Navigating HIPAA/HITECH Regulatory Compliance

EHR20.COM
INFO@EHR20.COM
866-276-8309

WHO WE ARE …

EHR 2.0
THE HIPAA COMPLIANCE EXPERTS

Assist healthcare organizations to develop and implement practices to secure IT systems and comply with HIPAA/HITECH regulations

EDUCATION

Online Training, Webinars and Customized Workshop

CONSULTING

Professional services to help you with your Compliance needs

DISCLAIMER

Consult your attorney

This webinar has been provided for educational and informational purposes only and is not intended and should not be construed to constitute legal advice.

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

AGENDA

1 Background

2 HIPAA Basics

3 Requirements

4 Security Risk Analysis

5 Other Requirements

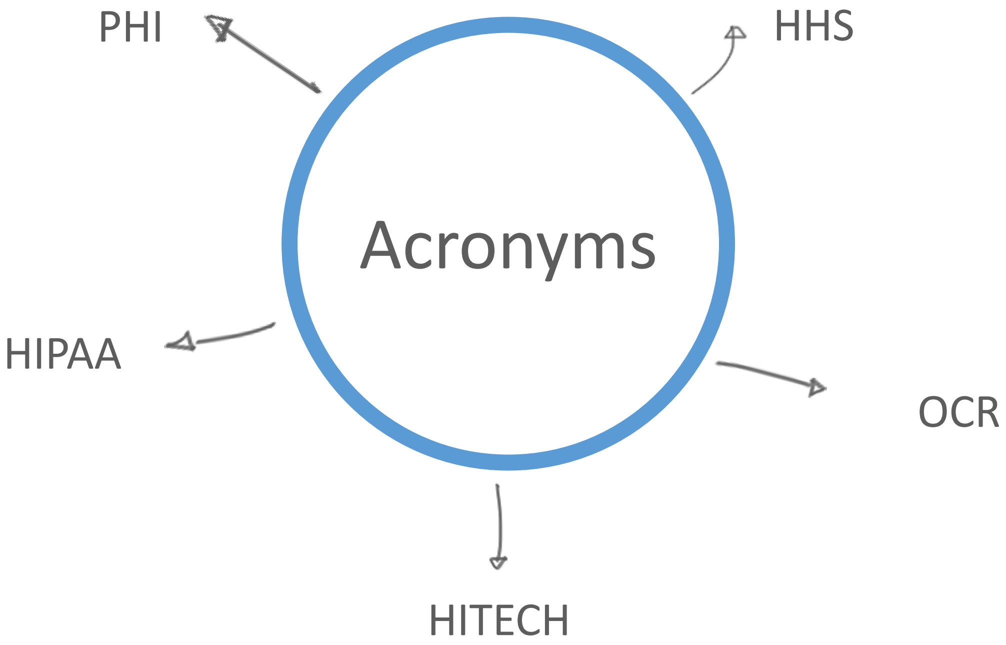
6 Key Takeaways

7 Our Approach

8 Questions & Answers

ℹ Always available via email to answer any questions

TERMS YOU MAY HEAR …



Acronyms

PHI

HHS

HIPAA

OCR

HITECH

Anyone who is not handling patients directly

TOP 5 REASONS FOR CONDUCTING A HIPAA/HITECH ASSESSMENT

1. Frequent threat of security breaches
2. First set of documents requested by OCR/CMS auditors
3. Security best practices, identify areas to improve
4. Avoid Civil Money Penalties (CMP)
5. Maintain patient trust

Basic building blocks for demonstrating HIPAA Compliance

LATEST HHS SETTLEMENTS

Careless handling of HIV information jeopardizes patient's privacy, costs entity $387k - May 23, 2017

Texas health system settles potential HIPAA violations for disclosing patient information - May 10, 2017

