



**Connecting
Healthcare**[®]
Engaging Patients[™]

HIPAASuccess - Physician Education Series

A HIPAA Approach - Getting Started

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)



The HIPAA Success Approach

HIPAA Compliance

- *HIPAA Compliance Methodology*
- *Comprehensive web-based software platform*
- *Framework for HIPAA assessment, remediation and ongoing management*
- *Consistent monitoring and measurement of HIPAA initiatives*
- *Enterprise-wide HIPAA project Tool ensures HIPAA initiatives are completed on time and under budget with supporting audit trails*

Legal Partners

- *Expertise In*
 - Healthcare Law*
 - Privacy Law*
 - Technology Law*
- *Legal Review and Oversight*

Technology Partners

- *Leading Technology Solutions*
- *Digital Certificate and Security Services*
- *Infrastructure and Networks*
- *Application Solutions for Remediation*

Training Services



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
- No magic formula to reach these conclusions, you need to evaluate your unique environment
- An assessment positions your organization to make informed decisions about how you will address HIPAA



Strategic Assessment

- The Strategic Assessment component is focused to identify and evaluate the impacts of HIPAA
 - Organization's strategic direction
 - Applicable business strategies
 - Applicable technology foundations
 - Business Partnership and Associate Relationships
 - Organization's resources



Strategic Assessment

- Techniques utilized in the assessment process:
 - Review of all corporate vision, and strategy documents
 - Review of business plans, marketing and E-Business strategies
 - Evaluation of technology strategies and organizational structure
 - Interview key stakeholders in your organization
 - Evaluate external and industry trends
 - Consider opportunities to leverage changes related to HIPAA compliance to improve competitive positioning



Strategic Assessment

- Outcomes from the strategic assessment:
 - Identification of high level industry trends that may impact future direction
 - Integration of potential HIPAA solutions into other strategic and business unit initiatives to maximize efficiency
 - Identification of complimentary opportunities
 - Integration of strategic trends with tactical discovery and assessment process

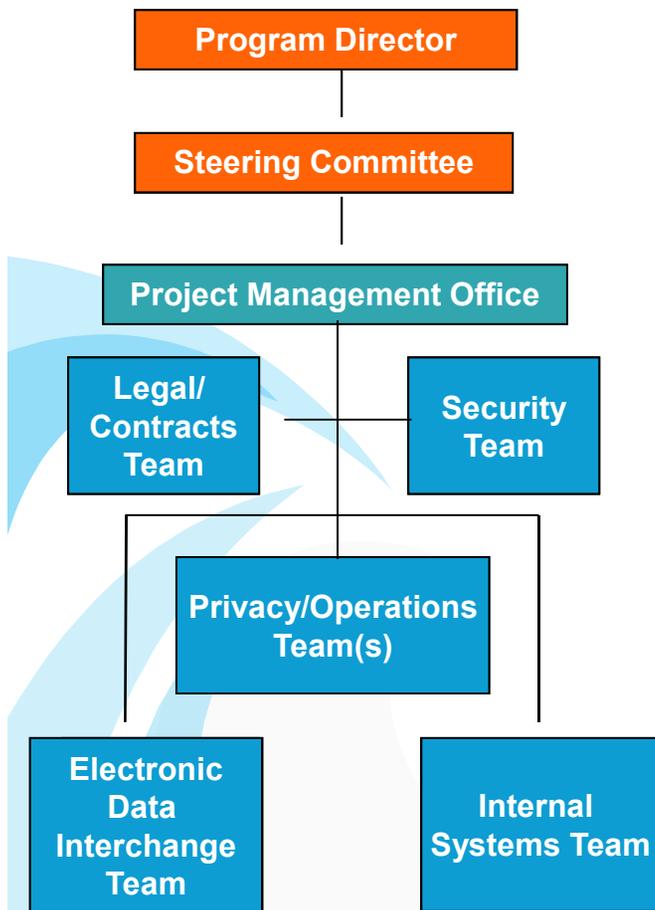


Tactical Gap Analysis

- Technology Analysis
- Privacy Analysis
- Security Analysis



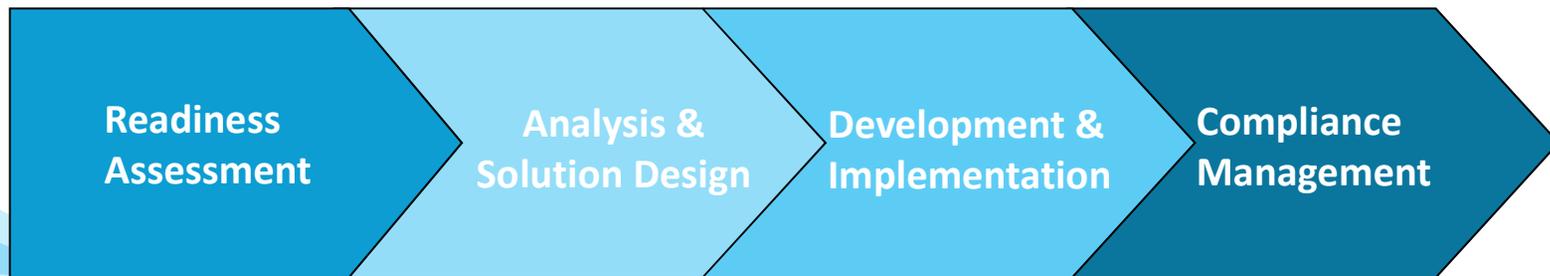
Project Management Structure



- Project Teams should be established to evaluate the specific aspects of HIPAA
- Project Teams must reflect the functional requirements of the regulations
- Staffed from business operations
- Execute assessment and operationalize solutions
- Report to Project Management Office



