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.

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 SAMH Health Care Cyberthreat Report

Black-market Value
$ 50 per medical record
$ 1 per credit card number

Healthcare organizations
81% permit BYOD
personally-owned devices connecting to their networks but only 21% scan
BYOD devices prior to connection to network

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

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

$ 188 average cost per breached record

700,000
HIPAA Covered Entities
(providers & payers)

2,000,000 – 3,000,000
HIPAA Business Associates (HBR-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

91% of healthcare organizations are using cloud-based services

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

91% of healthcare providers have an accurate inventory of employees’ and customers’ personal data

Healthcare
74% are not encrypting data on mobile medical devices

Pediatric Management
Institute

Presented by:
Paul D. Vanchiere, MBA
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?

• 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.

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

PediatricSupport.com
# Value of Your Data....

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>Social Security number</td>
<td>$30.00</td>
</tr>
<tr>
<td>Date of birth</td>
<td>$11.00</td>
</tr>
<tr>
<td>Health insurance credentials</td>
<td>$20.00</td>
</tr>
<tr>
<td>Visa or MasterCard credentials</td>
<td>$4.00</td>
</tr>
<tr>
<td>American Express credentials</td>
<td>$7.00</td>
</tr>
<tr>
<td>Discover credit credentials</td>
<td>$8.00</td>
</tr>
<tr>
<td>Credit card with magnetic stripe or chip data</td>
<td>$12.00</td>
</tr>
</tbody>
</table>

$61.00

Like Pediatrics, Volume is the Key...

$61 \times 4,000 \text{ Patients} = \$244,000

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!

Source: http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/index.html
Consequences are terrible

- Personal / Practice financial lability
- 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

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

<table>
<thead>
<tr>
<th>Name of Covered Entity</th>
<th>State</th>
<th>Covered Entity Type</th>
<th>Individuals Affected</th>
<th>Breach Submission Date</th>
<th>Type of Breach</th>
<th>Location of Breached Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Democracy Data &amp; Communications, LLC</td>
<td>VA</td>
<td>Business Associate</td>
<td>83000</td>
<td>12/08/2009</td>
<td>Other</td>
<td>Paper/Films</td>
</tr>
<tr>
<td>Health Behavior Innovations (HBI)</td>
<td>UT</td>
<td>Business Associate</td>
<td>5700</td>
<td>02/05/2010</td>
<td>Theft</td>
<td>Other</td>
</tr>
<tr>
<td>Wyoming Department of Health</td>
<td>WY</td>
<td>Health Plan</td>
<td>9023</td>
<td>03/02/2010</td>
<td>Theft</td>
<td>Network Server</td>
</tr>
<tr>
<td>Thrivent Financial for Lutherans</td>
<td>WI</td>
<td>Health Plan</td>
<td>9500</td>
<td>03/03/2010</td>
<td>Theft</td>
<td>Laptop</td>
</tr>
<tr>
<td>Laboratory Corporation of America/Dynacare Northwest, Inc.</td>
<td>WA</td>
<td>Healthcare Provider</td>
<td>5080</td>
<td>03/18/2010</td>
<td>Theft</td>
<td>Laptop</td>
</tr>
<tr>
<td>Tomah Memorial Hospital</td>
<td>WI</td>
<td>Healthcare Provider</td>
<td>600</td>
<td>04/16/2010</td>
<td>Other</td>
<td>Other</td>
</tr>
<tr>
<td>TOWERS WATSON</td>
<td>VA</td>
<td>Business Associate</td>
<td>1874</td>
<td>04/27/2010</td>
<td>Theft</td>
<td>Other</td>
</tr>
<tr>
<td>Rockbridge Area Community Services</td>
<td>VA</td>
<td>Healthcare Provider</td>
<td>500</td>
<td>04/29/2010</td>
<td>Theft</td>
<td>Desktop Computer, Laptop</td>
</tr>
<tr>
<td>(see explanation below)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prince William County Community Services (CS)</td>
<td>VA</td>
<td>Healthcare Provider</td>
<td>689</td>
<td>07/15/2010</td>
<td>Theft</td>
<td>Other Portable Electronic Device</td>
</tr>
<tr>
<td>Mercer</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ward A. Morris, DDS</td>
<td>WA</td>
<td>Healthcare Provider</td>
<td>2698</td>
<td>08/11/2010</td>
<td>Theft</td>
<td>Desktop Computer</td>
</tr>
<tr>
<td>Curtis R. Bryan, M.D.</td>
<td>VA</td>
<td>Healthcare Provider</td>
<td>2739</td>
<td>09/08/2010</td>
<td>Theft</td>
<td>Laptop</td>
</tr>
<tr>
<td>Utah Department of Workforce Services</td>
<td>UT</td>
<td>Business Associate</td>
<td>1298</td>
<td>10/13/2010</td>
<td>Other</td>
<td>Desktop Computer, Paper/Films</td>
</tr>
<tr>
<td>SW Seattle Orthopaedic and Sports Medicine</td>
<td>WA</td>
<td>Healthcare Provider</td>
<td>9493</td>
<td>10/15/2010</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
</tbody>
</table>
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:
- [ ] Hacking/IT Incident
- [ ] Theft
- [ ] Other
- [ ] Improper Disposal
- [ ] Unauthorized Access/Disclosure
- [ ] Loss
- [ ] Unknown

