

Security Risk Assessments

Presented by:

Paul D. Vanchiere, MBA



HIPAA by the numbers



Security First, then Compliance

Data breaches hurt patients, medical practices and businesses. Breach investigations are much more likely to occur than HIPAA audits. Data breaches can turn into expensive lawsuits. Only one federal agency conducts HIPAA audits, while many federal and state agencies enforce data breach penalties. We are focused first on protecting you against data breaches, then on compliance. Contact us for more information.

Black-market Value

\$ 50 per medical record
\$ 1 per credit card number

FBI Health Care Risk Notification, April 2014

Healthcare organizations

81% permit BYOD
personally-owned devices connecting to their networks
but only 21% scan BYOD devices

prior to connection to network
Ponemon survey of healthcare organizations

HIPAA Penalties

\$ 1.5 million
for a lost unencrypted laptop
\$ 1.7 million
for a lost unencrypted laptop
\$ 1.7 million
for a lost unencrypted hard drive

63% of healthcare institutions experienced a **reportable data breach**

Ponemon 2013 Economic & Productivity Impact of IT Security on Healthcare

\$ 188 average cost per breached record

Ponemon 2014 Cost of a Data Breach survey

56% of patients *whose data was breached* **lost trust and confidence in their healthcare provider**

Ponemon 2013 Survey on Medical Identity Theft

700,000 HIPAA Covered Entities
(providers & payers)

2,000,000 – 3,000,000

HIPAA Business Associates

HHS estimates

Only 115 HIPAA Audits

2009 – 2013 (out of 700,000 Covered Entities)

Only 100 per month starting in 2014 (of 3.7 million organizations required to comply with HIPAA)

But...13,000 Data Breach Investigations

HHS Office for Civil Rights

17,000 patient records breached per day, on average

September 2009 to present, HHS.gov

Compliance does not equal security.

Organizations may think they're compliant, but data shows that they are not secure.

2014 SANS Health Care Cyberthreat Report

Health Care 31% of all reported data breaches

EMC/RSA White Paper, 2013

74% are not encrypting data on mobile medical devices

HIMSS Security Survey, sponsored by Experian

Only 43% of healthcare providers have an accurate inventory of employees' and customers' personal data

Worldwidestudy by PwC, CIO Magazine & CSO Magazine

91% of healthcare organizations are **using cloud-based services**

47% are **not confident in the ability to keep data secure** in the cloud

Ponemon survey of 80 healthcare organizations, December 2012

Materials in Presentation

- We will not be reviewing everything “word for word”
- This presentation serves dual purpose
 - Facilitate the presentation / discussion
 - Be retained as a resource for future reference

Today's Agenda

- The specific compliance programs every practice needs to have in place
- Locations of self-paced tools to maintain compliance
- Discussion of third-party resources available to help you ensure compliance

Why are we doing this?

- Federal Law Requirement
- Privacy
 - Ensure all documents are up to date
 - Ensure appropriate training in place
- Security
 - Make sure your network is secure
 - Mitigate risks
 - Identify vulnerabilities
- Breaches
 - Documented process for reporting
 - Comply with notice requirements

Where are we headed?



The screenshot shows the HealthITSecurity website. The header includes the logo "HealthITSecurity" with the tagline "News and Resources for HealthIT Security Pros" and navigation links for "Home" and "News". A secondary navigation bar lists categories: "HIPAA and Compliance", "EHR Security", "HIE Security", "Mobile Security", "Data Breaches", and "C". The main article title is "Final ONC Roadmap Highlights Health Data Privacy, Security" by Elizabeth Snell on October 08, 2015. The article text states: "The Department of Health and Human Services (HHS) Office of the National Coordinator for Health IT (ONC) released the final version of its interoperability roadmap earlier this week, discussing the importance of health data privacy throughout the push for greater health information exchange." A quote from the executive summary reads: "If we steadily and aggressively advance our progress we can make it a reality," states the executive summary. "We must focus our collective efforts around making standardized, electronic health information securely available to those who need it and in ways that maximize the ease with which it can be useful and used." A "RELATED ARTICLES" section is partially visible with the title "Are Views on Consent Unclear with Health Data Sharing?".

- *2015-2017: Send, receive, find and use priority data domains to improve healthcare quality and outcomes.*
- *2018-2020: Expand data sources and users in the interoperable health IT ecosystem to improve health and lower costs.*
- *2021-2024: learning health system, with the person at the center of a system that can continuously improve care, public health, and science through real-time data access*

<http://healthitsecurity.com/news/final-onc-roadmap-highlights-health-data-privacy-security>

PediatricSupport.com



Helping Pediatricians Succeed

It's not just about credit cards anymore....

- Medical identity theft is often not immediately identified by a patient or their provider, giving criminals years to milk such credentials. That makes medical data more valuable than credit cards, which tend to be quickly canceled by banks once fraud is detected.
- Healthcare providers and insurers must publicly disclose data breaches affecting more than 500 people, but there are no laws requiring criminal prosecution. As a result, the total cost of cyber attacks on the healthcare system is difficult to pin down



Dangerous Little Kitty....

- 8 GB Capacity
 - >7,700 Pictures
 - >3,850 PowerPoints
 - >15,400 Word Documents
 - >61,600 Excel Spreadsheets
 - >14 Hours of Video
- 11-Provider practice
 - 7 Years of financial data and patient demographics
 - Approximately 215MB
 - Kitty can hold at least 32 copies
- \$14.99 @ Fry's Electronics



Value of Your Data....

	Price
Social Security number	\$ 30.00
Date of birth	\$ 11.00
Health insurance credentials	\$ 20.00
	\$ 61.00
Visa or MasterCard credentials	\$ 4.00
American Express credentials	\$ 7.00
Discover credit credentials	\$ 8.00
Credit card with magnetic stripe or chip data	\$ 12.00

Like Pediatrics,
Volume is the Key...
\$61 X 4,000 Patients
=
\$244,000

<http://www.bankrate.com/finance/credit/what-your-identity-is-worth-on-black-market.aspx>

Types of Violations

- Not wiping hard drives before disposing computers
- Not wiping photo copier memory
- Unencrypted hard drives lost
- USB hard drives not encrypted and lost
- Backup tapes gone missing
- Gmail and internet-based calendars
- Poor training
- Stolen laptops & cell phones
- Leaving patient chart on screen between patients
- Sharing log in credentials
- Employee looking up family info via hospital portal

Source of Violations

- Unencrypted Data
 - Don't have to report losses on encrypted drives
 - Windows Profession (Bit Locker)
 - XP should be gone
- Employee Error
 - Social Media Posting
 - Social Events
 - Wrong fax numbers / emails
 - Gmail, Hotmail & Yahoo mail
- Portable Devices
 - Phones
 - Tablets
 - Laptops
- Business Associates
 - Two-thirds of data breaches involve BA's
 - Make sure they are compliant!



Consequences are terrible


- Personal / Practice financial liability
- Fines run several hundred thousand dollars to \$1.5 million
- Community confidence lost
- Reputation / Credibility
- Public Notification

Publicity ain't always good....

As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals.

U.S. Department of Health and Human Services
Office for Civil Rights
Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information

Welcome | File a Breach | HHS | Office for Civil Rights | Contact Us



Breaches Affecting 500 or More Individuals

As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. These breaches are now posted in a new, more accessible format that allows users to search and sort the posted breaches. Additionally, this new format includes brief summaries of the breach cases that OCR has investigated and closed, as well as the names of private practice providers who have reported breaches of unsecured protected health information to the Secretary. The following breaches have been reported to the Secretary:

[Show Advanced Options](#)

Breach Report Results							
Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information	
Democracy Data & Communications, LLC (VA	Business Associate	83000	12/08/2009	Other	Paper/Films	
Health Behavior Innovations (HBI)	UT	Business Associate	5700	02/05/2010	Theft	Other	
Wyoming Department of Health	WY	Health Plan	9023	03/02/2010		Network Server	
Thrivent Financial for Lutherans	WI	Health Plan	9500	03/03/2010	Theft	Laptop	
Laboratory Corporation of America/Dynacare Northwest, Inc.	WA	Healthcare Provider	5080	03/18/2010	Theft	Laptop	
Tomah Memorial Hospital	WI	Healthcare Provider	600	04/16/2010	Other	Other	
TOWERS WATSON	VA	Business Associate	1874	04/27/2010	Theft	Other	
Rockbridge Area Community Services	VA	Healthcare Provider	500	04/29/2010	Theft	Desktop Computer, Laptop	
(see explanation below)		Business Associate	5220	05/24/2010	Loss	Other	
Prince William County Community Services (CS)	VA	Healthcare Provider	669	07/15/2010	Theft	Other Portable Electronic Device	
Mercer		Business Associate	1073	07/30/2010	Loss	Other	
Ward A. Morris, DDS	WA	Healthcare Provider	2698	08/11/2010	Theft	Desktop Computer	
Curtis R. Bryan, M.D.	VA	Healthcare Provider	2739	09/08/2010	Theft	Laptop	
Utah Department of Workforce Services	UT	Business Associate	1298	10/13/2010	Other	Desktop Computer, Paper/Films	
SW Seattle Orthopaedic and Sports Medicine	WA	Healthcare Provider	9493	10/15/2010	Hacking/IT Incident	Network Server	

What is OCR Saying?