HIPAA Methodology

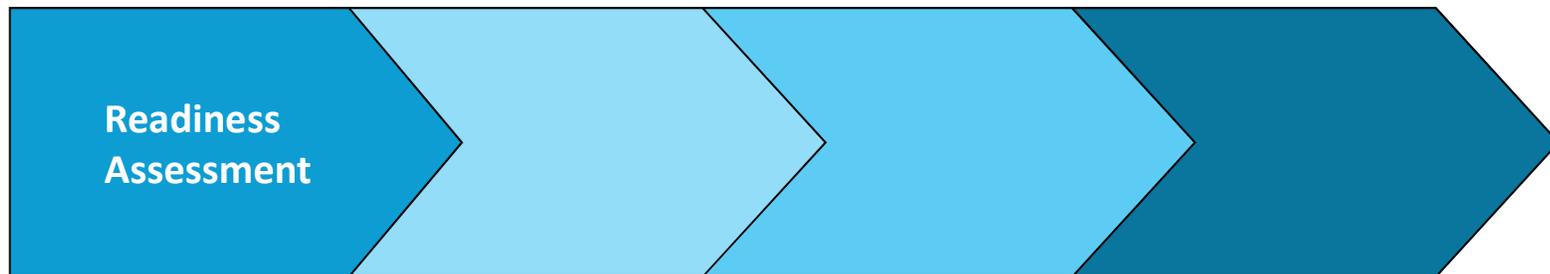


HIPAA Readiness Assessment

- Project Estimation
- Project Organization
- Project Initiation
- Organization Analysis
- Transactions and Code Sets
- National Identifiers
- Privacy and Security
- Reporting, Findings & Recommendations



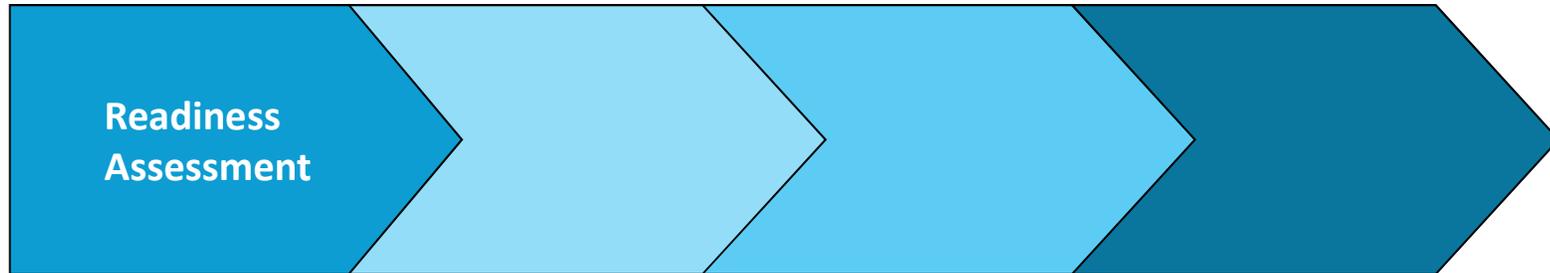
HIPAA Approach - Phase 1



- Conduct Senior Management Workshop and Staff Awareness Training
- Establish HIPAA Program Steering Committee
- Identify Executive Sponsor & Program Director(s)
- Develop Stakeholder Map
- Develop Risk Assessment



HIPAA Approach - Phase 1



- Complete Checklists/Assessments (includes information flow, technical & physical security, access controls, transaction formats, network infrastructure, legal, operations)
- Present Findings, Recommendations & Proposed Action Plans
- Determine HIPAA Compliance Strategies and Next Steps



Readiness Assessment Reports

- HIPAA Impacted Entities
- HIPAA Impacted Systems
- Systems Requiring HIPAA Privacy and Security Compliance Remediation
 - Detailed Security Report
 - HIPAA Impacted Transactions
 - HIPAA Trading Partner Impact Report
 - Business Processes Impacted by HIPAA
 - Many Others



Findings and HIPAA Strategies

- Complete Risk Assessment
- Prepare / Prioritize Overall Findings
- Prepare Detailed Findings & Recommendations Report
- Communicate Findings to Management
- Proposed HIPAA Compliance Strategies
- Next Steps to HIPAA Compliance