Location of Breach:
- [ ] Desktop Computer
- [ ] Laptop
- [ ] Paper/Films
- [ ] Electronic Medical Record
- [ ] Network Server
- [ ] Other Portable Electronic Device
- [ ] Email
- [ ] Other

Type of Covered Entity: [ ]
State: [ ]
Business Associate Present?: [ ]
Description Search: [ ]
CE / BA Name Search: [ ]
## Sample of Breaches > 500 Patients

<table>
<thead>
<tr>
<th>Name of Covered Entity</th>
<th>State</th>
<th>Covered Entity Type</th>
<th>Individuals Affected</th>
<th>Breach Submission Date</th>
<th>Type of Breach</th>
<th>Location of Breached Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grays Harbor Pediatrics, PLLC</td>
<td>WA</td>
<td>Healthcare Provider</td>
<td>12009</td>
<td>01/12/2011</td>
<td>Theft</td>
<td>Other, Other Portable Electronic Device</td>
</tr>
<tr>
<td>Pediatric Sports and Spine Associates</td>
<td>TX</td>
<td>Healthcare Provider</td>
<td>955</td>
<td>04/09/2010</td>
<td>Theft</td>
<td>Laptop</td>
</tr>
<tr>
<td>Good Care Pediatric, LP</td>
<td>NY</td>
<td>Healthcare Provider</td>
<td>2300</td>
<td>11/12/2015</td>
<td>Hacking/IT Incident</td>
<td>Desktop Computer</td>
</tr>
<tr>
<td>Adult &amp; Pediatric Dermatology, PC</td>
<td>MA</td>
<td>Healthcare Provider</td>
<td>2200</td>
<td>10/07/2011</td>
<td>Theft</td>
<td>Other, Other Portable Electronic Device</td>
</tr>
<tr>
<td>Pediatric Group LLC</td>
<td>IL</td>
<td>Healthcare Provider</td>
<td>10000</td>
<td>08/21/2015</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td>Barrington Orthopedic Specialists, Ltd</td>
<td>IL</td>
<td>Healthcare Provider</td>
<td>109</td>
<td>09/24/2015</td>
<td>Theft</td>
<td>Laptop, Other</td>
</tr>
<tr>
<td>Pediatric and Adult Allergy, PC</td>
<td>IA</td>
<td>Healthcare Provider</td>
<td>19222</td>
<td>09/11/2010</td>
<td>Loss</td>
<td>Other Portable Electronic Device</td>
</tr>
<tr>
<td>Pediatric Associates</td>
<td>FL</td>
<td>Healthcare Provider</td>
<td>627</td>
<td>03/24/2015</td>
<td>Loss</td>
<td>Paper/Films</td>
</tr>
<tr>
<td>Pediatric Gastroenterology Consultants</td>
<td>CO</td>
<td>Healthcare Provider</td>
<td>5000</td>
<td>12/19/2014</td>
<td>Theft</td>
<td>Laptop</td>
</tr>
<tr>
<td>Center for Orthopedic Research and Education, Inc.</td>
<td>AZ</td>
<td>Healthcare Provider</td>
<td>35488</td>
<td>12/21/2012</td>
<td>Theft</td>
<td>Paper/Films</td>
</tr>
<tr>
<td>Alaska Orthopedic Specialists, Inc.</td>
<td>AK</td>
<td>Healthcare Provider</td>
<td>553</td>
<td>11/19/2015</td>
<td>Theft</td>
<td>Email</td>
</tr>
</tbody>
</table>

