HIPAA Compliance for the Government Sector—What's changed—What you need to know

Jeff Grady, HCISPP

Senior Director

Three Pillars Security & Compliance
Security and Compliance Solutions Advisor
2701 International Lane Suite 201
Madison, WI 53704
608.807.5256
www.threepillarstechnology.com

Introduction

- Presenter background and information on Three Pillars Technology
- Goals for this presentation
- Audience Survey

What has changed with HIPAA and why is it important? **Some background and history**:

HIPAA (Health Insurance Portability and Accountability Act) a brief history and overview of it's evolution

- **HIPAA was enacted by Congress in 1996**
- **Privacy Rule** - The effective compliance date of the Privacy Rule was **April 14, 2003.**
- **Security Rule** - The effective date for most entities was **April 20, 2005**
- HIPAA Enforcement Rule – 2006
- HIPAA/HITECH enacted in 2009
- **HIPAA/HITECH Final Omnibus Rule** published in 1/2013 **with a compliance deadline**, for most of its provisions, of **September 23, 2013**

The Wizard of (Oz)HIPAA

Why Does HIPAA Compliance Intimidate So Many?

The ‘Problem’ with HIPAA

- It was ahead of it’s time – in advance of the wide spread adoption of Electronic Health Records
- Got off on the ‘wrong foot’ – the Privacy Rule foot
- Far too much of the initial HIPAA compliance process and methodology was built for large enterprise size organizations
- Initial ‘experts’ and practitioners were more comfortable with meeting compliance and the development of ‘Policy & Procedure’ documentation - than they were with technology and data security practice
- A HIPAA compliance ‘industry’ has evolved in such a way that too often the approach to HIPAA compliance adopts an audit like mentality

Let’s Get Real About HIPAA

Once you ‘pull back the curtain’ and get to really understand HIPAA, and what’s required for compliance – it’s not so overwhelming and intimidating

Major Changes Due to the HIPAA/HITECH Rules and Regulations

- **Expanded Definition of Business Associate**
- **Application of HIPAA to Business Associates**
- **New Requirements for Business Associate Agreements**
- **New Requirements for Notice of Privacy Practices**
- Fundraising
- Expanded Patient Rights
- Increased Flexibility with PHI of Deceased Patients
- **Breach Notification Threshold Standard Lowered**
- **Civil Monetary Penalties – "Willful Neglect"**

Consider the Potential Risks and Impact of Non-compliance

- **Risk of OCR Audit and Fines and Potential of Breach**
  - **OCR just announced details on the next wave of audits**
- **"Willful Neglect" to support a HIPAA Finding Does Not Require Wrongful or Bad Intent**
- **Costs of a PHI breach**
- **Loss of Goodwill and Reputation as a result of breach**
- **Protection of sensitive data has become an expectation of both your citizens and regional government partners**
- **Career Impact if it happens under your 'watch'**
- **Then there's the 'ticking time bomb' of HIPAA compliance**

III
THREE PILLARS TECHNOLOGY
SOLUTIONS THAT WORK

THE TICKING TIME BOMB OF HIPAA ENFORCEMENT

RIN Data HHS/OCR **RIN: 0945-AA04** Publication ID: Spring 2013

Title: HIPAA Enforcement: Distribution of a Percentage of Civil Money Penalties or Monetary Settlements to Harmed Individuals

Abstract: **This advance notice of proposed rulemaking would begin to establish a methodology under which an individual who is harmed by an offense punishable under HIPAA may receive a percentage of any civil money penalty or monetary settlement collected with respect to the offense,** as required by section 13410(c)(3) of the Health Information Technology for Economic and Clinical Health Act (title XIII of the American Recovery and Reinvestment Act of 2009). The Department plans to publish an advance notice of proposed rulemaking to solicit the public's views on establishing such a methodology.
Agency: Department of Health and Human Services(HHS) Priority: Other Significant
RIN Status: Previously published in the Unified Agenda Agenda Stage of Rulemaking: Prerule Stage
Major: Undetermined Unfunded Mandates: No
CFR Citation: 45 CFR 160
Legal Authority: Not Yet Determined
Legal Deadline: Action Source Description Date
Final Statutory Deadline for issuance of regulations under HITECH 02/00/2012

Timetable: Action Date FR Cite ANPRM 12/00/2013

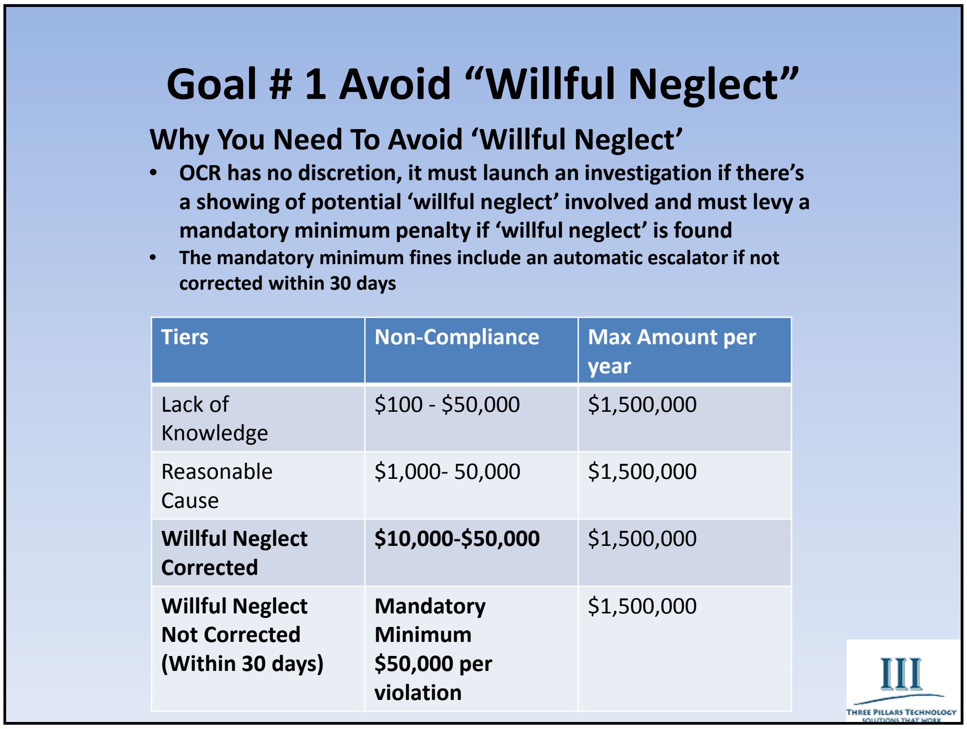
Regulatory Flexibility Analysis Required: No Government Levels Affected: None
Small Entities Affected: No Federalism: No
Included in the Regulatory Plan: No
RIN Data Printed in the FR: No
Agency Contact: Andra Wicks
Privacy Specialist, Office of Civil Rights
Department of Health and Human Services
200 Independence Avenue SW.,
Washington, DC 20201

Some Sample HIPAA Fines

- **$1.7 Million** to **State of Alaska** Department of Health and Human Services for Unencrypted USB Drive Stolen
- **$1.7** Million to WellPoint for not properly authorizing access to an on-line application database
- **$1.5 million** fine to Massachusetts Eye and Ear Infirmary for a data compromise involving a lost laptop
- **$4.8 Million** dollar settlement fine imposed upon **New York-Presbyterian Hospital** and **Columbia University Medical Center** for a HIPAA breach impacting 6,800 individuals

- **$215,000** monetary settlement payment paid by **Skagit County, Washington,** **to settle potential violations of the privacy and security rules and agreed to comply with a three-year HIPAA compliance program under Department of Health and Human Services (HHS) jurisdiction**
- **$400,000** fine to **Idaho State University** for failing to maintain strong firewall configuration
- **$150,000** fine to a **twelve (12) doctor Massachusetts dermatology practice** triggered by a lost thumb drive and failure to have conducted a security risk assessment along with a corrective action plan
- **$50,000 penalty assessed** to a **non-profit hospice in Idaho** for lost unencrypted laptop
- **$150,000 penalty** imposed upon a **five-facility mental health organization in Alaska** **for its failure to patch their systems and continued to run outdated, unsupported software that eventually led to a malware data breach affecting 2,743 individuals.**

III
THREE PILLARS TECHNOLOGY
SOLUTIONS THAT WORK

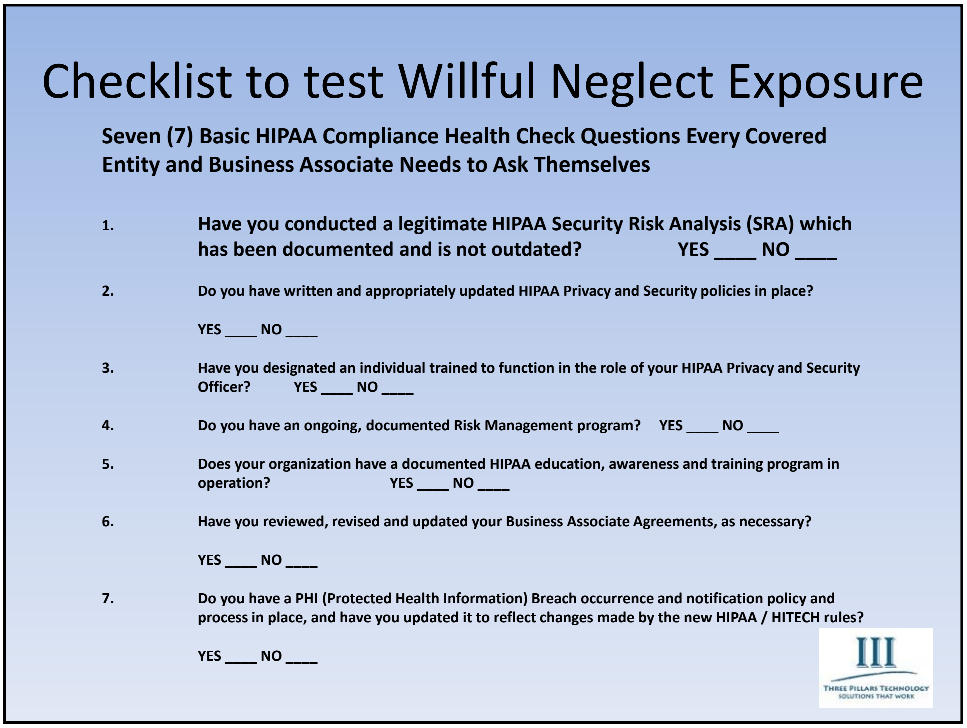


Goal # 1 Avoid “Willful Neglect”

Why You Need To Avoid ‘Willful Neglect’

