HCCA Regional Meeting
Scottsdale, AZ
November 9, 2018

Shawn Y. DeGroot, CHC-F, CCEP, CHRC, CHPC
Compliance Vitals

Topics

- Status of Regulations
- Gaps to avoid
- Privacy effectiveness

What's Old? 1996 HIPAA Privacy & Security

2009
- ARRA Required notification to the individual/DHHS
- HITECH Breach notification and HIPAA enforcement
- Privacy, security and breach notification
- FTC regulations on breach notification
- HIPAA Privacy rule genetic information nondiscrimination

2011 HITECH Act accounting for disclosures

2013 Omnibus Rule

What's new?

Status of Regulations

- 2013 Omnibus Rule
- OCR Guidance
  - https://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/index.html
  - https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html
- State Privacy Regulations

Additional Resources

Office of the National Coordinator for Health Information Technology:

- Provides resources to promote EHR's
- Offers educational tools and resources

- https://www.healthit.gov/topic/about-onc

Additional Resources

Health IT.gov: https://www.healthit.gov/topic/privacy-security-and-hipaa/health-it-privacy-and-security-resources-providers

Guide to Privacy and Security of Electronic Health Information
https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf

Guide to Privacy and Security of Electronic Health Information

HIPAA uses the term "audit" in two ways

1. Audit by monitoring the adequacy and effectiveness of your security infrastructure. Determine what to audit and outline the audit process to identify trigger indicators — or signs that ePHI could have been compromised and further investigation is needed

2. Audit also refers to an effort to examine what happened. This means your EHR must be set up to maintain retrospective documentation (i.e., an "audit log") on who, what, when, where, and how your patients' ePHI has been accessed.

Guide to Privacy and Security of Electronic Health Information

Investigations and Enforcement of Potential HIPAA Violations:

- OCR initiates investigations upon receipt of complaints, breach reports, information provided by other agencies, and the media.
- The HIPAA Enforcement Rule provides different penalties for each of four levels of culpability…

Guide to Privacy and Security of Electronic Health Information

Four areas of culpability

Intent	Minimum per incident
Did not know or could have known	$100 - $50,000
Reasonable cause and not willful neglect	$ 1,000 - $50,000
Willful neglect, but corrected within 30 days	$10,000 - $50,000
Willful neglect and not corrected within 30 days	$50,000

State Privacy Regulations

Every state in the Union now has a law requiring companies to publicly disclose when a data breach occurs.

The reporting timeframe varies state-to-state and some require notification to the AG's office.

February 2018 OCR
Business Associate

A "dumpster diver" brought medical records of 2,150 individual's PHI obtained from a Business Associate to a shredding and recycling facility to exchange for cash. OCR received an anonymous complaint and investigated. For an unrelated reason, the Business Associate went out of business.

May 2018 GDPR vs. U.S. HIPAA Privacy Laws

GDPR	US Privacy
Consent: Justify why	Consent: To access
Focus on the process	All about the breach
30 days to report	60 days to report
PO cannot be dismissed	PO can be terminated

July 2018 Guidance from OCR
Final Disposition of Hardware and Electronic Media

Policies/procedures

1) Document the appropriate methods to dispose hardware, software and data
2) Ensure that ePHI is
    1) destroyed and cannot be recreated
    2) cannot be accessed and reused
    3) removed from reusable media before new information is recorded
3) Identify removable media and their use

https://www.hhs.gov/sites/default/files/cybersecurity-newsletter-july-2018-Disposal.pdf

Privacy Effectiveness

Resolution Agreements: Risk Analysis

Advocate Health Care $5.5 million in penalties
- Failed to perform a risk assessment…

University of Mississippi, $2.75 million
- Failed to conduct risk management activities for known security risks

Oregon Health & Science University, $2.7 million
- Failed to address identified risks

Security Rule: Risk Analysis

Risk Analysis:

Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic protected health information held by the covered entity or business associate.

Security Risk Analysis

- Cybersecurity Testing
- Penetration Testing

Security Rule: Risk Analysis

Who will perform the assessment?

What procedures should be followed?

What systems should be subject to the assessment?

When should an assessment be performed?

How often should an assessment be performed?

Security Rule: Risk Analysis

Identify and document Threats and Vulnerabilities

- Technical
  - Weaknesses in the development of IT systems
  - Incorrectly implemented or configured IT systems
- Non-technical

Security Rule: Risk Analysis

Identify and document Threats and Vulnerabilities

Three categories of threats exist for a risk analysis of ePHI:

1. Natural
2. Human
3. Environmental

Security Rule: Risk Management

Risk Management:

Implementation of security measures to sufficiently reduce an organization's risk of losing or compromising ePHI and to meet the general security standard.

Steps should be taken FOLLOWING a risk analysis

To be effective…

1. Document each step
2. Create a timeline
3. Confirm accepted risks
4. Assign responsibilities
5. Update Compliance Committee

Privacy Effectiveness: Breach

Culture and incentives for good faith reporting
1. Outcome resulted in a change to a policy
2. Outcome resulted in an improved process

Policy outlining timeliness of reporting

Policy to support disciplinary action
1. Intentional and unintentional acts
2. Consequences for not reporting

Privacy Effectiveness: Breach

Documented Risk Assessments of a breach, action (mitigation)and corrective action are key to an effective privacy program.

Immediate mitigation, short-term and long-term corrective action and monitoring are crucial.

Third Party Privacy Effectiveness

- Orientation for a BA that handles PHI?
- Definition of an “incident” vs. a “breach” understood?
- What training is performed?
- Are policies and procedures exchanged and/or understood?
- Process outlined on requests for restrictions?
- Process outlined for AOD’s?

Third Party Privacy Risks and Effectiveness

- Where is data stored?
- Expectations clear regarding breach notification?
- Is there a history of breaches with the vendor?
- Contact information:
  - Email
  - Phone
  - Backup plan

To be effective…

1. Document each step
2. Create a timeline
3. Confirm accepted risks
4. Assign responsibilities
5. Update Compliance Committee

Thank you!!

Shawn@compliancevitals.com