### Additional Breaches

<table>
<thead>
<tr>
<th>Name of Covered Entity</th>
<th>State</th>
<th>Covered Entity Type</th>
<th>Individuals Affected</th>
<th>Breach Submission Date</th>
<th>Type of Breach</th>
<th>Location of Breached Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>M&amp;C Children's Clinic PA</td>
<td>TX</td>
<td></td>
<td></td>
<td>03/19/2013</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Children's Medical Center of Dallas</td>
<td>TX</td>
<td>Healthcare Provider</td>
<td>3800</td>
<td>01/18/2010</td>
<td>Loss</td>
<td>Other, Other Portable Electronic Device</td>
</tr>
<tr>
<td>Texas Children's Hospital</td>
<td>TX</td>
<td>Healthcare Provider</td>
<td>694</td>
<td>07/30/2010</td>
<td>Theft</td>
<td>Laptop</td>
</tr>
<tr>
<td>Children's Medical Center of Dallas</td>
<td>TX</td>
<td>Healthcare Provider</td>
<td>2462</td>
<td>07/10/2013</td>
<td>Theft</td>
<td>Laptop</td>
</tr>
<tr>
<td>St. Jude Children's Research Hospital</td>
<td>TN</td>
<td>Healthcare Provider</td>
<td>1745</td>
<td>06/08/2010</td>
<td>Loss</td>
<td>Laptop</td>
</tr>
<tr>
<td>The Children's Hospital of Philadelphia</td>
<td>PA</td>
<td>Healthcare Provider</td>
<td>943</td>
<td>11/24/2009</td>
<td>Theft</td>
<td>Laptop</td>
</tr>
<tr>
<td>The Children's Medical Center of Dayton</td>
<td>OH</td>
<td>Healthcare Provider</td>
<td>1001</td>
<td>06/14/2010</td>
<td>Other</td>
<td>Email</td>
</tr>
<tr>
<td>Children's Hospital Medical Center of Akron</td>
<td>OH</td>
<td>Healthcare Provider</td>
<td>7664</td>
<td>08/20/2015</td>
<td>Loss</td>
<td>Other Portable Electronic Device</td>
</tr>
<tr>
<td>Cincinnati Children's Hospital Medical Center</td>
<td>OH</td>
<td>Healthcare Provider</td>
<td>60998</td>
<td>06/01/2010</td>
<td>Theft</td>
<td>Laptop</td>
</tr>
<tr>
<td>St. Mary's Hospital for Children</td>
<td>NY</td>
<td>Business Associate</td>
<td>550</td>
<td>05/19/2011</td>
<td>Theft</td>
<td>Paper/Films</td>
</tr>
<tr>
<td>CristiKern's Heart &amp; Vascular</td>
<td>NV</td>
<td>Healthcare Provider</td>
<td>8791</td>
<td>04/03/2015</td>
<td>Unauthorized Access/Disclosure</td>
