HIPAA: It’s Hip to be Square & Prepared!

AGRiP Fall Forum
October 7, 2019
Conversation outline

• HIPAA Overview
• Privacy & Security Policies
• Training - Board, staff, BAAs
• Risk Assessment
  • New Hampshire Schools Pool experience
  • Washington Cities experience
• Breach procedures
  • Incident v. breach
  • Tales of woe
• Value of being prepared
HIPAA Overview
HIPAA Overview

What Is HIPAA?

Health Insurance Portability and Accountability Act of 1996 Requirements
- Administrative simplification
- Privacy and security standards
- Electronic data interchange ("EDI") standards
- Breach notification requirements
- Portability of group health insurance
- Special enrollment rules
- Preexisting condition exclusions (now gone)
- Nondiscrimination rules
- Wellness programs

HIPAA's Intent
- Establish a Federal safeguard to protect the confidentiality of medical information
- Implement standards to protect and guard against the misuse of an individual's medical information
- Change the way an individual's medical information is used and disclosed by covered entities
HIPAA Overview

What Is HIPAA? (cont.)

The Four Primary Components
1. Privacy standards—who is authorized to use and disclose information and the right of individuals to determine how their information is to be used or disclosed.
2. Security standards—safeguards to protect the confidentiality, availability, and integrity of electronic health information.
3. Breach notification—requiring notification to individuals and HHS (and, in some cases, to the news media) when there is an impermissible use or disclosure of health information that compromises the information.
4. Transaction standards—promoting the standardization of certain payment-related electronic transactions (also referred to as the electronic data interchange or "EDI" standards). Today’s training will not cover this standard in detail.

HIPAA Terms

HIPAA Applies To
- Covered Entities and Business Associates with respect to Protected Health Information ("PHI")
- What do these terms mean?
Training - Board, staff, BAAs

**HIPAA and the AWC Trust**

**Self-Funded Plans**
- AWC Trust is ultimately responsible for all HIPAA privacy and security compliance for self-funded plans.
- Health Care Program: Medical, dental, vision, EAP, wellness.
- HIPAA and FSAs sponsored by members are also self-funded plans, but the Trust is not responsible for HIPAA compliance.
- Business associates also have responsibility.

**Insured Plans**
- Insurers are responsible for most compliance with HIPAA privacy and security regulations.

**Impact On the AWC Trust**

- Appoint a Privacy and Security Official.
- Conduct risk assessments of potential vulnerabilities of ePHI.
- Establish internal safeguards to protect PHI/ePHI.
- Develop and implement Privacy and Security Policies that meet the HIPAA Rule requirements.
- Ensure workforce compliance.
- Ensure adequate separation between Trust and AWC.
- Amend contracts with service providers (Business Associates) to preclude impermissible disclosures and ensure compliance with Security Rule.
**SCHOOLCARE HEALTH BENEFIT PLANS**

<table>
<thead>
<tr>
<th><strong>Ongoing</strong></th>
<th><strong>Contract with outside firm</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• On-Line/On-Demand Training for all staff; includes testing</td>
<td>• ProHIPAA for annual risk assessment</td>
</tr>
<tr>
<td>• Review and update of HIPAA Privacy and Security policies</td>
<td>• Documentation for compliance checklist</td>
</tr>
<tr>
<td>• Business Associate Agreement</td>
<td>• Telephone interviews (including outsourced IT); walk through of operations</td>
</tr>
<tr>
<td>• Review and update of internal policy/procedures</td>
<td>• Book of Evidence</td>
</tr>
<tr>
<td>• Implement specific recommendations from annual assessment</td>
<td>• Assessment Report (including specific recommendations)</td>
</tr>
<tr>
<td></td>
<td>• Breach Mitigation Services in event of data breach</td>
</tr>
</tbody>
</table>
SCHOOLCARE RISK ASSESSMENT – OUTCOMES 2018

• “High Compliance Risk” for Technology Provider
  • Needed annual HIPAA HITECH policies, procedures, training, and assessment
  • Enforce password complexity and computer logoff policies
  • Security log capturing and retention for 6 months

• Other Recommendations
  • Use visitor log in reception area
  • Perform background checks on all employees
SchoolCare Risk Assessment – Outcomes 2019

- “93% compliant with HIPAA and HITECH regulation and data security”
  - Technology partner moved from high to low compliance risk!