- OCR has no discretion, it must launch an investigation if there’s a showing of potential ‘willful neglect’ involved and must levy a mandatory minimum penalty if ‘willful neglect’ is found
- The mandatory minimum fines include an automatic escalator if not corrected within 30 days

Tiers	Non-Compliance	Max Amount per year
Lack of Knowledge	$100 - $50,000	$1,500,000
Reasonable Cause	$1,000- 50,000	$1,500,000
Willful Neglect Corrected	**$10,000-$50,000**	$1,500,000
Willful Neglect Not Corrected (Within 30 days)	**Mandatory Minimum $50,000 per violation**	$1,500,000



Checklist to test Willful Neglect Exposure

Seven (7) Basic HIPAA Compliance Health Check Questions Every Covered Entity and Business Associate Needs to Ask Themselves

1. **Have you conducted a legitimate HIPAA Security Risk Analysis (SRA) which has been documented and is not outdated? YES ____ NO ____**

2. **Do you have written and appropriately updated HIPAA Privacy and Security policies in place?**

   YES ____ NO ____

3. **Have you designated an individual trained to function in the role of your HIPAA Privacy and Security Officer? YES ____ NO ____**

4. **Do you have an ongoing, documented Risk Management program? YES ____ NO ____**

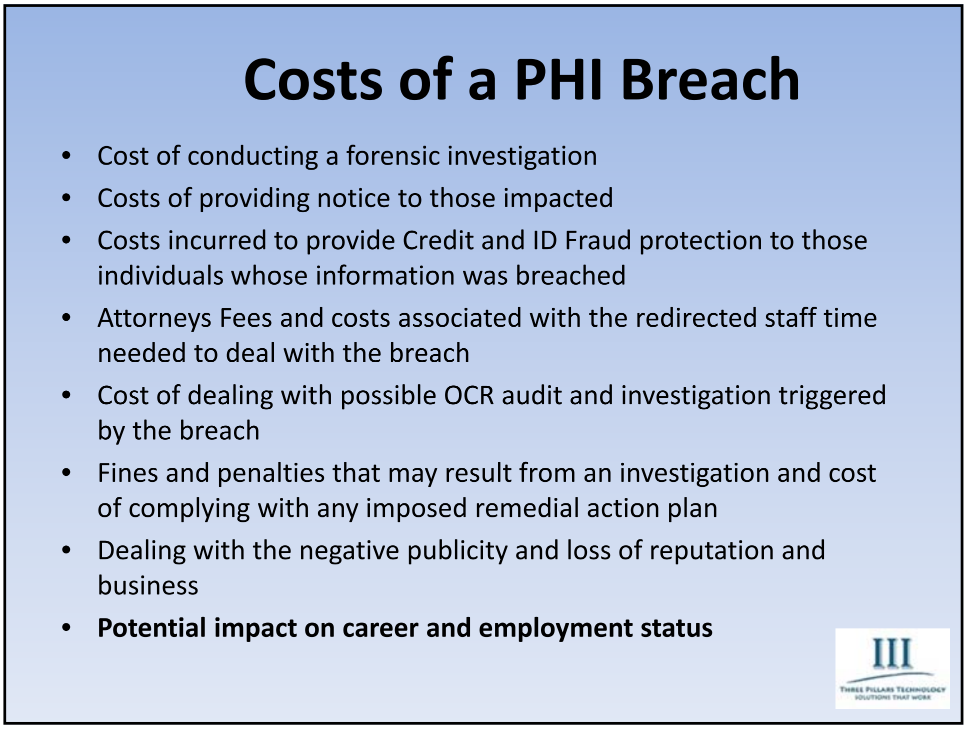
5. **Does your organization have a documented HIPAA education, awareness and training program in operation? YES ____ NO ____**

6. **Have you reviewed, revised and updated your Business Associate Agreements, as necessary?**

   YES ____ NO ____

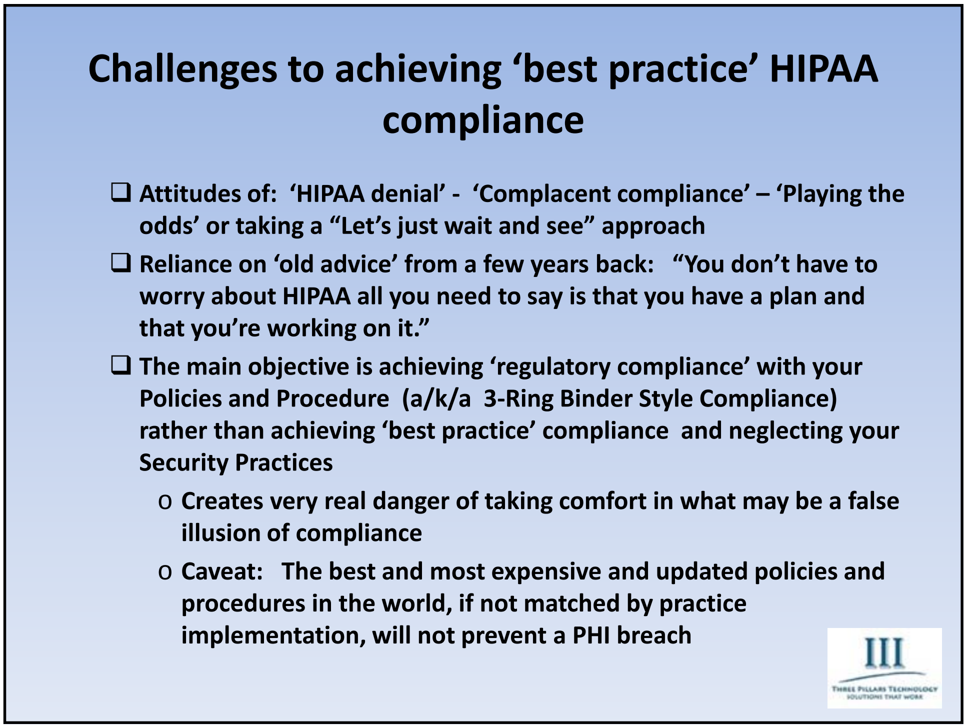
7. **Do you have a PHI (Protected Health Information) Breach occurrence and notification policy and process in place, and have you updated it to reflect changes made by the new HIPAA / HITECH rules?**

   YES ____ NO ____



Costs of a PHI Breach

- Cost of conducting a forensic investigation
- Costs of providing notice to those impacted
- Costs incurred to provide Credit and ID Fraud protection to those individuals whose information was breached
- Attorneys Fees and costs associated with the redirected staff time needed to deal with the breach
- Cost of dealing with possible OCR audit and investigation triggered by the breach
- Fines and penalties that may result from an investigation and cost of complying with any imposed remedial action plan
- Dealing with the negative publicity and loss of reputation and business
- **Potential impact on career and employment status**



Challenges to achieving 'best practice' HIPAA compliance

- ❑ **Attitudes of: 'HIPAA denial' - 'Complacent compliance' – 'Playing the odds' or taking a "Let's just wait and see" approach**
- ❑ **Reliance on 'old advice' from a few years back: "You don't have to worry about HIPAA all you need to say is that you have a plan and that you're working on it."**
- ❑ **The main objective is achieving 'regulatory compliance' with your Policies and Procedure (a/k/a 3-Ring Binder Style Compliance) rather than achieving 'best practice' compliance and neglecting your Security Practices**
  - o **Creates very real danger of taking comfort in what may be a false illusion of compliance**
  - o **Caveat: The best and most expensive and updated policies and procedures in the world, if not matched by practice implementation, will not prevent a PHI breach**

The Rise in Importance of the **HIPAA Security Rule** and the Security Risk Analysis (SRA)

Wake Up !! – it's no longer a Three Ring Binder Policy and Procedure compliance world

THREE PILLARS TECHNOLOGY
SOLUTIONS THAT WORK

HIPAA Security AND Compliance

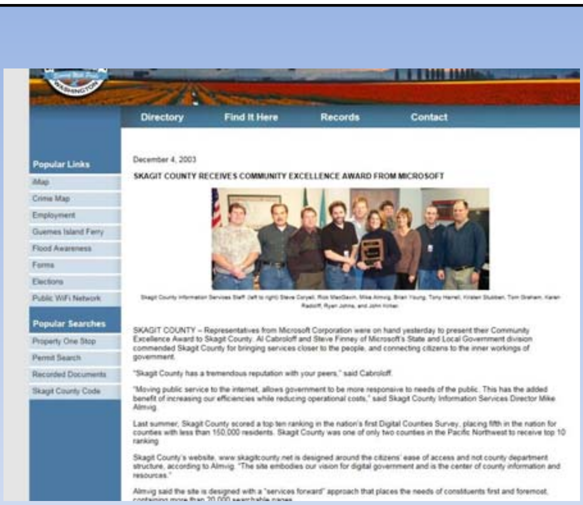
Compliance ≠ Security

Security ≠ Compliance

Skagit County, Washington

In 2014 Skagit County became the first county government in the United States to be sanctioned for a HIPAA violation. They were fined $215,000 and placed under a 'voluntary' 3 Year Corrective Action Plan monitored by HHS

- **Link to Skagit County Home Page:** http://www.skagitcounty.net/Departments/Home/main.htm
- **Link to HHS/OCR HIPAA Enforcement Action Press Release** http://www.hhs.gov/news/press/2014pres/03/20140307a.html
- **Link to HHS/OCR – Skagit County Resolution Agreement** http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/skagit-county-settlement-agreement.pdf
- **Link to Skagit County's Posted Notice of Breach** http://www.skagitcounty.net/Departments/Home/hipaa.htm



December 4, 2003

SKAGIT COUNTY RECEIVES COMMUNITY EXCELLENCE AWARD FROM MICROSOFT

Skagit County Information Services Staff (left to right) Steve Coryell, Rick MacGavin, Mike Almvig, Brian Young, Tony Harrell, Kristen Stubben, Tom Graham, Karen Radloff, Ryan Johns, and John Kirkan

SKAGIT COUNTY – Representatives from Microsoft Corporation were on hand yesterday to present their Community Excellence Award to Skagit County. Al Cabroloff and Steve Finney of Microsoft's State and Local Government division commended Skagit County for bringing services closer to the people, and connecting citizens to the inner workings of government.

"Skagit County has a tremendous reputation with your peers," said Cabroloff.

"Moving public service to the internet, allows government to be more responsive to needs of the public. This has the added benefit of increasing our efficiencies while reducing operational costs," said Skagit County Information Services Director Mike Almvig.

