Auditing for HIPAA Compliance: Evaluating security and privacy compliance in an organization that provides health insurance benefits to employees

San Antonio IIA: I HEART AUDIT CONFERENCE
February 24, 2017
Stinnett & Associates, LLC (Stinnett) is a professional advisory firm which excels at maximizing value for both public and private organizations. Our services are designed to help clients more effectively manage risk and improve performance by streamlining processes, reducing costs, and enhancing controls.

Stinnett offers co-source and outsource solutions within a diverse range of services, including:

- Process Design and Re-engineering
- Internal Audit
- Governance Risk and Compliance
- Sarbanes-Oxley
- Fraud Investigation
- Fraud Risk Assessment
- Cost Recovery
- Information Technology
- Enterprise Risk Management

**Doing the Right Thing**

Founded in 2001, Stinnett has grown to a professional staff of 83 in 2017 (58 permanent members and 25 contractors). We have offices in Dallas, Houston, Oklahoma City, San Antonio, and Tulsa. We provide services to several Fortune 1000 companies as well as many mid to large size organizations with global operations.

We are primarily recognized for offering relevant advisory assistance and exemplary client service with the unique ability to deliver what our clients need. Working toward solutions, we have a reputation for “doing the right thing.”

Stinnett is a certified Women’s Business Enterprise through the Women’s Business Enterprise National Council. We pride ourselves on being trusted business advisors who focus on assisting clients to reach strategic milestones positioning them for future success.
LEARNING OBJECTIVES

- Understand the HIPAA standards and their applications
- Understand the PHI Privacy & ePHI Security Rules
- Learn to audit for the federal HIPAA standards related to the Privacy & Security Rules
- Leave with useful tips for conducting HIPAA Privacy & Security audits
CONTENT

- What is HIPAA?
  - Security Rule
  - Privacy Rule
  - Protected Health Information
- What is a Covered Entity?
- What is a Business Associate?
- Audit Approach & Techniques
- Breaches and Penalties
HIPAA: Some background

“Somehow your medical records got faxed to a complete stranger. He has no idea what’s wrong with you either.”
BACKGROUND OF HIPAA


- Why HIPAA?
  - Pre-HIPAA, there was no universally recognized security standard for PHI. The standards established a security and privacy management framework for protecting the confidentiality, integrity, and availability of ePHI and PHI.
  - Goals: Simplify administrative processes, protect patient privacy


Source: www.hhs.gov
The **Office of Civil Rights (OCR)** is responsible for enforcing the HIPAA Privacy and Security Rules

- Investigates filed complaints as well as governs self-reporting
- OCR conducts compliance reviews
- OCR preforms education outreach

*Source: www.hhs.gov*
HIPAA: FIVE SECTIONS

Title I
- Healthcare Access, Portability, & Renewability

Title II
- Preventing Healthcare Fraud & Abuse
- Medical Liability Reform
- Administrative Simplification

Title III
- Tax-Related Health Provision

Title IV
- Group Health Plan Requirement
- Group Revenue Offsets

Title V
- Electronic Data Interchange
- Privacy
- Security
- Administrative Safeguards CFR § 164.308
- Physical Safeguards CFR § 164.310
- Technical Safeguards CFR § 164.312

Source: www.nist.gov
HIPAA: FIVE SECTIONS (cont’d)

- Title II
  - Preventing Healthcare Fraud & Abuse
  - Medical Liability Reform
  - Electronic Data Interchange
  - Administrative Simplification
  - Privacy
  - Security
    - Administrative Safeguards CFR § 164.308
    - Physical Safeguards CFR § 164.310
    - Technical Safeguards CFR § 164.312
PROTECTED HEALTH INFORMATION

- **PHI** - The Privacy Rule protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.

- “Individually identifiable health information” is information, including demographic data, that relates to:
  - the individual’s past, present or future physical or mental health or condition,
  - the provision of health care to the individual, or
  - the past, present, or future payment for the provision of health care to the individual,

- and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual.