- Recommendations
  - Create internal data destruction policy
  - Update disaster recovery plan
  - Table talk walk through of emergency, contingency and incident response plan with technology partner and ProHIPAA
SCHOOLCARE RISK ASSESSMENT – LESSONS LEARNED

• Outsourced IT vendor presents additional risks

• Performing self-assessment many not always be best
  • Third party raises questions that may not have otherwise been considered

• On-going and Annual Process – may never by 100% compliance, but keep trying

• Assessment Cost and Time
  • <$5,000 and about 10 hours of staff time
AWC Trust Risk Assessment

<table>
<thead>
<tr>
<th>Ongoing</th>
<th>Contract with outside firm</th>
</tr>
</thead>
<tbody>
<tr>
<td>• HIPAA assessment with legal council</td>
<td>• Moss Adams; attorney/client privilege with Trust legal</td>
</tr>
<tr>
<td>• Review and update of HIPAA Privacy and Security policies</td>
<td>council</td>
</tr>
<tr>
<td>• Discussion with staff regarding internal policy/procedures</td>
<td>• AWC and Trust assessment (IT services provided via contract</td>
</tr>
<tr>
<td>• Review and update of internal policy/procedures</td>
<td>by AWC)</td>
</tr>
<tr>
<td></td>
<td>• Documentation request list</td>
</tr>
<tr>
<td></td>
<td>• Onsite and phone interviews; walk through of operations</td>
</tr>
<tr>
<td></td>
<td>• Draft and Final reports</td>
</tr>
</tbody>
</table>
AWC Trust Risk Assessment - Outcomes

- Few recommendations under HIPAA Security Policies
  - Continued work on internal disaster recovery planning
  - Review of contracts for services, BAA's

- Recommendations under HIPAA Privacy Policies
  - In progress, although draft would indicate minimal internal process change
AWC Trust Risk Assessment - Lessons Learned

- **RFP - select most appropriate vendor**
  - Understand the vendor, core strengths
  - Understand the client (us/you) and how services are provided

- **This is not an audit, this is an assessment**
  - Understand how risk level ratings are determined
  - Determine basis of assessment (HIPAA Privacy/Security Rules, Office of Civil Rights (OCR) guidance, etc.)

- **Timeline**
  - Significantly more time was needed than anticipated/planned for
Is it an Incident or a Breach?

**What Is a Reportable Breach? (cont.)**

**Four-factor risk assessment**
1. Nature and extent of PHI involved
   - Can PHI be used in a manner “adverse” to the individual?
2. Identity of unauthorized user or recipient
   - Also subject to HIPAA privacy rules?
3. Whether PHI was actually acquired or viewed
   - Laptop recovered, no PHI actually viewed
4. Extent to which risk to PHI has been mitigated
   - Confidentiality agreement

**Basic Breach Notification Rule**

If a Reportable Breach of the HIPAA Rules Has Occurred, the Covered Entity Must Give Notice of the Breach To
- Affected individuals
- HHS
- Media (in certain situations)
Civil Actions For Health Privacy Violations: Unauthorized Disclosure of Medical Information

– Plaintiff underwent psychiatric treatment around same time he was being sued by wife for divorce.
– Wife’s attorney subpoenaed plaintiff’s psychiatric records but parties settled divorce so records never admitted into evidence.
– Wife’s attorney also gave plaintiff’s psychiatric records to prosecutor in criminal assault case against plaintiff.
– Ohio Supreme Court said waiver for divorce not cover criminal case.

• “it is for the patient…to determine what the patient’s interests are with regard to personal confidential medical information”
Civil Actions For Health Privacy Violations:
Invasion of Privacy

- Public Disclosure of Private Facts
  - A civil tort in some states, including Ohio.