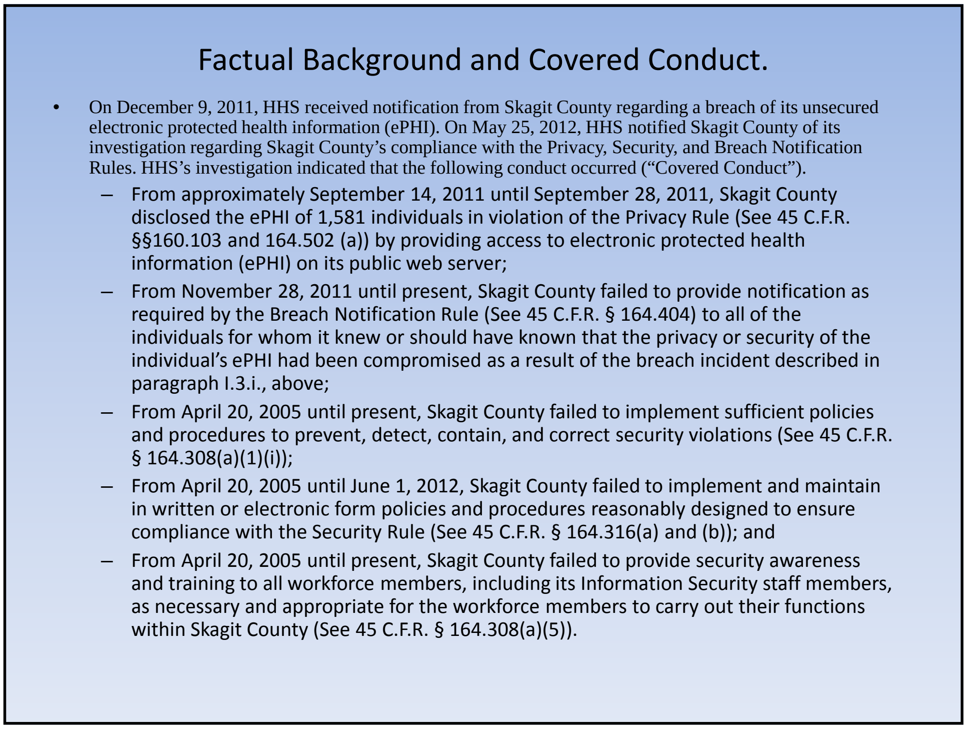
Last summer, Skagit County scored a top ten ranking in the nation's first Digital Counties Survey, placing fifth in the nation for counties with less than 150,000 residents. Skagit County was one of only two counties in the Pacific Northwest to receive top 10 ranking.

Skagit County's website, www.skagitcounty.net is designed around the citizens' ease of access and not county department structure, according to Almvig. "The site embodies our vision for digital government and is the center of county information and resources."

Almvig said the site is designed with a "services forward" approach that places the needs of constituents first and foremost, containing more than 20,000 searchable pages.

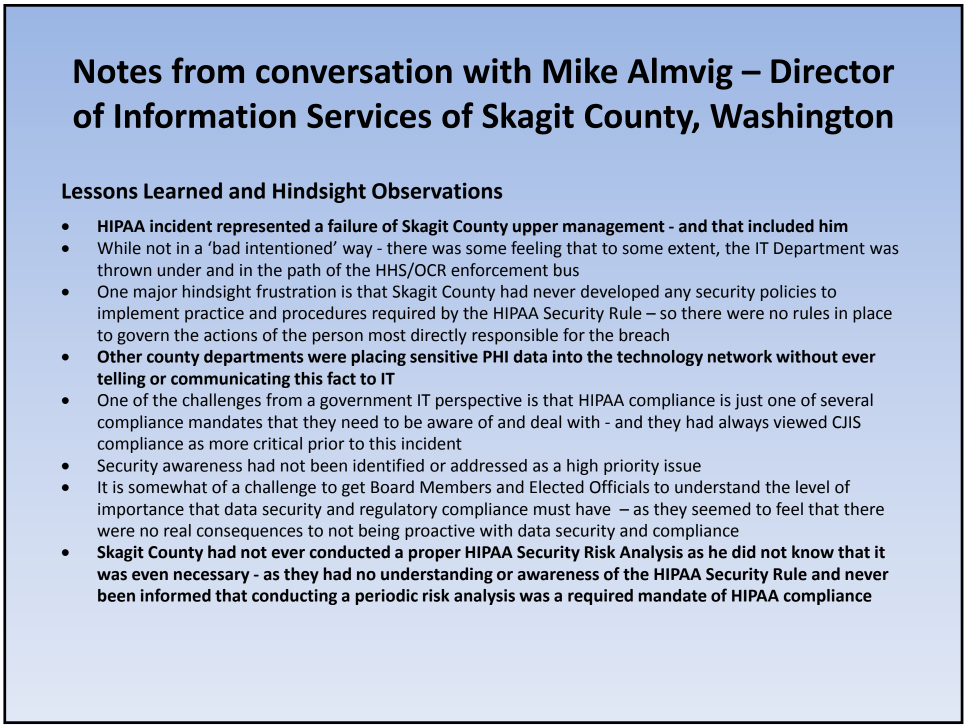
Skagit County, WA   Population 118,837 (2013)

Even being an award winning IT Department didn't make Skagit County immune from a HHS/OCR HIPAA enforcement sanction.



Factual Background and Covered Conduct.

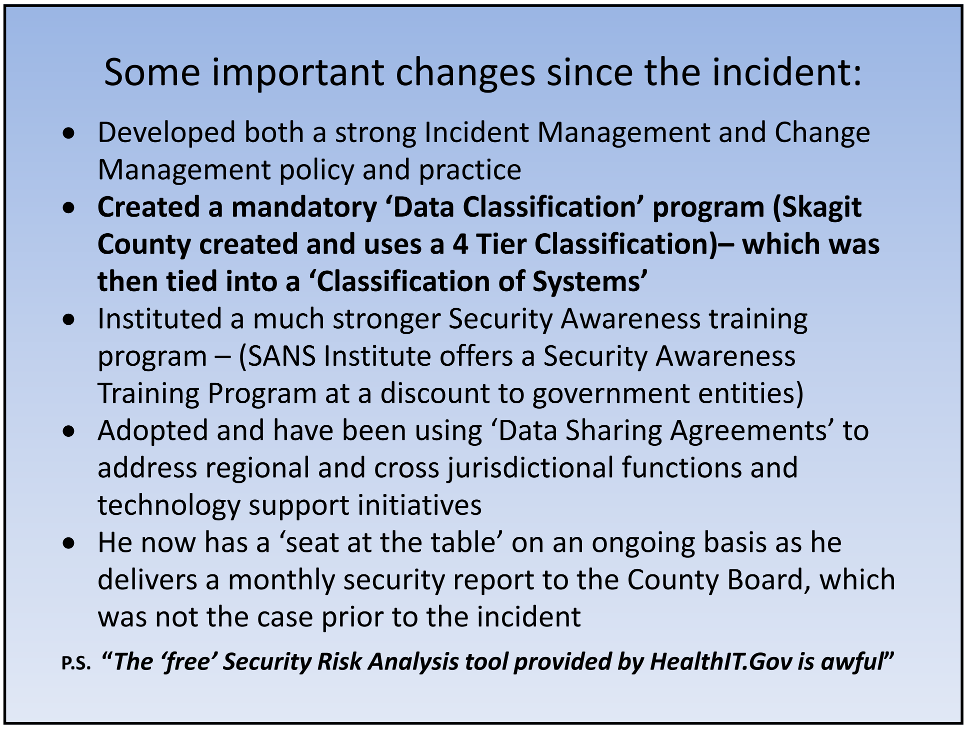
- On December 9, 2011, HHS received notification from Skagit County regarding a breach of its unsecured electronic protected health information (ePHI). On May 25, 2012, HHS notified Skagit County of its investigation regarding Skagit County's compliance with the Privacy, Security, and Breach Notification Rules. HHS's investigation indicated that the following conduct occurred ("Covered Conduct").
  - From approximately September 14, 2011 until September 28, 2011, Skagit County disclosed the ePHI of 1,581 individuals in violation of the Privacy Rule (See 45 C.F.R. §§160.103 and 164.502 (a)) by providing access to electronic protected health information (ePHI) on its public web server;
  - From November 28, 2011 until present, Skagit County failed to provide notification as required by the Breach Notification Rule (See 45 C.F.R. § 164.404) to all of the individuals for whom it knew or should have known that the privacy or security of the individual's ePHI had been compromised as a result of the breach incident described in paragraph I.3.i., above;
  - From April 20, 2005 until present, Skagit County failed to implement sufficient policies and procedures to prevent, detect, contain, and correct security violations (See 45 C.F.R. § 164.308(a)(1)(i));
  - From April 20, 2005 until June 1, 2012, Skagit County failed to implement and maintain in written or electronic form policies and procedures reasonably designed to ensure compliance with the Security Rule (See 45 C.F.R. § 164.316(a) and (b)); and
  - From April 20, 2005 until present, Skagit County failed to provide security awareness and training to all workforce members, including its Information Security staff members, as necessary and appropriate for the workforce members to carry out their functions within Skagit County (See 45 C.F.R. § 164.308(a)(5)).



Notes from conversation with Mike Almvig – Director of Information Services of Skagit County, Washington