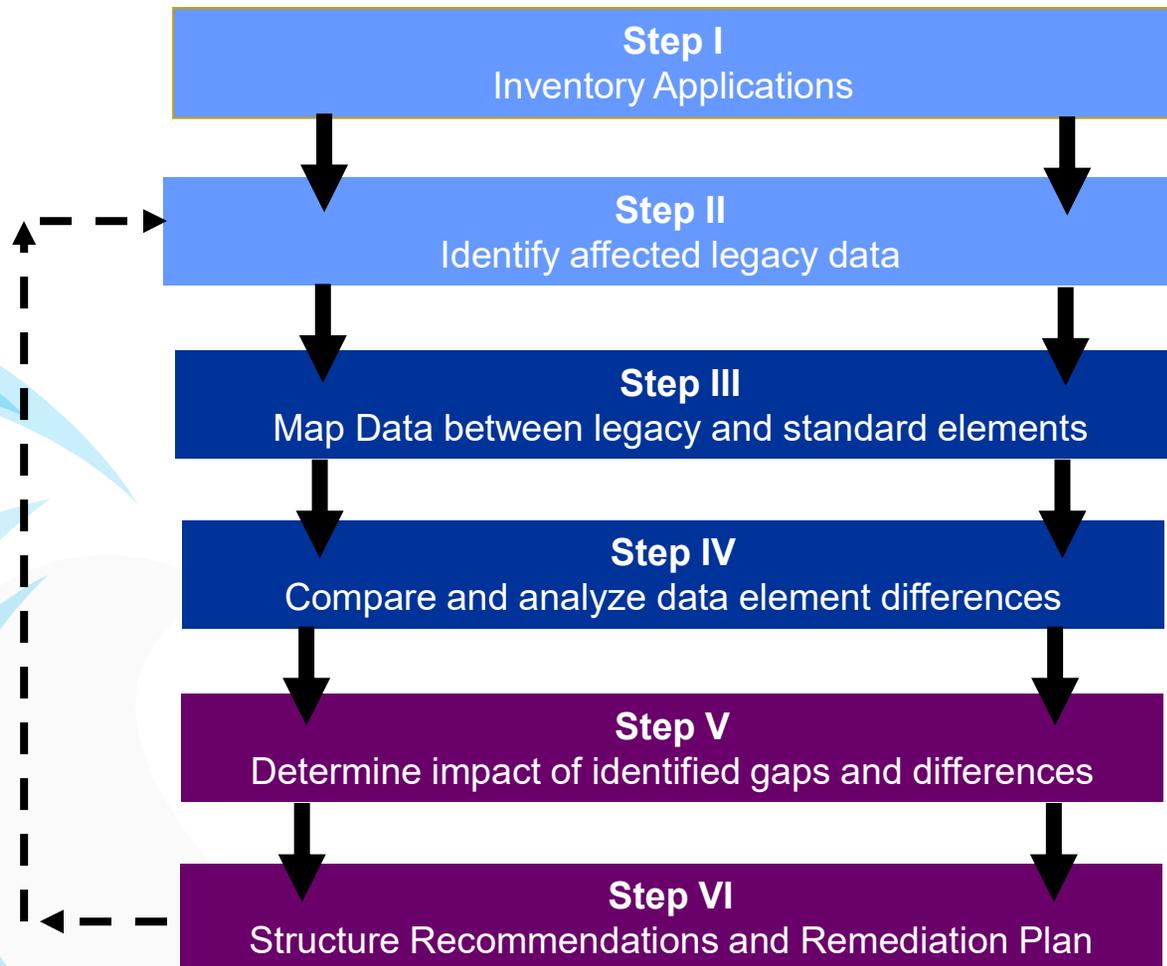


Technology Gap Analysis Overview

- EDI capabilities
- Translation engine
- Application interfaces
- Impact of new data elements on applications and databases
 - Identifiers
 - Code sets
- Trading partners
 - Contracts
 - Readiness
 - Capabilities



EDI Assessment and Gap Analysis



Technology Assessments

Baseline Assessment	Compliance Assessment	Code Sets Assessment	Transaction Assessment
<ul style="list-style-type: none"> • Determine existing technology, data and data exchange foundations • Interview key business and technology staff • Identify key processes and systems • Assess and refine existing documentation • Current EDI Data Exchange mappings or dataflows • Data Models • System or processing diagrams • Trading Partner Data Requirements 	<ul style="list-style-type: none"> • Complete code/set and standard data set toolset • Determine what current EDI transactions are ANSI Standard • Determine what non-standard code sets are used • Determine use of standard national identifiers • Determine transaction security issues • How does transaction and code set data flow through legacy or outsourced application programs and databases 	<ul style="list-style-type: none"> • Determine which non-compliant codes are defined by a standard code • Determine frequency of use of non-compliant codes • Define codes used for: <ul style="list-style-type: none"> • Administration • Adjudication • Procedure • Diagnosis • Unique Identifier • Utilization impact of Identifiers • Compare current use and proposed use 	<ul style="list-style-type: none"> • Determine current EDI transactions • Determine transaction data element definitions • Map and match current EDI to transactions • Map the data elements • Map the code set data elements • Map the Identifier data elements • Identify internally processed versus outsourced • How are non-compliant transactions processed



Transactions Gap Analysis

HIPAA Standard	Used	HIPAA Compliant	Compliance Effort
Claim Institutional X12N837-I	Yes	No	Medium
Claim Professional X12N837-P	Yes	No	Medium
Claim Dental X12N837-D	Outsourced	Outsourced	N/A
Claims Pharmacy NCPDP	Outsourced	Outsourced	N/A
Claims Status/Inquiry X12N276/277	No	No	High
Claims Payment Advice X12N835	Yes	No	Medium
Referral/Pre-certification X12N278	No	No	High
Benefit Enroll/Maint. X12N834	Yes	No	Medium
Eligibility Inquiry/response X12N270/271	No	No	Medium
Premium Remittance Advice X12N820	No	No	Low