Breach Report Results						
Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
Grays Harbor Pediatrics, PLLC	WA	Healthcare Provider	12009	01/21/2011	Theft	Other, Other Portable Electronic Device
Pediatric Sports and Spine Associates	TX	Healthcare Provider	955	04/09/2010	Theft	Laptop

Business Associate Present: No

Web Description: An unencrypted laptop was stolen from an employee's vehicle. The laptop contained the protected health information of approximately 955 individuals. The protected health information involved in the breach included names, addresses, dates of birth, social security numbers, diagnoses, medications and other treatment information. Following the discovery of the breach, the covered entity revised policies, retrained staff and implemented additional physical and technical safeguards including encryption software. The covered entity also removed the stolen laptop's access to the server, sanctioned the involved employee, notified the affected individuals and notified the local media.

1. An unencrypted laptop was stolen from an employee's vehicle.
2. The laptop contained the protected health information of approximately 955 individuals.
3. The protected health information involved in the breach included names, addresses, dates of birth, social security numbers, diagnoses, medications and other treatment information.
4. Following the discovery of the breach, the covered entity revised policies, retrained staff and implemented additional physical and technical safeguards including encryption software.
5. The covered entity also removed the stolen laptop's access to the server, sanctioned the involved employee, notified the affected individuals and notified the local media.

Search Capabilities of OCR Online Reporting System

Breach Submission Date: From: To:

Type of Breach:

<input type="checkbox"/> Hacking/IT Incident	<input type="checkbox"/> Improper Disposal	<input type="checkbox"/> Loss
<input type="checkbox"/> Theft	<input type="checkbox"/> Unauthorized Access/Disclosure	<input type="checkbox"/> Unknown
<input type="checkbox"/> Other		

Location of Breach:

<input type="checkbox"/> Desktop Computer	<input type="checkbox"/> Electronic Medical Record	<input type="checkbox"/> Email
<input type="checkbox"/> Laptop	<input type="checkbox"/> Network Server	<input type="checkbox"/> Other Portable Electronic Device
<input type="checkbox"/> Paper/Films	<input type="checkbox"/> Other	

Type of Covered Entity:

State:

Business Associate Present?:

Description Search:

CE / BA Name Search:

Sample of Breaches > 500 Patients

Breach Report Results

Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
Grays Harbor Pediatrics, PLLC	WA	Healthcare Provider	12009	01/21/2011	Theft	Other, Other Portable Electronic Device
Pediatric Sports and Spine Associates	TX	Healthcare Provider	955	04/09/2010	Theft	Laptop
Good Care Pediatric, LLP	NY	Healthcare Provider	2300	11/12/2015	Hacking/IT Incident	Desktop Computer
Adult & Pediatric Dermatology, PC	MA	Healthcare Provider	2200	10/07/2011	Theft	Other, Other Portable Electronic Device
Pediatric Group LLC	IL	Healthcare Provider	10000	08/21/2015	Hacking/IT Incident	Network Server
Barrington Orthopedic Specialists, Ltd	IL	Healthcare Provider	1009	09/24/2015	Theft	Laptop, Other
Pediatric and Adult Allergy, PC	IA	Healthcare Provider	19222	09/11/2010	Loss	Other Portable Electronic Device
Bulloch Pediatric Group, LLC	GA	Healthcare Provider	10000	09/04/2014	Unauthorized Access/Disclosure	Paper/Films
Pediatric Associates	FL	Healthcare Provider	627	03/24/2015	Loss	Paper/Films
Pediatric Gastroenterology, Hepatology & Nutrition of Florida, P.A.	FL	Healthcare Provider	13000	08/24/2015	Theft	Paper/Films
Pediatric Gastroenterology Consultants	CO	Healthcare Provider	5000	12/19/2014	Theft	Laptop
Center for Orthopedic Research and Education, Inc.	AZ	Healthcare Provider	35488	12/21/2012	Theft	Paper/Films
Alaska Orthopedic Specialists, Inc.	AK	Healthcare Provider	553	11/19/2015	Theft	Email

(Displaying 1 - 13 of 13)

Breach Report Results

Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
Children's Medical Clinics of East Texas	TX	Healthcare Provider	16000	10/28/2015	Unauthorized Access/Disclosure	Desktop Computer
M&C Children's Clinic PA	TX			03/19/2013		
Children's Medical Center of Dallas	TX	Healthcare Provider	3800	01/18/2010	Loss	Other, Other Portable Electronic Device
Texas Children's Hospital	TX	Healthcare Provider	694	07/30/2010	Theft	Laptop
Children's Medical Center of Dallas	TX	Healthcare Provider	2462	07/10/2013	Theft	Laptop
St. Jude Children's Research Hospital	TN	Healthcare Provider	1745	06/08/2010	Loss	Laptop
The Children's Hospital of Philadelphia	PA	Healthcare Provider	943	11/24/2009	Theft	Laptop
The Children's Medical Center of Dayton	OH	Healthcare Provider	1001	06/14/2010	Other	Email
Children's Hospital Medical Center of Akron	OH	Healthcare Provider	7664	08/26/2015	Loss	Other Portable Electronic Device
Cincinnati Children's Hospital Medical Center	OH	Healthcare Provider	60998	06/01/2010	Theft	Laptop
St. Mary's Hospital for Children	NY	Business Associate	550	05/19/2011	Theft	Paper/Films
Children's Heart Center	NV	Healthcare Provider	8791	04/03/2015	Unauthorized Access/Disclosure	Electronic Medical Record
Children's Mercy Hospital	MO		4067	08/15/2014	Hacking/IT Incident	Network Server
Children's Hospital Boston	MA	Healthcare Provider	2159	05/22/2012	Theft	Laptop
Florida Department of Health, Children's Medical Services	FL	Healthcare Provider	500	10/23/2015	Unauthorized Access/Disclosure	Paper/Films
Children's National Medical Center	DC	Healthcare Provider	18000	02/24/2015	Hacking/IT Incident	Email
Health Services for Children with Special Needs, Inc.	DC	Health Plan	3800	11/17/2009	Loss	Laptop
Lucille Packard Children's Hospital	CA	Healthcare Provider	532	02/21/2010	Other	Desktop Computer
Children's Eyewear Sight	CA	Healthcare Provider	1030	01/12/2015	Theft	Desktop Computer
Rady Children's Hospital - San Diego	CA	Healthcare Provider	6307	06/25/2014	Unauthorized Access/Disclosure	Email, Other
Rady Children's Hospital - San Diego	CA	Healthcare Provider	14121	06/24/2014	Unauthorized Access/Disclosure	Email
Lucille Packard Children's Hospital	CA	Healthcare Provider	12900	06/13/2013	Theft	Laptop
Children's Hospital & Research Center at Oakland	CA	Healthcare Provider	1000	06/29/2010	Other	Paper/Films
StanfordSchoolMedicine& LP Children Hosp, Privacy Manager Breach	CA			01/23/2013		

(Displaying 1 - 24 of 24)

Notice Requirements

- The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.
 - Individual Notice
 - Media Notice (>500)
 - Notice to Secretary of HHS

Individual Notice

1. Covered entities must notify affected individuals following the discovery of a breach of unsecured protected health information.
2. Covered entities must provide this individual notice in written form by **first-class mail**, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically.
3. If the covered entity has insufficient or out-of-date contact information for **10 or more individuals**, the covered entity must provide substitute individual notice by either **posting the notice on the home page of its web site for at least 90 days** or by providing the notice in major print or broadcast media where the affected individuals likely reside.
4. The covered entity must include a **toll-free phone number** that remains active for at least 90 days where individuals can learn if their information was involved in the breach.
5. If the covered entity has insufficient or out-of-date contact information for fewer than 10 individuals, the covered entity may provide substitute notice by an alternative form of written notice, by telephone, or other means.

Source: <http://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html>

PediatricSupport.com



Helping Pediatricians Succeed

Media Notice

1. Covered entities that experience a breach affecting more than **500 residents** of a State or jurisdiction are, in addition to notifying the affected individuals, required to **provide notice to prominent media outlets** serving the State or jurisdiction.
2. Covered entities will likely provide this notification in the form of a **press release to appropriate media outlets** serving the affected area.
3. Like individual notice, this media notification must be provided without unreasonable delay and in no case later than **60 days** following the discovery of a breach and must include the same information required for the individual notice.

California State Law: 5 Days to Report instead of Federally mandated 60

Source: <http://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html>

PediatricSupport.com



Helping Pediatricians Succeed

Notice to Secretary of HHS

1. In addition to notifying affected individuals and the media (where appropriate), covered entities **must notify the Secretary of breaches of unsecured protected health information.**
2. Covered entities will notify the Secretary by visiting the HHS web site and [filling out and electronically submitting a breach report form.](#)
3. If a breach affects 500 or more individuals, covered entities must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach.
4. If, however, a breach affects fewer than 500 individuals, the covered entity may notify the Secretary of such breaches on an annual basis.
5. Reports of breaches affecting **fewer than 500 individuals** are due to the Secretary no later than **60 days after the end of the calendar year** in which the breaches are discovered.

Source: <http://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html>

PediatricSupport.com



Helping Pediatricians Succeed

Penalty / Fine Levels

- **Unknowning.** The covered entity or business associate did not know, and reasonably should not have known, of the violation.
- **Reasonable cause.** The covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission was a violation—but the covered entity or business associate didn't act with willful neglect.
- **Willful neglect, corrected.** The violation was the result of conscious, intentional failure or reckless indifference to fulfill the obligation to comply with HIPAA. However, the covered entity or business associate corrected the violation within 30 days of discovery.
- **Willful neglect, uncorrected.** The violation was the result of conscious, intentional failure or reckless indifference to fulfill the obligation to comply with HIPAA, and the covered entity or business associate did not correct the violation within 30 days of discovery.