<td>Electronic Medical Record</td>
</tr>
<tr>
<td>Children's Mercy Hospital</td>
<td>MO</td>
<td>Healthcare Provider</td>
<td>4067</td>
<td>08/15/2014</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td>Children's Hospital Boston</td>
<td>MA</td>
<td>Healthcare Provider</td>
<td>2159</td>
<td>05/22/2012</td>
<td>Theft</td>
<td>Laptop</td>
</tr>
<tr>
<td>Children's National Medical Center</td>
<td>DC</td>
<td>Healthcare Provider</td>
<td>18000</td>
<td>02/24/2015</td>
<td>Hacking/IT Incident</td>
<td>Email</td>
</tr>
<tr>
<td>Health Services for Children with Special Needs, Inc.</td>
<td>DC</td>
<td>Health Plan</td>
<td>3800</td>
<td>11/17/2009</td>
<td>Loss</td>
<td>Laptop</td>
</tr>
<tr>
<td>Lucille Packard Children's Hospital</td>
<td>CA</td>
<td>Healthcare Provider</td>
<td>532</td>
<td>02/21/2010</td>
<td>Other</td>
<td>Desktop Computer</td>
</tr>
<tr>
<td>Children's Eyewear Sight</td>
<td>CA</td>
<td>Healthcare Provider</td>
<td>1030</td>
<td>01/12/2015</td>
<td>Theft</td>
<td>Desktop Computer</td>
</tr>
<tr>
<td>Rady Children's Hospital - San Diego</td>
<td>CA</td>
<td>Healthcare Provider</td>
<td>6307</td>
<td>06/25/2014</td>
<td>Unauthorized Access/Disclosure</td>
<td>Email, Other</td>
</tr>
<tr>
<td>Rady Children's Hospital - San Diego</td>
<td>CA</td>
<td>Healthcare Provider</td>
<td>14121</td>
<td>06/24/2014</td>
<td>Unauthorized Access/Disclosure</td>
<td>Email</td>
</tr>
<tr>
<td>Lucile Packard Children's Hospital</td>
<td>CA</td>
<td>Healthcare Provider</td>
<td>12900</td>
<td>06/13/2013</td>
<td>Theft</td>
<td>Laptop</td>
</tr>
<tr>
<td>Children's Hospital &amp; Research Center at Oakland</td>
<td>CA</td>
<td>Healthcare Provider</td>
<td>1000</td>
<td>06/29/2010</td>
<td>Other</td>
<td>Paper/Films</td>
</tr>
<tr>
<td>Standford School Medicine &amp; LP Children Hosp, Privacy Manager Breach</td>
<td>CA</td>
<td></td>
<td></td>
<td>01/23/2013</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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 website 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
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 days

