Connecting Healthcare®
Engaging Patients™

HIPAASuccess - Physician Education Series

HIPAA Security – What Does it Require?

Your Faculty:
Walt Culbertson

- President and Founder, Connecting Healthcare®
- Host and Producer, Medical Update Show
- Served as Technical and Operations Lead, HIE Project Manager
  Florida Health Information Exchange
- Served as the State of Florida - Technical SME for the ONC State Health Policy Consortium, Southeast Regional HIT-HIE Collaboration (SERCH)
- Founding Executive Director, ePrescribe Florida and President, ePrescribe America
- Founding Chair of the Southern Healthcare Administrative Regional Process (SHARP), a regional collaborative workgroup alliance of private and public health care organizations and HHS, HRSA and CMS
- Founding Co-Chair of the CMS Sponsored Southern Insurance Commissioner Task Force, a regional collaborative workgroup alliance for State-level HIPAA Education
- Founding Security and Privacy Co-Chair for the Workgroup for Electronic Data Interchange (WEDi) Strategic National Implementation Process (SNIP)

Agenda

- Introduction to HIPAA Security
- HIPAA Security Requirements
- Security Policies and Procedures
- Meeting HIPAA Security Compliance

Security is a P.A.I.N.

P rivacy	is what you have to secure
A uthentication	identifying those sending & receiving information and accessing systems
I ntegrity	guaranteeing non-altered information
N on-Repudiation	being able to prove that the sender did in fact send the information

Final Security Rules – Part 1

- The initial Security Rule was published February 20, 2003 with a final compliance date of April 21, 2005
- The Security Rule specifies a series of administrative, technical, and physical security procedures for covered entities to use to assure the confidentiality, integrity, and availability of e-PHI
- Protect data against *reasonably* anticipated threats or hazards
- Addresses security from both administrative and technical perspective to safeguard
  - Integrity of data
  - Confidentiality of information

Final Security Rules – Part 2

- As part of the Health Information Technology for Economic and Clinical Health (HITECH) Act, the initial HIPAA Security rile was amended by the Omnibus Rule on January 25, 2013
- It included provisions that change several important aspects of the rule
- The Omnibus Rule requires the compliance of business associates (BAs) and their subcontractors
- It also requires the Office for Civil Rights (OCR) to perform audits that include stiffer penalties for non-compliance

Who is Covered?

- Who must comply?
  - Health plans
  - Clearinghouses
  - Any healthcare provider who transmits any health information in electronic form in connection with a standard transaction
- Business associates (BAs) and their subcontractors
- Covered Entities must obtain assurances regarding security from their agents and chain of trust (Business Associate Agreements)

Security Applies to ALL Electronic Data

- Provides ***standards*** for security but does not mandate specific technology
- Applies to data electronically transmitted or maintained
- Scalable and flexible and technology neutral
  - Allows entity to implement standards in best way to meet business requirements
  - Implement requirements differently in large versus small organizations

Security Requires Documentation

- Documentation is a core component of the Security requirements:
  - Analyze security risks and document
  - Document how will mitigate risks to protect data and meet security standards
  - If do not implement a requirement, use documentation to justify why
  - Document administrative policies and procedures will follow to enforce security requirements

Security Rule Requirements

- Security requirements in four areas:
  - Administrative procedures
  - Physical safeguards
  - Technical services
  - Technical mechanisms (networks)
- 75 - 80% of requirements are administrative rather than technical