Lessons Learned and Hindsight Observations

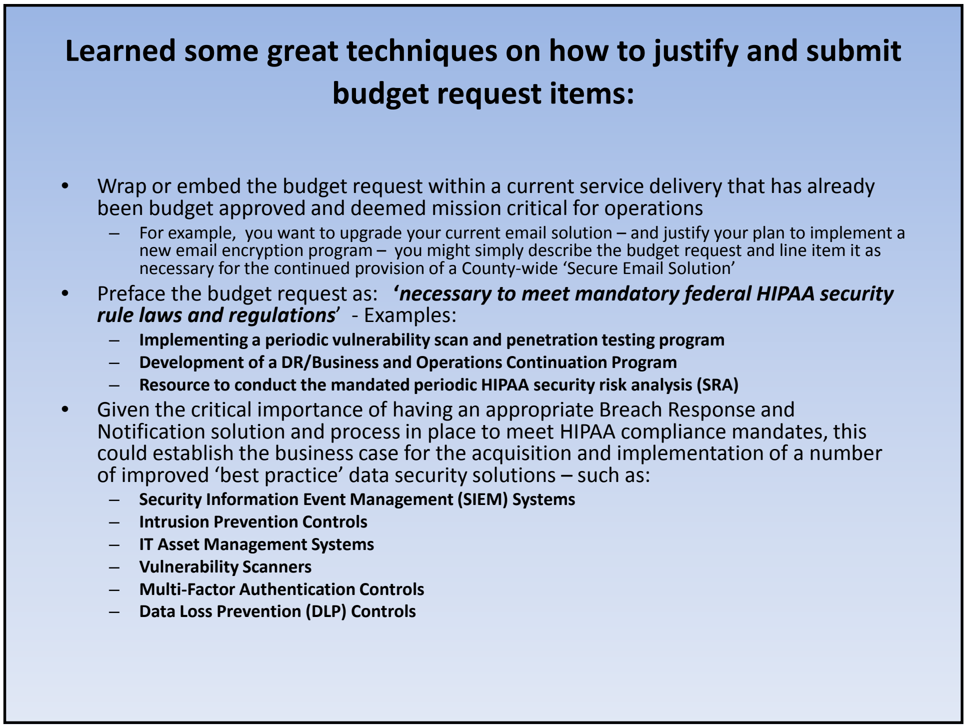
- **HIPAA incident represented a failure of Skagit County upper management - and that included him**
- While not in a 'bad intentioned' way - there was some feeling that to some extent, the IT Department was thrown under and in the path of the HHS/OCR enforcement bus
- One major hindsight frustration is that Skagit County had never developed any security policies to implement practice and procedures required by the HIPAA Security Rule – so there were no rules in place to govern the actions of the person most directly responsible for the breach
- **Other county departments were placing sensitive PHI data into the technology network without ever telling or communicating this fact to IT**
- One of the challenges from a government IT perspective is that HIPAA compliance is just one of several compliance mandates that they need to be aware of and deal with - and they had always viewed CJIS compliance as more critical prior to this incident
- Security awareness had not been identified or addressed as a high priority issue
- It is somewhat of a challenge to get Board Members and Elected Officials to understand the level of importance that data security and regulatory compliance must have – as they seemed to feel that there were no real consequences to not being proactive with data security and compliance
- **Skagit County had not ever conducted a proper HIPAA Security Risk Analysis as he did not know that it was even necessary - as they had no understanding or awareness of the HIPAA Security Rule and never been informed that conducting a periodic risk analysis was a required mandate of HIPAA compliance**



Some important changes since the incident:

- Developed both a strong Incident Management and Change Management policy and practice
- **Created a mandatory 'Data Classification' program (Skagit County created and uses a 4 Tier Classification)– which was then tied into a 'Classification of Systems'**
- Instituted a much stronger Security Awareness training program – (SANS Institute offers a Security Awareness Training Program at a discount to government entities)
- Adopted and have been using 'Data Sharing Agreements' to address regional and cross jurisdictional functions and technology support initiatives
- He now has a 'seat at the table' on an ongoing basis as he delivers a monthly security report to the County Board, which was not the case prior to the incident

P.S. ***"The 'free' Security Risk Analysis tool provided by HealthIT.Gov is awful"***

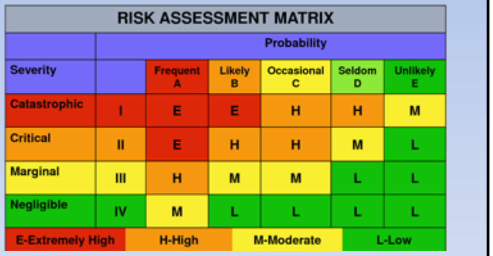


Learned some great techniques on how to justify and submit budget request items:

- Wrap or embed the budget request within a current service delivery that has already been budget approved and deemed mission critical for operations
  - For example, you want to upgrade your current email solution – and justify your plan to implement a new email encryption program – you might simply describe the budget request and line item it as necessary for the continued provision of a County-wide 'Secure Email Solution'
- Preface the budget request as: ***'necessary to meet mandatory federal HIPAA security rule laws and regulations***' - Examples:
  - **Implementing a periodic vulnerability scan and penetration testing program**
  - **Development of a DR/Business and Operations Continuation Program**
  - **Resource to conduct the mandated periodic HIPAA security risk analysis (SRA)**
- Given the critical importance of having an appropriate Breach Response and Notification solution and process in place to meet HIPAA compliance mandates, this could establish the business case for the acquisition and implementation of a number of improved 'best practice' data security solutions – such as:
  - **Security Information Event Management (SIEM) Systems**
  - **Intrusion Prevention Controls**
  - **IT Asset Management Systems**
  - **Vulnerability Scanners**
  - **Multi-Factor Authentication Controls**
  - **Data Loss Prevention (DLP) Controls**

Compliance Assessment vs. Risk Analysis (watch out for this confusion)

- A Compliance Assessment is a gap analysis that identifies gaps in the organization on HIPAA Administrative, Physical and Technical specifications
- A Risk Analysis is more in depth and includes these critical elements in the report and work papers:
  - Threat Source List
  - Inventory Asset List
  - Risk Level of High, Medium and Low for each risk based on Likelihood and Impact scores
  - Likelihood determination for each risk
  - Impact determination for each risk



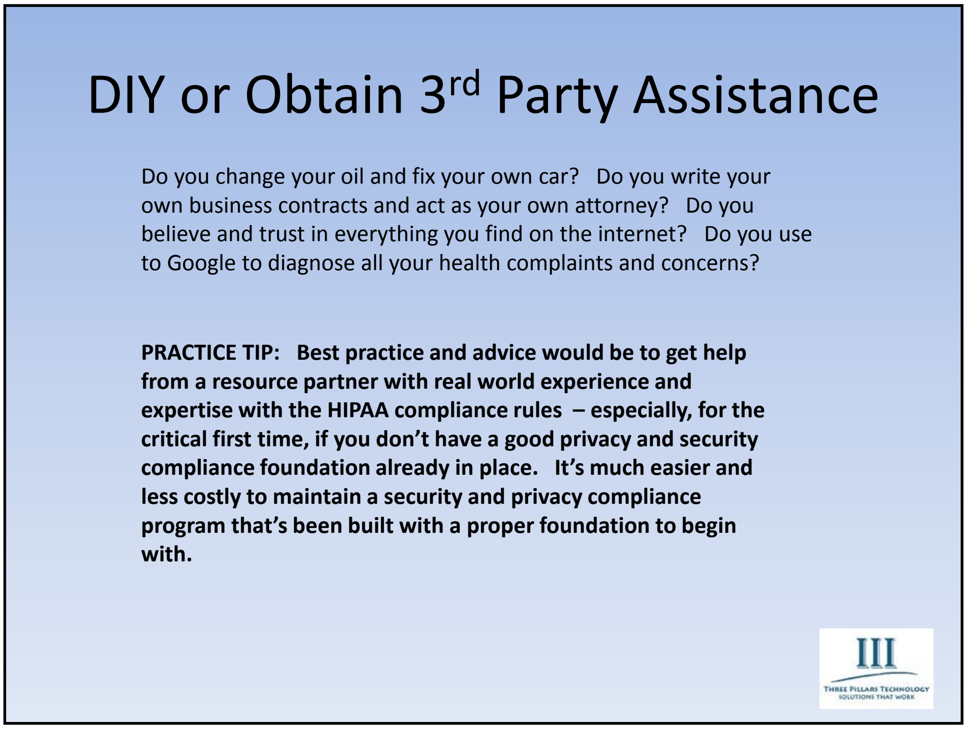
RISK ASSESSMENT MATRIX

		Probability				
Severity		Frequent A	Likely B	Occasional C	Seldom D	Unlikely E
Catastrophic	I	E	E	H	H	M
Critical	II	E	H	H	M	L
Marginal	III	H	M	M	L	L
Negligible	IV	M	L	L	L	L

E-Extremely High | H-High | M-Moderate | L-Low

Integral aspects of HIPAA Security Rule Compliance that Require the Involvement and Input of IT

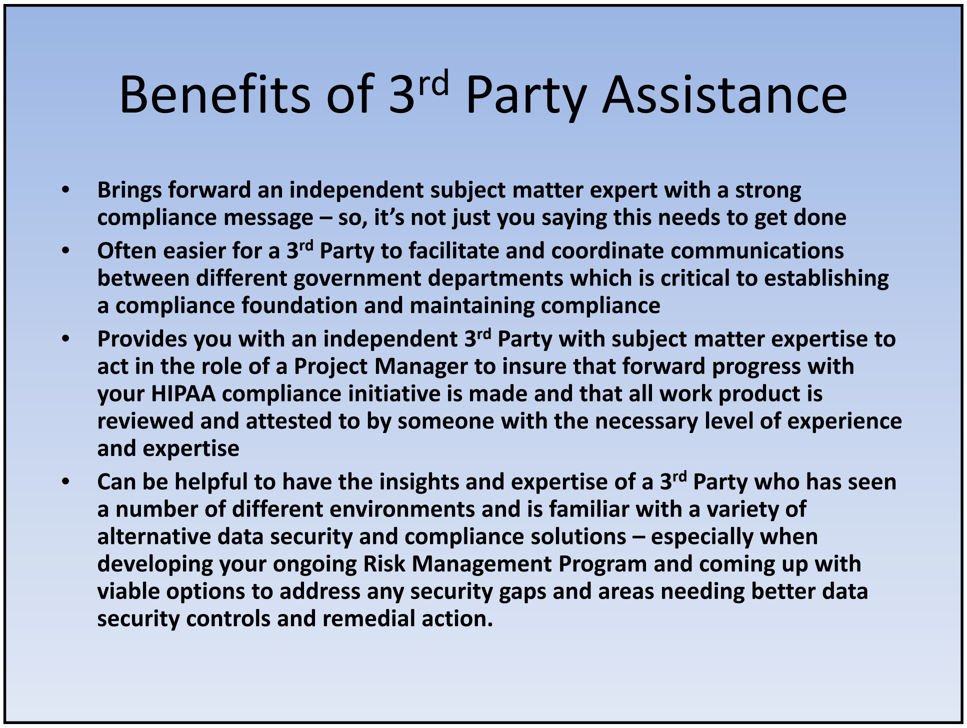
- **Help in conducting a proper HIPAA Security Risk Analysis**
  - Insuring there exists a complete and accurate ePHI and Technology Inventory
  - Accurate description of current data security controls
  - Having input in the development of any remedial action plan to address existing gaps or areas of potential risk
- **Participation and input in developing a sound ongoing Risk Management Program**
- **Assist in developing appropriate and mandatory HIPAA security policies and procedures**
- **Security Awareness Training for staff**
- **Insuring that you have in place a functional Breach Response and Notification plan**



DIY or Obtain 3rd Party Assistance

Do you change your oil and fix your own car? Do you write your own business contracts and act as your own attorney? Do you believe and trust in everything you find on the internet? Do you use to Google to diagnose all your health complaints and concerns?

PRACTICE TIP: Best practice and advice would be to get help from a resource partner with real world experience and expertise with the HIPAA compliance rules – especially, for the critical first time, if you don't have a good privacy and security compliance foundation already in place. It's much easier and less costly to maintain a security and privacy compliance program that's been built with a proper foundation to begin with.



