HIPAA
How to Comply with Limited Time & Resources

Jonathan Pantenburg, MHA, Senior Consultant
JPantenburg@Stroudwater.com
August 17, 2017

STROUDWATER

Stroudwater Associates is a **leading national healthcare consulting firm serving healthcare clients exclusively.**

We focus on strategic, operational, and financial areas where our perspective offers the highest value and are proud of our 32-year track record with rural hospitals, community hospitals, healthcare systems, and large physician groups.

Presenter Bio

STROUDWATER

JONATHAN R. PANTENBURG, MHA
Senior Consultant

Jonathan joined Stroudwater in 2016, and brings to the firm a strong record of leadership in rural healthcare. A highly accomplished, results-driven senior executive, Jonathan has more than 12 years of progressively responsible experience advising profit, non-profit, and governmental entities through complex issues including cost reduction, acquisitions, contracts, financial analysis, and operations.

Representative Accomplishments

- Improving performance through strategic, financial, and operational engagements
- Assessing the financial feasibility of CAHs and STAC facilities accessing significant capital through HUD, USDA, municipal bonds, and or other lending mechanisms
- Health system redevelopment: collaborating with hospitals, health systems, and networks to determine optimal clinical and operational integration strategies
- Assessing the financial feasibility and net benefits of system integration for primary care practices, CAHs, and short-term acute care facilities

We assist healthcare organizations and business associates develop and implement practices to secure patient data, and comply with HIPAA/HITECH regulations and Meaningful Use (MU) EHR incentive programs.
http://www.ehr20.com/

Disclaimer

This webinar has been provided for education and information purposes only and is not intended and should not be construed to constitute legal advice nor does this presentation cover every aspect of the Privacy and Security Rules

Please consult your attorney(s) in connection with any fact-specific situation under federal law and applicable state or local laws that may impose additional obligations on you and your company

Overview

Stroudwater

Overview

HIPAA Compliance

- Privacy Rule
- Security Rule
- Breach / Notification

HIPAA Violations and Enforcement

Steps Towards HIPAA Compliance

Common Terms

PHI: Protected Health Information

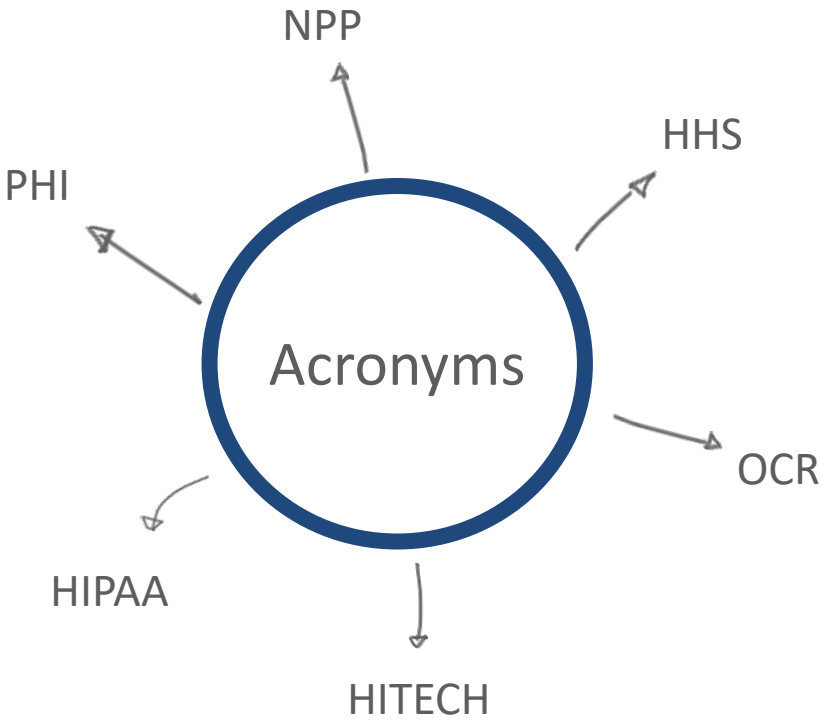
NPP: Notice of Privacy Practices

HHS: Health and Human Services

OCR: Office for Civil Rights

HITECH: Health Information Technology for Economic and Clinical Health

HIPAA: Health Insurance Portability and Accountability Act



What is HIPAA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) made significant changes to healthcare in the following areas:

1. **Health Insurance Reform**
2. **Administrative Simplification**
3. **Tax Related Health Provisions**
4. **Group Health Plan Requirements**
5. **Revenue Offsets**

The goal of HIPAA was to:

- Require the protection and confidential handling of PHI
- Reduce health care fraud and abuse
- Set industry-wide standards for health care information on electronic billing, etc.
- Allow individuals to transfer health insurance coverage

Why Comply With HIPAA

HIPAA compliance is not an option and is required by law

Failure to comply with HIPAA requirements could lead to the following:

- Personal risk including penalties and sanctions
- Organizational risk including financial penalties and reputational harm

We are entrusted by our patients to preserve and protect the privacy of sensitive and personal information

HIPAA COMPLIANCE

HIPAA Compliance Overview

STROUDWATER

Privacy

- Confidentiality of PHI
- Permitted Uses
- Patient Rights

Security

- Protection of ePHI

Breach

- Notification

Changes to HIPAA

The Health Information Technology for Economic and Clinical Health Act (HITECH), which was a part of the American Recovery and Reinvestment Act (ARRA) of 2009, widened the scope of privacy and security protections available under HIPAA

Specifically, ARRA/HITECH impacted the following areas with regard to HIPAA:

- Business Associates and Business Associate Agreements
- Enforcement
- Notification of Breach
- Electronic Health Record Access

What is Protected

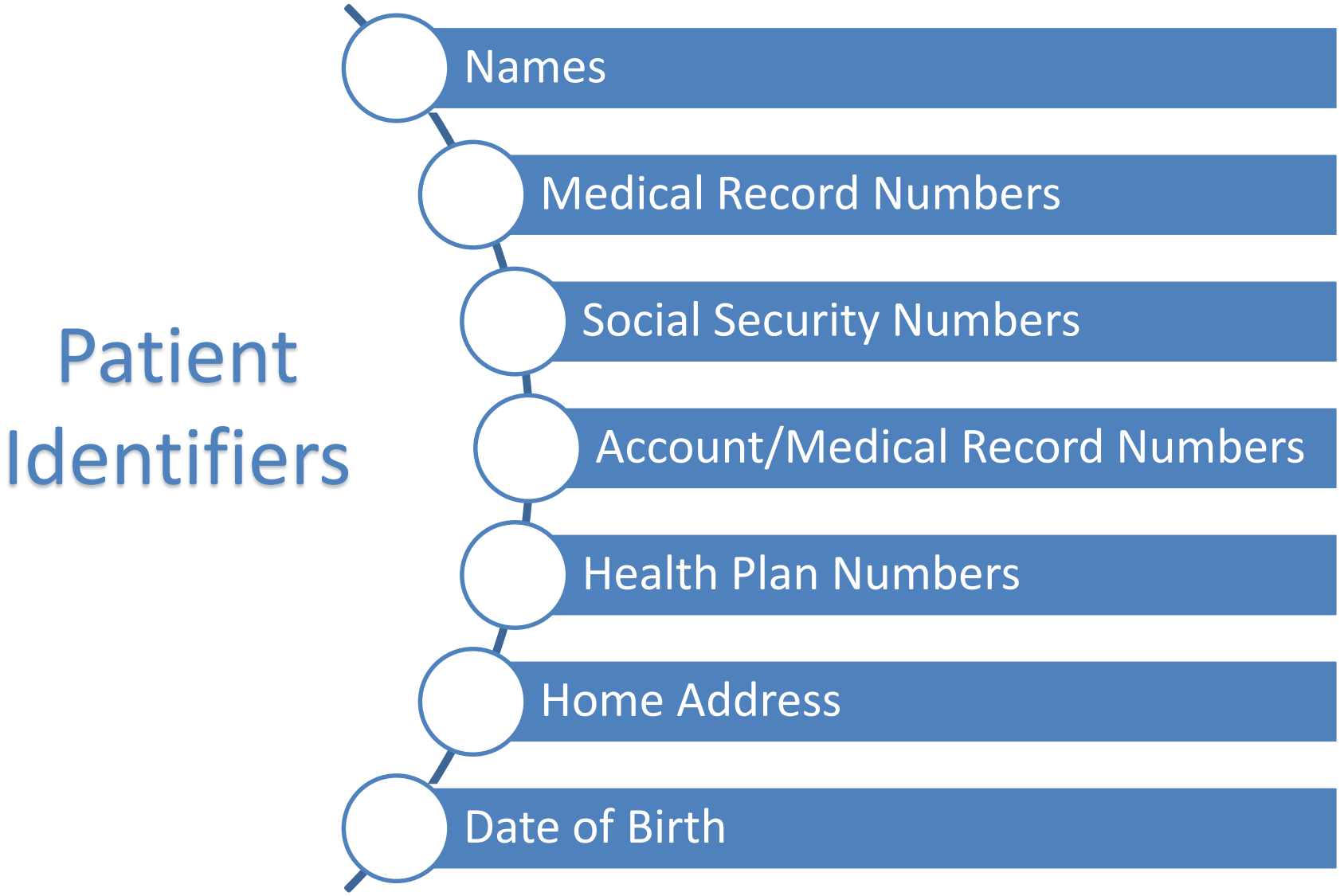
Protected Health Information (PHI) is all individually identifiable health information created, held, and or transmitted by a covered entity or its business associate, including demographic data, that relates to:

- The individual's past, present or future physical or mental health or condition
- The provision of healthcare to the individual, or
- The past, present, or future payment for the provision of healthcare to an individual

PHI also includes any information that identifies an individual or could be used through a reasonable basis to identify an individual

Patient Identifier Examples

STROUDWATER



PHI Uses and Disclosures

- **Uses**
  - When an organization reviews or uses PHI internally
    - This includes, but is not limited to: audits, trainings, quality improvement, and customer service

- **Disclosures**
  - When an organization releases or provides PHI to someone or another organization
    - This includes, but is not limited to: attorneys, patients, other providers, and business associates

Minimum Necessary

Regardless of use or disclosure, healthcare organizations must apply the “Minimum Necessary” principle for PHI

The Minimum Necessary principle states organizations must use and or disclose/release only the minimum necessary information to accomplish the intended purpose of the use, disclosure, or request

- Use Request:
  - Identify those who need access to PHI
  - Restrict access on a “need-to-know” basis
  - Continue to monitor access to PHI
- Disclosure Request:
  - When releasing information, limit PHI to no more than what is need to accomplish the purpose for which the request is made

Patient Rights

HIPAA grants patients the following rights:

- Access to patient health information
- An expectation that healthcare organizations will protect their health information
- Notice of Privacy Practices and Reminders
  - This summarizes how an organization will use and disclose PHI
- The right to alternative communication methods
- The right to individual privacy
- The right to file complaints

Security Rule Application

STROUDWATER

Administrative Safeguards

Organizations are required to have policies and procedures for employees to maintain security (e.g. disaster, internet and e-mail use)

Technical Safeguards

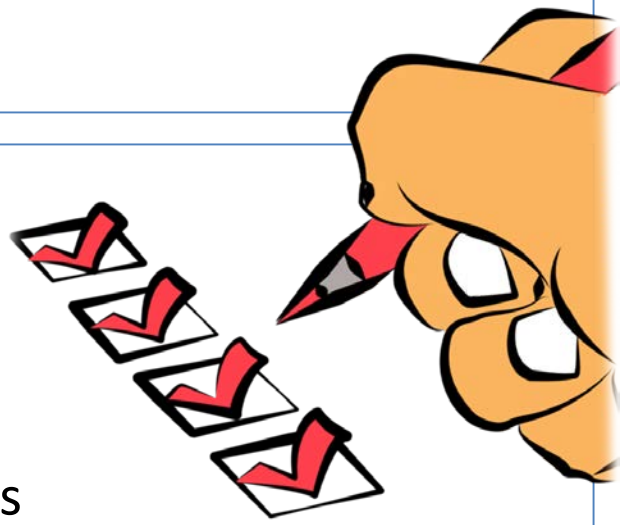
System-driven technical safeguards

- Assignment of different levels of access
- Automatic screen savers
- Email encryption

Physical Safeguards

Must have physical barriers and devices:

- Lock doors to medical records
- Restricted access to facility
- Restricted access to servers and computers



Breach Notification

When an organization suspects a breach, the organization must conduct a risk assessment which includes at least the following four factors:

- The nature and extent of the PHI involved, including types of identifiers and the likelihood of re-identification;
- The unauthorized person who used the PHI or to whom the disclosure was made;
- Whether the PHI was actually acquired or viewed; and
- The extent to which the risk to the PHI has been mitigated

Business Associate Agreements

A "business associate" is a person or entity who performs functions, activities, and or services to a covered entity that involves access to PHI, who is not a member/employee of the covered entity