Source: Moss Adams CPS- <http://www.mossadams.com/articles/2014/october/new-hipaa-compliance-requirements#sthash.Xz7M157b.dpuf>

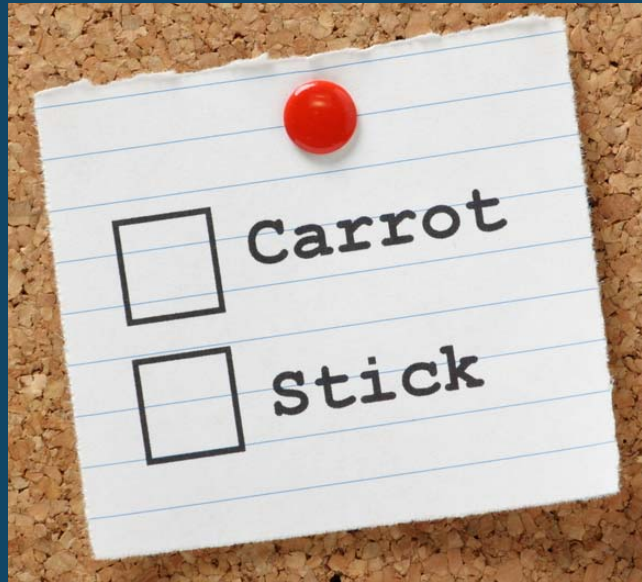


Penalty Guidelines

Violation	Amount per violation	Violations of an identical provision in a calendar year
Did Not Know	\$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	\$50,000	\$1,500,000

Source: Federal Register

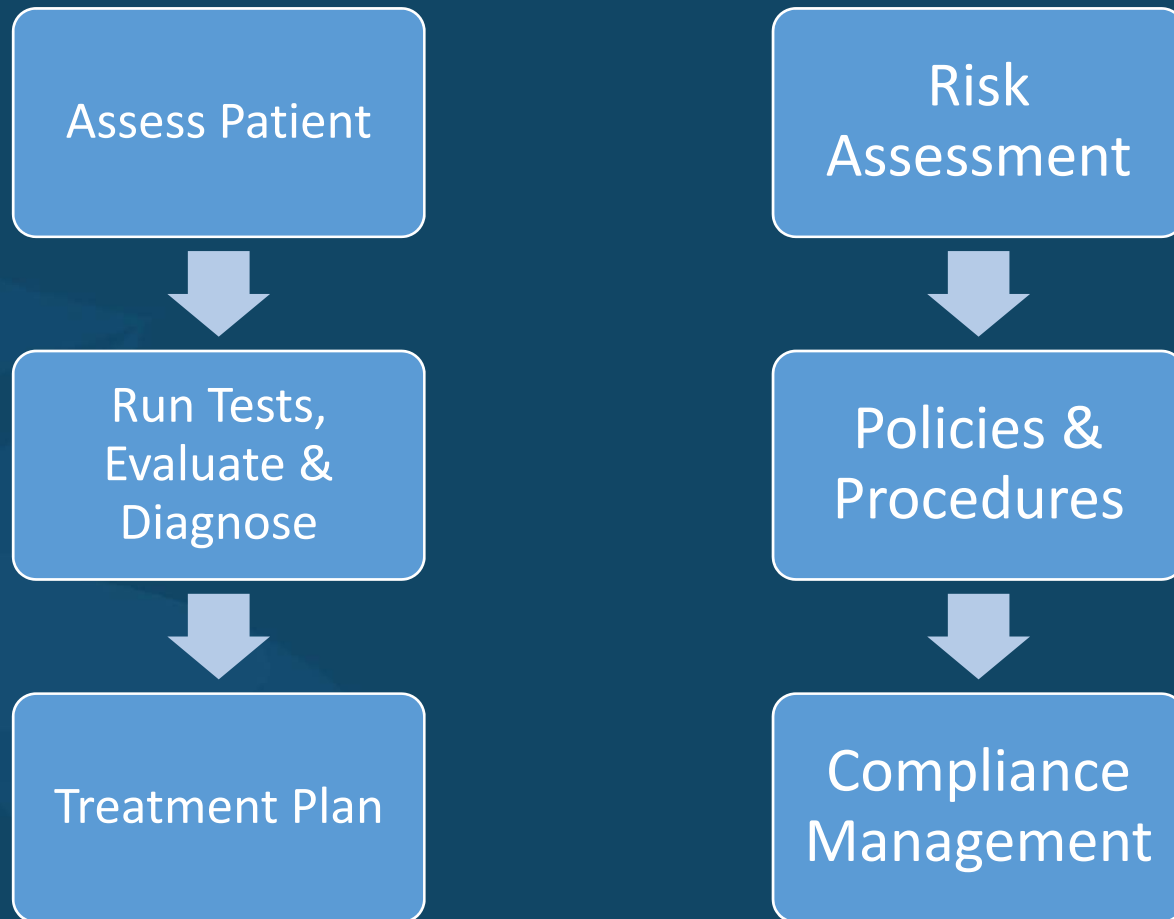
<https://www.federalregister.gov/articles/2013/01/25/2013-01073/modifications-to-the-hipaa-privacy-security-enforcement-and-breach-notification-rules-under-the#h-95>



	Carrot	Stick
Privacy	Right thing to do	Fines & Penalties
Security	Adopt best practices	Fines & Penalties
Risk Mitigation	Keep your data secure	Fines & Penalties
Data Breach Management	Maintain the trust of patients	Fines, Penalties & Notifications

Only you can weigh your appetite for risk with the potential consequences

What to Do to Ensure HIPAA Compliance?



Bare Minimum Compliance

- Risk Assessment Report
 - Self-Answered Questions
 - Interviews
 - Observations
 - Policy & Procedures Manual
 - Employee Meeting

Minimum Compliance is Not Enough

The screenshot shows the Modern Healthcare website interface. At the top left is the logo 'Modern Healthcare' with the tagline 'The leader in healthcare business news, research & data'. To the right is a search bar and a 'My account' link with a gear icon. Below the header is a navigation menu with categories: Providers, Insurance, Government, Finance, Technology, Safety & Quality, and People. The main content area shows a breadcrumb trail: Home > Technology > Healthcare Information Technology. Below this are social media sharing icons. The article title is 'New HIPAA audits will target healthcare industry's business partners'. The author is 'By Joseph Conn | March 21, 2016'. The article text begins with 'A new round of federal privacy and security audits will target the business associates of healthcare providers, insurers and other HIPAA-covered entities along with the entities themselves, according to the Office for Civil Rights at HHS.' A 'RELATED CONTENT' section lists 'Feinstein Institute, North Memorial Health Care to pay nearly \$5.5M for HIPAA violations'. At the bottom of the article, it mentions 'The health IT sections of the American Recovery and Reinvestment Act of 2009'.

According to a 2013 report by the OCR, two-thirds of the entities audited...lacked complete and accurate risk assessments

<http://www.modernhealthcare.com/article/20160321/NEWS/160329977/new-hipaa-audits-will-target-healthcare-industrys-business-partners>

PediatricSupport.com



Helping Pediatricians Succeed

Elements of Appropriate Compliance

- Evidence of HIPAA Compliance
- HIPAA Management Plan
- HIPAA Policies & Procedures
- HIPAA Risk Analysis
- Computer System Inventory
 - Computer Type & OS
 - Drive Encryption Status
 - Login History
- User Identification Worksheet
- Internal Network Scan
- External Network Scan
- Security Breach Tracking Process
- Forms
 - Privacy Notices
 - Release Authorizations
 - Complaint Form
 - Communication Consent
 - PHI restriction / disclosure
 - Breach Response Plan

What to Expect With HIPAA Compliance Process

- 169 Questions Minimum
 - Privacy
 - Security
 - Breaches
- Employee training (staff meeting or online training)
- Spend 2 -3 hours on initial assessment
- Each month spend an hour reviewing management plan
- Each subsequent year redo network scans
- Using third party will save as many as 15 hours of time

Components of HIPAA Regulations

- Made up of 2 Sets of Regulations
 - Portability & Accountability Act (August 21, 1996)
 - HITECH Act (February 17, 2009)
- HIPAA Trilogy/Trinity
 - Privacy Rule (October 16, 2003)
 - Security Rule (April 20, 2005)
 - Omnibus Final Rule (January 25, 2013)
- Regulations apply to all medical entities and companies who work with them.
 - Anyone who MAY come in contact with patient healthcare information

HIPAA Protects...

- Protected Health Information (PHI)
 - Identifiers
 - Treatment
 - Diagnoses
 - Payment Information
- Electronic Protected Health Information
 - Written Documents
 - Images
 - Audio files

Security Rule Requirements

- Guidelines designed to prevent data breaches
 - Very little guidance
 - A lot of ambiguity
 - Reliance on practices implementing “Best Practices” or “Industry Standards”
- Risk Assessment
 - Inventory location(s) of all ePHI
 - Tracking movement of ePHI within the organization
 - Identify possible lapse(s) in IT security
 - Weigh likelihood of an adverse event occurring with the impact of such event.