Source: http://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html
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 website 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
Penalty / Fine Levels

- **Unknowing.** 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.

## Penalty Guidelines

<table>
<thead>
<tr>
<th>Violation</th>
<th>Amount per violation</th>
<th>Violations of an identical provision in a calendar year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did Not Know</td>
<td>$100 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Reasonable Cause</td>
<td>$1,000 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful Neglect — Corrected</td>
<td>$10,000 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful Neglect — Not Corrected</td>
<td>$50,000</td>
<td>$1,500,000</td>
</tr>
</tbody>
</table>

Source: Federal Register
Carrot Stick

<table>
<thead>
<tr>
<th>Privacy</th>
<th>Right thing to do</th>
<th>Fines &amp; Penalties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>Adopt best practices</td>
<td>Fines &amp; Penalties</td>
</tr>
<tr>
<td>Risk Mitigation</td>
<td>Keep your data secure</td>
<td>Fines &amp; Penalties</td>
</tr>
<tr>
<td>Data Breach Management</td>
<td>Maintain the trust of patients</td>
<td>Fines, Penalties &amp; Notifications</td>
</tr>
</tbody>
</table>

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

PediatricSupport.com
What to Do to Ensure HIPAA Compliance?

- Assess Patient
- Run Tests, Evaluate & Diagnose
- Treatment Plan
- Risk Assessment
- Policies & Procedures
- Compliance Management

PediatricSupport.com
Bare Minimum Compliance

- Risk Assessment Report
  - Self-Answered Questions
  - Interviews
  - Observations
  - Policy & Procedures Manual
  - Employee Meeting
Minimum Compliance is Not Enough

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


PediatricSupport.com
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
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.
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.


PediatricSupport.com
# Technical Safeguards Implementation

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

## Physical Safeguards Implementation

### Part 1 of 2

<table>
<thead>
<tr>
<th>Standard</th>
<th>Action Item</th>
<th>Status</th>
<th>Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facility Access Controls</td>
<td>Contingency Operations</td>
<td>Addressable</td>
<td>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.</td>
</tr>
<tr>
<td>Facility Access Controls</td>
<td>Facility Security Plan</td>
<td>Addressable</td>
<td>Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.</td>
</tr>
<tr>
<td>Facility Access Controls</td>
<td>Access Control and Validation Procedures</td>
<td>Addressable</td>
<td>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.</td>
</tr>
<tr>
<td>Facility Access Controls</td>
<td>Maintenance Records</td>
<td>Addressable</td>
<td>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.</td>
</tr>
<tr>
<td>Workstation Use</td>
<td>Required</td>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

## Physical Safeguards Implementation

### Part 2 of 2

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

### Administrative Safeguards Implementation

**Part 1 of 3**

<table>
<thead>
<tr>
<th>Standard</th>
<th>Action Item</th>
<th>Status</th>
<th>Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Management Process</td>
<td>Risk Analysis</td>
<td>Required</td>
<td>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.</td>
</tr>
<tr>
<td>Security Management Process</td>
<td>Risk Management</td>
<td>Required</td>
<td>Implement sufficient measures to reduce these risks to an appropriate level.</td>
</tr>
<tr>
<td>Security Management Process</td>
<td>Information Systems Activity Reviews</td>
<td>Required</td>
<td>Regularly review system activity, logs, audit trails, etc.</td>
</tr>
<tr>
<td>Assigned Security Responsibility Officers</td>
<td>Officers</td>
<td>Required</td>
<td>Designate HIPAA Security and Privacy Officers.</td>
</tr>
</tbody>
</table>

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

PediatricSupport.com
# Administrative Safeguards Implementation

**Part 2 of 3**

<table>
<thead>
<tr>
<th>Standard</th>
<th>Action Item</th>
<th>Status</th>
<th>Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workforce Security</td>
<td>Employee Oversight</td>
<td>Addressable</td>
<td>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.</td>
</tr>
<tr>
<td>Information Access Management</td>
<td>Multiple Organizations</td>
<td>Required</td>
<td>Ensure that PHI is not accessed by parent or partner organizations or subcontractors that are not authorized for access.</td>
</tr>
<tr>
<td>Information Access Management</td>
<td>ePHI Access</td>
<td>Addressable</td>
<td>Implement procedures for granting access to ePHI that document access to ePHI or to services and systems that grant access to ePHI.</td>
</tr>
<tr>
<td>Security Awareness and Training</td>
<td>Security Reminders</td>
<td>Addressable</td>
<td>Periodically send updates and reminders about security and privacy policies to employees.</td>
</tr>
<tr>
<td>Security Awareness and Training</td>
<td>Protection Against Malware</td>
<td>Addressable</td>
<td>Have procedures for guarding against, detecting, and reporting malicious software.</td>
</tr>
<tr>
<td>Security Awareness and Training</td>
<td>Login Monitoring</td>
<td>Addressable</td>
<td>Institute monitoring of logins to systems and reporting of discrepancies.</td>
</tr>
</tbody>
</table>

Source: https://www.truevault.com/blog/how-do-i-become-hipaa-compliant.html
## Administrative Safeguards Implementation
### Part 3 of 3