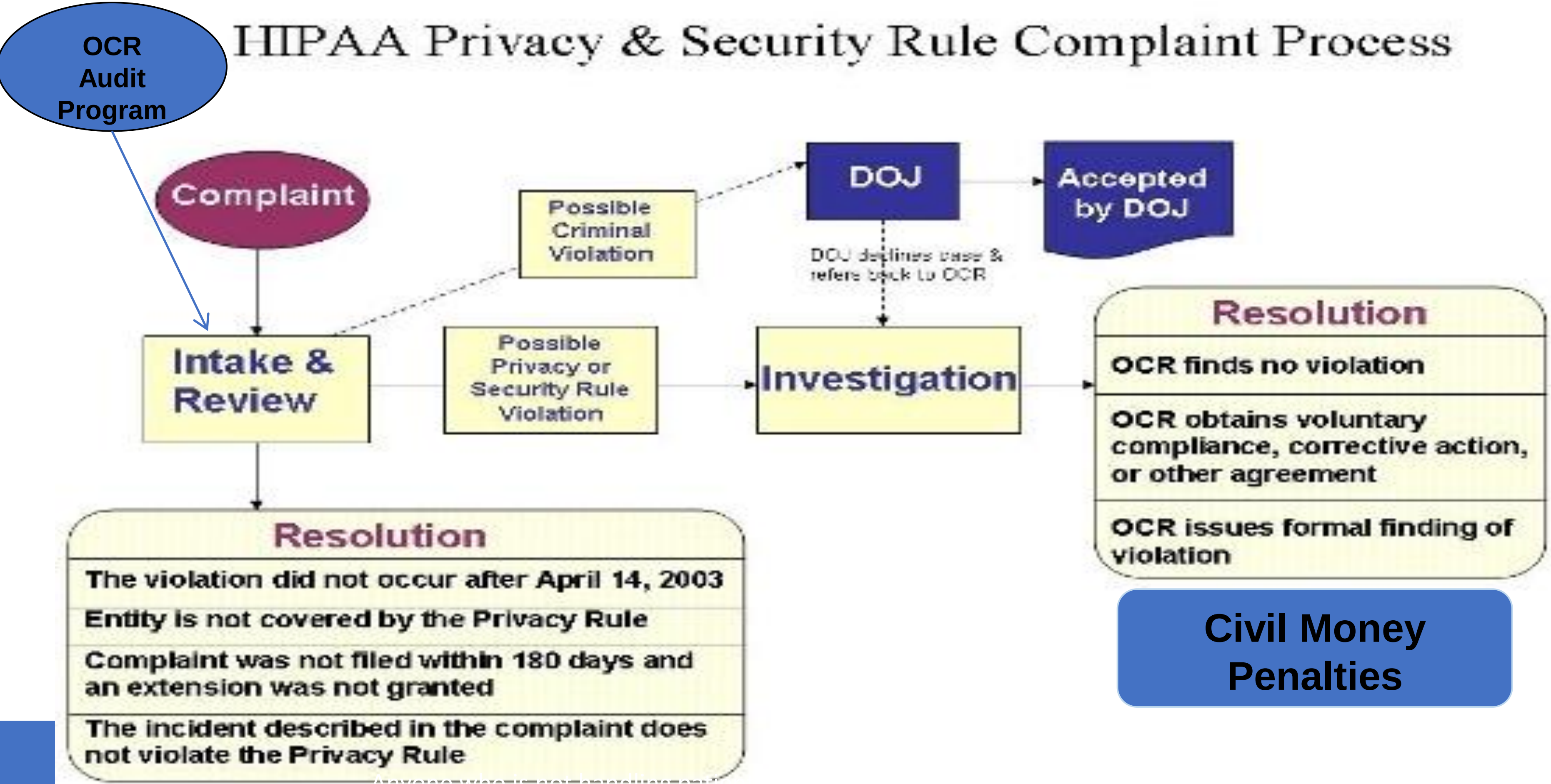
$2.5 million settlement shows that not understanding HIPAA requirements creates risk – April 24, 2017

No Business Associate Agreement? $31K Mistake - April 20, 2017
Overlooking risks leads to breach, $400,000 settlement - April 12, 2017

and many more …

Settlements and CMP are not the same

HIPAA Privacy & Security Rule Complaint Process



OCR Audit Program

Complaint

Intake & Review

Possible Criminal Violation

DOJ

Accepted by DOJ

DOJ declines case & refers back to OCR

Possible Privacy or Security Rule Violation

Investigation

Resolution

- OCR finds no violation
- OCR obtains voluntary compliance, corrective action, or other agreement
- OCR issues formal finding of violation

Resolution

- The violation did not occur after April 14, 2003
- Entity is not covered by the Privacy Rule
- Complaint was not filed within 180 days and an extension was not granted
- The incident described in the complaint does not violate the Privacy Rule