Security Rule Requirements

- Risk Management
 - Eliminate the Risk
 - Avoid the Risk
 - Minimize the effect of the Risk
- File-sharing Programs on Computers- Eliminate the Risk
- Thumb Drives- Avoid the risk
- Email Systems- Minimize the effect

Security Rule Safeguards

- Technical
 - Access Control
 - Audit Controls
 - Integrity
 - Authentication
 - Transmission Security
- Physical
 - Facility Access Controls
 - Workstation Use
 - Workstation Security
 - Device & Media Controls
- Administrative
 - Security Management Process
 - Assigned Security Responsibility
 - Workforce Security
 - Information Access Management
 - Security Awareness & Training
 - Contingency Plan
 - Evaluation
 - Business Associate Contracts

PediatricSupport.com



Helping Pediatricians Succeed

Addressable vs. Required (Actual Text)

The screenshot shows the HHS.gov website with the following elements:

- Header: HHS.gov logo, U.S. Department of Health & Human Services, and a search icon.
- Section: Health Information Privacy
- Navigation: HIPAA for Individuals, Filing a Complaint (selected), HIPAA for Professionals, Newsroom.
- Left Sidebar (Table of Contents):

Authorizations (30)
Business Associates (33)
Compliance Dates (5)
Covered Entities (16)
Decedents (8)
Disclosures for Law Enforcement Purposes (7)
Disclosures for Rule Enforcement (2)
Disclosures in Emergency Situations (2)
Disclosures Required by Law (6)
Disclosures to Family and Friends (27)
Disposal of Protected Health Information (6)
Facility Directories (6)
Family Medical History Information (3)
FERPA and HIPAA (10)
Group Health Plans (2)
Health Information Technology (35)
- Main Content:

What is the difference between addressable and required implementation specifications in the Security Rule?

Answer:

If an implementation specification is described as "required," the specification must be implemented. The concept of "addressable implementation specifications" was developed to provide covered entities additional flexibility with respect to compliance with the security standards. In meeting standards that contain addressable implementation specifications, a covered entity will do one of the following for each addressable specification: (a) implement the addressable implementation specifications; (b) implement one or more alternative security measures to accomplish the same purpose; (c) not implement either an addressable implementation specification or an alternative. The covered entity's choice must be documented. The covered entity must decide whether a given addressable implementation specification is a reasonable and appropriate security measure to apply within its particular security framework. For example, a covered entity must implement an addressable implementation specification if it is reasonable and appropriate to do so, and must implement an equivalent alternative if the addressable implementation specification is unreasonable and inappropriate, and there is a reasonable and appropriate alternative. This decision will depend on a variety of factors, such as, among others, the entity's risk analysis, risk mitigation strategy, what security measures are already in place, and the cost of implementation. The decisions that a covered entity makes regarding addressable specifications must be documented in writing. The written documentation should include the factors considered as well as the results of the risk assessment on which the decision was based.
- Footer: Text Resize A A A, Print, Share (Facebook, Twitter, +).

Source: <http://www.hhs.gov/hipaa/for-professionals/faq/2020/what-is-the-difference-between-addressable-and-required-implementation-specifications/index.html>

Addressable vs. Required (Breakdown)

- If an implementation specification is described as “required,” the specification must be implemented.
- The concept of "addressable implementation specifications" was developed to provide covered entities additional flexibility with respect to compliance with the security standards.
- In meeting standards that contain addressable implementation specifications, a covered entity will do one of the following for each addressable specification:
 - (a) implement the addressable implementation specifications;
 - (b) implement one or more alternative security measures to accomplish the same purpose;
 - (c) not implement either an addressable implementation specification or an alternative.
- The covered entity’s choice must be documented. The covered entity must decide whether a given addressable implementation specification is a reasonable and appropriate security measure to apply within its particular security framework.

Source: <http://www.hhs.gov/hipaa/for-professionals/faq/2020/what-is-the-difference-between-addressable-and-required-implementation-specifications/index.html>

PediatricSupport.com



Helping Pediatricians Succeed

Technical Safeguards Implementation

Standard	Action Item	Status	Implementation
Access Control	Unique User Identification	Required	Assign a unique name and/or number for identifying and tracking user identity.
Access Control	Emergency Access Procedure	Required	Establish and implement (as needed) procedures for obtaining necessary ePHI during an emergency.
Access Control	Automatic Logoff	Addressable	Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
Access Control	Encryption and Decryption	Addressable	Implement a mechanism to encrypt and decrypt ePHI.
Audit Control		Required	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.
Integrity	Mechanism to Authenticate ePHI	Addressable	Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.
Authentication		Required	Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.
Transmission Security	Integrity Controls	Addressable	Implement security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of.
Transmission Security	Encryption	Addressable	Implement a mechanism to encrypt ePHI whenever deemed appropriate.

Source: <https://www.truevault.com/blog/how-do-i-become-hipaa-compliant.html>

Physical Safeguards Implementation

Part 1 of 2

Standard	Action Item	Status	Implementation
Facility Access Controls	Contingency Operations	Addressable	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 Access Controls	Facility Security Plan	Addressable	Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
Facility Access Controls	Access Control and Validation Procedures	Addressable	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.
Facility Access Controls	Maintenance Records	Addressable	Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security e.g. hardware, walls, doors, and locks).
Workstation Use		Required	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 ePHI.

Source: <https://www.truevault.com/blog/how-do-i-become-hipaa-compliant.html>

PediatricSupport.com



Helping Pediatricians Succeed

Physical Safeguards Implementation

Part 2 of 2

Standard	Action Item	Status	Implementation
Workstation Security		Required	Implement physical safeguards for all workstations that access ePHI, to restrict access to authorized users.
Device and Media Controls	Disposal	Required	Implement policies and procedures to address the final disposition of ePHI, and/or the hardware or electronic media on which it is stored.
Device and Media Controls	Media Re-Use	Required	Implement procedures for removal of ePHI from electronic media before the media are made available for re-use
Device and Media Controls	Accountability	Addressable	Maintain a record of the movements of hardware and electronic media and any person responsible therefore.
Device and Media Controls	Data Backup and Storage	Addressable	Create a retrievable, exact copy of ePHI, when needed, before movement of equipment.

Source: <https://www.truevault.com/blog/how-do-i-become-hipaa-compliant.html>

PediatricSupport.com



Helping Pediatricians Succeed

Administrative Safeguards Implementation

Part 1 of 3

Standard	Action Item	Status	Implementation
Security Management Process	Risk Analysis	Required	Perform and document a risk analysis to see where PHI is being used and stored in order to determine all the ways that HIPAA could be violated.
Security Management Process	Risk Management	Required	Implement sufficient measures to reduce these risks to an appropriate level.
Security Management Process	Sanction Policy	Required	Implement sanction policies for employees who fail to comply.
Security Management Process	Information Systems Activity Reviews	Required	Regularly review system activity, logs, audit trails, etc.
Assigned Security Responsibility	Officers	Required	Designate HIPAA Security and Privacy Officers.

Source: <https://www.truevault.com/blog/how-do-i-become-hipaa-compliant.html>

PediatricSupport.com



Helping Pediatricians Succeed

Administrative Safeguards Implementation

Part 2 of 3

Standard	Action Item	Status	Implementation
Workforce Security	Employee Oversight	Addressable	Implement procedures to authorize and supervise employees who work with PHI, and for granting and removing PHI access to employees. Ensure that an employee's access to PHI ends with termination of employment.
Information Access Management	Multiple Organizations	Required	Ensure that PHI is not accessed by parent or partner organizations or subcontractors that are not authorized for access.
Information Access Management	ePHI Access	Addressable	Implement procedures for granting access to ePHI that document access to ePHI or to services and systems that grant access to ePHI.
Security Awareness and Training	Security Reminders	Addressable	Periodically send updates and reminders about security and privacy policies to employees.
Security Awareness and Training	Protection Against Malware	Addressable	Have procedures for guarding against, detecting, and reporting malicious software.
Security Awareness and Training	Login Monitoring	Addressable	Institute monitoring of logins to systems and reporting of discrepancies.

Source: <https://www.truevault.com/blog/how-do-i-become-hipaa-compliant.html>

PediatricSupport.com



Helping Pediatricians Succeed

Administrative Safeguards Implementation

Part 3 of 3

Standard	Action Item	Status	Implementation
Security Awareness and Training	Password Management	Addressable	Ensure that there are procedures for creating, changing, and protecting passwords.
Security Incident Procedures	Response and Reporting	Required	Identify, document, and respond to security incidents.
Contingency Plan	Contingency Plans	Required	Ensure that there are accessible backups of ePHI and that there are procedures for restore any lost data.
Contingency Plan	Contingency Plans Updates and Analysis	Addressable	Have procedures for periodic testing and revision of contingency plans. Assess the relative criticality of specific applications and data in support of other contingency plan components.
Contingency Plan	Emergency Mode	Required	Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode.
Evaluations		Required	Perform periodic evaluations to see if any changes in your business or the law require changes to your HIPAA compliance procedures.
Business Associate Agreements		Required	Have special contracts with business partners who will have access to your PHI in order to ensure that they will be compliant. Choose partners that have similar agreements with any of their partners to which they are also extending access.

Source: <https://www.truevault.com/blog/how-do-i-become-hipaa-compliant.html>

PediatricSupport.com



Helping Pediatricians Succeed

Business Associates Under Scrutiny

The screenshot shows the Modern Healthcare website interface. At the top, there's a navigation bar with 'Opinion & Editorial' and 'Research & Data C'. The main header features the 'Modern Healthcare' logo and the tagline 'The leader in healthcare business news, research & data'. A search bar is present with the text 'Search Modern Healthcare'. Below the header is a menu with categories: Providers, Insurance, Government, Finance, Technology, Safety & Quality, and People. The article breadcrumb is 'Home > Technology > Healthcare Information Technology'. The article title is 'Wider HIPAA audits may drive stronger vendor contracts' by Joseph Conn, dated March 23, 2016. The article text discusses the volume of patient data handled by vendors and the role of analytics and mobile devices. A quote from David is also visible: 'There are so many people who are doing innovations and startups and want to get into healthcare and are unaware of the rules and regulations,' said David. A 'RELATED CONTENT' section lists other articles: 'HIPAA hurdles: New rules pose complex challenges for providers', 'Feinstein Institute, North Memorial Health Care to pay nearly \$5.5M for HIPAA violations', and 'HIPAA rule change part of move to fight gun violence'.