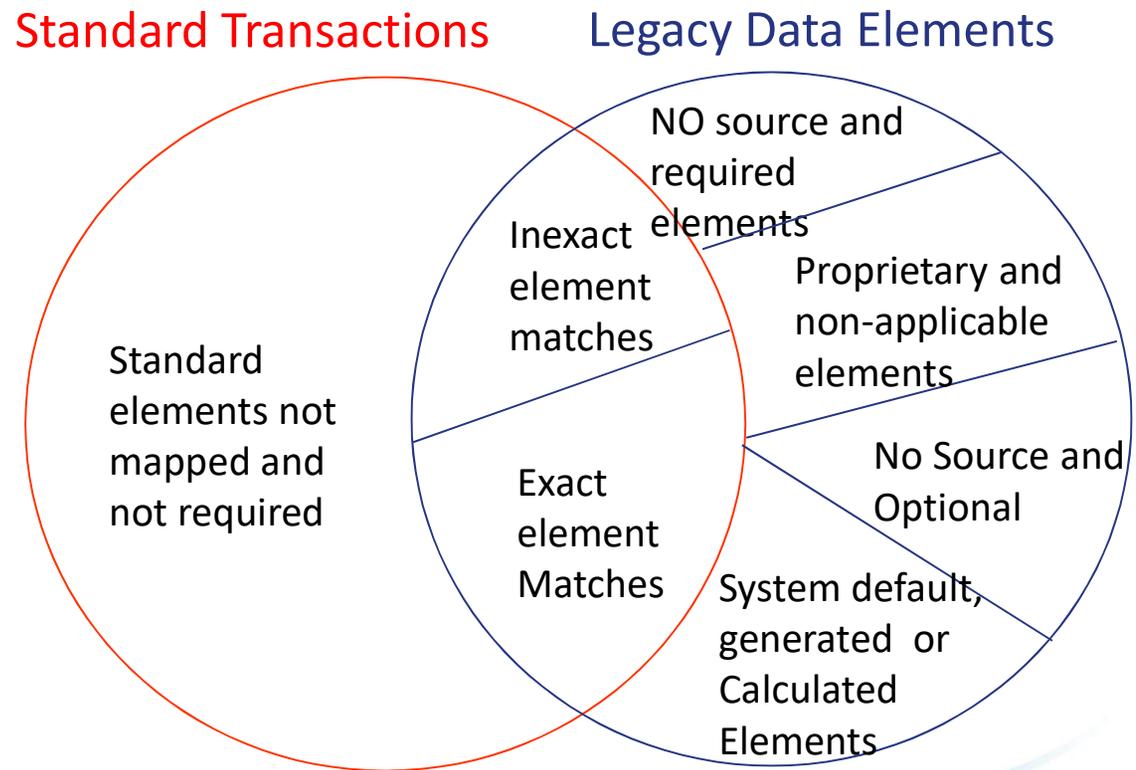
Code Sets and Identifiers Gap Assessment

HIPAA Standard	Used	HIPAA	Compliance Effort
		Compliant	
Provider IDN	No	No	Medium
Employer IDN	Yes	Yes	Low
Patient IDN	No	No	High
Health Plan IDN	No	No	Low
ICD-9-CM	Yes	Yes	Low
CPT-4	Yes	Yes	Low
HCPCS	Yes	No	Medium
CDT-2	No	No	Medium
NDC	Yes	Yes	Low
Supporting Code Sets	Yes	No	High



Data Element Gap Assessment

- The mapping of inbound and outbound transactions will produce an intersection of standard and legacy data elements



Data Element Translation Assessment

Translation Assessment	Definition
Copy	The source element can be copied to the target element with no transformation
Simple Transaction	The source element can be translated to the target element with simple transformations such as numeric to alphanumeric or other data typing
Lookup Translation	The source element can be translated to the target element with the use of a static table lookup
Truncation	The source element is longer than the target element and can be truncated without creating attribute integrity issues
Interpret Qualifiers	Interpretation of a standard qualifier element is necessary to define, locate, and or format another standard element which is the source for a target element
Complex Translation	The source element can be translated to the target element through the use of multiple source or target elements, the use of a dynamic lookup table, or program logic
Calculation	The source element can be translated to the target element through the use of a calculation or other program logic or method
Attribute Type	The source element can not be translated to the target element because of data type or length which is generally a significant issue
Non-transformable	It is not possible to translate the source element into the target element which is generally a significant issue



Inbound Transaction Gap Analysis

HCO Support Applications	Standard Elements not Used by HCO	Exact Element Matches	Inexact element matches	System generated calculated or default elements	Unsourced optional elements	Unsourced required elements
HCO Admin & Supply	N/A	N/A	N/A	N/A	N/A	N/A
Admissions and Discharge	144	121	33	21	11	0
Utilization Management	N/A	N/A	N/A	N/A	N/A	N/A
Capitation	298	127	80	34	13	1
Care/Clinical Management						
Benefit Plan Administration	100	57	20	19	0	0
Plan Membership Administration	88	100	44	43	0	0
Eligibility	120	100	44	43	0	0
Customer Service						
Claims & Billing	298	127	80	34	13	1



Outbound Transaction Gap Analysis

HCO Support Applications	Not Applicable	Exact Element Matches	Inexact Element Matches	Calculated required standard elements	Optional standard elements	Other Required Elements
HCO Admin & Supply	N/A	N/A	N/A	N/A	N/A	N/A
Admissions and Discharge	144	121	33	21	11	0
Utilization Management	N/A	N/A	N/A	N/A	N/A	N/A
Capitation	298	127	80	34	13	1
Care/Clinical Management						
Benefit Plan Administration	100	57	20	19	0	0
Plan Membership Administration	88	101	44	43	0	0
Eligibility	89	101	44	43	0	0
Customer Service						
Claims & Billing	521	127	80	34	13	1



Privacy Gap Analysis Overview

- Organizational structure
 - corporate activities
 - business unit activities
- Existing HIPAA data use, storage, and disclosure
- Existing policy and procedure documentation
 - corporate
 - business unit
- Business partner contracting



Privacy Assessment & Gap Analysis

General Provisions

	✓	○	○	Responsibility Procedures Operations	Gap	Risk	Solution
Privacy Official	✓	○	○		There is a privacy official	none	
Document retention	✓	○	○		The privacy official is responsible for maintaining documentation	low	
Training and Certification	✓	⊖	⊖		Training is inadequate, and there is no formal certification program	high	New employee orientation training program, and current employee continuing education must be modified to include Privacy. Security training/education should be incorporated into compliance training program.
Sanctions	✓	○	○		P&P define sanctions. HR administers	low	
Complaint management	✓	●	⊖		Although operationally complaints are handled by the Privacy official, this is not documented in the policies and procedures	low	Current operations should be memorialized in policy
Duty to mitigate		●	●		Although there is nothing in place regarding mitigation, this will normally be handled ad hoc.	low	Amend P&P to acknowledge duty and assign responsibility. This is not a high exposure or high risk concern.
Notification of Privacy Practices	✓						
Content of notice		○	⊖		Notice is in compliance, except for contact phone # (see above)	low	Amend notice
Delivery of Notice		○	⊖		Policies and procedures c/w 164.512, but in practice notification is spotty	high	Privacy official needs to monitor notification