*Source: www.hhs.gov*
PROTECTED HEALTH INFORMATION

- Name
- Address
- Dates
- Telephone & Fax numbers
- Email addresses
- SSN
- Medical Record Numbers
- Health plan beneficiary number
- Account number
- Certificate/License number
- Web URL
- IP address
- Fingerprints, voice prints
- Photographic images
- Any other characteristic that could uniquely identify the individual

- Medical records
- Claims
- Payments
- Eligibility
- Other health plan-related insurance data
HIPAA PRIVACY RULE

• “Standards for Privacy of Individually Identifiable Health Information”

• Organizations must identify the uses and disclosures of Protected Health Information (PHI) and put into effect appropriate safeguards to protect against an unauthorized use or disclosure of that PHI. When material breaches or violations of privacy are identified, the organizations must take reasonable steps to solve those problems in order to limit exposure of PHI.

   **Goal:** assure that individuals’ health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well-being.

   **Summary:**
   • Sets forth standards to protect individuals’ medical records and other PHI
   • Imposes restrictions on the use and disclosure of PHI
   • Establishes patients’ rights over their health information, including rights to obtain copies of their health records and request corrections.

   *Source: www.hhs.gov*
HIPAA SECURITY RULE

- “Security Standards for the Protection of *Electronic* Protected Health Information”

- Defines the administrative, physical, and technical safeguards to protect the confidentiality, integrity and availability of *electronic* Protected Health Information (ePHI)

**Goal:** To protect the privacy of individuals’ health information while allowing covered entities to adopt new technologies to improve the quality and efficiency of patient care.

**Summary:**
- Intended to protect *electronic* PHI
- Secure the confidentiality, integrity, and availability of the data while still being flexible enough to allow authorized use and disclosure
- Acknowledging that Covered Entities are adopting new technologies to improve the quality and efficient of patient care

*Source:* www.hhs.gov
HITECH

• Health Information Technology for Economic and Clinical Health (HITECH)
• American Recovery and Reinvestment Act of 2009 (the “Stimulus Bill”)
• Expanded on requirements in the 1996 HIPAA rule and its regulations to protect the privacy and security of protected health information (“PHI”)
  • Create incentives to accelerate the adoption of Electronic Health Records (EHR) systems among providers
  • Broaden the scope of privacy and security protections listed under HIPAA, increase the penalties and enforcement potential for non-compliance
  • Change the liability and responsibilities of Business Associates
  • Redefine what a breach is
  • Create stricter notification standards
  • Tighten enforcement
  • Create new code and transaction sets (HIPAA 5010, ICD10)

Source: www.hhs.gov
What is a Covered Entity?

Knock Knock!
-Who's there?
HIPAA!
-HIPAA who?

I can't tell you that.
A **Covered Entity** is any organization or corporation that directly handles Personal Health Information (PHI) or Personal Health Records (PHR).

*Is my organization considered a Covered Entity?*


*Source: www.hhs.gov*
COVERED ENTITY: THREE TYPES

1. A Health Care Provider
   - Doctors, Dentists
   - Psychologists, Chiropractors
   - Clinics, Pharmacies

2. A Health Plan
   - Health insurance companies
   - HMOs
   - Company health plans
   - Government programs that pay for healthcare (e.g. Medicare, Medicaid)

3. A Health Care Clearinghouse
   - This includes entities that process nonstandard health information they receive from another entity into a standard (i.e., standard electronic format or data content), or vice versa.

Source: www.hhs.gov
A self-insured health plan program is permitted under the Employee Retirement Income Security Act (ERISA), and may be known as an “ERISA plan.”

Self-insured health plans are considered Group Health Plans (GHPs) and are subject to HIPAA regulations § 160.103.

A group health plan, as defined by HIPAA (p. 82,799), is:

- an employee welfare benefit plan (as defined in... ERISA), including insured and self-insured plans, to the extent that the plan provides medical care..., including items and services paid for as medical care, to employees or their dependents directly or through insurance, reimbursement, or otherwise that:
  - Has 50 or more participants (as defined in...ERISA); or
  - Is administered by an entity other than the employer that established and maintains the plan.

Question: As an employer, I sponsor a group health plan for my employees. Am I a Covered Entity under HIPAA?