- *Of the 1,472 major healthcare data breaches on the OCR's "wall of shame" website, 309 (21%) involved a business associate.*
- *Those breaches exposed 32.8 million individuals' records.*

<http://www.modernhealthcare.com/article/20160323/NEWS/160329942/wider-hipaa-audits-may-drive-stronger-vendor-contracts>

PediatricSupport.com



Helping Pediatricians Succeed

OCR to Step up BA Audits

- *HHS' Office for Civil Rights has started sending out e-mails to obtain and verify contact information for covered entities and business associates of various types for possible inclusion in the pool of potential audit subjects.*
- *...the 2009 stimulus law placed the businesses that do data handling, processing and analysis in healthcare on the same legal footing as the hospitals, physicians, insurance companies and claims clearinghouses they work for.*

The screenshot shows the Modern Healthcare website interface. At the top, there is a navigation bar with links for 'Opinion & Editorial' and 'Research & Data C'. The main header features the 'Modern Healthcare' logo and the tagline 'The leader in healthcare business news, research & data'. A search bar is located on the right side of the header. Below the header is a secondary navigation bar with categories: 'Providers', 'Insurance', 'Government', 'Finance', 'Technology', 'Safety & Quality', and 'People'. The main content area displays the article title 'New HIPAA audits will target healthcare industry's business partners' by Joseph Conn, dated March 21, 2016. The article text states: 'A new round of federal privacy and security audits will target the business associates of healthcare providers, insurers and other HIPAA-covered entities along with the entities themselves, according to the Office for Civil Rights at HHS. HHS' Office for Civil Rights has started sending out e-mails to obtain and verify contact information for covered entities and business associates of various types for possible inclusion in the pool of potential audit subjects. The health IT sections of the American Recovery and Reinvestment Act of 2009'. A 'RELATED CONTENT' section is visible on the left, featuring a link to 'Feinstein Institute, North Memorial Health Care to pay nearly \$5.5M for HIPAA violations'.

<http://www.modernhealthcare.com/article/20160321/NEWS/160329977/new-hipaa-audits-will-target-healthcare-industrys-business-partners>

PediatricSupport.com



Helping Pediatricians Succeed

Choose your Business Associates Wisely

- HIPAA-Compliant

- Must comply with the Security Rule with regard to electronic PHI
- Must report breaches of unsecured PHI to covered entities
- Must require that any subcontractors agree to the same restrictions and conditions that apply to the business associate
- Must comply with the same requirements of the Privacy Rule that apply to the covered entity

- HIPAA-Certified

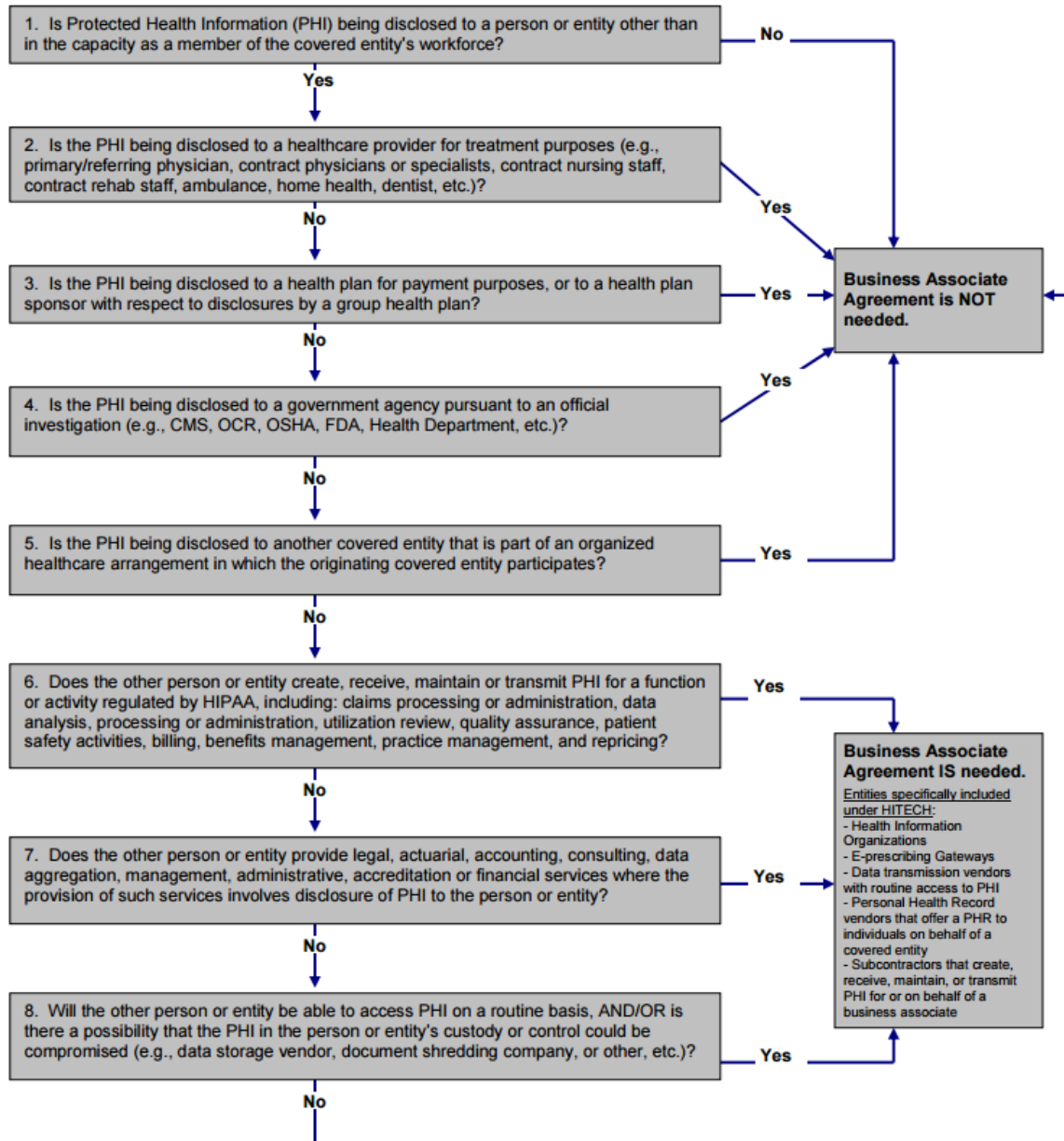
- OCR & HHS does NOT certify any product, person or company as “HIPAA-Certified”

Source: Moss Adams CPS- <http://www.mossadams.com/articles/2014/october/new-hipaa-compliance-requirements#sthash.XnTUHEtb.dpuf>

Who has to comply with HIPAA?

- Covered Entities
 - Medical Practices
 - Hospitals
 - Clearinghouses
- Business Associates & Subcontractors
 - IT Service Providers
 - Shredding Companies
 - Document storage companies
 - Attorneys
 - Accountants
 - Collection Agencies
 - Consultants
 - Data Centers / Cloud Storage Companies
 - The guy who cleans your fish tank...

**HIPAA/HITECH
Business Associate Decision Tree**



Source:
http://www.wedi.org/forms/uploadFiles/35FE700000DC.filename.7.26_BA-Decision-Tree_V2.pdf