Civil Money Penalties

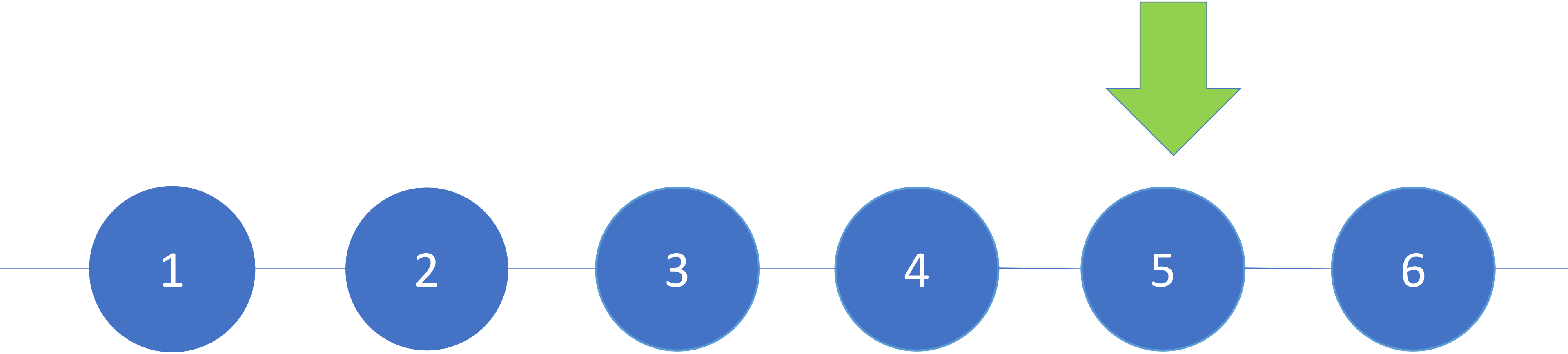
CIVIL MONEY PENALTIES

Violation category	Each violation
Did Not Know	**$100–$50,000**
Reasonable Cause	**1,000–50,000**
Willful Neglect-Corrected	**10,000–50,000**
Willful Neglect-Not Corrected	**50,000**

- Max. of $1.5m per calendar year
- No. of days violated
- No. of regulatory provisions violated

OCR/HHS is hiring lot of HIPAA auditors to handle complaints and data breach reporting.