A "Business Associate Agreement" (BAA) is a contract between the covered entity and the business associate that:

- Establishes permitted use and disclosure of PHI
- Requires subcontractors to meet HIPAA compliance
- Ensures appropriate safeguards to PHI
- Report breaches of information
- Ensure compliance to the HIPAA Privacy Rule
- Defines the destruction of PHI
- Authorizes the termination of the contract

HIPAA VIOLATIONS AND COMPLAINTS

HIPAA Violations & Enforcement

The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) is responsible for enforcing the HIPAA Privacy and Security Rules in several ways:

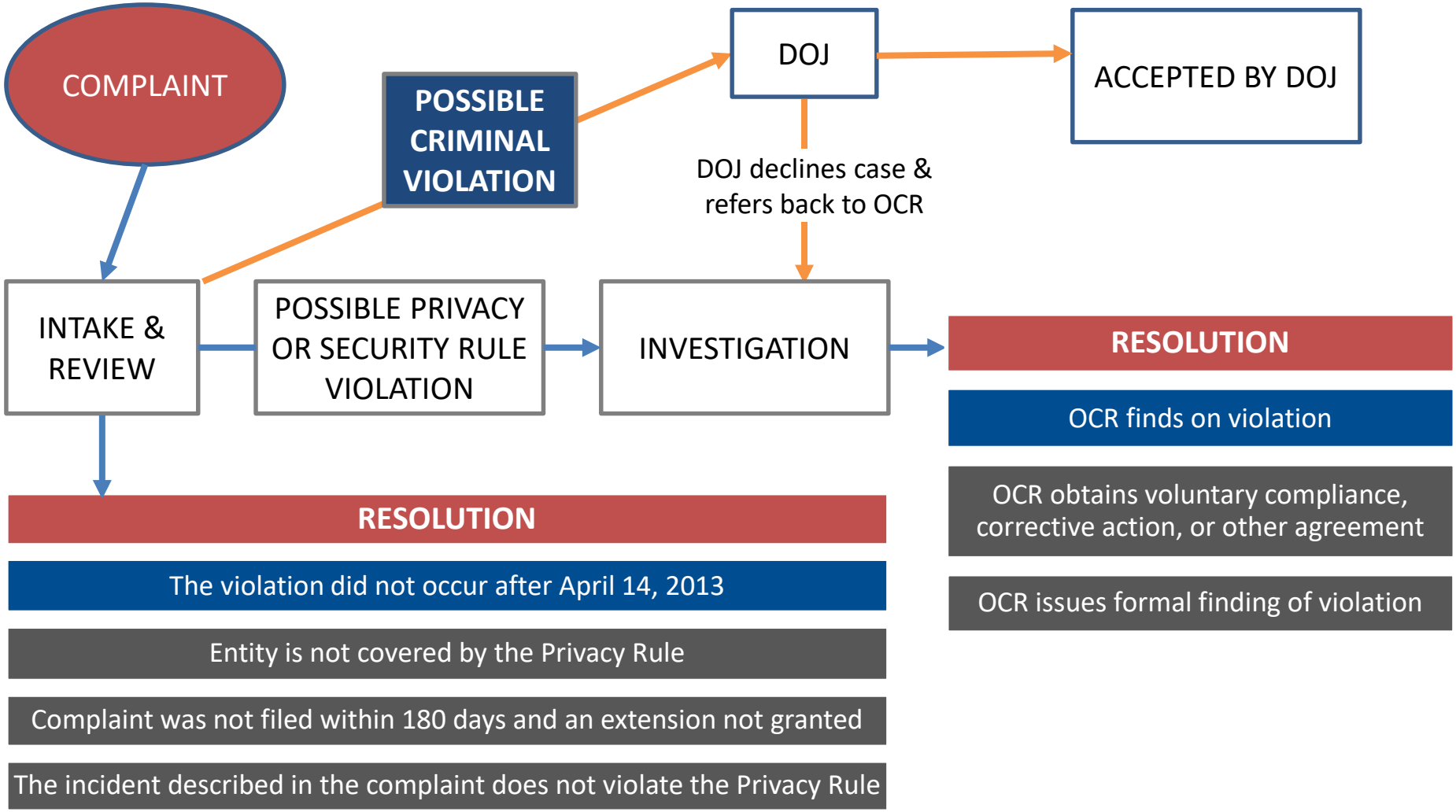
- Investigating filed complaints
- Conducting compliance reviews
- Performing education and outreach

