ALICE G. GOSFIELD
& ASSOCIATES, P.C.
EST. 1986

The ABCs of HIPAA Security

Daniel F. Shay, Esq
24th Annual Health Law Institute
Pennsylvania Bar Institute
March 13, 2018

ALICE G. GOSFIELD
& ASSOCIATES, P.C.
EST. 1986

Daniel F. Shay, Esq.
Alice G. Gosfield and Associates, PC
2309 Delancey Place
Philadelphia, PA 19103
(215) 735-2384
Dshay@gosfield.com

ALICE G. GOSFIELD & ASSOCIATES, P.C.
EST. 1986

Introduction

- HIPAA is a fact of life for most physicians. True since 1996.
  - First regulations (Privacy Rule) published in 2000.
    - Deals with common obligations for health care providers with respect to patient protected health information (PHI), such as:
      - Leaving messages on answering machines.
      - Calling patients names in waiting rooms.
      - Issues with business associates.
    - Also established patient rights, such as:
      - Access to copies of their PHI.
      - Right to request amendments to their PHI.
      - Right to request restrictions on uses and disclosures of their PHI.
  - Our clients are most familiar with the Privacy Rule.

ALICE G. GOSFIELD
& ASSOCIATES, P.C.
EST. 1986

Introduction (Part 2)

- Security Rule has proven much more difficult for our clients to grasp.
  - First published in 2003.
  - Addresses more technical issues.
    - Requires an understanding of technological infrastructure, or having IT staff who knows this.
    - Federal Government is now enforcing Security Rule much more. E.g., OCR's auditing program.

Steps to Security Compliance

- Security Rule is broken into three general areas.
  - Administrative Safeguards
  - Physical Safeguards
  - Technical Safeguards
- First step in compliance:
  - Appoint a Security Officer.
    - Required under Administrative Safeguards.
    - Should be someone familiar with the technological infrastructure of the covered entity.
    - Should be comfortable discussing technological issues.
    - Current Security Officer should be listed in covered entity's security policies.

ALICE G. GOSFIELD
& ASSOCIATES, P.C.
EST. 1986

Security Risk Assessment

- Keystone of HIPAA compliance. Also required under Administrative Safeguards.
  - HHS Office of Civil Rights (OCR) has described security risk assessments (SRAs) as “foundational.”
  - Necessary to identify covered entity’s risk areas, and know whether it has implemented effective security measures, or if not, where to begin implementing such measures.
  - If a covered entity has not conducted one, it is flying blind!
- OCR Security Rule enforcement frequently finds that no SRA was conducted before an incident.
  - Afterwards is too late.
  - Example: Adult & Pediatric Dermatology.

ALICE G. GOSFIELD
& ASSOCIATES, P.C.
EST. 1986

Security Risk Assessment (Part 2)

- SRAs can be "outsourced." May be helpful to seek outside assistance.
  - Consultants can perform the SRA for a covered entity, if covered entity lacks the internal capabilities to do so itself.
  - Outside consultants are often experts in security matters, capable of thinking of risks our clients might never consider.
    - E.g., wifi printers; where passwords are written down; how workstations are physically positioned within the office.
  - Also understand electronic security standards in connection with legal obligations.
- Can be done "under the privilege."
  - Won't protect the SRA document itself, but may protect the documents generated in the process of creating it.

Security Risk Assessment (Part 3)

- OCR has published guidance on SRA elements:
  - Scope of SRA.
  - Data collection re: storage, use, maintenance, and transmission of electronic PHI (ePHI).
  - Identifying and documenting potential threats and vulnerabilities.
  - Assessing current security measures (if any).
  - Determining impact of potential threats occurring.
  - Determining level of risk.
  - Finalized documentation.
- SRA need only be conducted periodically, e.g. when infrastructure changes.

ALICE G. GOSFIELD
& ASSOCIATES, P.C.
EST. 1986

Security Rule Safeguards

- Once SRA is conducted, can establish the Administrative, Physical, and Technical Safeguards, based on results of SRA.
- Administrative Safeguards
  - Security management. (e.g., policies/procedures re: preventing/detecting/correcting security violations)
  - Assignment of security responsibilities.
  - Workforce security. (e.g., ensuring only appropriate workforce members have access to ePHI)
  - Security awareness and training.
  - Incident procedures for security violations.
  - Information access management. (e.g., who can access what levels of ePHI)

ALICE G. GOSFIELD
& ASSOCIATES, P.C.
EST. 1986

Security Rule Safeguards (Part 2)

- Administrative Safeguards (continued)
  - Technical and non-technical evaluations.
  - Obtaining assurances from business associates that they will protect ePHI in accordance with HIPAA requirements.
  - Conduct/update SRA.
- Physical Safeguards
  - Facility access controls. (e.g., floorplan, locks on doors, etc.)
  - Workstation use policies. (e.g., when to log off)
  - Workstation security. (e.g., only authorized individuals can use workstations.
  - Device and media controls. (e.g., policies re: removing thumb drives)

ALICE G. GOSFIELD & ASSOCIATES, P.C. EST. 1986

Security Rule Safeguards (Part 3)

- Technical Safeguards
  - What most people think of when they think of “security.”
  - Authentication. (e.g., passwords to prove you are who you say you are; 2-factor authentication)
  - Audit controls. (e.g., tracking user activity on systems with ePHI)
  - Integrity policies/procedures. (e.g., ensuring ePHI isn’t improperly modified/destroyed)
  - Transmission security. (e.g., encryption)

ALICE G. GOSFIELD
& ASSOCIATES, P.C.
EST. 1986

Security Rule Enforcement & Audits

- First Security Rule enforcement action came in 2009 – 4 years after Security Rule effective date, and 6 years after OCR given authority to enforce.
  - Enforcement was previously focused on larger institutions.
  - Phoenix Cardiac Surgery, P.C., in 2012, changed that.
- HITECH Act created duty to conduct “periodic audits.”

ALICE G. GOSFIELD
& ASSOCIATES, P.C.
EST. 1986

Security Rule Enforcement & Audits (Part 2)

- Audit Pilot Program launches in 2011.
  - Main purpose: “To examine mechanisms for compliance, identify best practices and discover risk and vulnerabilities that may not have come to light through OCR’s ongoing complaint investigations and compliance reviews.”
- Led to Audit Evaluation Program from November, 2011 – December, 2012.
- Led to “Phase 2” in October, 2014.
  - Continues today. Conducted on-site where possible, but usually a “desk audit.”

What Goes Wrong?

- Audit program discovered:
  - Small providers have many problems, usually with Security Rule compliance.
- Can also look at Resolution Agreements.
- Common problems:
  - Ineffective/no SRA.
  - Lost/stolen thumb drive/laptop.
  - Improperly configured computer systems that make ePHI public.
  - Ineffective/no risk-management plans.
  - Failed to implement policies and procedures to detect/prevent/contain/correct security violations.
- Expensive settlements. $100,000 up to multiple millions!

ALICE G. GOSFIELD & ASSOCIATES, P.C. EST. 1986

Practical Advice

- Look at educational materials from Federal agencies.
  - HealthIT.gov website.
  - “Reassessing Your Security Practices in a Health IT Environment: A Guide for Small Health Care Practices.”
  - “Cybersecurity – 10 Best Practices for the Small Healthcare Environment.”
  - Resolution Agreements = “How not to do it.”