Benefits of 3rd Party Assistance

- **Brings forward an independent subject matter expert with a strong compliance message – so, it's not just you saying this needs to get done**
- **Often easier for a 3rd Party to facilitate and coordinate communications between different government departments which is critical to establishing a compliance foundation and maintaining compliance**
- **Provides you with an independent 3rd Party with subject matter expertise to act in the role of a Project Manager to insure that forward progress with your HIPAA compliance initiative is made and that all work product is reviewed and attested to by someone with the necessary level of experience and expertise**
- **Can be helpful to have the insights and expertise of a 3rd Party who has seen a number of different environments and is familiar with a variety of alternative data security and compliance solutions – especially when developing your ongoing Risk Management Program and coming up with viable options to address any security gaps and areas needing better data security controls and remedial action.**

Practice Tips for Proactive Staff of Government Entities

- **Whenever possible secure 'buy-in' from the appropriate government oversight board or committee**
- **At a minimum alert and educate them to the issue and encourage them to take action to address HIPAA compliance**
- **It's helpful to have all 'stakeholders' engaged and committed to any compliance initiative – reach out to other Department heads who are impacted by HIPAA**
- **One way to begin and to generate support is to have a 3rd Party conduct a baseline HIPAA compliance assessment and produce a report of your current compliance status**

(Though if you've never conducted a Security Risk Analysis (SRA) – you'd probably want to have that as part of the deliverable)

Some Observations from our Experience in Working with Wisconsin Counties

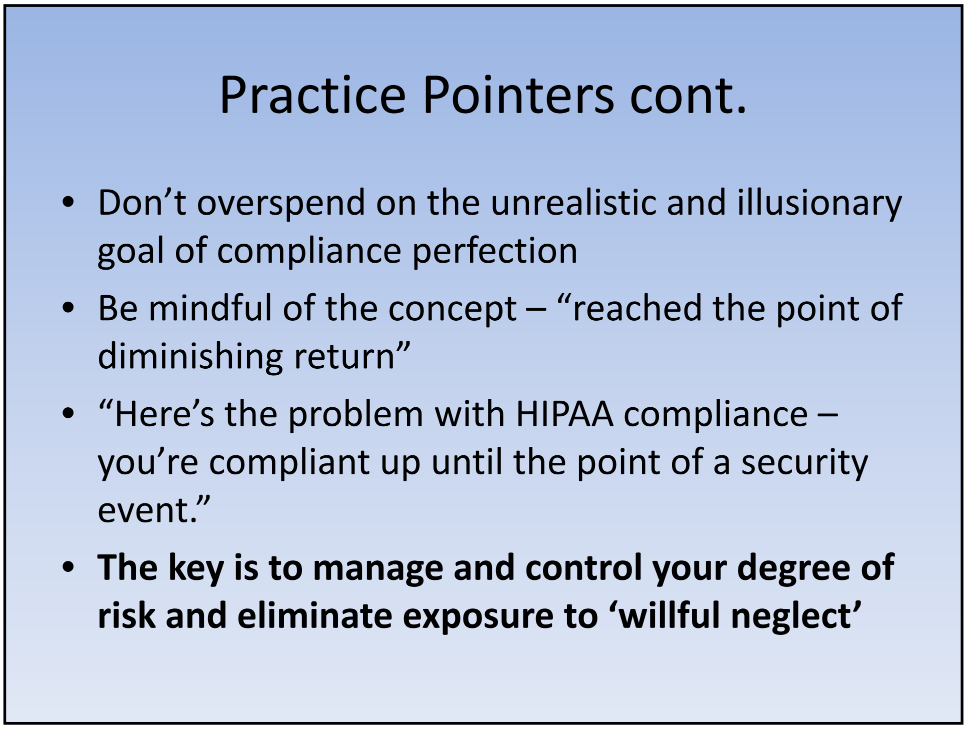
- **I'll begin with an insightful spin on the cliché: "If you've met one – you've met them all" When it comes to working within Wisconsin County Government sector - *If you've worked with one Wisconsin County – you've worked with one Wisconsin County***
- **Easy and understandable the degree to which one can 'point to others' when it comes to determining who should be taking the initiative.**
- **Assumption that because we already comply with other compliance requirements – such as CJIS, we can simply 'point to that' as proof of our HIPAA compliance.**
- **Significant lack of knowledge and understanding as to the impact of HIPAA/HITECH and how critical meeting compliance with the HIPAA Security Rule has become – which requires an approach and actions which are significantly different than meeting compliance with the HIPAA Privacy Rule**

Observations in working with Wisconsin Counties cont.

- Special challenges posed by dealing with compliance with the HIPAA Security Rule:
  - Which Departments should be involved?
  - Which Department should 'lead' this aspect of HIPAA compliance?
  - How should the cost be budgeted?
- A belief that it would be 'best to wait' until we have things in a better condition before undertaking a HIPAA security risk analysis. This is just the complete opposite of what the proper mind set and approach should be.
- Belief that the County Insurance Carrier that provides Cyber Liability insurance will cover any financial exposure and costs caused by our possible lack of HIPAA compliance.
- Belief that the vendor/provider of you EHR (electronic health record), claims submittal or other software that handles your sensitive data or ePHI – will satisfy and take care of your HIPAA compliance.

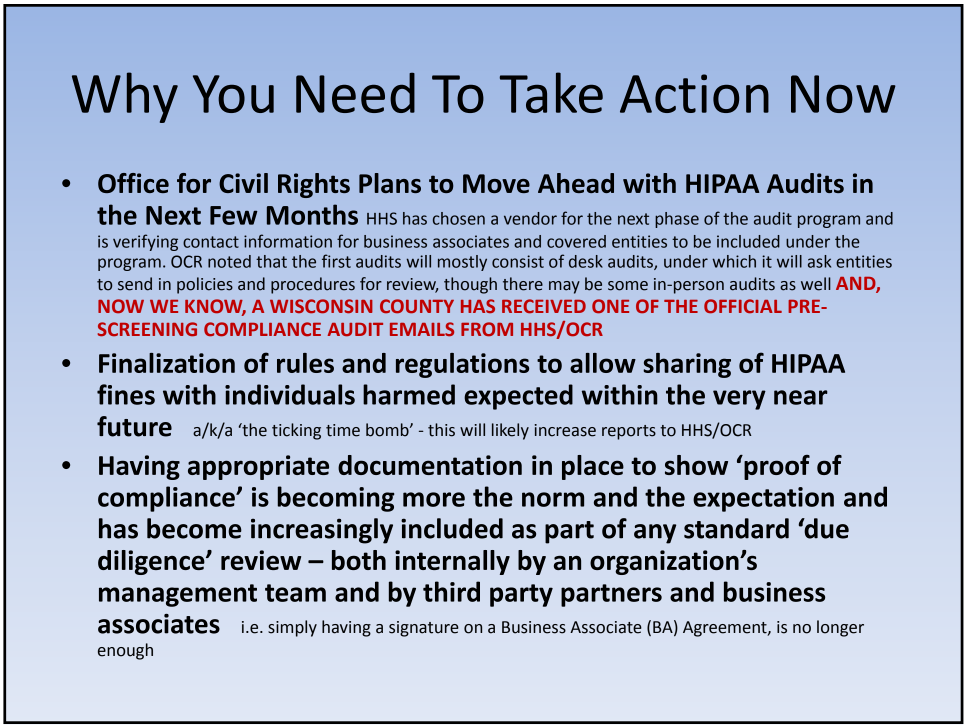
Some Practical Observations

- **Document – Document – Document**
- Remember to Review – Update – Revise (Compliance and especially, security compliance is never a "one and done")
- Avoid the 'Off the Shelf' Solution and taking the "Checklist to Compliance" approach
- **Check into your Insurance Coverage – Cyber Insurance coverage – Don't be a passive consumer - Ask Questions**
- There is no such thing as 'Certified HIPAA Compliant' that is recognized by HHS/OCR
- **Be very careful of any software vendor (i.e. your EHR vendor) or insurance company who states that they have taken care of all your HIPAA compliance needs and will protect you from all risks**



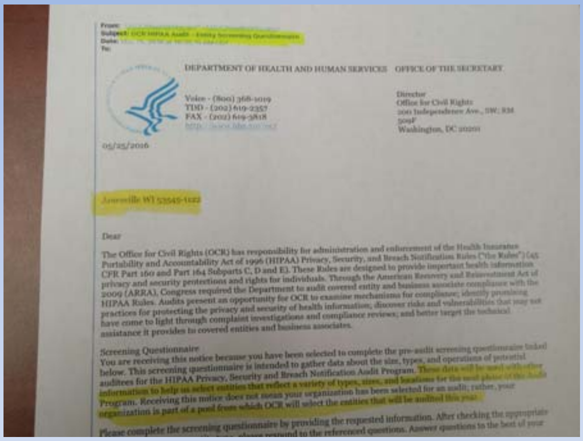
Practice Pointers cont.

- Don’t overspend on the unrealistic and illusionary goal of compliance perfection
- Be mindful of the concept – “reached the point of diminishing return”
- “Here’s the problem with HIPAA compliance – you’re compliant up until the point of a security event.”
- **The key is to manage and control your degree of risk and eliminate exposure to ‘willful neglect’**



Why You Need To Take Action Now

- **Office for Civil Rights Plans to Move Ahead with HIPAA Audits in the Next Few Months** HHS has chosen a vendor for the next phase of the audit program and is verifying contact information for business associates and covered entities to be included under the program. OCR noted that the first audits will mostly consist of desk audits, under which it will ask entities to send in policies and procedures for review, though there may be some in-person audits as well **AND, NOW WE KNOW, A WISCONSIN COUNTY HAS RECEIVED ONE OF THE OFFICIAL PRE-SCREENING COMPLIANCE AUDIT EMAILS FROM HHS/OCR**
- **Finalization of rules and regulations to allow sharing of HIPAA fines with individuals harmed expected within the very near future** a/k/a ‘the ticking time bomb’ - this will likely increase reports to HHS/OCR
- **Having appropriate documentation in place to show ‘proof of compliance’ is becoming more the norm and the expectation and has become increasingly included as part of any standard ‘due diligence’ review – both internally by an organization’s management team and by third party partners and business associates** i.e. simply having a signature on a Business Associate (BA) Agreement, is no longer enough



From:
Subject: OCR HIPAA Audit - Entity Screening Questionnaire
Date: [illegible]
To:

DEPARTMENT OF HEALTH AND HUMAN SERVICES OFFICE OF THE SECRETARY

Voice - (800) 368-1019
TDD - (202) 619-2357
FAX - (202) 619-3818
http://www.hhs.gov/ocr/

Director
Office for Civil Rights
200 Independence Ave., SW; RM
509F
Washington, DC 20201

05/25/2016

Janesville WI 53545-1122

Dear

The Office for Civil Rights (OCR) has responsibility for administration and enforcement of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy, Security, and Breach Notification Rules ("the Rules") (45 CFR Part 160 and Part 164 Subparts C, D and E). These Rules are designed to provide important health information privacy and security protections and rights for individuals. Through the American Recovery and Reinvestment Act of 2009 (ARRA), Congress required the Department to audit covered entity and business associate compliance with the HIPAA Rules. Audits present an opportunity for OCR to examine mechanisms for compliance; identify promising practices for protecting the privacy and security of health information; discover risks and vulnerabilities that may not have come to light through complaint investigations and compliance reviews; and better target the technical assistance it provides to covered entities and business associates.