Answer:

- A "group health plan" is one type of health plan and is a Covered Entity (except for self-administered plans with fewer than 50 participants).
- The group health plan is considered to be a separate legal entity from the employer or other parties that sponsor the group health plan.
- Neither employers nor other group health plan sponsors are defined as Covered Entities under HIPAA.
- The Privacy Rule does control the conditions under which the group health plan can share PHI with the employer or plan sponsor when the information is necessary for the plan sponsor to perform certain administrative functions on behalf of the group health plan. See 45 CFR 164.504(f).

Source: www.hhs.gov
What is a Business Associate?

I DON'T KNOW WHO YOU ARE

BUT HIPAA WON'T LET ANYONE ELSE KNOW EITHER

negenerator.net
BUSINESS ASSOCIATES

- A Business Associate ("BA") is an entity or person, other than a member of the workforce of a covered entity, that performs functions or activities on behalf of, or provides certain services to, a covered entity that involves creating, receiving, maintaining, or transmitting PHI and any subcontractor that creates, receives, maintains, or transmits PHI on behalf of another business associate.

- Examples: Billing company, prescription drug vendors, malpractice insurer, data storage entities, EMR companies, paper shredding companies, claims recovery, medical plan data warehouse, and cloud service provider.

Source: www.hhs.gov
• BAs are now directly subject to HIPAA rules, not just required to comply with terms of Business Associate Agreements (BAA). (See HITECH.)

• If an organization has engaged an external party to perform any of the services we discussed, you should have a contract with that third party to set forth the services provided and any rules and obligations of the relationship. That contract is referred to as a BAA.

• If your current BAA was signed on or before January 24, 2013, then it will be deemed HIPAA compliant through September 23, 2014. Any new BAAs signed after January 24, 2013 should comply with the new requirements.

Source: www.hhs.gov
BUSINESS ASSOCIATES (cont’d)
When a covered entity engages the services of a Cloud Service Provider (CSP) to create, receive, maintain, or transmit ePHI, on its behalf, the CSP is a BA under HIPAA.

- When a BA subcontracts with a CSP, the CSP subcontractor itself is also a BA.
- If the CSP processes or stores only encrypted ePHI and lacks an encryption key for the data, it’s a BA.

The Covered Entity (or BA) and the CSP must enter into a HIPAA-compliant BAA, and the CSP is both contractually liable for meeting the terms of the BAA and directly liable for compliance with the applicable requirements of the HIPAA Rules.


Source: www.hhs.gov
Auditing for the HIPAA Security & Privacy Rules

BRACE YOURSELF

HIPAA AUDITS ARE COMING!
WHY AUDIT FOR HIPAA COMPLIANCE?

• 164.308(a) **Standard**: Evaluation. Perform a periodic technical and nontechnical evaluation (AUDIT).

• 2016 announcement by HHS Office for Civil Rights (OCR)
  • As a part of continued efforts to assess compliance with the HIPAA Privacy, Security and Breach Notification Rules, the OCR has begun its next phase of **audits of Covered Entities (CE)** and their BAs.
  • The 2016 Phase 2 HIPAA Audit Program will **review the policies and procedures adopted and employed by CEs and their BAs to meet selected standards and implementation specifications of the Privacy, Security, and Breach Notification Rules.**
  • Comprehensive onsite audits of both CEs and BAs will begin in early 2017

• Evaluate the effectiveness of internal compliance policies, procedures, and processes to compare ePHI-related security practices and PHI-related privacy practices to the HIPAA standards.

*Source: www.hhs.gov*
AUDIT SCOPE

- Whole organization
- Specific functions
- Specific departments
- Specific CFR safeguards
- Design review (verbal and walkthroughs)
- Substantive review (proof of compliance)
- Targeted risk areas: e.g. Transmission Security, Access Controls, Integrity
- Business Associate reviews
- Policies and procedures review
- Organizational requirements
- Security standards
CODE OF FEDERAL REGULATIONS (CFR)

Title II

Security Standards: General Rules
CFR § 164.306

Administrative Safeguards
CFR § 164.308

Physical Safeguards
CFR § 164.310

Technical Safeguards
CFR § 164.312

Organizational Requirements
CFR § 164.314

Policies & Procedures & Documentation Requirements
CFR § 164.316

- Security Management Process
- Assigned Security Responsibility
- Workforce Security
- Information Access Management
- Security Awareness & Training
- Security Incident Procedures
- Contingency Plan
- Evaluation