Helping Pediatricians Succeed

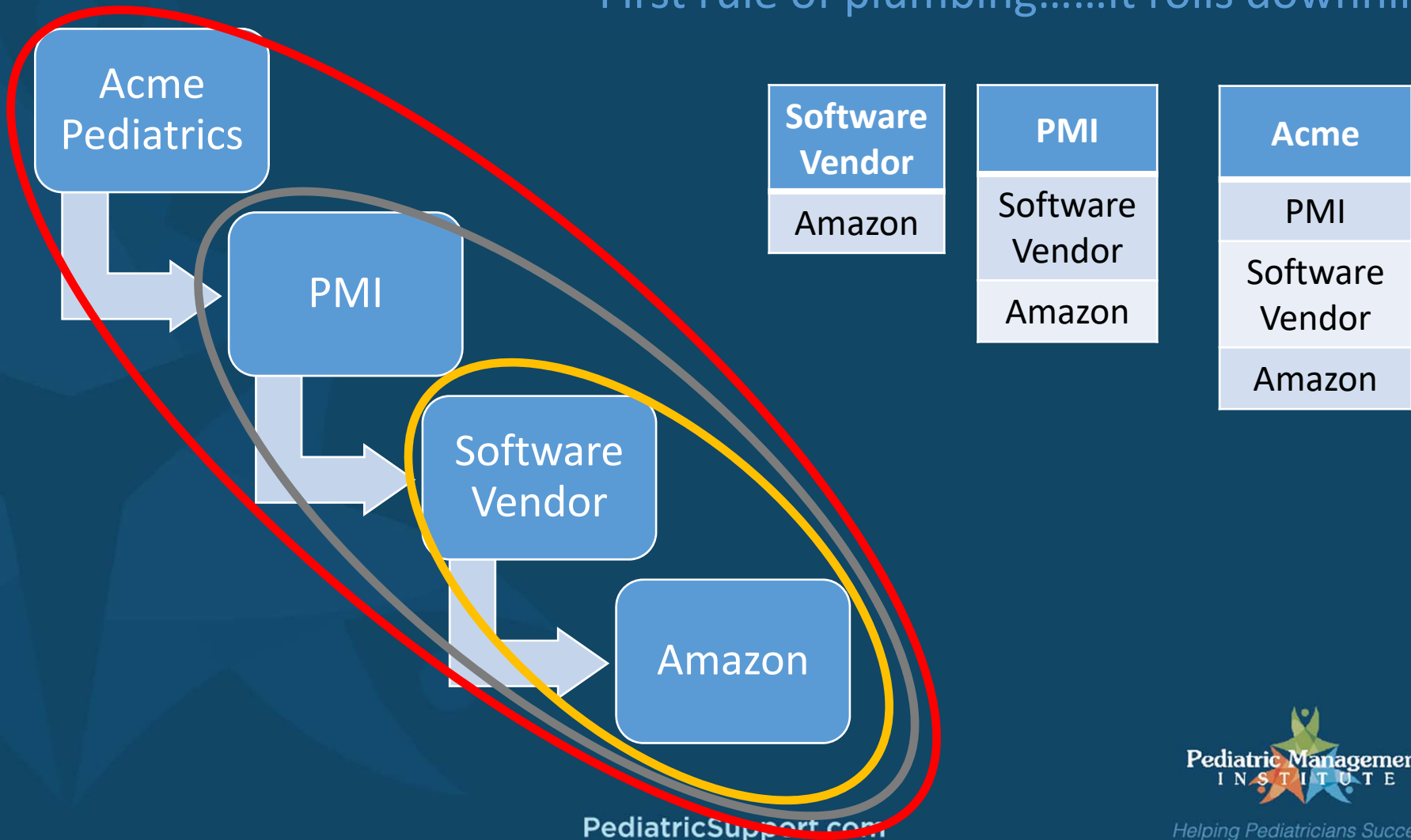
Business Associate Agreements

- Between Covered Entities & Business Associates
- Between Business Associates & Subcontractors

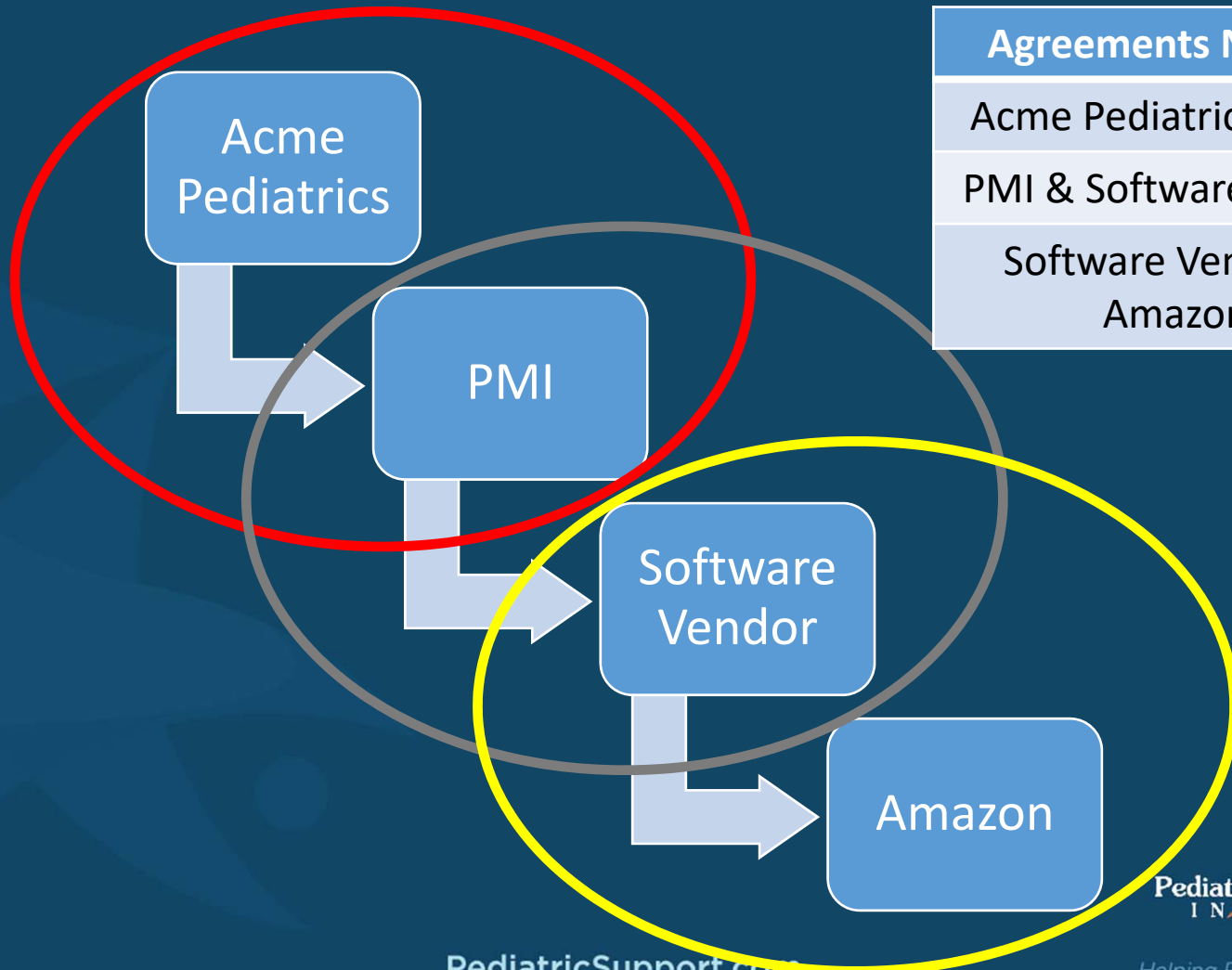
- HIPAA Specific Contract
- Limits Use of Protected Data
- Protects Confidentiality

Responsibility Hierarchy

First rule of plumbing.....it rolls downhill



Agreements Needed



Agreements Needed
Acme Pediatrics & PMI
PMI & Software Vendor
Software Vendor & Amazon

HIPAA Compliance Options

- Do it Yourself
 - Google
 - Office for Civil Rights website
 - State Medical Society
 - Specialty Societies
- Hybrid
 - Pediatric Management Institute
 - Layer Compliance
 - HIPAAOne.com
 - Malpractice Carriers
 - Hospitals
 - Clearwater Compliance
- Farm it Out
 - OCITSolutions.com
 - MedSafe.com

HIPAA Compliance Options

	Do It Yourself	Hybrid	Farm It Out
Cost	\$100 - 500	\$1,000 - 3,000	\$5,000+
Time to Complete	1 – 2 Months	2 Weeks	2 Weeks
Learn Regulations	??	Readily Available	Readily Available
Resources to Help	Various	Library	Library

"A qualified professional's expertise and focused attention will yield quicker and more reliable results than if your staff does it piecemeal over several months. The professional will suggest cost-effective ways to mitigate risks so you do not have to do the research yourself and evaluate options"- *ONC guide on HIPAA Security*



