Bricker & Eckler
ATTORNEYS AT LAW

HIPAA Self-Audits as Compliance Tool

NIST/OCR Safeguarding Health Information
September 5, 2017

Allen Killworth
614.227.2334
akillworth@bricker.com

Outline

- OCR Audit Protocol
- Risk Analysis/Assessment Requirement
- Self-Audit Tools
  - HHS/OCR Guidance
  - NIST Publications
  - Enforcement Actions
- Incidents/Compliance Events
  - Use in Mitigation
- Additional Audits – Business Associates?

Audit Protocol

- OCR audits “primarily a compliance improvement activity” designed to help OCR:
  - better understand compliance efforts with particular aspects of the HIPAA Rules
  - determine what types of technical assistance OCR should develop
  - develop tools and guidance *to assist the industry in compliance self-evaluation and in preventing breaches*

www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html

Audit Protocol

Example of how the protocol may assist in a self-audit:

- §164.310(a)(1): Implement policies and procedures to limit physical access to [an entity's] electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

Audit Protocol

Bricker & Eckler
ATTORNEYS AT LAW

- Audit Inquiry:

Does the entity limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring properly authorized access is allowed?

Obtain and review policies and procedures regarding facility access control. Evaluate the content in relation to the relevant specified performance criteria regarding physical access to electronic information systems and use of facilities and equipment that house ePHI.

Evaluate and determine if policies and procedures identify the countermeasures implemented to control physical access and to detect, deter, and/or prevent unauthorized access and unlimited access to electronic information systems and facilities where systems are housed.

Elements to review may include but are not limited to:

- Workforce members’ roles and responsibilities in facility access control procedures
- Management involvement in the facility's access controls procedures
- The process of how authorization credentials for facility access are issued
- The process of removing workforce members’ authorization credentials for physical access when such access it is no longer required
- Identification of how visitors’ access is monitored
- Methods for controlling and managing physical access devices
- Facilities and areas that have physical access control implemented to safeguard ePHI

Obtain and review documentation of workforce members with authorized physical access to electronic information systems and the facility or facilities in which they are housed. Evaluate and determine if authorized workforce members are listed in areas where electronic information system resides; listed authorized members have been approved by appropriate management; list of authorized workforce members are reviewed on a continuous basis; and removed when access is no longer required.

Obtain and review documentation of procedures for granting individuals access to entity facility or facilities where electronic information systems are housed. Evaluate and determine if physical access authorization is enforced at entry/exit points of the facility; individual access authorization is verified before granted access to facility; and physical access audit logs of entry/exit points are maintained and reviewed on continuous basis.

Obtain and review documentation of visitor physical access to electronic information systems and the facility or facilities where it is housed. Evaluate and determine if visitors are supervised in locations where electronic information resides and if activities are documented and monitor

Audit Protocol

- Phase 2 desk audits controls :
  - ➢ Privacy
    - Notification of Privacy Practices & Content Requirements – 45 CFR 164.520(a)(1) & (b)(1)
    - Provision of Notice / Electronic Notice – 45 CFR 164.520(c)(3)
    - Right to Access – 45 CFR 164.524
  - ➢ Breach
    - Timeliness of Notification – 45 CFR 164.404(b)
    - Content of Notification – 45 CFR 164.404(c)
  - ➢ Security
    - Security Management Process / Risk Analysis – 45 CFR 164.308(a)(1)(ii)(A)
    - Security Management Process / Risk Management – 45 CFR 164.308(a)(1)(ii)(B)

Risk Analysis/Assessment Requirement

Bricker & Eckler
ATTORNEYS AT LAW

- 45 CFR 164.308(a)(1)(ii):

  (A) *Risk analysis (Required).* 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.

  (B) *Risk management (Required).* Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a).