OCR attempts to resolve HIPAA violations through the following methods:

- Voluntary compliance
- Corrective action and/or
- Resolution agreement

HIPAA Violations & Enforcement

HIPAA Privacy & Security Rule Complaint Process



Source: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/enforcement-process/index.html

HIPAA Violations & Enforcement

Failure to comply with HIPAA requirements can lead to the following civil and criminal penalties:

CIVIL PENALITIES		
Violation category	**Minimum Penalty**	**Maximum Penalty**
Did Not Know	**$100 – $50,000**	**$50,000 per violation with an annual maximum of $1.5 million**
Reasonable Cause	**$1,000 – $50,000**	
Willful Neglect-Corrected	**$10,000 – $50,000**	
Willful Neglect-Not Corrected	**50,000**	
CRIMINAL PENALTIES		
$50,000 fine and 1 year prison for knowingly obtaining and wrongfully sharing information		
$100,000 fine and 5 years prison for obtaining and disclosing through false pretenses		
$250,000 fine and 10 years prison for obtaining and disclosing for commercial advantage, personal gain, or malicious harm		

Common HIPAA Violations

The following are examples of the most common HIPAA violations:

1. **Lost or Stolen Devices**
    - **Example:** An unencrypted laptop containing ePHI was left in an unsecured location and available to the public
        - **Settlements:** In November 2015, an entity paid $850K to settle potential violations of the HIPAA Act when an unencrypted laptop was stolen

2. **Hacking**
    - **Example:** An employee downloaded a file that included malware which gave an unauthorized user access to PHI
        - **Settlements:** In November 2016, an entity paid $650K to settle potential violations of the HIPAA Act due to malware infected computer which may have resulted in the release of PHI

Common HIPAA Violations

The following are examples of the most common HIPAA violations (*continued*):

3. **Unauthorized Employee Access**
    - **Example:** An employee accesses the health record of a family member, without authorization, to check their health status
        - **Settlements:** In February 2017, an entity paid $5.5M to settle potential violations of the HIPAA Act when employees inappropriately accessed patient names, DOBs, and SS#s

4. **Improper Disposal**
    - **Example:** A clinic purchases new desktop computers and does not delete ePHI before disposing of the old equipment
        - **Settlements:** In June 2010, an entity paid $1.0M to settle potential violations of the HIPAA Act for failure to properly dispose of PHI

Common HIPAA Violations

The following are examples of the most common HIPAA violations (*continued*):

5. **Third-Party Disclosure**
    - **Example**: A covered entity discloses PHI to another entity without executing a BAA
        - **Settlements**: In April 2016, an entity paid $750K to settle potential violations of the HIPAA Act for failure to execute a BAA prior to sending PHI

6. **Unauthorized Release**
    - **Example:** An organization sends a patient's lab results to the wrong fax number
        - **Settlements:** In May 2017, an entity paid $387K to settle potential violations of the HIPAA Act when the entity faxed PHI to a patient's employer