Online Resources for HIPAA

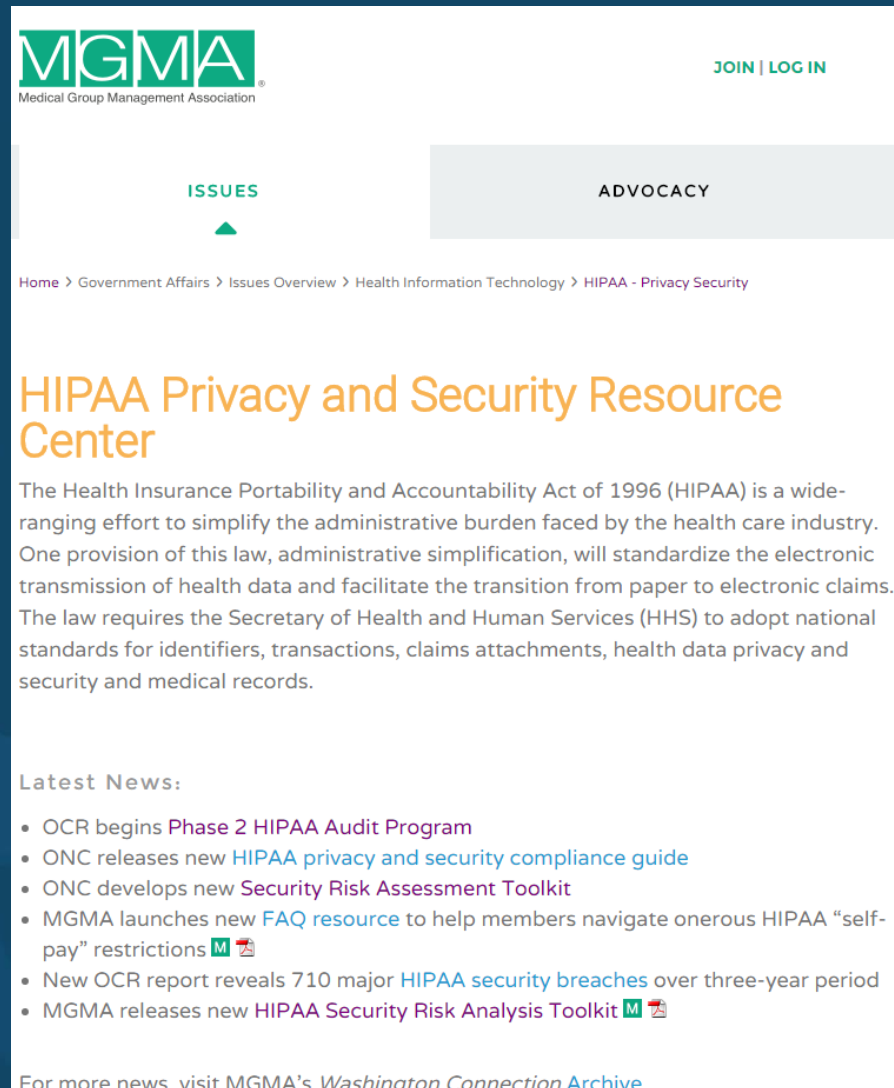
- Office for Civil Rights

The screenshot shows the HHS.gov website interface. At the top, it says "HHS.gov" and "U.S. Department of Health & Human Services". Below that is the "Health Information Privacy" section. A search bar contains the text "I'm looking for...". To the right of the search bar is a magnifying glass icon and a link to "HHS A-Z Index". Below the search bar are four main navigation buttons: "HIPAA for Individuals", "Filing a Complaint", "HIPAA for Professionals", and "Newsroom". The "HIPAA for Professionals" button is selected. Below the navigation buttons is a breadcrumb trail: "HHS Home > HIPAA > HIPAA for Professionals". On the left side, there is a sidebar menu with the following items: "HIPAA for Professionals", "Privacy", "Security", "Breach Notification", "Compliance & Enforcement", "Special Topics", "Patient Safety", and "Covered Entities & Business Associates". The main content area has a "Text Resize" tool with "A A A" buttons, a "Print" button, and "Share" buttons for Facebook, Twitter, and a plus sign. The main heading is "HIPAA for Professionals". The text below the heading reads: "To improve the efficiency and effectiveness of the health care system, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, included Administrative Simplification provisions that required HHS to adopt national standards for electronic health care transactions and code sets, unique health identifiers, and security. At the same time, Congress recognized that advances in electronic technology could erode the privacy of health information. Consequently, Congress incorporated into HIPAA provisions that mandated the adoption of Federal privacy protections for individually identifiable health information." Below this text are two bullet points: "• HHS published a final [Privacy Rule](#) in December 2000, which was later modified in August 2002. This Rule set national standards for the protection of individually identifiable health information by three types of covered entities: health plans, health care clearinghouses, and health care providers who conduct the standard health care transactions electronically. Compliance with the Privacy Rule was required as of April 14, 2003 (April 14, 2004, for small health plans).", and "• HHS published a final [Security Rule](#) in February 2003. This Rule sets national standards for protecting the confidentiality, integrity, and availability of electronic protected health information."

Online Resources for HIPAA

The screenshot shows the HealthIT.gov website. At the top, there is a navigation bar with links for Newsroom, Blog, Get Email Updates, and social media icons for Facebook, RSS, Twitter, YouTube, and LinkedIn. The HealthIT.gov logo is on the left, and a search bar is on the right. Below the navigation bar, the main content area features a large section titled "Interoperability Pledge". This section includes a paragraph stating that 90% of electronic health records used by hospitals nationwide and the top five largest health care systems have agreed to implement three core commitments: consumer access, no blocking/transparency, and standards. A circular graphic displays "90%". A "Pledge Now" button is visible. To the right of the pledge section is a "CHOOSE YOUR INFORMATION PATH" sidebar with four buttons: "For Providers & Professionals", "For Patients & Families", "For Policy Researchers & Implementers", and "Federal Advisory Committees (FACAS)". Below the main content area are three smaller sections: "ABOUT HealthIT.gov", "UPDATES from HealthIT.gov" (with a "View additional updates" link), and "From HealthIT's Social Channels" (featuring a tweet from @ONC_HealthIT and a HealthITBuzz logo).

Online Resources for HIPAA



The screenshot shows the MGMA (Medical Group Management Association) website. At the top left is the MGMA logo with the text "Medical Group Management Association". At the top right are links for "JOIN | LOG IN". Below the logo is a navigation menu with "ISSUES" (highlighted with a green triangle) and "ADVOCACY". A breadcrumb trail reads: "Home > Government Affairs > Issues Overview > Health Information Technology > HIPAA - Privacy Security". The main heading is "HIPAA Privacy and Security Resource Center" in orange. The text below explains the HIPAA law and its goals. A "Latest News:" section lists six items with bullet points and links. At the bottom, it says "For more news, visit MGMA's Washington Connection Archive."

MGMA
Medical Group Management Association

JOIN | LOG IN

ISSUES ▲



ADVOCACY

Home > Government Affairs > Issues Overview > Health Information Technology > HIPAA - Privacy Security

HIPAA Privacy and Security Resource Center

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a wide-ranging effort to simplify the administrative burden faced by the health care industry. One provision of this law, administrative simplification, will standardize the electronic transmission of health data and facilitate the transition from paper to electronic claims. The law requires the Secretary of Health and Human Services (HHS) to adopt national standards for identifiers, transactions, claims attachments, health data privacy and security and medical records.

Latest News:

- OCR begins [Phase 2 HIPAA Audit Program](#)
- ONC releases new [HIPAA privacy and security compliance guide](#)
- ONC develops new [Security Risk Assessment Toolkit](#)
- MGMA launches new [FAQ resource](#) to help members navigate onerous HIPAA “self-pay” restrictions 
- New OCR report reveals 710 major [HIPAA security breaches](#) over three-year period
- MGMA releases new [HIPAA Security Risk Analysis Toolkit](#) 

For more news, visit MGMA's [Washington Connection Archive](#).

PediatricSupport.com



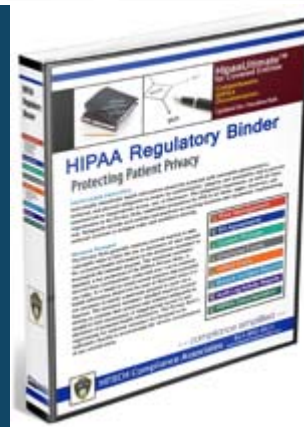
Helping Pediatricians Succeed

HIPAA DIY- Online Purchase



The screenshot shows the HITECH Associates website banner. At the top left, the logo reads "HITECH Associates" with the tagline "Risk Assessment Experts 813-892-4411". To the right is a navigation menu with links for "Home Page", "Risk Assessment", "About Us", "News", and "HIPAA Kit". The main banner text is as follows:

Comprehensive HIPAA Solution for CEs & BAs
HIPAA Compliance Kit starts at \$299, Complete with Risk Assessment.
Surpasses Meaningful Use Security Risk Assessment Requirements.
Full "Meaningful Program" as Required by The Office of Civil Rights.
Less Money, More HIPAA!



PediatricSupport.com



Helping Pediatricians Succeed

HIPAA DIY- Books

The screenshot shows the Medical Coding.net website. The header includes the logo, a search bar, and contact information. A blue navigation bar contains categories like CPT, ICD-10-CM, ICD-10-PCS, HCPCS, BY SPECIALTY, CLAIM FORMS, DATA FILES, and E-BOOKS. The breadcrumb trail is Home > Books > HIPAA Tool Kit 2016 (Includes a customizable compliance plan). On the left, a 'CATEGORIES' sidebar lists CPT, ICD-10-CM, HCPCS, ICD-10-PCS, and SHOP BY SPECIALTY. The main content area features the book cover for 'HIPAA Tool Kit 2016' by Optum (Ingenix), priced at \$299.95. The product details include the SKU HTKT16, a quantity selector set to 1, and a condition dropdown. 'ADD TO CART' and 'CHECKOUT' buttons are visible below the price.

Medical Coding.net
Your Medical Coding Superstore

Search Entire Store

Sales Support (888) 28...
Hi Guest, S...

Home : Books : HIPAA Tool Kit 2016 (Includes a customizable compliance plan)

CATEGORIES

- + CPT
- + ICD-10-CM
- + HCPCS
- + ICD-10-PCS
- + SHOP BY SPECIALTY

HIPAA Tool Kit
A medical practice guide to assessment, implementation and policy and procedure development
2016

Optum (Ingenix)
HIPAA Tool Kit 2016 (Includes a customizable compliance plan)
\$299.95
SKU: HTKT16 Quantity: 1 Condition:
ADD TO CART **CHECKOUT**

Click to enlarge

HIPAA DIY- Monthly Subscription

HIPAA One
PROTECT YOUR ePHI

PRODUCTS SELF-ASSESSMENTS RESOURCES ABOUT TESTIMONIALS

Automated HIPAA Compliance Software

Get Started Now with our HIPAA One® Solution

Find out how easy it is to become and stay HIPAA compliant.

HIPAA Security, Privacy and Breach Compliance

★★★★★ 5/5 6 reviews

Our teams work tirelessly to provide the best HIPAA compliance software and professional services in the industry. Owned and professional services provided by Modern Compliance Solutions, HIPAA One® was designed from the ground-up to be the most simple, automated and affordable solution.

PediatricSupport.com



Helping Pediatricians Succeed

HIPAA Hybrid Solution- Monthly Subscription



With [LayerCompliance™](#) (formerly the Online HIPAA Security Manager), organizations can get the expert help and tools they need to achieve and maintain compliance.

RISK ANALYSIS - A full risk analysis that assess systems and provides both HIPAA Security compliance and threat analysis.

IMPLEMENTATION - You can document HIPAA Security compliance activities including the implementation of policies and security measures.

RISK MANAGEMENT - A once a year audit or assessment isn't enough. Breaches happen every day and you are required to stay in compliance all year round.