Screening Questionnaire
You are receiving this notice because you have been selected to complete the pre-audit screening questionnaire linked below. This screening questionnaire is intended to gather data about the size, types, and operations of potential auditees for the HIPAA Privacy, Security and Breach Notification Audit Program. These data will be used with other information to help us select entities that reflect a variety of types, sizes, and locations for the next phase of the Audit Program. Receiving this notice does not mean your organization has been selected for an audit; rather, your organization is part of a pool from which OCR will select the entities that will be audited this year.

Please complete the screening questionnaire by providing the requested information. After checking the appropriate [illegible] please respond to the referenced questions. Answer questions to the best of your

OCR HIPAA Audit Entity Screening Questionnaire

This one 'landed' on a small independent physician practice in Janesville WI – and at least one Wisconsin County has received one as well

Three Pillar's Approach

- Collaborative Customized Approach – We follow the maxim '**One Size DOES NOT Fit All**'
- We Do Not Wish To Be Viewed As Your Auditor but Rather As Your Trusted Advisor and Subject Matter Expert Guide
- **Our Focus and Approach is Different from 'Traditional' HIPAA Compliance Consultants**
- Our Goal is to Avoid Unnecessary Duplication and Repetition of Effort and to Respect Staff Time and Utilization
- Educate and Promote Knowledge Transfer to Your Staff
- Offer a sensible and budget friendly 'ongoing' HIPAA compliance and maintenance solution

The Case in Support of an Ongoing Compliance Solution

- **HIPAA Security Rule has Periodic Required Mandates that Must be Met with Documented Proof of Ongoing Compliance**
- No need or justification to redo from scratch your compliance foundation, once established
- Once 'built' the objective is to maintain and work upon areas that could use improvement
- Basic question to ask at the time of the periodic reviews is: "What's Changed?" and address any changes

Overview of Process

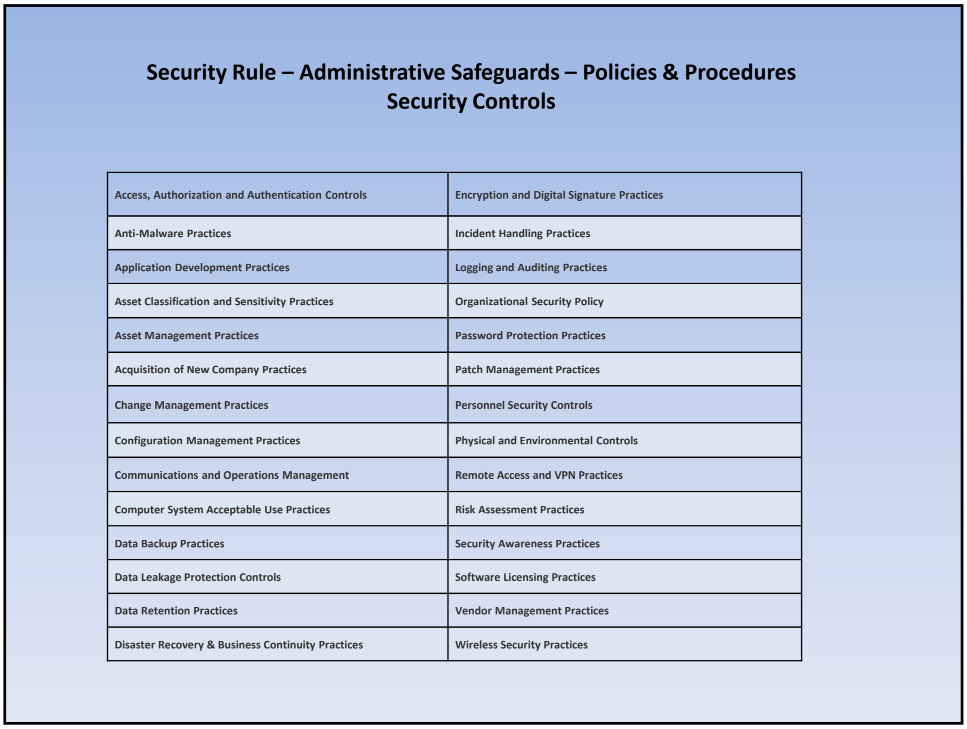
- **Scope the Project – Identify Budget Parameters and Timeframes**
- **Proposal Preparation and Submittal**
- **Project Kick-off**
- **Documentation and Information Request List**
- **Review and Analyze Information Submittal and Document Production from Client**
- **Conduct Interviews and Onsite 'Walk Through'**
- **Undertake Security Risk Analysis Process**
- **Production and Delivery of Reports and Work Product**
- **Assist Client in Development of Strategic Action Plan**

Links to HIPAA Compliance and Data Security Resources

- **HealthIT.gov** http://www.healthit.gov/
- **Guide to Privacy and Security of Electronic Health Information**
  http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf
- **SANS** **https://www.sans.org/critical-security-controls/**
- **California Data Breach Report 2016 –**
  https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf
- **NIST Cybersecurity Framework** **http://www.nist.gov/cyberframework/index.cfm**
- **NIST Special Publication 800-30** **Guide for Conducting Risk Assessments**
  http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf
- **HHS.gov** **(Summary of the HIPAA Security Rule)**
  http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html
- **HIPAA COW** **http://hipaacow.org/resources/**

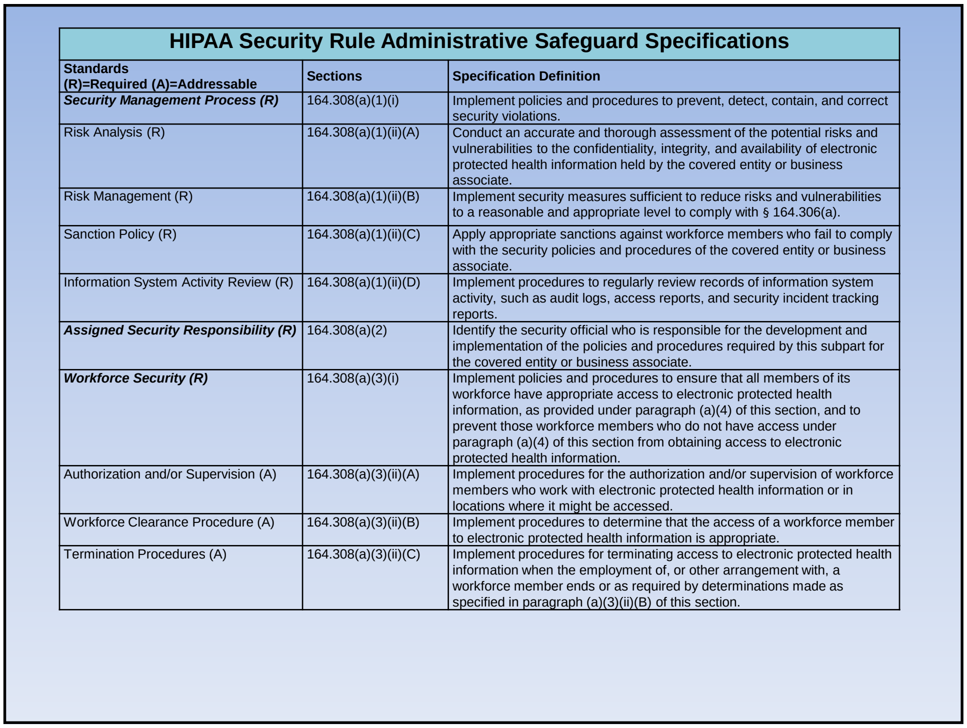
CIS Critical Security Controls - Version 6.0

CSC 1: Inventory of Authorized and Unauthorized Devices
CSC 2: Inventory of Authorized and Unauthorized Software
CSC 3: Secure Configurations for Hardware and Software on Mobile Device Laptops, Workstations, and Servers
CSC 4: Continuous Vulnerability Assessment and Remediation
CSC 5: Controlled Use of Administrative Privileges
CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs
CSC 7: Email and Web Browser Protections
CSC 8: Malware Defenses
CSC 9: Limitation and Control of Network Ports, Protocols, and Services
CSC 10: Data Recovery Capability
CSC 11: Secure Configurations for Network Devices such as Firewall Routers, and Switches
CSC 12: Boundary Defense
CSC 13: Data Protection
CSC 14: Controlled Access Based on the Need to Know
CSC 15: Wireless Access Control
CSC 16: Account Monitoring and Control
CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps
CSC 18: Application Software Security
CSC 19: Incident Response and Management
CSC 20: Penetration Tests and Red Team Exercises



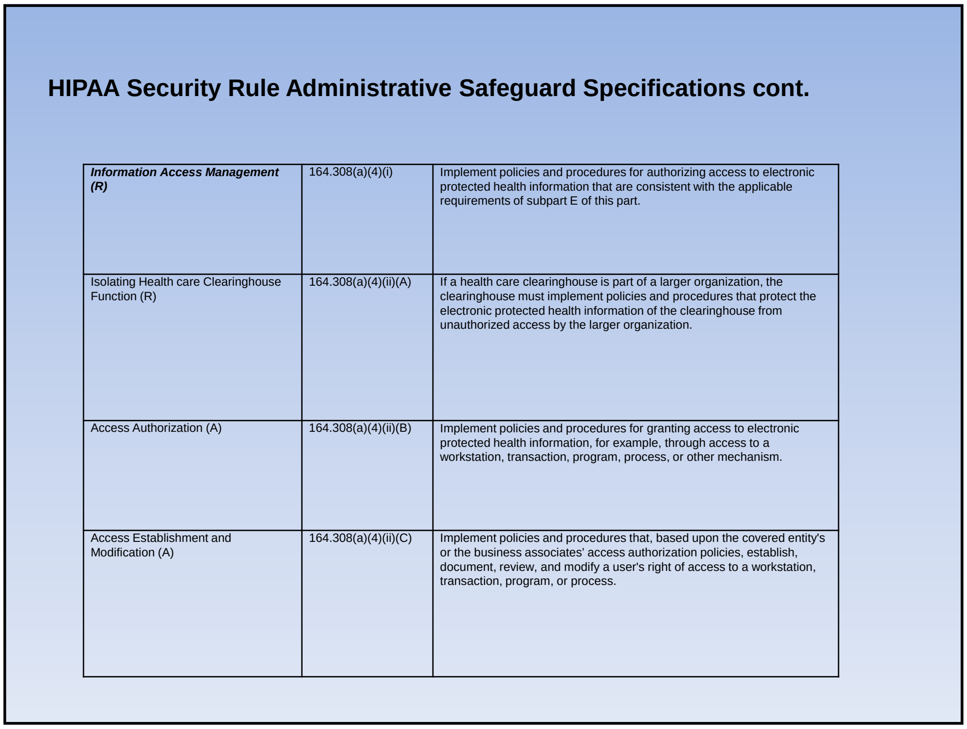
Security Rule – Administrative Safeguards – Policies & Procedures
Security Controls