Privacy Assessment & Gap Analysis

Patient Rights

	Responsibility	Procedures	Operations	Gap	Risk	Solution
Access (view/copy)	☞	○	●	Patients are provided access to billing records, EOB's etc. Policies and procedures need updating to reflect this	low	Revise P&Ps
Request correction/amendment	☞	●	●	Pt accounting has a formal mechanism for investigation pt complaint. Need to add allowance for attaching explanation when request denied	low	Create mechanism for attaching explanation when request denied
Request restriction on use	☞	●	●	There is no mechanism by which a patient can request restriction on use	low	Create a general policy precluding special restrictions, with head of Pt accounting reviewing each request for special circumstances
Authorization management	☞	●	●	Currently, only a signature by pt is required for release of paper record.	high	Develop photo-ID authentication for paper record access, trusted 3rd party authentication (PKI?) for electronic access
Authorization Control	☞	●	●	Documentation is mailed to address of record.	low	Require signature for release of information



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
Contingency Plan	☒	◐	●	Contingency Plan	low	Disaster recovery plan is established and tested
Records 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
Internal Audit	☒	◐	●	Internal Audit	mod	Internal audit policy must be restarted after Mainframe Security package implementation
Personnel Security	☒	◐	●	Personnel Security, clearance procedures, etc.	high	Documented clearance policy needed
Config. Management	☒	◐	●	Security Configuration Management	mod	Based on change management policy, need separate policy for security configuration management
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



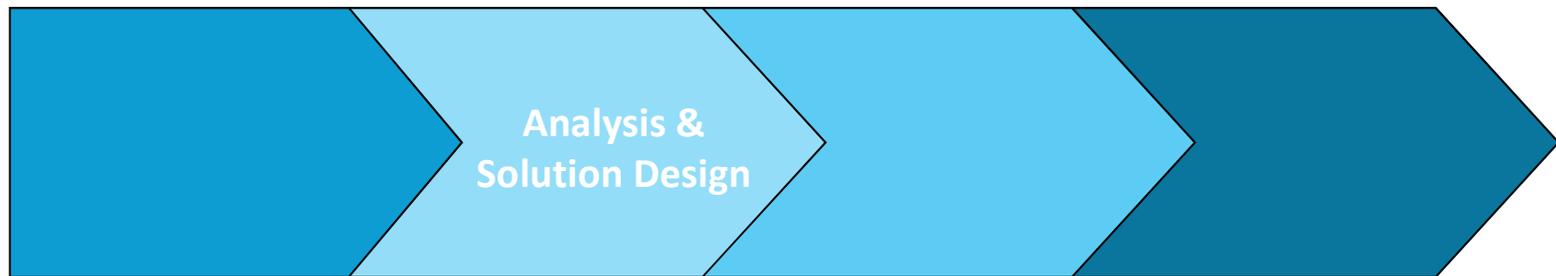
Security Assessment & Gap Analysis

Security Services

	Responsibility	Policies & Proc	Operations	Gap	Risk	Solution
Security Official	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	There is a security official	none	
Access Procedures	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Access Control: Procedures for emergency access	low	Amend documentation, Covered in departmental policy.
Access Controls	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	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	<input type="checkbox"/>					see Security assessment
Audit	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Audit Controls	low	Application audit functionality is not sufficient. Audit policy needs to be approved and implemented.
Data	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Data Authentication	low	Role-based access by job function but sensitive data is not properly segmented within application.
Entity		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Entity Authentication	low	Amend P&P to acknowledge duty and assign responsibility. This is not a high exposure or high risk concern.
Device	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Automatic Logoff	low	All user have a 5 min. timeout, except departments with pre-authorization.



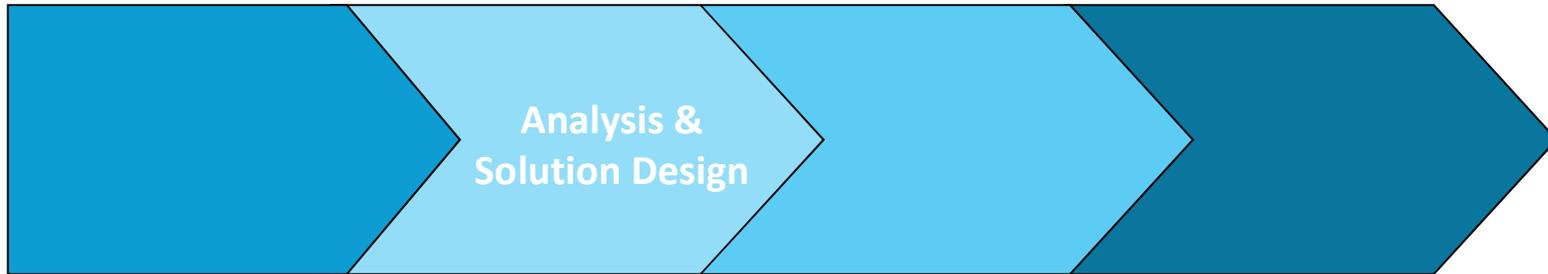
HIPAA Approach - Phase 2



- Analyze systems, business operations, and information process flows
- Develop detailed Project Plans to accomplish compliance in deficient areas
- Develop Technical Infrastructure and Security Design
- Develop Detail Designs for Applications, Interfaces and Conversions



HIPAA Approach - Phase 2



- Initiate Development of Policies and Procedures
- Develop Implementation Plan and Staff Training Plan
- Revise Business Process Flows
- Develop Vendor & Product Alliance Plan
- Conduct Legal Review