- BA Contracts & Other Arrangements

- Facility Access Control
- Workstation Use
- Device & Media Control

- Access Control
- Audit Controls
- Integrity
- Person or entity authentication
- Transmission Security
CODE OF FEDERAL REGULATIONS (CFR) (cont’d)

- CFR § 164.308 – Administrative Safeguards
- CFR § 164.310 – Physical Safeguards
- CFR § 164.312 – Technical Safeguards

“REQUIRED” vs “ADDRESSABLE”

- “Required”: the specification must be implemented
- “Addressable”: Covered Entity must do one of the following:
  ◦ implement the specification,
  ◦ implement an alternative solution that achieves the same purpose, or
  ◦ document why they are not implementing the specification

- provides covered entities flexibility in complying with the security standards
- The covered entity’s choice must be documented

Source: www.hhs.gov
HIPAA COMPLIANCE MANUAL

- HIPAA Policies
- Internal PHI Flowchart
- External PHI Flowchart
- Business Associate Listing
- Copies of Business Associate Agreements
- Privacy Officer Responsibilities
- HIPAA Privacy Procedures
- Security Officer Responsibilities
- HIPAA Security Procedures
- Security Breach Notification Procedure
- Security Compliance Review

- Authorization Forms / Notices
  - Notice of Privacy Practices
  - Right to Access PHI
  - Right to Amend PHI
  - Right to an Accounting of PHI
  - Right to Restrict Use and/or Disclosure of PHI
  - Right to Alternative Communications of PHI
  - Authorization Forms for Release of Information
SECURITY OFFICER, PRIVACY OFFICER

- Under HIPAA, Covered Entities must designate a Privacy Officer and a Security Officer.
  - The Security Officer and Privacy Officer may have other titles and duties in addition to this designation.

- The **Privacy Officer** is typically a high-ranking HR/Benefits manager / executive.
  - In terms of HIPAA compliance, the **Privacy Officer shall oversee all ongoing activities related to the development, implementation and maintenance of the practice/organization’s privacy policies in accordance with applicable federal and state laws.**

- The **Security Officer** is typically a high-ranking IT manager / executive.
  - **The Security Officer is responsible for the development and implementation of the relevant security policies and procedures** for the entity. (164.308(a)(2))
## Example Audit Plan

### Evaluation

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2.8</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>A</strong></td>
<td>Obtain a copy of the periodic technical and nontechnical evaluation policies and procedures.</td>
<td>164.308(a)(8) Standard: Evaluation. Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which an entity’s security policies and procedures meet the requirements of this subpart.</td>
</tr>
<tr>
<td><strong>B</strong></td>
<td>Verify the policies and procedures conform to 164.308(a)(8).</td>
<td>164.308(a)(8) Standard: Evaluation. Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which an entity’s security policies and procedures meet the requirements of this subpart.</td>
</tr>
</tbody>
</table>

### Business Associate Contracts and Other Arrangements

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2.9</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>A</strong></td>
<td>Obtain a copy of the standard HIPAA Business Associate agreement template and verify there are satisfactory assurances that the Business Associate will appropriately safeguard PHI.</td>
<td>164.308(b)(1) Standard: Business associate contracts and other arrangements. A covered entity, in accordance with 164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity’s behalf only if the covered entity obtains satisfactory assurances, in accordance with 164.314(a) that the business associate will appropriately safeguard the information.</td>
</tr>
<tr>
<td><strong>B</strong></td>
<td>Verify there are established written contracts or other arrangements with Business Associates that document satisfactory assurances required by §164.308(b)(1) that meets the applicable requirements of §164.314(a).</td>
<td>164.308(b)(4) Written contract or other arrangement (Required). Document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).</td>
</tr>
</tbody>
</table>

### Physical Safeguards

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>A</strong></td>
<td>Obtain and verify policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.</td>
<td>164.310(a)(1) Standard: Facility access controls. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.</td>
</tr>
<tr>
<td><strong>B</strong></td>
<td>Verify there are established (and implemented 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>
<td>163.310(a)(2)(i) 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.</td>
</tr>
<tr>
<td><strong>C</strong></td>
<td>Verify there are implemented policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.</td>
<td>164.310(a)(2)(ii) Facility security plan (ADDRESSABLE). Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.</td>
</tr>
<tr>
<td><strong>D</strong></td>
<td>Verify there are implemented procedures to control and validate a</td>
<td>163.310(a)(2)(iii) Access control and validation procedures (ADDRESSABLE). Implement procedures to control and validate a</td>
</tr>
</tbody>
</table>
1. **Security Management Process:** verify procedures are in place to prevent, detect and correct security violations