HIPAA PHASE 2 AUDIT



1 Communication from OCR

2 Pre-audit Questionnaire

3 Sample Selection

4 Desk Audit

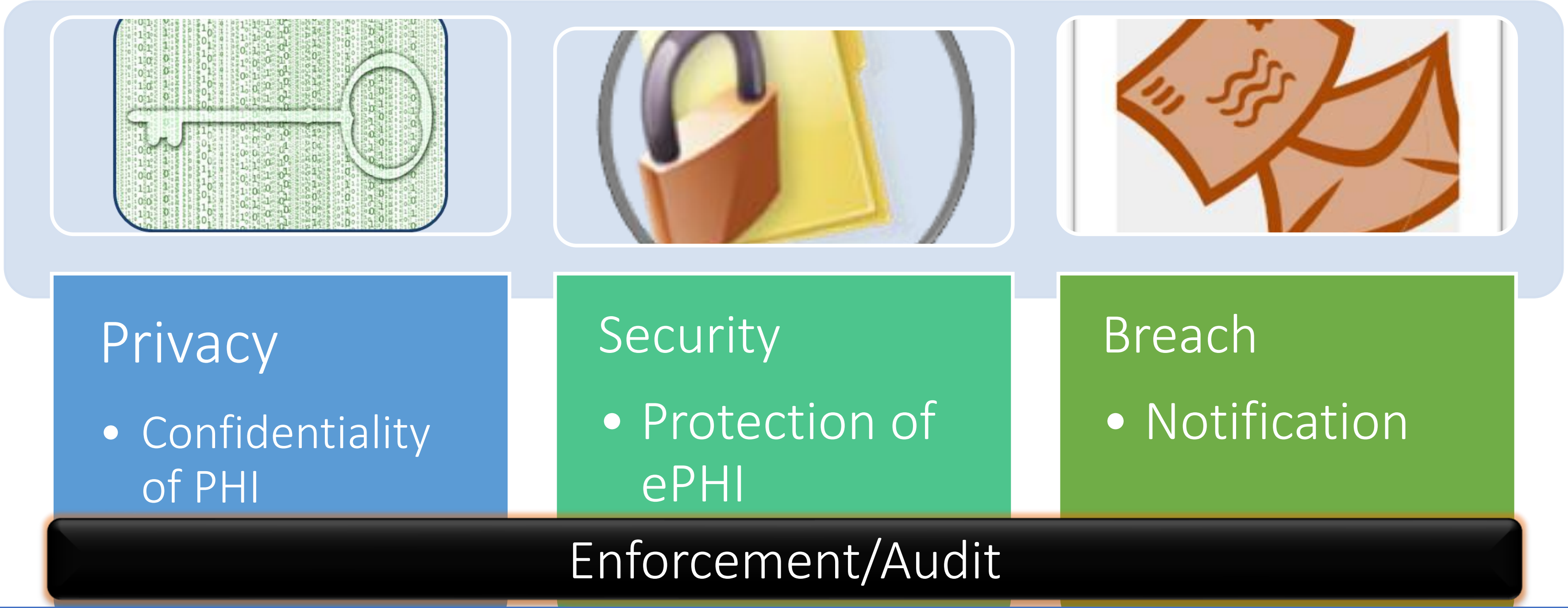
5 Onsite Audit

6 Potential Compliance Review

Office for Civil Right Under HHS conducts HIPAA Phase 2 Audit

HIPAA/HITECH RULES

Review



Privacy

- Confidentiality of PHI

Security

- Protection of ePHI

Breach

- Notification

Enforcement/Audit

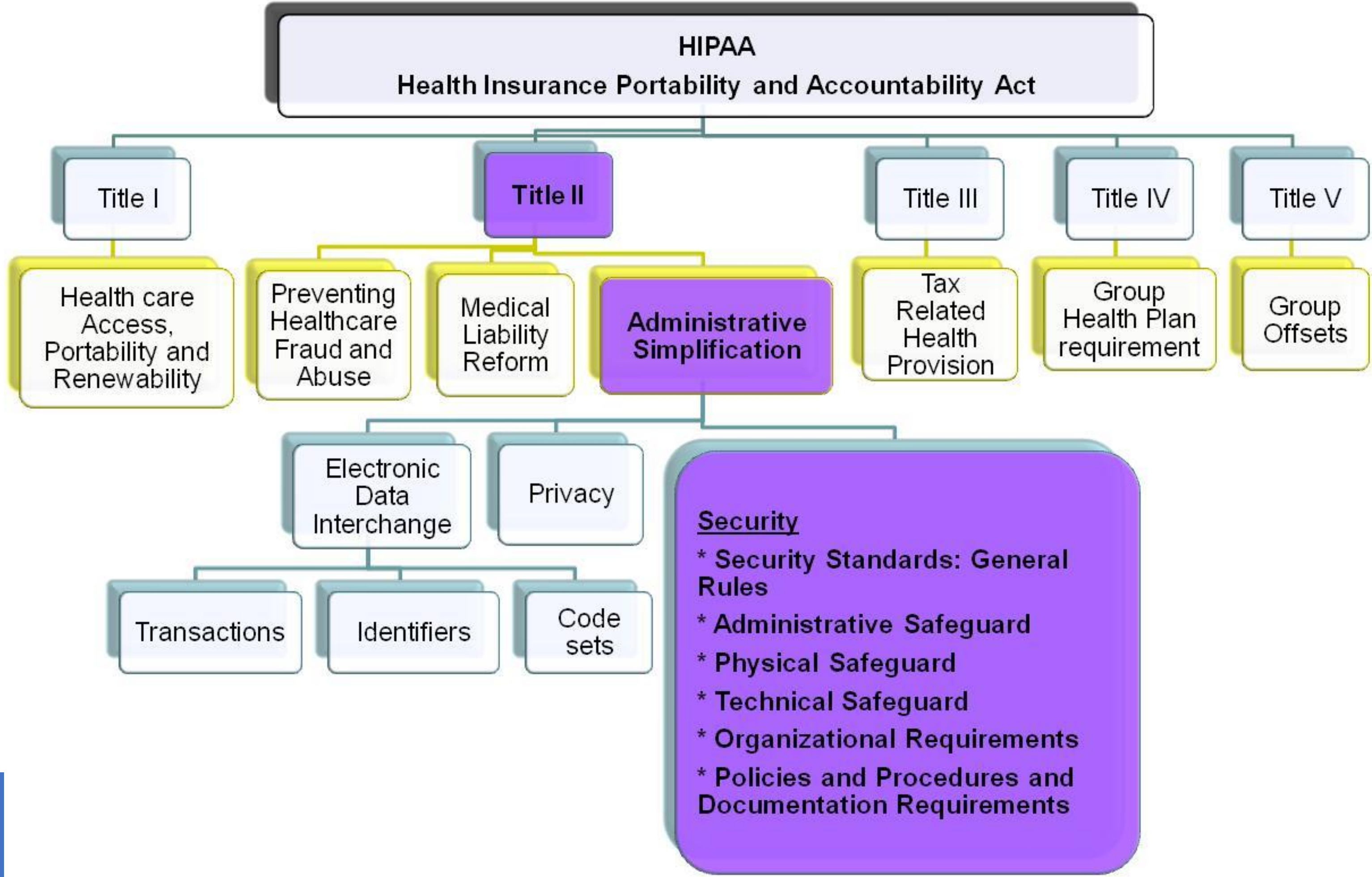
Business Associates need to comply with limited privacy rule

HITECH MODIFICATIONS TO HIPAA

- Creating incentives for developing a meaningful use of electronic health records
- Changing the liability and responsibilities of Business Associates
- Redefining what a breach is
- Creating stricter notification standards
- Tightening enforcement
- Raising the penalties for a violation
- Creating new code and transaction sets (HIPAA 5010, ICD10)

ℹ Since 2011 Medicare/Medicaid have paid more than 30+ billion as incentive for adopting EHR

HIPAA TITLES


HIPAA
Health Insurance Portability and Accountability Act
Title I
Title II
Title III
Title IV
Title V
Health care Access, Portability and Renewability
Preventing Healthcare Fraud and Abuse
Medical Liability Reform
Administrative Simplification
Tax Related Health Provision
Group Health Plan requirement
Group Offsets
Electronic Data Interchange
Privacy
Transactions
Identifiers
Code sets