Implementation Alternatives

	Remediate	Replace	Outsource
Advantages	<ul style="list-style-type: none"> • Lesser cost • Lower Risk of disruption of core systems • Postpones replacement evaluation of legacy system • Allows selective replacement of legacy data elements with standard data elements 	<ul style="list-style-type: none"> • Enables improvements and eBusiness strategy • Eliminates proprietary data elements and values for compliant standards • Does not require ongoing maintenance of proprietary to standard data elements 	<ul style="list-style-type: none"> • Potentially the least cost option • Lowest Risk of disruption of core systems • Postpones replacement evaluation of legacy system • Fastest time to compliance implementation
Disadvantages	<ul style="list-style-type: none"> • Does not improve usability or adaptability of legacy systems • Will require ongoing maintenance of proprietary to standard data elements • More complicated infrastructure to enable real-time transactions • May complicate communications and error inquiries 	<ul style="list-style-type: none"> • Greatest Cost option • Highest risk of disruption and down-time for core legacy processes • Still may require interim non-standard to standard translation • May not be able to implement in time for compliance timeframes • Relies heavily on the vendor for compliance targets 	<ul style="list-style-type: none"> • Does not improve usability or adaptability of legacy systems • Will require ongoing maintenance of proprietary to outsourced structures • More complicated infrastructure to enable real-time transactions • May complicate communications, error inquiries and data exchanges • Limited options other than claims and remittances

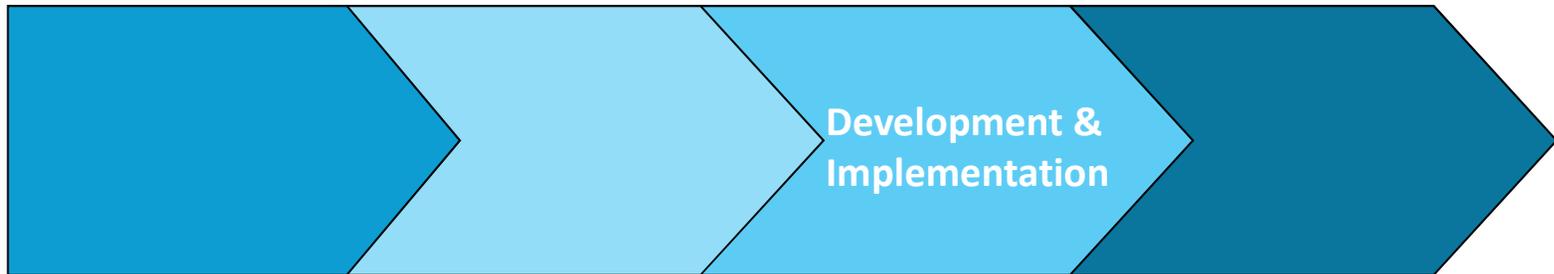


Solution can be Combinations

HIPAA Standard	Modify Existing Applications	Replace or New Application	Outsource Application	Compliance Effort
Claim Institutional X12N837-I	X		X	Medium
Claim Professional X12N837-P	X		X	Medium
Claim Dental X12N837-D	X	X		Medium
Claims Pharmacy NCPDP	X		X	Low
Claims Status/Inquiry X12N276/277		X		High
Claims Payment Advice X12N835	X	X	X	Medium
Referral/Pre-certification X12N278		X		High
Benefit Enroll/Maint. X12N834	X			Medium
Eligibility Inquiry/response X12N270/271		X		Medium
Premium Remittance Advice X12N820	X	X		Low



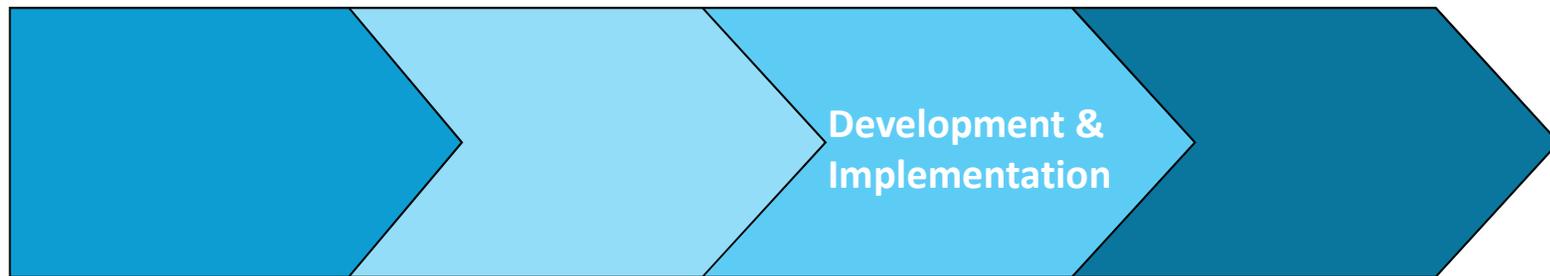
HIPAA Approach - Phase 3



- Finalize Vendor & Product Alliances
- Develop & Test System Modifications, Interfaces and Conversions
- Implement Technical Infrastructure & Security Design
- Execute Implementation Plans
- Conduct Staff Training