<table>
<thead>
<tr>
<th>Standard</th>
<th>Action Item</th>
<th>Status</th>
<th>Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Awareness and Training</td>
<td>Password Management</td>
<td>Addressable</td>
<td>Ensure that there are procedures for creating, changing, and protecting passwords.</td>
</tr>
<tr>
<td>Security Incident Procedures</td>
<td>Response and Reporting</td>
<td>Required</td>
<td>Identify, document, and respond to security incidents.</td>
</tr>
<tr>
<td>Contingency Plan</td>
<td>Contingency Plans</td>
<td>Required</td>
<td>Ensure that there are accessible backups of ePHI and that there are procedures for restore any lost data.</td>
</tr>
<tr>
<td>Contingency Plan</td>
<td>Contingency Plans Updates and Analysis</td>
<td>Addressable</td>
<td>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.</td>
</tr>
<tr>
<td>Contingency Plan</td>
<td>Emergency Mode</td>
<td>Required</td>
<td>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.</td>
</tr>
<tr>
<td>Evaluations</td>
<td></td>
<td>Required</td>
<td>Perform periodic evaluations to see if any changes in your business or the law require changes to your HIPAA compliance procedures.</td>
</tr>
<tr>
<td>Business Associate Agreements</td>
<td></td>
<td>Required</td>
<td>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.</td>
</tr>
</tbody>
</table>

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

PediatricSupport.com
Business Associates Under Scrutiny

- 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.


PediatricSupport.com
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.
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”

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…
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

<table>
<thead>
<tr>
<th>Agreements Needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acme Pediatrics &amp; PMI</td>
</tr>
<tr>
<td>PMI &amp; Software Vendor</td>
</tr>
<tr>
<td>Software Vendor &amp; Amazon</td>
</tr>
</tbody>
</table>
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

PediatricSupport.com
### HIPAA Compliance Options

<table>
<thead>
<tr>
<th></th>
<th>Do It Yourself</th>
<th>Hybrid</th>
<th>Farm It Out</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cost</strong></td>
<td>$100 - 500</td>
<td>$1,000 - 3,000</td>
<td>$5,000+</td>
</tr>
<tr>
<td><strong>Time to Complete</strong></td>
<td>1 – 2 Months</td>
<td>2 Weeks</td>
<td>2 Weeks</td>
</tr>
<tr>
<td><strong>Learn Regulations</strong></td>
<td>??</td>
<td>Readily Available</td>
<td>Readily Available</td>
</tr>
<tr>
<td><strong>Resources to Help</strong></td>
<td>Various</td>
<td>Library</td>
<td>Library</td>
</tr>
</tbody>
</table>

"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

PediatricSupport.com
Online Resources for HIPAA

- Office for Civil Rights

[HHS.gov](https://www.hhs.gov)

Health Information Privacy

I'm looking for...

HIPAA for Professionals

- Privacy
- Security
- Breach Notification
- Compliance & Enforcement
- Special Topics
- Patient Safety
- Covered Entities & Business Associates

HIPAA for Professionals

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.

- HHS published a final [Privacy Rule](https://www.hhs.gov) in December 2000, which was later modified in August 2002. This Rule sets 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 standard health care transactions electronically. Compliance with the Privacy Rule was required as of April 14, 2003 (April 14, 2004, for small health plans).
Online Resources for HIPAA

Interoperability Pledge
Companies that provide 90 percent of electronic health records used by hospitals nationwide as well as the top five largest health care systems in the country have agreed to implement three core commitments: consumer access, blocking/transparency, and standards.

Pledge Now

About HealthIT.gov
Health information technology (health IT) makes it possible for health care providers to better manage patient care through secure use and sharing of health information. Health IT includes the use of electronic health records (EHRs) instead of paper medical records to maintain patient's health information.

Learn more about the Office of the National Coordinator for Health Information Technology (ONC)

Learn more about the National Learning Consortium

Updates from HealthIT.gov
View additional updates

Discovery Infrastructure for Clinical Health IT Apps Cooperative Agreement Webinar
ONC will host an informational webinar about Funding Opportunity NAP-AX-16-001 "Discovery Infrastructure for Clinical Health IT Apps Cooperative Agreement" on Friday, March 25 from 2-3pm ET. Register for the event today!