2. **Assigned Security Responsibility:** verify a Security Officer is established and documented roles and responsibilities exist

3. **Workforce Security:** confirm controls around appropriate access to ePHI

4. **Information Access Management:** confirm controls around granting authorization to electronic health information

5. **Security Awareness Training:** verify training is in place for workforce

6. **Security Incident Procedures:** verify policies and procedures are in place to address security incidents

7. **Contingency Plan:** verify policies and procedures to ensure the integrity of data in responding to an emergency or other occurrence

8. **Evaluation:** verify policies and procedures exist for periodic technical and nontechnical evaluation

9. **Business Associate Contracts and Other Arrangements:** verify appropriate agreements and contracts are in place with Business Associates to appropriately safeguard PHI

*Source: [www.hhs.gov](http://www.hhs.gov)*
Workforce Security – confirm controls around appropriate access to ePHI

CFR § 164.308(a)(3)

Testing approach:

1. Obtain policies and procedures ensuring all members of the workforce have appropriate access to ePHI.

2. Verify there are implemented procedures for the authorization and/or supervision of employees who work with ePHI or in locations where it might be accessed.

3. Verify there are procedures implemented to determine whether personnel access to ePHI is appropriate.

4. Verify there are implemented procedures for terminating access to ePHI when an employee leaves the organization or no longer has a valid business need to access the data.
Information Access Management – confirm controls around granting authorization to electronic health information

CFR § 164.308(a)(4)

Testing approach:
1. Obtain policies and procedures for authorizing access to ePHI that are consistent with the applicable requirements of the Privacy of Individually Identifiable Health Information (§164.5xx).
2. If a clearinghouse that is part of a larger organization, verify there are implemented policies and procedures to protect ePHI from the larger organization.
3. Verify there are implemented policies and procedures for granting access to ePHI, for example, through access to a workstation, transaction, program, or process.
4. Verify there are implemented policies and procedures that are based upon access authorization policies, establish, document, review, and modify a user’s right of access to a workstation, transaction, program, or process.
HIGHLIGHT ON: SECURITY AWARENESS TRAINING

- **Security Awareness Training** – verify training is in place for workforce
- **CFR § 164.308(a)(5)**
- **Testing approach:**
  1. Obtain a copy of the security awareness and training program for all members of its workforce (including management). Perform testing to confirm training was delivered to new hires.
  2. Determine whether periodic information security reminders are provided to relevant personnel.
  3. Verify policies and procedures for guarding against, detecting, and reporting malicious software are in place.
  4. Verify procedures for monitoring login attempts and reporting discrepancies are in place.
  5. Verify that procedures for creating, changing, and safeguarding passwords are in place.
1. **Facility Access Controls**: verify policies and procedures are in place to appropriately limit physical access to facilities and systems which contain PHI.

2. **Workstation Use**: verify policies and procedures are in place to specify the proper functions to be performed, and the manner which those functions are to be performed on workstations which can access ePHI.

3. **Workstation Security**: verify policies and procedures are in place to safeguard systems which can access ePHI.

4. **Device and Media Controls**: examine controls regarding receipt and removal of hardware and electronic media containing PHI.

---

**Source**: www.hhs.gov
HIGHLIGHT ON: FACILITY ACCESS

- **Facility Access** – verify policies and procedures are in place to appropriately limit physical access to facilities and systems which contain PHI

- **CFR § 164.310(a)**

- Testing approach:
  1. Obtain and verify policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.
  2. Verify there are established (and implemented 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.
  3. Verify there are implemented policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
  4. Verify there are implemented 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.
  5. Verify there are implemented policies and procedures to document repairs and modifications to the physical components of a facility, which are related to security (for example, hardware, walls, doors, and locks).
**HIGHLIGHT ON: DEVICE & MEDIA CONTROLS**