Common HIPAA Violations

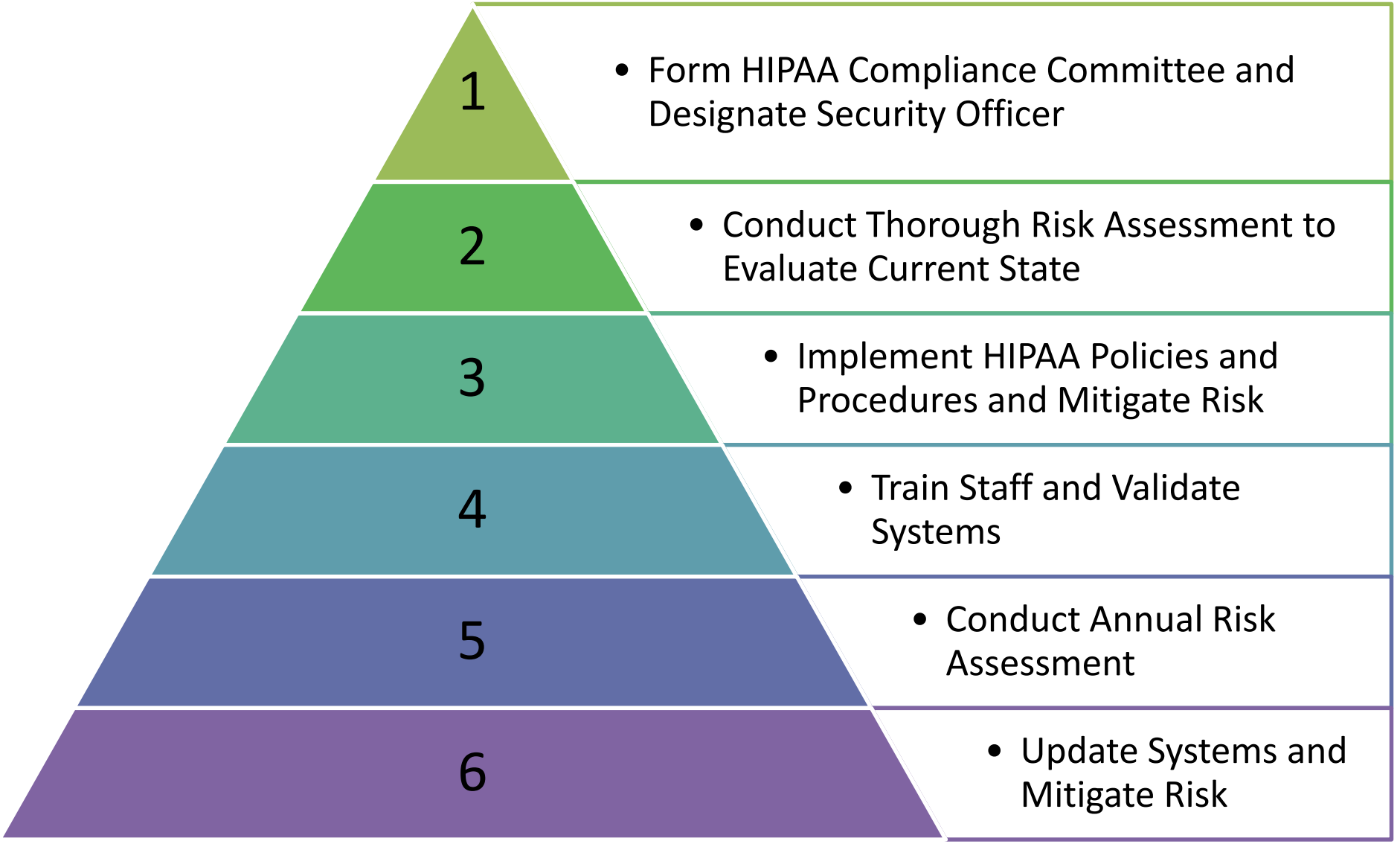
The following are examples of the most common HIPAA violations (*continued*):

7. **Risk Assessments**
    - **Example:** An entity does not periodically assess the risk associated with maintaining HIPAA compliance
        - **Settlements:** In 2015, an entity paid $750K to settle potential violations of the HIPAA Act by failing to conduct an accurate and through assessment of the potential risk and vulnerabilities

8. **Unsecured Records**
    - **Example:** A file cabinet containing patient medical records is left unlocked and accessible in a public area
        - **Settlements:** In 2014, an entity paid $800K to settle potential violations of the HIPAA Act for failure to ensure the security of PHI when transferring medical records to another location

Steps Towards HIPAA Compliance

Steps Towards HIPAA Compliance



Steps Towards HIPAA Compliance

STROUDWATER

Step 1: Form HIPAA Compliance Committee and Designate Security Officer

- HIPAA compliance cannot be maintained by a single individual and will require multiple people
- Security Officer Responsibilities Include:
  - Develop and revise HIPAA policies and procedures
  - Internal resource for HIPAA compliance and PHI questions
  - Ensure completion of security audits and risk assessments
  - Monitor compliance with security laws
  - Develop appropriate security training
  - Investigate system security breaches