Access, Authorization and Authentication Controls	Encryption and Digital Signature Practices
Anti-Malware Practices	Incident Handling Practices
Application Development Practices	Logging and Auditing Practices
Asset Classification and Sensitivity Practices	Organizational Security Policy
Asset Management Practices	Password Protection Practices
Acquisition of New Company Practices	Patch Management Practices
Change Management Practices	Personnel Security Controls
Configuration Management Practices	Physical and Environmental Controls
Communications and Operations Management	Remote Access and VPN Practices
Computer System Acceptable Use Practices	Risk Assessment Practices
Data Backup Practices	Security Awareness Practices
Data Leakage Protection Controls	Software Licensing Practices
Data Retention Practices	Vendor Management Practices
Disaster Recovery & Business Continuity Practices	Wireless Security Practices



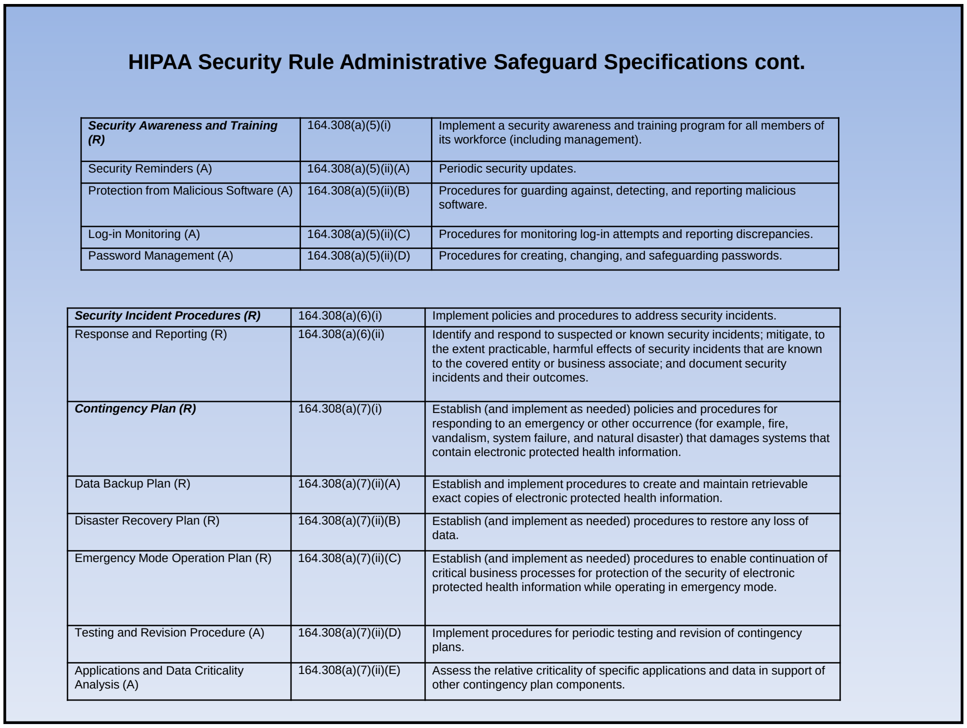
HIPAA Security Rule Administrative Safeguard Specifications

Standards **(R)=Required (A)=Addressable**	**Sections**	**Specification Definition**
Security Management Process (R)	164.308(a)(1)(i)	Implement policies and procedures to prevent, detect, contain, and correct security violations.
Risk Analysis (R)	164.308(a)(1)(ii)(A)	Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.
Risk Management (R)	164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).
Sanction Policy (R)	164.308(a)(1)(ii)(C)	Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.
Information System Activity Review (R)	164.308(a)(1)(ii)(D)	Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
Assigned Security Responsibility (R)	164.308(a)(2)	Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.
Workforce Security (R)	164.308(a)(3)(i)	Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.
Authorization and/or Supervision (A)	164.308(a)(3)(ii)(A)	Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.
Workforce Clearance Procedure (A)	164.308(a)(3)(ii)(B)	Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.
Termination Procedures (A)	164.308(a)(3)(ii)(C)	Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.



HIPAA Security Rule Administrative Safeguard Specifications cont.

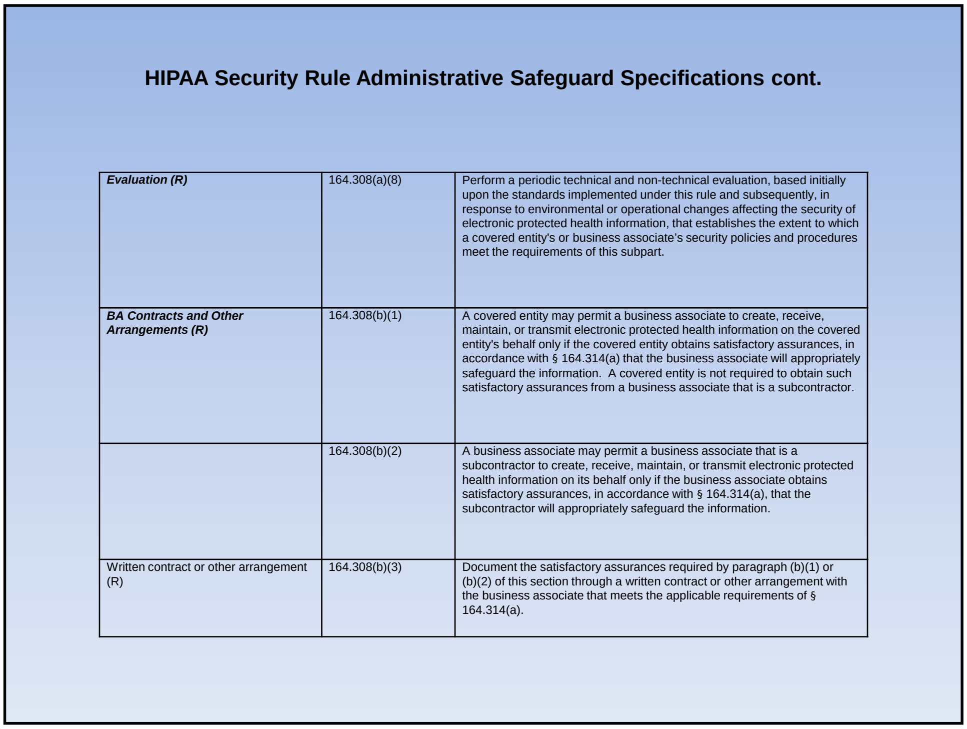
Information Access Management (R)	164.308(a)(4)(i)	Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.
Isolating Health care Clearinghouse Function (R)	164.308(a)(4)(ii)(A)	If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.
Access Authorization (A)	164.308(a)(4)(ii)(B)	Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.
Access Establishment and Modification (A)	164.308(a)(4)(ii)(C)	Implement policies and procedures that, based upon the covered entity's or the business associates' access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.



HIPAA Security Rule Administrative Safeguard Specifications cont.

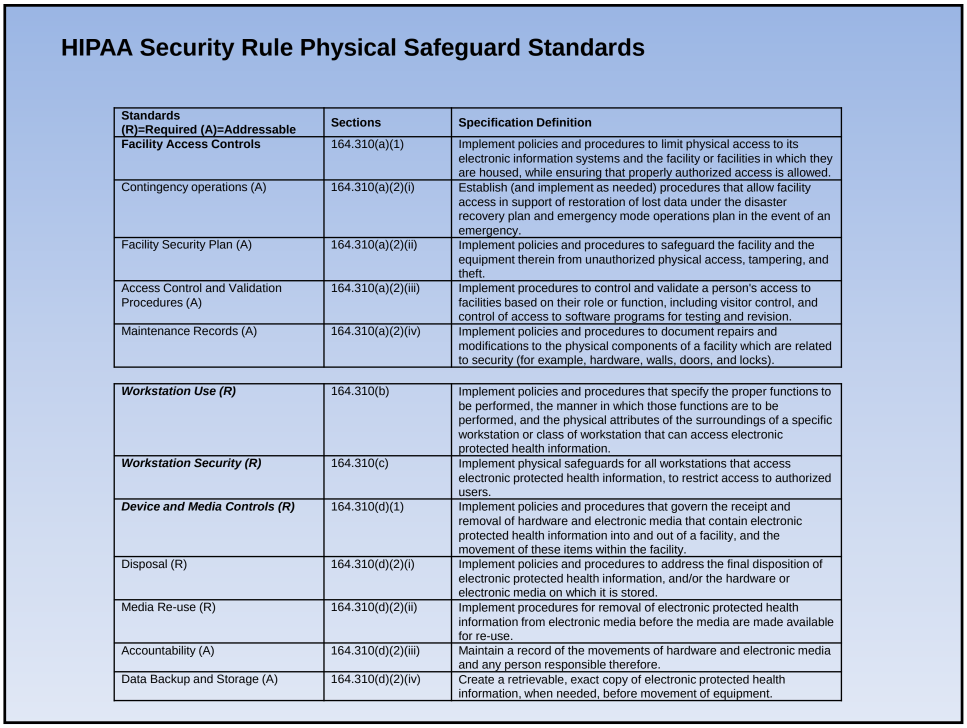
Security Awareness and Training (R)	164.308(a)(5)(i)	Implement a security awareness and training program for all members of its workforce (including management).
Security Reminders (A)	164.308(a)(5)(ii)(A)	Periodic security updates.
Protection from Malicious Software (A)	164.308(a)(5)(ii)(B)	Procedures for guarding against, detecting, and reporting malicious software.
Log-in Monitoring (A)	164.308(a)(5)(ii)(C)	Procedures for monitoring log-in attempts and reporting discrepancies.
Password Management (A)	164.308(a)(5)(ii)(D)	Procedures for creating, changing, and safeguarding passwords.