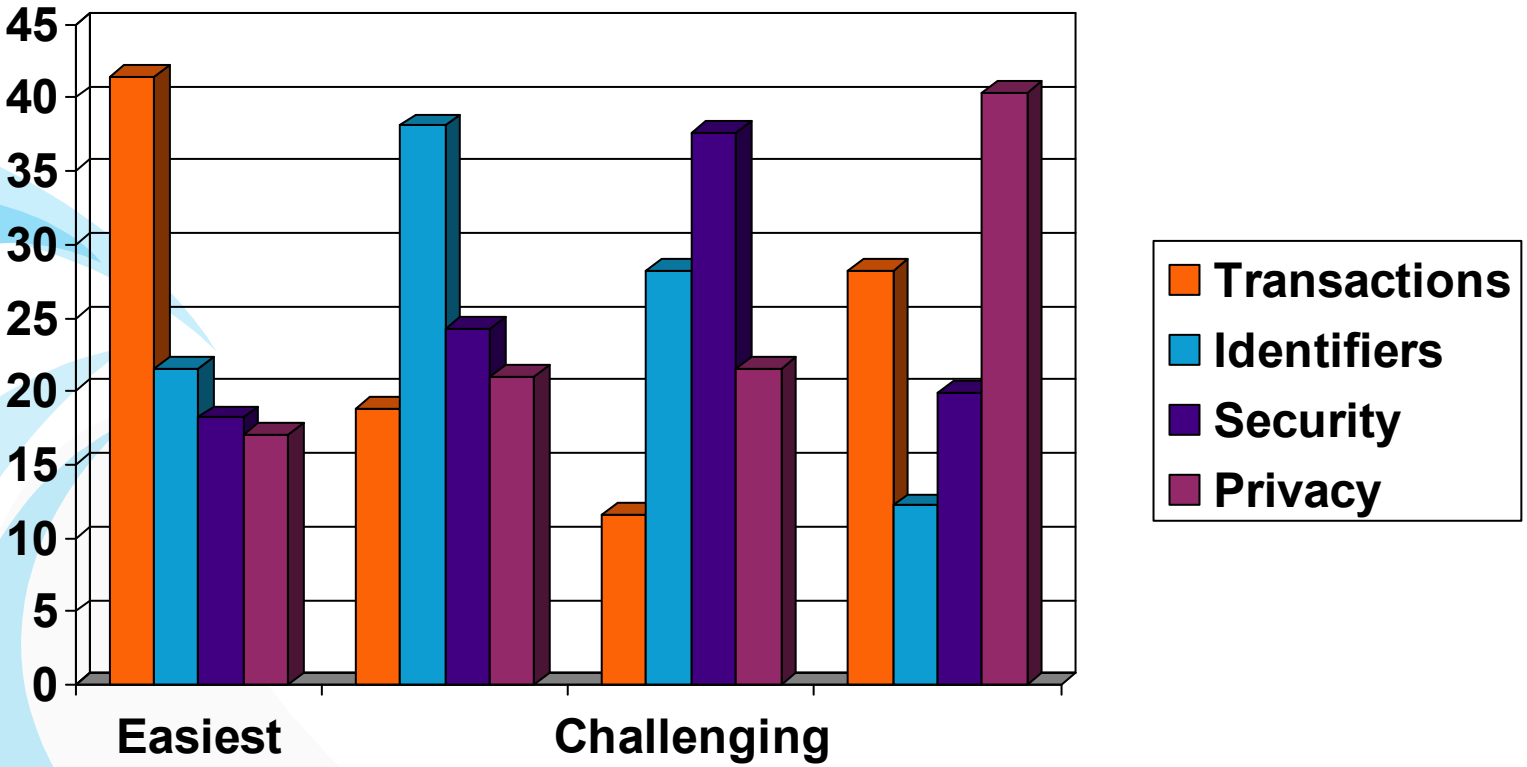
Security Covers ALL

- While most of the HIPAA EDI provisions apply only to electronically transmitted claims and related transactions, the security provisions cover *all* electronic health data
  - Standards cover information transmitted over networks, stored in a database or maintained on PCs
  - Security standards make little distinction between internal or external communications
  - All covered entities that electronically maintain or transmit identifiable health information must comply

Security Facts

- The HIPAA security requirements are very comprehensive and extend far beyond the information technology environment
- Most security requirements impact administrative areas and cannot be solved merely by technology
- To meet HIPAA compliance, many organizations will have to make major system, workflow, policy and procedure modifications

The CIO's View of HIPAA Rules



Source: Faukner and Gray 2000 Survey of Healthcare CIOs

Security Effects

- Because they were designed to be very broad, the effects and implementation issues of HIPAA will vary across the industry from providers to payers
- Implementation issues will vary dramatically in each organization based minimally on:
  - Size and structure
  - Technology foundations
  - Business and trading partner arrangements
  - Role of identified healthcare information

Impact of the Security

- The major impact areas of the security provisions include:
  - Requirement for Security Certification
  - Assessment of risks
  - Implementation of a written Security Plan
  - Implementation of specific personnel, physical and operational security measures
  - Use of access control rules
  - Development and maintenance of audit trails
  - Use of “approved” security technologies

HIPAA Security Requirements

HIPAA's "Cure" for P.A.I.N.