Steps Towards HIPAA Compliance

STROUDWATER

Step 2: Conduct Thorough Risk Assessment to Evaluate Current State

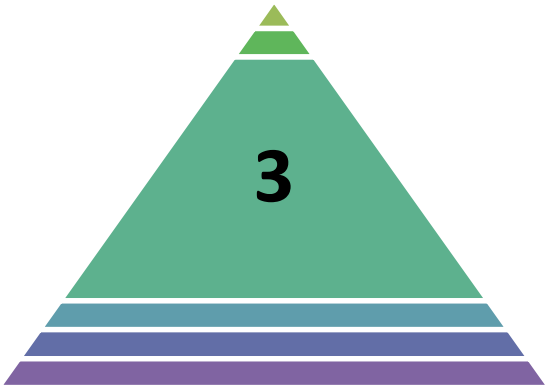
- A thorough risk assessment will allow the organization to evaluate the following:
  - Policies and Procedures
  - Data Collection
  - Identify and document potential threats and vulnerabilities
  - Determine the likelihood of threat occurrence
  - Determine the potential impact of threat occurrence
  - Determine the level of risk
  - Assess current security measures

Steps Towards HIPAA Compliance

STROUDWATER

Step 3: Implement HIPAA Policies and Procedures and Mitigate Current risk

- HIPAA Policies and Procedures
  - After the risk assessment, policies and procedures should be updated or established as necessary to meet HIPAA requirements
    - Policies and procedures should be updated at a minimum on an annual basis
- Mitigate Potential Risk
  - Review risk assessment and make necessary changes to systems
    - A comprehensive risk assessment will inform the entity of items needing resolution to meet compliance requirements



Steps Towards HIPAA Compliance

STROUDWATER

Step 4: Train Staff and Validate Systems

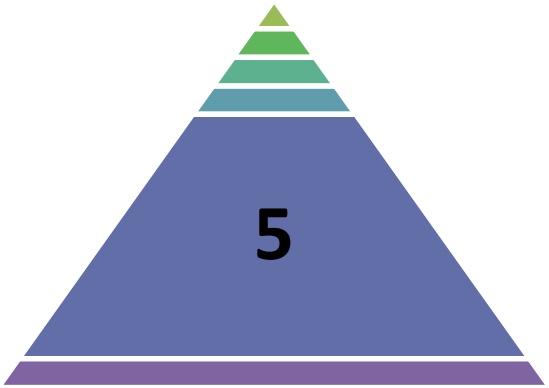
- Train Staff
  - Healthcare organizations should ensure all staff who come into contact with PHI receive training when hired and then on an annual basis
- Validate Systems
  - The Security Officer should work with IT and other staff as necessary to validate systems
    - This includes ensuring systems meet privacy and security rule compliance requirements
      - Healthcare organizations should regularly test systems to ensure continued compliance

Steps Towards HIPAA Compliance

STROUDWATER

Step 5: Conduct Annual Risk Assessment

- Healthcare organizations need to conduct periodic risk assessments to evaluate the current state of operations with regard to both the privacy and security role
  - Healthcare organizations do not have to engage an outside party to conduct a risk assessment; however, organizations are responsible for HIPAA compliance
    - An entity should evaluate internal knowledge with regard to HIPAA compliance to determine if the risk assessment can be completed internally
- The annual risk assessment will provide an organization with specific areas of improvement to meet and or maintain HIPAA compliance

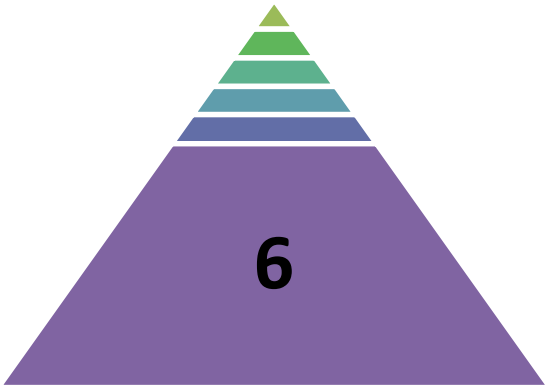


Steps Towards HIPAA Compliance

STROUDWATER

Step 6: Update Systems and Mitigate Risk

- Update Systems
  - Whether through changes in legislation, administrative rules, system changes, or operational changes, healthcare organizations need to evaluate and update systems as necessary to maintain HIPAA compliance
- Mitigate Risk
  - The annual risk assessment will provide specific areas of risk that organization must resolve
- System updates and risk mitigation will require constant attention and cannot be done solely on an annual basis



Conclusions

- ✓ Following HIPAA is not an option and all organizations that handle PHI must ensure compliance

- ✓ Not knowing the HIPAA requirements is not an excuse for not following

QUESTIONS

Thank you

STROUDWATER

1685 Congress St. Suite 202
Portland, Maine 04102
(207) 221-8250

JPantenburg@stroudwater.com
www.stroudwater.com