Security Incident Procedures (R)	164.308(a)(6)(i)	Implement policies and procedures to address security incidents.
Response and Reporting (R)	164.308(a)(6)(ii)	Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.
Contingency Plan (R)	164.308(a)(7)(i)	Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.
Data Backup Plan (R)	164.308(a)(7)(ii)(A)	Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.
Disaster Recovery Plan (R)	164.308(a)(7)(ii)(B)	Establish (and implement as needed) procedures to restore any loss of data.
Emergency Mode Operation Plan (R)	164.308(a)(7)(ii)(C)	Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.
Testing and Revision Procedure (A)	164.308(a)(7)(ii)(D)	Implement procedures for periodic testing and revision of contingency plans.
Applications and Data Criticality Analysis (A)	164.308(a)(7)(ii)(E)	Assess the relative criticality of specific applications and data in support of other contingency plan components.



HIPAA Security Rule Administrative Safeguard Specifications cont.

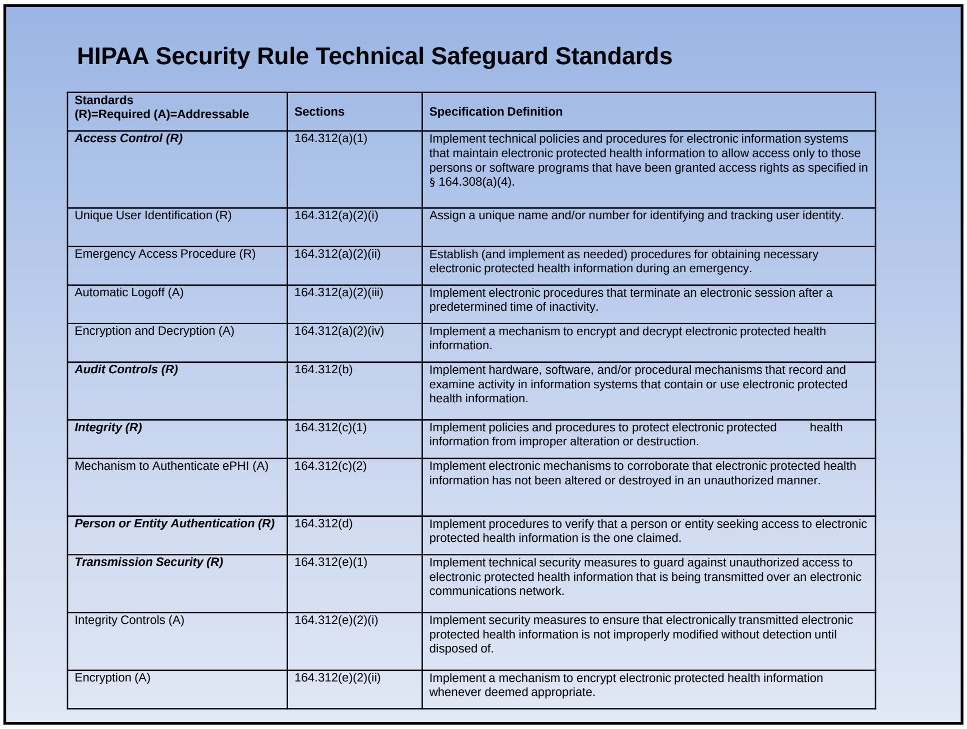
Evaluation (R)	164.308(a)(8)	Perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.
BA Contracts and Other Arrangements (R)	164.308(b)(1)	A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a) that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.
	164.308(b)(2)	A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic protected health information on its behalf only if the business associate obtains satisfactory assurances, in accordance with § 164.314(a), that the subcontractor will appropriately safeguard the information.
Written contract or other arrangement (R)	164.308(b)(3)	Document the satisfactory assurances required by paragraph (b)(1) or (b)(2) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).



HIPAA Security Rule Physical Safeguard Standards

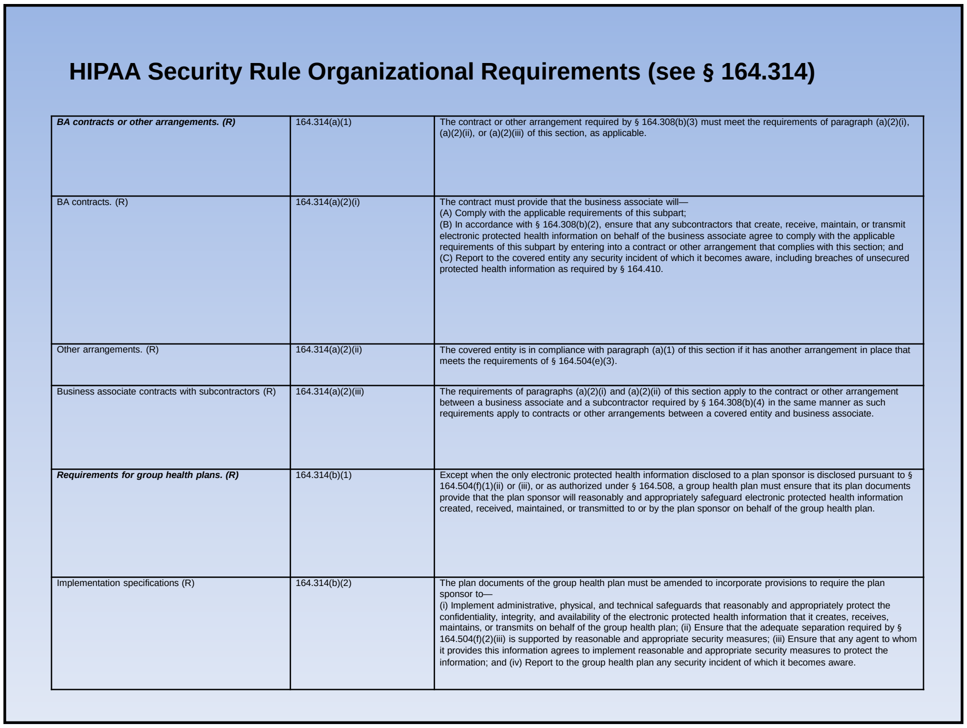
Standards (R)=Required (A)=Addressable	**Sections**	**Specification Definition**
Facility Access Controls	164.310(a)(1)	Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.
Contingency operations (A)	164.310(a)(2)(i)	Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
Facility Security Plan (A)	164.310(a)(2)(ii)	Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
Access Control and Validation Procedures (A)	164.310(a)(2)(iii)	Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.
Maintenance Records (A)	164.310(a)(2)(iv)	Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

Workstation Use (R)	164.310(b)	Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.
Workstation Security (R)	164.310(c)	Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.
Device and Media Controls (R)	164.310(d)(1)	Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.
Disposal (R)	164.310(d)(2)(i)	Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.
Media Re-use (R)	164.310(d)(2)(ii)	Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.
Accountability (A)	164.310(d)(2)(iii)	Maintain a record of the movements of hardware and electronic media and any person responsible therefore.
Data Backup and Storage (A)	164.310(d)(2)(iv)	Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.



HIPAA Security Rule Technical Safeguard Standards

Standards **(R)=Required (A)=Addressable**	**Sections**	**Specification Definition**
Access Control (R)	164.312(a)(1)	Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).
Unique User Identification (R)	164.312(a)(2)(i)	Assign a unique name and/or number for identifying and tracking user identity.
Emergency Access Procedure (R)	164.312(a)(2)(ii)	Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.
Automatic Logoff (A)	164.312(a)(2)(iii)	Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
Encryption and Decryption (A)	164.312(a)(2)(iv)	Implement a mechanism to encrypt and decrypt electronic protected health information.
Audit Controls (R)	164.312(b)	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.
Integrity (R)	164.312(c)(1)	Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.
Mechanism to Authenticate ePHI (A)	164.312(c)(2)	Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.
Person or Entity Authentication (R)	164.312(d)	Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.
Transmission Security (R)	164.312(e)(1)	Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.
Integrity Controls (A)	164.312(e)(2)(i)	Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.
Encryption (A)	164.312(e)(2)(ii)	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.



HIPAA Security Rule Organizational Requirements (see § 164.314)

BA contracts or other arrangements. (R)	164.314(a)(1)	The contract or other arrangement required by § 164.308(b)(3) must meet the requirements of paragraph (a)(2)(i), (a)(2)(ii), or (a)(2)(iii) of this section, as applicable.
BA contracts. (R)	164.314(a)(2)(i)	The contract must provide that the business associate will— (A) Comply with the applicable requirements of this subpart; (B) In accordance with § 164.308(b)(2), ensure that any subcontractors that create, receive, maintain, or transmit electronic protected health information on behalf of the business associate agree to comply with the applicable requirements of this subpart by entering into a contract or other arrangement that complies with this section; and (C) Report to the covered entity any security incident of which it becomes aware, including breaches of unsecured protected health information as required by § 164.410.
Other arrangements. (R)	164.314(a)(2)(ii)	The covered entity is in compliance with paragraph (a)(1) of this section if it has another arrangement in place that meets the requirements of § 164.504(e)(3).
Business associate contracts with subcontractors (R)	164.314(a)(2)(iii)	The requirements of paragraphs (a)(2)(i) and (a)(2)(ii) of this section apply to the contract or other arrangement between a business associate and a subcontractor required by § 164.308(b)(4) in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.
Requirements for group health plans. (R)	164.314(b)(1)	Except when the only electronic protected health information disclosed to a plan sponsor is disclosed pursuant to § 164.504(f)(1)(ii) or (iii), or as authorized under § 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.
Implementation specifications (R)	164.314(b)(2)	The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to— (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; (ii) Ensure that the adequate separation required by § 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures; (iii) Ensure that any agent to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and (iv) Report to the group health plan any security incident of which it becomes aware.

HIPAA Security Rule Policies and Procedures and Documentation Requirements (see § 164.316)

Policies and procedures (R)	164.316(a)	Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in § 164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity or business associate may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.
Documentation (R)	164.316(b)(1)	(i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and (ii) If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.
Time limit (R)	164.316(b)(2)(i)	Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.
Availability (R)	164.316(b)(2)(ii)	Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.
Updates (R)	164.316(b)(2)(iii)	Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.

Note: **Required (R) = Must implement it. Addressable (A) = Implement if reasonable and appropriate (make all attempts possible to do this). If not reasonable and appropriate, document the reason and implement an equivalent alternative measure.**

Thank You !! …and 'good luck'

with your HIPAA compliance initiatives

Jeff Grady, HCISPP, Senior Director
jgrady@threepillarstechnology.com
Three Pillars Technology Solutions
www.threepillarstechnology.com

Three Pillars Technology
Solutions That Work