Security

* Security Standards: General Rules

* Administrative Safeguard

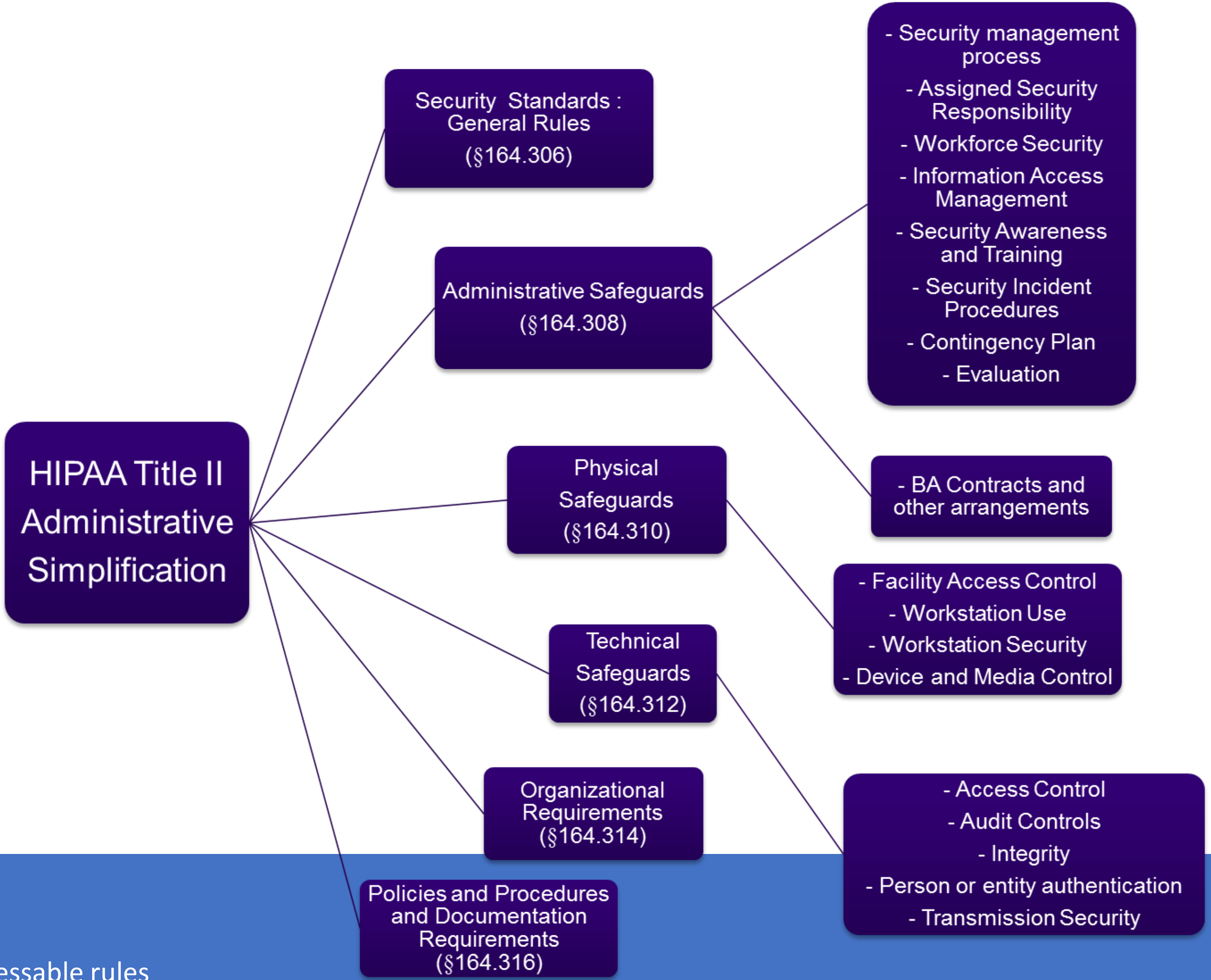
* Physical Safeguard

* Technical Safeguard

* Organizational Requirements

* Policies and Procedures and Documentation Requirements

HIPAA SECURITY RULE



HIPAA Title II Administrative Simplification

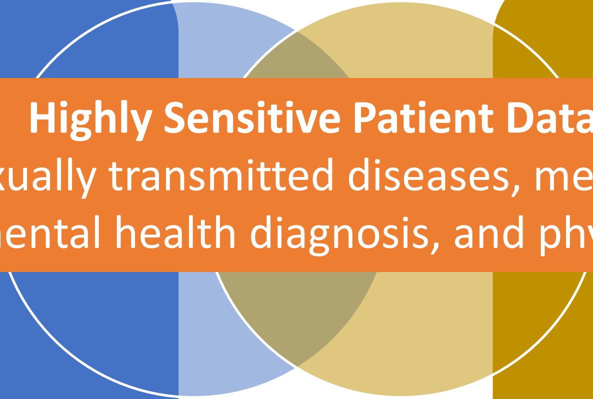
- Security Standards : General Rules (§164.306)
- Administrative Safeguards (§164.308)
  - Security management process
  - Assigned Security Responsibility
  - Workforce Security
  - Information Access Management
  - Security Awareness and Training
  - Security Incident Procedures
  - Contingency Plan
  - Evaluation
  - BA Contracts and other arrangements
- Physical Safeguards (§164.310)
  - Facility Access Control
  - Workstation Use
  - Workstation Security
  - Device and Media Control
- Technical Safeguards (§164.312)
  - Access Control
  - Audit Controls
  - Integrity
  - Person or entity authentication
  - Transmission Security