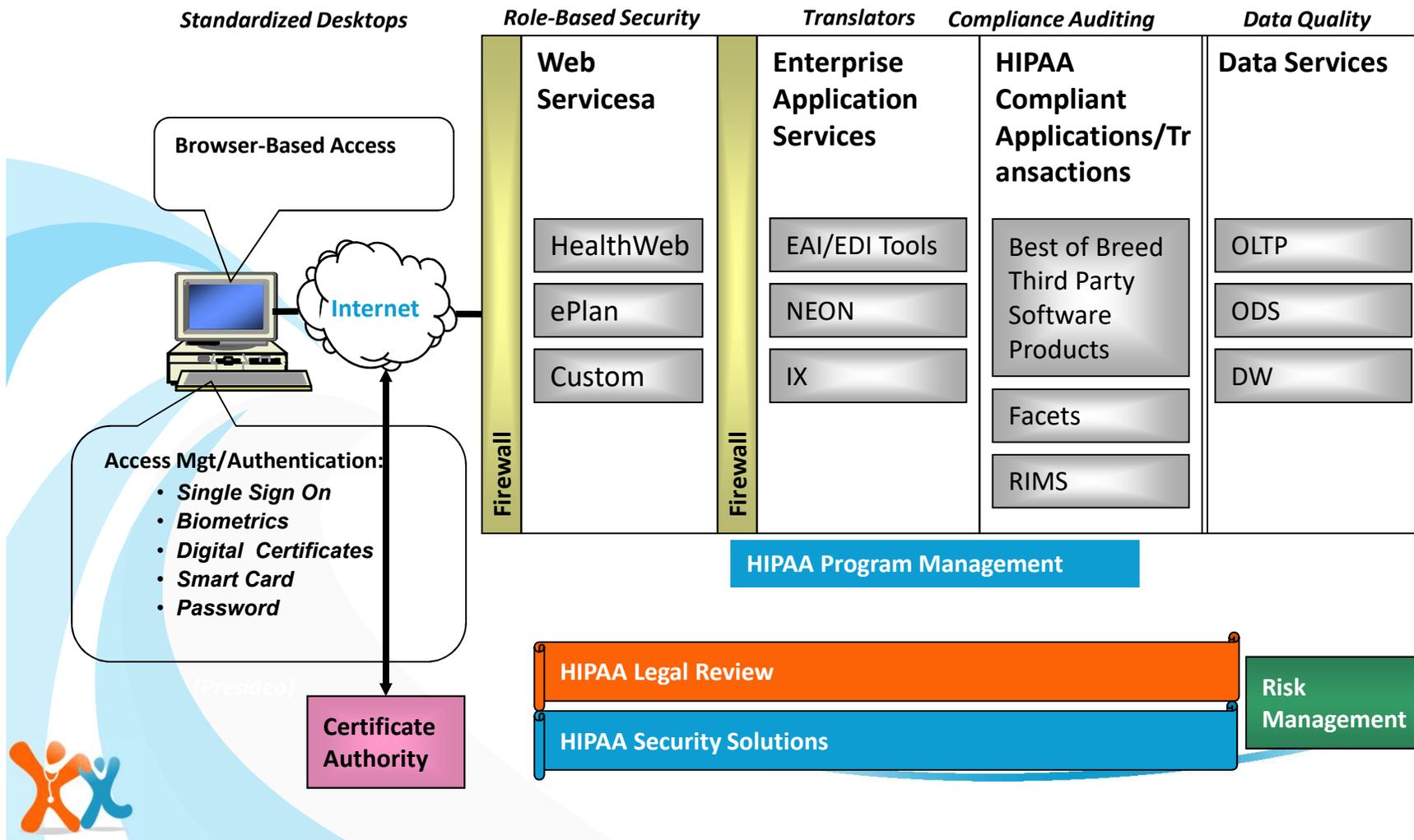
HIPAA Approach - Phase 3



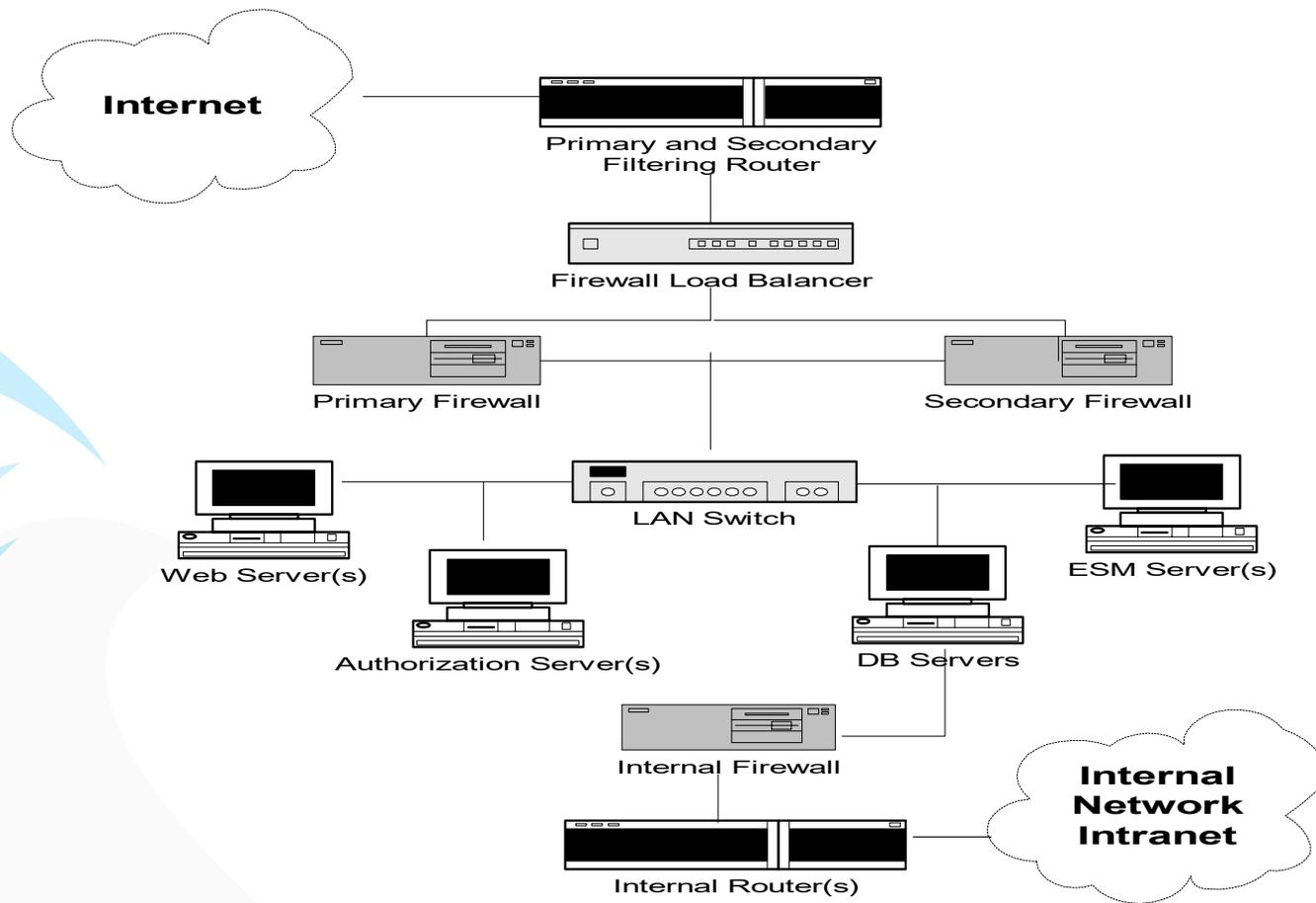
- Transition to Production Systems
- Implement Revised Business Process Flows
- Implement Policies and Procedures
- Conduct Post-Implementation Review (Technical, Operational, Legal)