Step-up to be part of the Interoperability Proving Ground
Read about the Interoperability Proving Ground, an open, community platform where you can share, learn, and be inspired by interoperability projects. If you lead an interoperability project, join us and add it to the IPG

From HealthIT’s Social Channels
Tweets by @ONC_HealthIT

ONC and @CMSgov are unlocking data, transforming care to work better for all Americans early2017 

#Medicaid

HealthITBuzz

Bridging the Healthcare Digital Divide
The great promise of technology is...

helpful.gov

PediatricSupport.com

Helping Pediatricians Succeed
Online Resources for HIPAA

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.
HIPAA DIY- Online Purchase

Comprehensive HIPAA Solution for CEs & BAs


PediatricSupport.com
HIPAA DIY- Books

Optum (Ingenix)

HIPAA Tool Kit 2016 (Includes a customizable compliance plan)

$299.95

SKU: HTKT16 Quantity: 1 Condition:

ADD TO CART CHECKOUT
HIPAA DIY- Monthly Subscription

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

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
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.
## GUIDED HIPAA COMPLIANCE PACKAGES

<table>
<thead>
<tr>
<th>HIPAA PRO</th>
<th>HIPAA PLUS</th>
<th>HIPAA BASIC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Annual: $2,399</td>
<td>Monthly: $209</td>
<td>Annual: $1,998</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Monthly: $159</td>
</tr>
</tbody>
</table>

### HIPAA PRO
- 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 24/7
- Customizable HIPAA Policy Templates (including a Breach Notification Policy)
- Business Associate Agreement Template
- Mobile Device Scanning
- HIPAA Training (8 seats for Security Awareness, Privacy and Security, and Responsible Use of Social Media trainings)

### HIPAA PLUS
- 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
- Mobile Device Scanning
- Unlimited Live Technical Support Available 24/7
- Customizable HIPAA Policy Templates (including a Breach Notification Policy)
- Business Associate Agreement Template

### HIPAA BASIC
- 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
- One Hour/Month Live Technical Support

© 2015 SecurityMetrics

PediatricSupport.com

Pediatric Management Institute
Helping Pediatricians Succeed
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 - 0.5 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.

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)
§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

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, palm-tops, MP3 players, cellular telephones, thumb drives, video cameras, and pagers.

Electronic storage media includes
Security Risk Assessment Tool

§164.308(a)(1)(ii) - Standard

Does your practice develop, document, and implement policies and procedures for assessing and managing risk to its ePH?

Yes ☐ No ☐ Flag ☐

Current Activities Notes Remediation

With respect to a threat/vulnerability affecting your ePH:

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.

<table>
<thead>
<tr>
<th>Black-market Value</th>
<th>$ 50 per medical record</th>
<th>$ 1 per credit card number</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Healthcare organizations</th>
<th>81% permit BYOD personally-owned devices connecting to their networks but only 21% scan BYOD devices prior to connection to network</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>HIPAA Penalties</th>
<th>$ 1.5 million for a lost unencrypted laptop</th>
<th>$ 1.7 million for a lost unencrypted laptop</th>
<th>$ 1.7 million for a lost unencrypted hard drive</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>HIPAA Covered Entities</th>
<th>700,000</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>HIPAA Business Associates</th>
<th>2,000,000 – 3,000,000</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Health Care</th>
<th>31% of all reported data breaches</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Only 115 HIPAA Audits</th>
<th>2009 – 2013 (out of 700,000 Covered Entities)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Only 100 per month</th>
<th>starting in 2014 (of 3.7 million organizations required to comply with HIPAA)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>But...13,000 Data Breach Investigations</th>
<th>HIPAA Office for Civil Rights</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>91% of healthcare organizations are using cloud-based services</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>47% are not confident in the ability to keep data secure in the cloud</th>
</tr>
</thead>
</table>