- Organizational Requirements (§164.314)
- Policies and Procedures and Documentation Requirements (§164.316)

Required and Addressable rules

PROTECTED HEALTH INFORMATION

BASICS

1. Name
2. Address
3. Dates related to an individual
4. Teleph
5. Fax nur
6. Email a
7. Social S
8. Medica
9. Health plan beneficiary number
10. Account number
11. Certificate/license number
12. Any vehicle or other device serial
13. Device identifiers or serial numbers
14. Web URL
15. Internet Protocol (IP) address
16. Finger or voice prints
17. Photographic images
18. Any other characteristic that would uniquely identify the individual



Highly Sensitive Patient Data:

HIV status, sexually transmitted diseases, medications, sexual orientation, mental health diagnosis, and physical abuse, etc.

1. **Medical records:**

   paper case

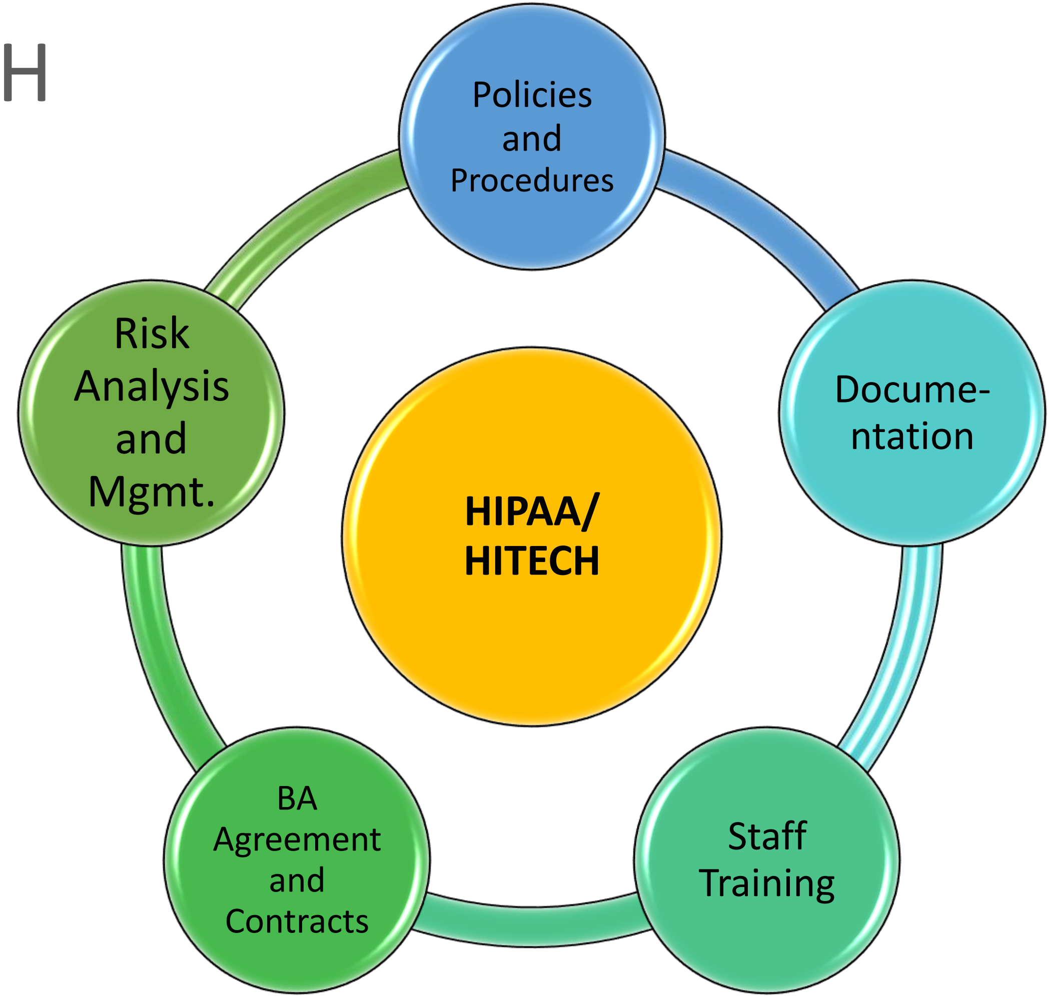
   rds

   - **progress reports**
   - **X-rays**
   - **MRI's**

2. **Claims**
3. **Payments**
4. **Eligibility**
5. **Other health plan related insurance data**