- Administrative Procedures
  - Formal practices to manage security and personnel
- Physical Safeguards
  - Protection of computer systems
- Technical Security Services
  - Control and monitor information access (data-at-rest)
- Technical Security Mechanisms
  - Includes technology to secure data-in-transit

Administrative Procedures

- Largest category of standards
- Relates primarily to policies, procedures and organizational practices dealing with the behavioral side of security
- Will require representatives and input from all areas of the organization

Administrative Procedure Requirements

Certification Requirement

Contingency Planning

Each organization will be required to have a plan of response to system emergencies

[1] These features must be implemented

Implementation

- Internal or external review
- Applications and data criticality analysis [1]
- Data backup plan [1]
- Disaster recovery plan[1]
- Emergency mode operation plan[1]
- Testing and revision[1]

Administrative Procedure Requirements

Information Access Control

[1] These features must be implemented

Formal Mechanism for Processing Records

Routine and non-routine receipt, manipulation, storage, dissemination and.or disposal of health information

Implementation

- Access authorization [1]
- Access establishment [1]
- Access modification [1]
- Documented polices and procedures

Administrative Procedure Requirements

Security Configuration Management

Implementation of measures, practices, and procedures for the security of information systems

[1] These features must be implemented

Implementation

- Documentation [1]
- Hardware/software installation & maintenance review and testing for security features [1]
- Inventory [1]
- Security testing [1]
- Virus checking [1]

Administrative Procedure Requirements

Security Incident Procedures

[1] These features must be implemented

Security Management Process

[1] These features must be implemented

Implementation

- Report procedures [1]
- Response procedures [1]
- Risk analysis [1]
- Risk management [1]
- Sanction policy [1]
- Security policy [1]

Administrative Procedure Requirements

Termination Procedures

[1] These features must be implemented

Chain of Trust Agreement

[2] These features must be implemented

Implementation

- Combination locks changed [1]
- Removal from access lists [1]
- Removal of user account(s) [1]
- Turn in keys, tokens, or cards that allow access [1]
- Training [1]
- Binding legal agreements [2]

Administrative Procedure Requirements

Training

A security training program should be established for all employees and certain third parties with access to health information, e.g. consultants and temps

[1] These features must be implemented

Implementation

- Awareness training for all personnel including management [1]
- Periodic security reminders [1]
- User education concerning virus protection [1]
- User education in importance of monitoring log-in success/failure and reporting discrepancies [1]
- User education in password management [1]

Administrative Procedure Requirements

Internal Audit

Ongoing in-house audit & review of records of system activity

Implementation

- Procedures for review of logins, file accesses, security incidents

Administrative Procedure Requirements

Personnel Security

[1] These features must be implemented

Implementation

- Ensure supervision of maintenance personnel by authorized, knowledgeable personnel [1]
- Maintain access authorizations records [1]
- Ensure that operating and maintenance personnel have proper access [1]
- Employ personnel clearance procedures [1]
- Employ personnel security procedures [1]
- Ensure that system users, including maintenance personnel, are trained in system security [1]

Physical Safeguards

- Protection of computer systems
- Documented policies on the receipt and removal of hardware and software
- Policies and procedures for ensuring authorized physical access
- Policies and procedures for ensuring authorized use and location of work stations
- Security Awareness training for all employees, agents and contractors

Physical Safeguard Requirements

Assigned Security Responsibility

[1] Documented assignment of security responsibility

Media Controls

[2] Documented policies on the receipt and removal of hardware and software. These features must be implemented

Implementation

- Use of Security Measures [1]
- Conduct of personnel in relation to protecting data [1]

- Access control [2]
- Accountability (tracking)[2]
- Data backup [2]
- Data storage [2]
- Disposal [2]

Physical Safeguard Requirements

Physical Access Controls

Policies and procedures for ensuring authorized physical access

All listed features must be implemented

Implementation

- Disaster recovery
- Emergency mode operation
- Equipment control (into and out of site)
- Facility security plan
- Maintenance records
- Need-to-know procedures for personnel access
- Procedures for verifying authorizations prior to physical access
- Sign-in for visitors and escort, if appropriate
- Testing and revision