LIVE CLIENT SUPPORT - Our LayerCompliance team is ready to assist with HIPAA Security questions, incidents and potential breaches.

HIPAA Hybrid Solution- Monthly /Annual Pay

securityMETRICS®

GUIDED HIPAA COMPLIANCE PACKAGES

HIPAA PRO	HIPAA PLUS	HIPAA BASIC
<i>Annual: \$2,399 Monthly: \$209</i>	<i>Annual: \$1,899 Monthly: \$169</i>	<i>Annual: \$1,099 Monthly: \$99</i>
<ul style="list-style-type: none"> • Breach Protection Checklist • \$100,000 HIPAA Breach Protection (after attesting to Breach Protection Checklist) • Online Portal Access (for real-time HIPAA guidance, logging, storage, documentation, and training) • PHI Map and Vulnerability Identification • Risk Analysis (RA) • Prioritized Risk Management Plan (RMP) • Guided Implementation of Risk Management Plan • Unlimited External Vulnerability Scans (3 IP addresses) • Monthly Publication • Certificates of HIPAA Completion (RA and RMP) • Certificate of HIPAA Compliance (upon full implementation of RMP) • Assigned a Dedicated HIPAA Support Advisor • Unlimited Live Technical Support Available 24x7 • Customizable HIPAA Policy Templates (including a Breach Notification Policy) • Business Associate Agreement Template • Mobile Device Scanning • HIPAA Training (3 seats for Security Awareness, Privacy and Security, and Responsible Use of Social Media trainings) 	<ul style="list-style-type: none"> • Breach Protection Checklist • \$100,000 HIPAA Breach Protection (after attesting to Breach Protection Checklist) • Online Portal Access (for real-time HIPAA guidance, logging, storage, documentation, and training) • PHI Map and Vulnerability Identification • Risk Analysis (RA) • Prioritized Risk Management Plan (RMP) • Guided Implementation of Risk Management Plan • Unlimited External Vulnerability Scans (2 IP addresses) • Monthly Publication • Certificates of HIPAA Completion (RA and RMP) • Certificate of HIPAA Compliance (upon full implementation of RMP) • Assigned a Dedicated HIPAA Support Advisor • Mobile Device Scanning • Unlimited Live Technical Support Available 24x7 • Customizable HIPAA Policy Templates (including a Breach Notification Policy) • Business Associate Agreement Template 	<ul style="list-style-type: none"> • Breach Protection Checklist • \$100,000 HIPAA Breach Protection (after attesting to Breach Protection Checklist) • Online Portal Access (for real-time HIPAA guidance, logging, storage, documentation, and training) • PHI Map and Vulnerability Identification • Risk Analysis (RA) • Prioritized Risk Management Plan (RMP) • Guided Implementation of Risk Management Plan • Unlimited External Vulnerability Scans (1 IP address) • Monthly Publication • Certificates of HIPAA Completion (RA and RMP) • Certificate of HIPAA Compliance (upon full implementation of RMP) • Assigned a Dedicated HIPAA Support Advisor • One Hour/Month Live Technical Support

© 2015 SecurityMetrics

securityMETRICS®

PediatricSupport.com



Helping Pediatricians Succeed

Free HIPAA Assessment Tool- Desktop & iPad Apps

The screenshot shows the HealthIT.gov website with a blue header and navigation menu. The main content area is titled "Security Risk Assessment" and features a central article about the "Security Risk Assessment Tool". The article includes a sub-header "What is the Security Risk Assessment Tool (SRA Tool)?", a photograph of three healthcare professionals reviewing a tablet, and a "Download Tool" button. A sidebar on the left lists various resources, and a right sidebar contains links to "Top 10 Myths of Security Risk Analysis" and "SRA Tool (iPad version)".

HealthIT.gov | Federal Advisory Committees (FACAs) | Contact | Get Email Updates | RSS | Facebook | YouTube | LinkedIn | Twitter

in Partnership with the National Learning Consortium

Newsroom | FAQs | Multimedia | Implementation Resources

Providers & Professionals | Patients & Families | Policy Researchers & Implementers

Benefits of EHRs | How to Implement EHRs | Privacy & Security | EHR Incentives & Certification | Success Stories & Case Studies | Resource Center

HealthIT.gov > For Providers & Professionals > Privacy & Security > Security Risk Assessment > Security Risk Assessment Tool

Security Risk Assessment

Security Risk Assessment Tool

What is the Security Risk Assessment Tool (SRA Tool)?

The Office of the National Coordinator for Health Information Technology (ONC) recognizes that conducting a risk assessment can be a challenging task. That's why ONC, in collaboration with the HHS Office for Civil Rights (OCR) and the HHS Office of the General Counsel (OGC), developed a downloadable [SRA Tool \[.exe - 69 MB \]](#) to help guide you through the process. This tool is not required by the HIPAA Security Rule, but is meant to assist providers and professionals as they perform a risk assessment.

We understand that users with Windows 8.1 Operating Systems may experience difficulties downloading the SRA Tool, we are working to resolve the issue and will post here when a resolution is identified and implemented.

The SRA Tool is a self-contained, operating system (OS) independent application that can be run on various environments including Windows OS's for desktop and laptop computers and Apple's iOS for iPad only. The iOS SRA Tool application for iPad, available at no cost, can be downloaded from Apple's [App Store](#).

The SRA Tool takes you through each HIPAA requirement by presenting a question

Top 10 Myths of Security Risk Analysis

As with any new program or regulation, there may be misinformation making the rounds. [Read the top 10 list distinguishing fact from fiction.](#)

SRA Tool (Windows version)

[Download Tool](#)

SRA Tool (iPad version)

HHS - Risk Assessment Tool

Security Risk Assessment Tool Tutorial

Current User: JD | Logout | www.HealthIT.gov

A01

§164.308(a)(1)(i) - Standard
 Does your practice develop, document, and implement policies and procedures for assessing and managing risk to its ePHI?

Yes No Flag

Things to Consider Threats and Vulnerabilities Examples of Safeguards

An information system is an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and users.

A portable electronic device is any electronic apparatus with singular or multiple capabilities of recording, storing, and/or transmitting data, voice, video, or photo images. This includes but is not limited to laptops, personal digital assistants, pocket personal computers, palmtops, MP3 players, cellular telephones, thumb drives, video cameras, and pagers.

Electronic storage media includes

HHS - Risk Assessment Tool

Security Risk Assessment Tool

Tutorial

Current User: JD | Logout | www.HealthIT.gov

A01

§164.308(a)(1)(i) - Standard
Does your practice develop, document, and implement policies and procedures for assessing and managing risk to its ePHI?

Yes No Flag

Current Activities	Notes	Remediation
--------------------	-------	-------------

With respect to a threat/vulnerability affecting your ePHI:

Likelihood: Low Medium High

Impact: Low Medium High

Things to Consider | Threats and Vulnerabilities | Examples of Safeguards

An information system is an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and users.

A portable electronic device is any electronic apparatus with singular or multiple capabilities of recording, storing, and/or transmitting data, voice, video, or photo images. This includes but is not limited to laptops, personal digital assistants, pocket personal computers, palmtops, MP3 players, cellular telephones, thumb drives, video cameras, and pagers.

Electronic storage media includes

Security Risk Assessments

Presented by:

Paul D. Vanchiere, MBA



HIPAA by the numbers



Security First, then Compliance

Data breaches hurt patients, medical practices and businesses. Breach investigations are much more likely to occur than HIPAA audits. Data breaches can turn into expensive lawsuits. Only one federal agency conducts HIPAA audits, while many federal and state agencies enforce data breach penalties. We are focused first on protecting you against data breaches, then on compliance. Contact us for more information.

Black-market Value

\$ 50 per medical record
\$ 1 per credit card number

FBI Health Care Risk Notification, April 2014

Healthcare organizations

81% permit BYOD
personally-owned devices connecting to their networks
but only 21% scan BYOD devices

prior to connection to network
Ponemon survey of healthcare organizations

HIPAA Penalties

\$ 1.5 million
for a lost unencrypted laptop
\$ 1.7 million
for a lost unencrypted laptop
\$ 1.7 million
for a lost unencrypted hard drive

63% of healthcare institutions experienced a **reportable data breach**

Ponemon 2013 Economic & Productivity Impact of IT Security on Healthcare

17,000 patient records breached per day, on average

September 2009 to present, HHS.gov

Compliance does not equal security.

Organizations may think they're compliant, but data shows that they are not secure.

2014 SANS Health Care Cyberthreat Report

\$ 188 average cost per breached record

Ponemon 2014 Cost of a Data Breach survey

56% of patients *whose data was breached* **lost trust and confidence in their healthcare provider**

Ponemon 2013 Survey on Medical Identity Theft

700,000 HIPAA Covered Entities
(providers & payers)

2,000,000 – 3,000,000

HIPAA Business Associates

HHS estimates

Only 115 HIPAA Audits

2009 – 2013 (out of 700,000 Covered Entities)

Only 100 per month starting in 2014 (of 3.7 million organizations required to comply with HIPAA)

But...13,000 Data Breach Investigations

HHS Office for Civil Rights

Health Care 31% of all reported data breaches

EMC/RSA White Paper, 2013

74% are not encrypting data on mobile medical devices

HIMSS Security Survey, sponsored by Experian

Only 43% of healthcare providers have an accurate inventory of employees' and customers' personal data

Worldwidestudy by PwC, CIO Magazine & CSO Magazine

91% of healthcare organizations are **using cloud-based services**

47% are **not confident in the ability to keep data secure** in the cloud

Ponemon survey of 80 healthcare organizations, December 2012