- To be actionable, it must:
  - Be a public disclosure;
  - The facts disclosed must concern the private life of an individual, not his or her public life;
  - The matter disclosed must be one which would be highly offensive and objectionable to a reasonable person of ordinary sensibilities;
  - The disclosure must have been made intentionally, not negligently; and
  - The matter disclosed must not be of legitimate concern to the public.
Civil Actions For Health Privacy Violations: Public Disclosure of Private Facts

– Employee pursuing workers compensation claim obtained a psychological report from physician.
– The report was given to the employee responsible for managing workers compensation claims and she intended to forward to the employer’s attorney.
– But she accidentally forwarded to other employees instead of the attorney.
– The Court dismissed the plaintiff’s claim because:
  • The disclosure was not intentional; and
  • The disclosure did not constitute “publication” for purposes of a claim of invasion of privacy.
Civil Actions For Health Privacy Violations:
Invasion of Privacy

- **Wrongful Intrusion**
  - Must be wrongful intrusion into one’s private activities in such a manner as to outrage or cause mental suffering, shame or humiliation to a person of ordinary sensibilities.
  - Does not require publicity of private matters.
  - But must be intentional and highly offensive to a reasonable person.

- There are various defenses:
  - Plaintiff did not intend to keep information private;
  - Plaintiff did not have reasonable expectation of privacy;
  - Plaintiff voluntarily and without any coercion consented to disclosure.
Civil Actions For Health Privacy Violations: Invasion of Privacy

– Plaintiffs alleged that the defendant failed to protect their electronic medical information, and the defendant’s administration improperly accessed and disclosed that information.

– However, the court dismissed plaintiffs’ claims because the court found that defendant *negligently* failed to protect privacy by not taking reasonable steps to protect information.

– But the improper actions by defendant were not intentional.
Compliance Enforcement

**Compliance Enforcement**

**Civil Penalties Imposed By HHS**
- Tens of millions ranging from $100 to a maximum of $1.9M (inflation adjusted, currently $1,877,399)
- "Did not know, "reasonable cause," "willful neglect, corrected," "willful neglect, not corrected"
- Same act or omission may violate privacy and security—penalties for each
- On April 20, 2018, OCR announced new penalty levels for annual limits for "will not know" (SNK), "reasonable cause" (RBC), and "willful neglect, corrected" (SBNRK) (inflation adjusted)

**Criminal Penalties (DOJ): U.S. Attorneys General**
- Up to $250,000 and 10 years
- As of 3/31/2018, HHS has referred 184 complaints to DOJ

**Civil Actions By State Attorneys General**
- Up to $100 per violation, capped at $25,000.
Compliance Enforcement

OCR Settlement Of $16M With Anthem—Largest Ever
- Largest health data breach in U.S. history between December 2014 – January 2015
- Cybercriminals gained access to Anthem’s systems via spear phishing emails
- Breach affecting records of 78.8M members

OCR Settlements of $5.5M
- Memorial Healthcare System
  - PHI of 100,000+ individuals impermissibly accessed by employees and impermissibly disclosed to affiliated physician office staff with use of former employee’s login
- Advocate Health Plan:
  - Multiple data protection violations, including noncompliance with data security laws following three breach notification reports in four months
Compliance Enforcement

- Staff of unrestrained entities and covered BUs should be made aware of HIPAA requirements.
- OCR settlement with National Science Foundation.
- Improvement of patient privacy, includingypsy patient access to medical records.
- OCR settlement with Boston Medical.
- Unlawful use of electronic equipment.
- OCR settlement with Duke University.
- Theft of unsecured storage.
- OCR settlement with University of Texas Medical Center.

The Moral Of The Story:
- It is not enough to comply with the rules; compliance and the process must be documented.
- OCR is auditing Covered Entities and Business Associates, focusing on:
  - Breach notification: timeliness and content of notices.
  - Notice of privacy practices.
  - Security risk assessment.
  - Not only "desk audits" (requests for documents), but also on-site inspections.
Value of Being Prepared - It’s Hip to be Square!

- Understand who your Privacy & Security Officials are and review your policies/procedures regularly
- Frequently review policy/procedures with staff handling PHI, and provide training
- Review/update contracts with vendors/Business Associates on a regular basis
- Contracting out with a vendor to provide a HIPAA Assessment can provide valuable information to your organization
- Consult with your legal counsel when in doubt!