Physical Safeguard Requirements

Policy/guideline on Work Station Use

Secure Work Station Location

Security Awareness Training

Implementation

- Documented work station instructions and procedures
- Physical safeguards to minimize the possibility of unauthorized access to information
- Training required for all employees, agents and contractors

Technical Security Services

- Relates to the processes that must be put in place to protect, control, and monitor information access
  - Procedures to assess and maintain security programs and identify suspect data access
  - Procedures to control access to information based on user identity or role
  - Procedures to corroborate non-altered data and proper disposal

Technical Security Service Requirements

Access Control

[1] Procedure for emergency access must be implemented

[2] At least one of these features must be implemented

[3] Encryption is optional

Implementation

- Procedure for emergency access [1]
- Context-based access [2]
- Role-based access [2]
- User-based access [2]
- Encryption [3]

Technical Security Service Requirements

Audit Controls

[1] Procedures to assess and maintain security programs and identify suspect data access

Implementation

- Mechanisms to record and examine system activity [1]

Authorization Control

[2] At least one of these features must be implemented

- Role-based access [2]
- User-based access [2]

Technical Security Service Requirements

Data Authentication

Procedures to corroborate non-altered data and proper disposal

[1] Examples may include these features

Entity Authentication

[2] These features must be implemented

[3] At least one of these features must be implemented

Implementation

- check sum, double keying, message authentication code, digital signature [1]
- Automatic logoff [2]
- Unique user identification [2]
- Biometrics [3]
- Password [3]
- PIN [3]
- Telephone callback [3]
- Token [3]

Technical Security Mechanisms

- Technical security requirements to guard Data Integrity, Confidentiality, and Availability
- Relates to the “data-in-transit” processes that are to be implemented in order to prevent unauthorized access to data that is transmitted over a communications network

Technical Security Mechanisms

Requirement

[1] If communications or networking is employed these must be implemented and either [2] access controls or encryption

[3] These features must be implemented if using a network

Implementation

- Integrity controls [1]
- Message authentication [1]
- Access controls [2]
- Encryption [2]
- Alarm [3]
- Audit trail [3]
- Entity authentication [3]
- Event reporting [3]

Digital Signature

Requirement

[1] Optional at this time. If digital signature is employed these must be implemented

[2] These features are optional

Implementation

- Message Integrity [1]
- Non-repudiation [1]
- User Authentication [1]
- Ability to add new attributes [2]
- Continuity of signature capability [2]
- Counter signatures [2]
- Independent Verifiability [2]
- Interoperability [2]
- Multiple signatures [2]
- Transportability [2]

Security Policies and Procedures

Security Policies and Procedures

- Access control
- Records processing
- Security configuration - documentation, testing, inventory, virus control
- Security incident procedures - reporting and response

Security Policies and Procedures

- Security management - prevention, detection, containment, correction of breaches
- Termination procedures - physical and system access of terminated users
- Personnel security - supervision, authorization and clearance, training, record keeping
- Media controls - Receipt and removal of hardware/software and media

Security Policies and Procedures

- Physical access controls - limit access but ensure proper access for disaster recovery and emergency operation, control of equipment, facility security, maintenance records, need-to-know procedures, visitor access, on-going testing and revision
- Workstation use - proper use and log off procedures

Security Policies and Procedures

- Contingency planning - criticality analysis, backup, disaster recovery, emergency mode operation, on-going security verification
- Internal audits of system activity
- Training - for all employees, agents and contractors - awareness training and user education related to security, virus protection, login problems, password management

Meeting HIPAA Security Compliance

Security Recommendations

- Generate awareness
  - Establish a framework for management buy-in
  - Develop an awareness program
  - Establish a security implementation team
  - Establish security training tailored to types of staff
- Determine the magnitude of the compliance effort with a Business Impact Analysis
  - Organizations need to determine scope of BIA, narrow focus on compliance or business opportunity

Security Organization

- Maintain a project governance structure
- Identify key stakeholders
- Identify project manager(s)
- Determine workgroups
- Develop communications plan
- Identify vendor and business associate relationships

Security Awareness and Training

- Identify resources to participate
- Evaluate Security Assessment tools and resources
- Develop training materials
- Conduct educational sessions
- Schedule frequent update sessions

Why Perform an Assessment?