- Self-audits vs. Assessment/Analysis

Self Audit Tools – HealthIT.gov

- ONC/OCR guidance at HealthIT.gov:
    - Health IT Privacy and Security Resources
    - Guide to Privacy and Security of Electronic Health Information
    - Security Risk Assessment Tool
    - Security Risk Guidance
    - HIPAA Security Toolkit Application
    - Sample BA Contract Provisions
    - Template Model Notice of Privacy Practices
    - Mobile Devices – Keeping Health Information Private and Secure

https://www.healthit.gov/providers-professionals/ehr-privacy-security/resources

Self Audit Tools – Cybersecurity

Bricker&Eckler
ATTORNEYS AT LAW

- NIST Cybersecurity Framework
  - *Addressing Gaps in Cybersecurity – Crosswalk Between HIPAA Security Rule and NIST Cybersecurity Framework*
- Baldrige Cybersecurity Excellence Builder
  - Self-assessment tool to help organizations better understand the effectiveness of their cybersecurity risk management efforts
- OCR Cyber-Awareness Newsletters
- Top 10 Tips for Cybersecurity in Health Care

www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html

Self Audit Tools – Cybersecurity

- Excerpt from April 2017 Cybersecurity Newsletter:

> *Further, a recent security analysis (The Security Impact of HTTPS Interception) of HTTPS interception products found that poor implementation of many of these products may actually reduce end-to-end security and introduce new vulnerabilities. US-CERT recently issued an Alert, TA17-075A, warning of the vulnerabilities that organizations expose themselves to when they use HTTPS interception products. Covered entities and business associates using HTTPS interception products or considering their use should consider the risks presented to their electronic PHI transmitted over HTTPS, and intercepted with an HTTPS interception products, as part of their risk analysis, particularly considering the pros and cons discussed by the US-CERT alerts, and the increased vulnerability to malicious third-party MITM attacks.*

Self Audit Tools – Guidance Materials

- HHS HIPAA Guidance Materials
  - Understanding Some of HIPAA's Permitted Uses and Disclosures
  - Individual's Right of Access
  - HIPAA Privacy and Security and Workplace Wellness Programs
  - Guidance Regarding Methods for De-identification of Protected Health Information
  - HIPAA Privacy Rule and Sharing Information Related to Mental Health

https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/index.html

Self-Audit Tools – Enforcement Actions

- Children's Digestive Health (April 2017)
  - $31,000 settlement for failure to have BAA with storage company.
  - HHS had investigated the BAA, Filefax, originally and discovered CCDH used Filefax since 2003 to store PHI but "neither party could produce a signed Business Associate Agreement (BAA) prior to Oct. 12, 2015."
- St. Joseph Health (October 2016)
  - $2.14M settlement. SJH "…potentially disclosed the PHI of 31,800 individuals…"
  - Files created for MU program containing ePHI, were publicly accessible on the internet from 2/1/11 until 2/13/12. SJH installed server to store the files which included a file sharing application whose default settings allowed anyone with an internet connection to access them. SJH did not examine or modify it.
  - CEs "…must also evaluate and address potential security risks when implementing enterprise changes impacting ePHI," said OCR Director Jocelyn Samuels.
- Memorial Healthcare System (February 2017)
  - $5.5M penalty for breach affecting 115,143 individuals.
  - For 12 months, log-in credentials of a former workforce member, which had not been terminated, were used to access ePHI on a daily basis.

Incidents/Breach

- 45 CFR 164.308(a)(6)(ii) :
  - (ii) *Implementation specification: Response and reporting (Required).* Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.
- 45 CFR 164.530(f):
  - *Standard: mitigation*. A covered entity must mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of this subpart by the covered entity or its business associate.

Audits of BAs

- 2002 Privacy Rule commentary (67 Fed. Reg. 53252):

  > *The Privacy Rule does not require a covered entity to actively monitor the actions of its business associates nor is the covered entity responsible or liable for the actions of its business associates. Rather, the Rule only requires that, where a covered entity knows of a pattern of activity or practice that constitutes a material breach or violation of the business associate's obligations under the contract, the covered entity take steps to cure the breach or end the violation.*

- Necessary? Good practice?
  - Pros/Cons

Allen Killworth

Bricker & Eckler
100 S. Third Street
Columbus, OH 43215

614-227-2334
akillworth@bricker.com