PII when combined with health data becomes PHI

HIPAA/HITECH APPROACH



Documentation is to be maintained for 6 years

SCOPE

Any device that electronically stores or transmits information using a EHR software program

- EHR/LIS/PMS
- Computers
- Storage Devices (HD, FD, CD, DVD)
- Networking Devices (Routers, Switches, & Wireless)
- Smart-Phones, Tablets
- Cloud-Based Services
- Any other interfaces

ⓘ Up to date ePHI inventory sheet to be maintained

Sample Risk Analysis Prioritization

		Likelihood		
		High	Medium	Low
Impact	High	Unencrypted laptop ePHI	Lack of auditing on EHR systems	Missing security patches on web server hosting patient information
	Medium	Unsecured wireless network in doctor’s office	Outdated anti-virus software	External hard drives not being backed up
	Low	Sales presentation on USB thumb drive	Web server backup tape not stored in a secured location	Weak password on internal document server

Updated risk management plan to be maintained

POLICIES AND PROCEDURES

- □ **Physical Security Policy**
  - □ Maintenance record
  - □ Disposal
  - □ Access
- □ **Information Security Policy**
  - □ Access Policy
  - □ Sanction Policy
- □ **Contingency Plan Policy**
- □ **Security Incident Procedure/Breach**

- Master Security Policy
- Master Privacy Policy
- Master Breach Policy

ROLE-BASED TRAINING

❑ Privacy and Security Officers

❑ Workforce Handling PHI (End-Users, Clinical Staff)

❑ IT Team/Practice Administration (Admin)

❑ Senior Management

Frequent user awareness training and assessment

BA AGREEMENTS

❑ A person or entity that performs certain functions or activities, on behalf of a covered entity (CE), that involve the use or disclosure of protected health information

❑BA contract must be signed/in-place before accessing PHI

Keep an up-to-date list of BA vendors

Documentation

- □ Privacy and Security Notices
- □ Health Record Request Log
- □ Training Records
- □ PHI/Chart Access Review
- □ Inventory List
- □ User Access Levels
- □ Maintenance Log

Potentially up to 6 years worth of documentation are required

HIPAA and Crypto

HIPAA Technical Safeguard Requirements	Crypto Tools	Examples
Access Control	Encryption	AES, Triple-DES
Integrity	Hash Functions, MACs, Digital Signatures	SHA-1, SHA-2 HMAC, CMAC
Person or Entity Authentication	Digital Signatures	DSA, ECDSA, RSA
Transmission Security	Encryption, Hash Functions, MACs, Digital Signatures	

In case of a third-party vendor ensure approved encryption technology is used.

KEY TAKEAWAYS

- HHS/OCR enforcement on HIPAA Covered Entities and Business Associates
- Processing of PHI elements drives HIPAA compliance requirements
- Security risk analysis, training and policies and procedures are key required documents
- Healthcare entities have wide footprint of patient data
- Budget, Type and Size of the entity doesn’t matter