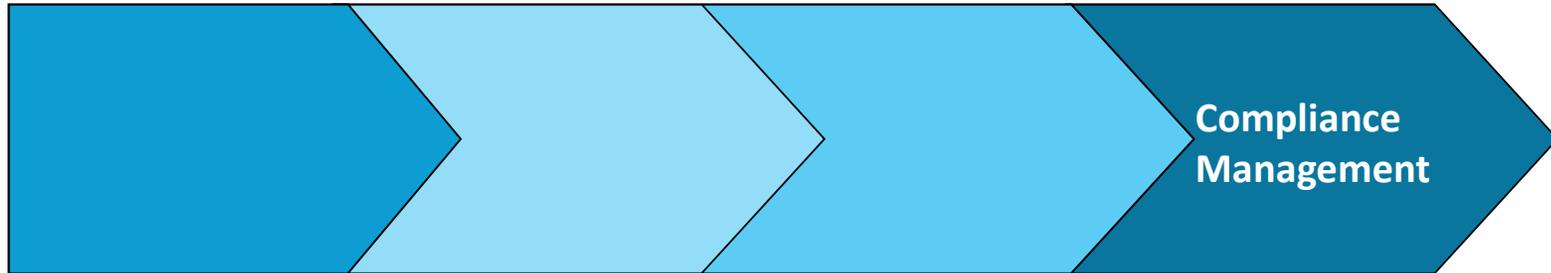
HIPAA Architecture Example



Detailed Security Architecture



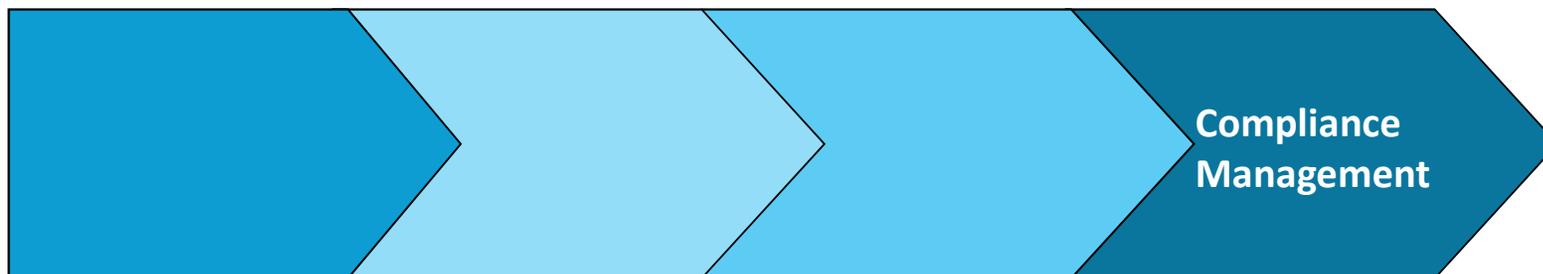
HIPAA Approach - Phase 4



- Confirm Program Charter and Objectives for Compliance Management
- Define and Implement Organization Model Required for Compliance Management
- Establish Compliance Program Management Office (PMO) & Integrate with Existing Compliance Programs



HIPAA Approach - Phase 4



- Initiate Compliance Monitoring, Management, and Audit Plan
 - Operations
 - Technical
 - Legal



HIPAA Success

- Enterprise-wide planning
- Establish clear governance structure to manage complexities and interdependencies among business units requirements of HIPAA
 - Technology
 - Security
 - Privacy



HIPAA Success

- Secure management support and awareness
- Leverage historic and on-going initiatives and accumulated knowledge
 - E-Business
 - Business Transformation, etc..



HIPAA Success

- Align HIPAA initiatives with corporate strategies and integrate into operations
- Ensure on-going communication channels for HIPAA specific initiatives
- Build HIPAA into existing change initiatives
- Raise corporate awareness of HIPAA and its potential impacts on the origination and its stakeholders
- Incorporate HIPAA into existing compliance program





Have Questions?

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

(904) 435-3456 

(904) 435-3457 

Questions@ 

ConnectingHealthcare.com 

