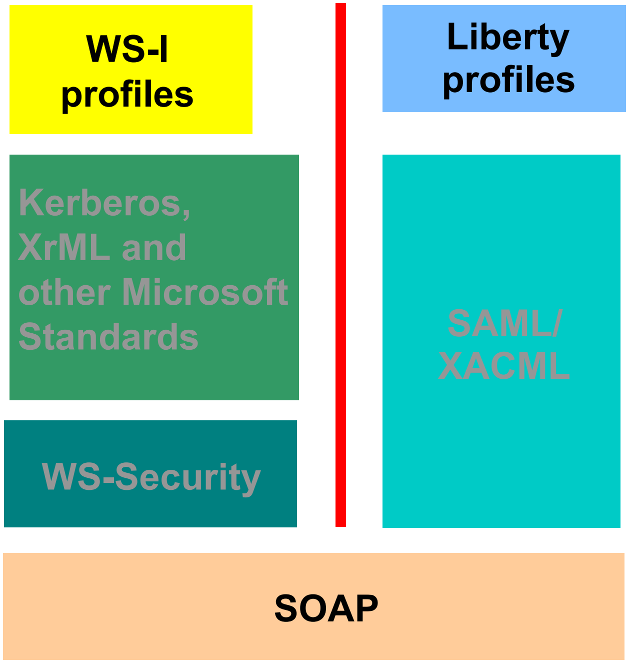
- Application service provider
  - Processes more than 116 million transactions daily and manages more than 67 terabytes of data
  - Employs 30,000 people worldwide
  - Hosts applications such as registration, financial tracking and clinical systems for more than 1,000 HCOs
- Objectives
  - Provide secure Internet access to mission-critical applications and patient information hosted by Siemens
  - Employ security protocols equivalent to HCOs
    - i.e. Meet the requirements of HIPAA

Siemens Medical Solutions Health Services Corporation

- Solution
  - Two-factor Authentication
  - 11,000 external users
  - 4,000 internal employees
- Key factors
  - Only authorized users to gain entry to networks and confidential healthcare information
  - Interoperability with Cisco VPN

Glimpse to tomorrow: Federated Identities

- Use of agreements, standards, and technologies to make identity and entitlements portable across autonomous domains
- Rate of adoption depends on standards efforts



WS-I profiles

Liberty profiles

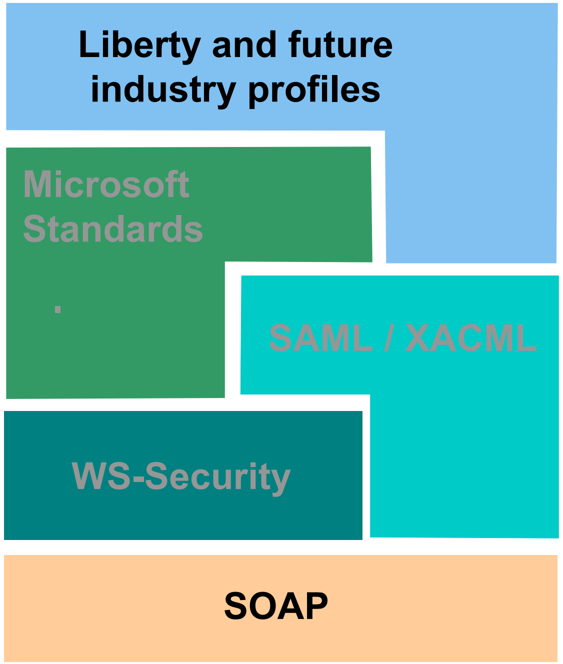
Kerberos, XrML and other Microsoft Standards

SAML/ XACML

WS-Security

SOAP

Possible scenario



Liberty and future industry profiles

Microsoft Standards

.