Annual update is required

REFERENCES

HHS Wall of Shame

HHS FAQ on Business Associates

NIST SP 800-111, Guide to Storage Encryption Technologies

HHS Public Health Guidance

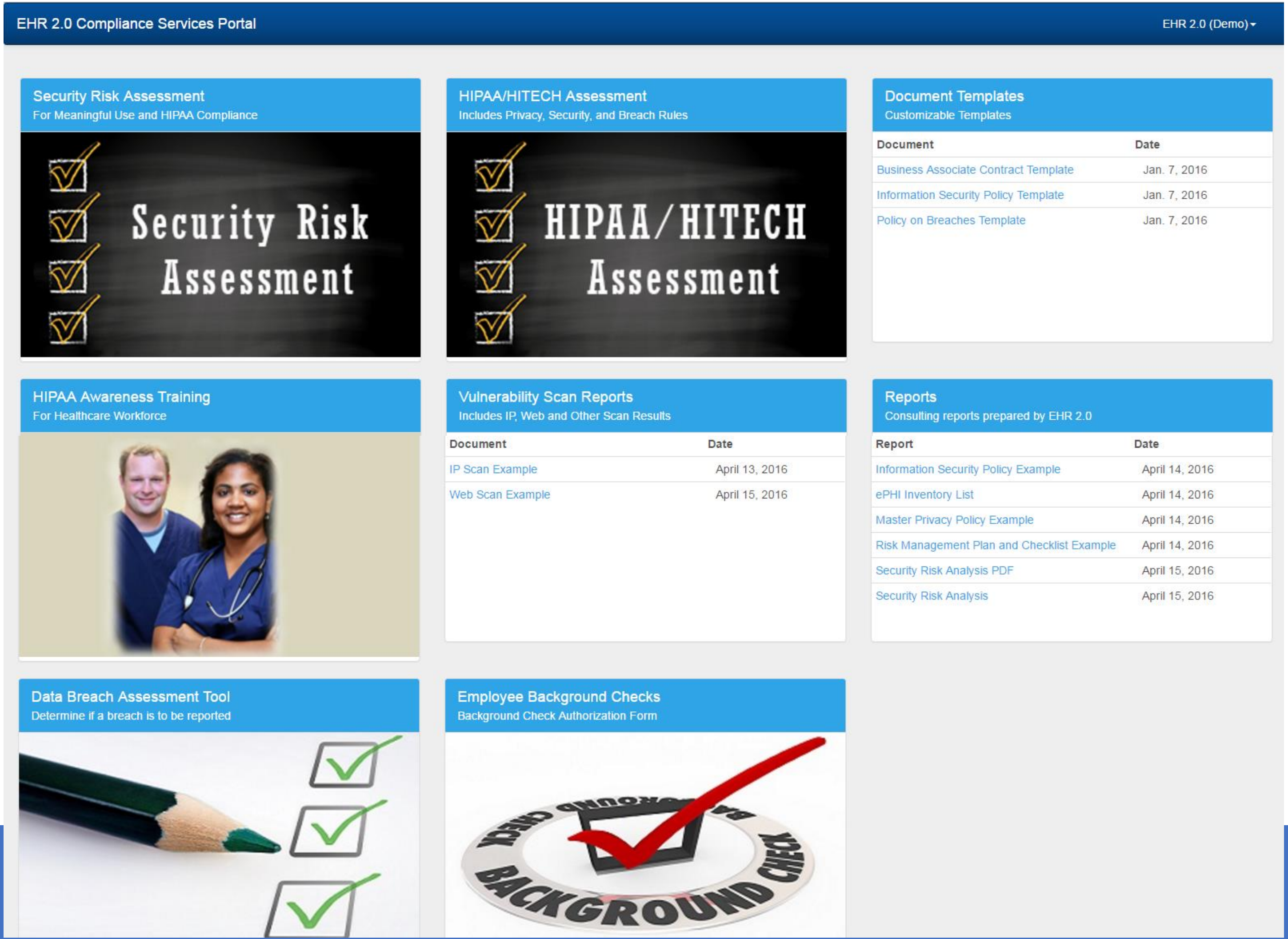
Deliverables

- ✓ ePHI Inventory Sheet
  - ✓ Scoping and Profiling
- ✓ Security Risk Analysis Report
  - ✓ Vulnerability assessment
- ✓ Risk Management Plan
- ✓ Updated Policies and Pro s
- ✓ Online User Training
- ✓ Executive Summar rt
- ✓ Portal Access

Audit Support Guarantee

We provide audit support/guarantee for all our consulting customers

COMPLIANCE PORTAL



EHR 2.0 Compliance Services Portal

EHR 2.0 (Demo)▾

Security Risk Assessment

For Meaningful Use and HIPAA Compliance

HIPAA/HITECH Assessment

Includes Privacy, Security, and Breach Rules

Document Templates

Customizable Templates

Document	Date
Business Associate Contract Template	Jan. 7, 2016
Information Security Policy Template	Jan. 7, 2016
Policy on Breaches Template	Jan. 7, 2016

HIPAA Awareness Training

For Healthcare Workforce

Vulnerability Scan Reports

Includes IP, Web and Other Scan Results

Document	Date
IP Scan Example	April 13, 2016
Web Scan Example	April 15, 2016

Reports

Consulting reports prepared by EHR 2.0

Report	Date
Information Security Policy Example	April 14, 2016
ePHI Inventory List	April 14, 2016
Master Privacy Policy Example	April 14, 2016
Risk Management Plan and Checklist Example	April 14, 2016
Security Risk Analysis PDF	April 15, 2016
Security Risk Analysis	April 15, 2016

Data Breach Assessment Tool

Determine if a breach is to be reported

Employee Background Checks

Background Check Authorization Form

FIND US

CALL US
866-276 8309

SERVICE
info@ehr20.com

LOCATION
150, Cornerstone Dr.
Cary, NC

SOCIALIZE
Facebook
Twitter

Twitter: [@ehr_20]

Facebook: [ehr20]

Questions

Please don’t hesitate to ask

Thank You

for your attention!

To purchase reprints of this document, please email info@ehr20.com.

Thank you for joining us today

25 May, 2017