- HIPAA is an enterprise-wide issue that will impact each organization differently
- Establishing budget levels and effectively understanding future capital and resource needs requires a base-line level of analysis
- There is no magic formula to reach these conclusions
- You need to evaluate your unique environment
- An assessment positions you organization to make informed decisions about how you will address HIPAA

Evaluate Compliance Requirements

- Baseline Assessment
  - Inventory of current security with respect to policies, processes and technology
- Gap Analysis
  - Current environment versus regulatory requirements
- Risk Assessment
  - Characterize your business process
  - Value the Asset
  - Determine how current controls mitigate the risk
  - Assess the vulnerability or the threat
  - Assess the probability that the threat will happen

Perform an Assessment and Analysis

- Conduct a Security Tactical Analysis
  - Start with a High-level review
  - Conduct a Business Impact Analysis and Assessment
  - Conduct Security Gap Analysis
- Strategic Assessment
  - Identify business strategy
  - Identify IT strategy
  - Identify business initiatives (i.e., e-Business)
  - Develop HIPAA approach statement
  - Identify benefits and costs of HIPAA approach
  - Obtain executive and board of directors buy-in
  - Develop an internal compliance team

Security Gap Analysis
Overview

- Organizational structure
  - Information Technology across all platforms
  - Security
- Systems environment
  - Platforms
  - Operating systems
  - Security mechanisms
  - Access paths
- Security management and administration
  - Policy and procedures
  - Control processes

Security Assessment & Gap Analysis

Administrative Procedures

	Responsibility	Procedures	Operations	Gap	Risk	Solution
Certification	✍	○	◒	Periodic Security evaluation and certification	high	Currently high-level evaluation, can be external or internal
Chain of Trust	✍	◒	◒	Chain of Trust Partner agreements	mod	Need to be created, Chain of Trust agreements with all business partners mandatory
Contingency Plan	✍	◒	●	Contingency Plan	low	Disaster recovery plan is established and tested
Rcords Processing	✍	◒	◒	Formal mechanism for Processing records	high	Formal documented policy required for processing health information organizationally
Access Control	✍	◒	●	Information Access Control	high	Need formal policy, access control policy must be in place, at least departmentally
Incident Procedures	✍	◒	●	Security Incident Response Procedures	mod	Need formal incident response policies and procedures
Security Process	✍	◒	●	Security Management Process	mod	Policy and implementation not consistent
Termination Procedures	✍	◒	●	Termination Procedures	mod	Notice currently inconsistent, drawn from untimely source
Training	✍	◒	●	Training	high	Development of mandatory security training for all individuals is required

Security Assessment & Gap Analysis

Security Services

	Responsibility	Policies & Procedures	Operations	Gap	Risk	Solution
Security Official	✍	○	○	There is a security official	none	
Access Procedures	✍	○	◒	Access Control: Procedures for emergency access	low	Amend documentation, Covered in departmental policy.
Access Controls	✍	◒	◒	Access/Authorization Control: Either context-based, role-based, or user-based access control	high	Role-based, access control based on being "like" another user; menu access is not consistent or always rational.
Authentication	✍					see Security assessment
Audit	✍	●	◒	Audit Controls	low	Application audit functionality is not sufficient. Audit policy needs to be approved and implemented.
Data	✍	○	○	Data Authentication	low	Role-based access by job function but sensitive data is not properly segmented within application.
Entity		●	●	Entity Authentication	low	Amend P&P to acknowledge duty and assign responsibility. This is not a high exposure or high risk concern.
Device	✍	○	○	Automatic Logoff	low	All user have a 5 min. timeout, except departments with pre-authorization.