- **Device and Media Controls** - examine controls regarding receipt and removal of hardware and electronic media containing PHI.
- **CFR § 164.310(d)**
- **Testing approach:**
  1. Obtain policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility, and the movement of these items within the facility.
  2. Verify there are implemented policies and procedures to address final disposition of ePHI, and/or hardware or electronic media on which it is stored.
  3. Verify there are implemented procedures for removal of ePHI from electronic media before the media are available for reuse.
  4. Verify there is a maintained record of the movements of hardware and electronic media and the person responsible for its movement.
  5. Verify creation of a retrievable, exact copy of ePHI, when needed, before movement of equipment.
1. **Access Controls:** review and verify monitoring and access control procedures to ensure only authorized personnel can access health information.

2. **Audit Controls:** verify mechanisms are in place to monitor and record activity in information systems which contain ePHI.

3. **Integrity Controls:** verify controls exist to monitor and track electronic access to health information and that proper retention schedules are maintained and adhered to.

4. **Person or Entity Authentication:** verify procedures are in place to validate the person or entity seeking access to ePHI is the one claimed.

5. **Transmission Security:** verify technical security measures are in place and effective at safeguarding ePHI in transit over electronic communication networks.

*Source: www.hhs.gov*
**HIGHLIGHT ON: AUDIT CONTROLS**

- **Audit Controls** – verify mechanisms are in place to monitor and record activity in information systems which contain ePHI.
- **CFR § 164.312(b)**
- **Testing approach:**
  1. Obtain policies and procedures for Audit Controls, hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI and verify compliance with 164.312(b).
TOOLS & TECHNOLOGIES AUDITED

- Data Loss Prevention
- Email Encryption
- Vulnerability Scanners
- Policy Management Scanners
- Configuration Managers
- Log Management and Correlation (SIEM)
- Identity Management
- Intrusion Prevention Systems
Breaches and Penalties

DO YOU WANT A HIPAA VIOLATION?

BECAUSE THAT'S HOW YOU GET A HIPAA VIOLATION
BREACH NOTIFICATION

- Breaches need to be reported to the Office of Civil Rights (OCR) Secretary
- Examples of non-healthcare companies reporting breaches:
  - Omaha Construction Industry
  - Indiana University
  - Ashley Industrial Molding, Inc.
  - Burlington Northern
  - Omaha Construction Industry
  - Alamo
  - Sheet Metal Local 36 Welfare Fund
- [https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf](https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf)

**Source:** www.hhs.gov
## HIPAA VIOLATIONS

<table>
<thead>
<tr>
<th>HIPAA Violation</th>
<th>Minimum Penalty</th>
<th>Maximum Penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Individual did not know</strong> (and by exercising reasonable diligence would not have known) that he/she violated HIPAA</td>
<td>$100 per violation, with an annual maximum of $25,000 for repeat violations (Note: maximum that can be imposed by State Attorneys General regardless of the type of violation)</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
<tr>
<td>HIPAA violation <strong>due to reasonable cause</strong> and not due to willful neglect</td>
<td>$1,000 per violation, with an annual maximum of $100,000 for repeat violations</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
<tr>
<td>HIPAA violation <strong>due to willful neglect</strong> but violation is corrected within the required time period</td>
<td>$10,000 per violation, with an annual maximum of $250,000 for repeat violations</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
<tr>
<td>HIPAA violation is due to <strong>willful neglect and is not corrected</strong></td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
</tbody>
</table>

*Source: www.hhs.gov*
HELPFUL TOOLS & REFERENCES

- HHS.GOV
  https://www.hhs.gov/hipaa/for-professionals/training/index.html

- HHS.GOV List Server
  https://www.hhs.gov/hipaa/for-professionals/list-serve/index.html

- HSR Toolkit
  https://scap.nist.gov/hipaa/

- NIST Special Publication 800-66 Revision 1
  https://www.nist.gov/healthcare/security/hipaa-security-rule

- HITRUST
  https://hitrustalliance.net/

- BLOGS (follow researchers for up-to-date information)
Jennifer Brandt | Principal
mobile (888) 808-1795
jennifer.brandt@stinnett-associates.com

Jeremy Price | Senior Manager
mobile (918) 281-8475
jeremy.price@stinnett-associates.com