SAML / XACML

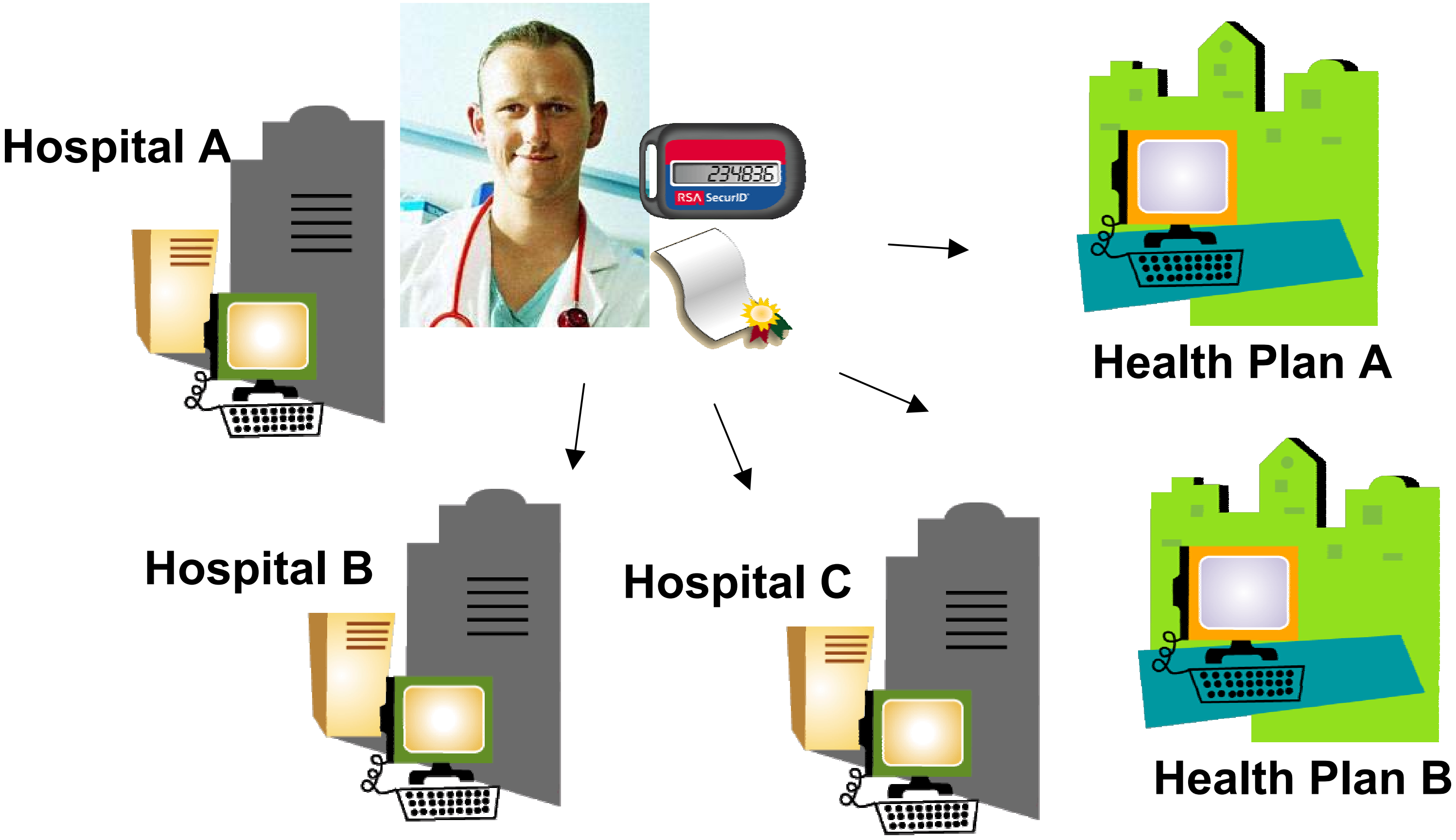
WS-Security

SOAP

Most likely scenario

Source: Burton Group

Glimpse to tomorrow: Federated Identities



Hospital A

Health Plan A

Hospital B

Hospital C

Health Plan B

RSA

SECURITY®

www.rsasecurity.com

lrobinson@rsasecruity.com