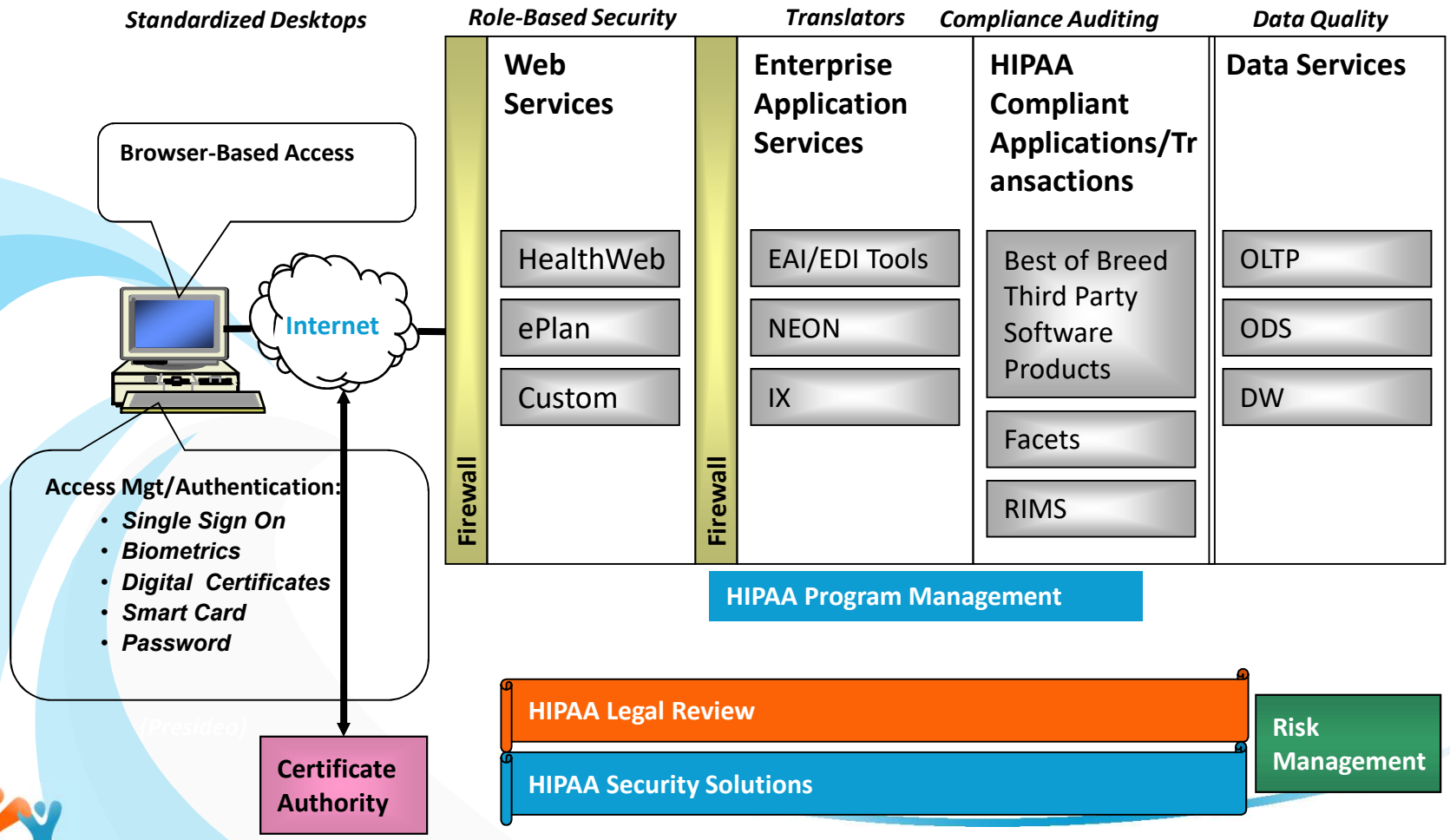
Solution Design and Development

- Analyze solution alternatives
- Develop cost/benefit analysis
- Consider effect on business partners
- Present solutions paths to management
- Select appropriate solution
- Develop implementation plan
- Identify resources for implementation

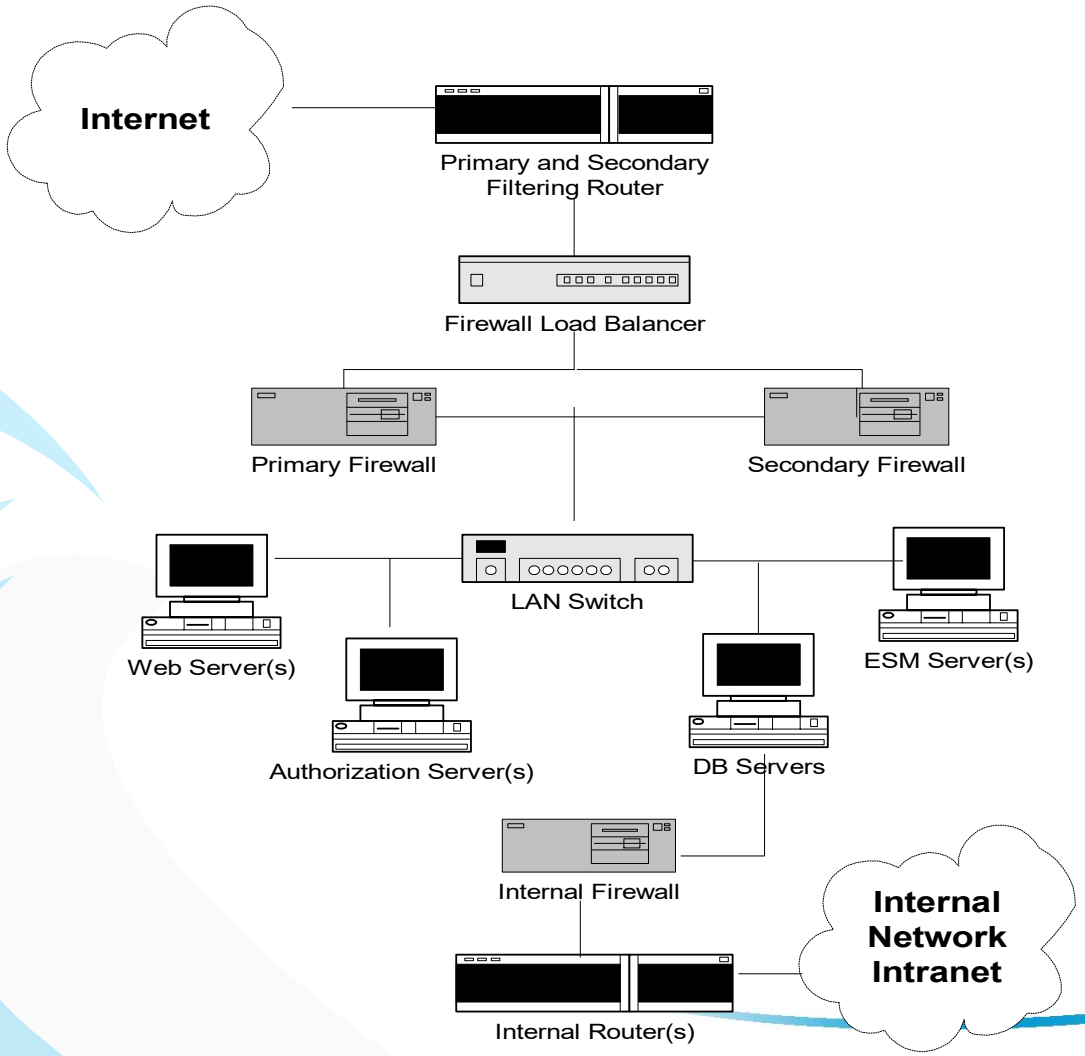
Solution Implementation

- Execute implementation plan
- Monitor status of progress
- Identify project risks
- Develop mitigation strategies
- Test and perform quality assurance
- Train users

HIPAA Architecture Example



Detailed Security Architecture



Security Impacts

- Administrative Changes
  - Certification/testing of computer network security
  - Chain of trust agreements with business partners
  - Data backup procedures and contingency planning

Security Impacts

- Physical Building and Access Changes
  - Facility and workstation security
  - Physical control of storage media use and disposal
  - Visitor/maintenance authorization and escort

Security Impacts

- Personnel Changes
  - Awareness training for all system users
  - Breach reporting and sanctions
  - Assignment of security responsibility

Security Impacts

- Operational Changes
  - User authentication
  - Audit trails and periodic review
  - Incident alarms and reporting
  - Internal audit procedures and controls
  - Change controls

Connecting Healthcare®
Engaging Patients™
Communicate Educate Motivate™

Have Questions?

Visit our Website,
send us an email,
or give us a call!

(904) 435-3456
(904) 435-3457
Questions@
ConnectingHealthcare.com