The Lifecycle of Vendor Management

STEPHANE FABUS, DAVID JEMMETT, FRANK RUELAS
MEGHAN O'CONNOR
2022 HIPAA COW SPRING CONFERENCE
APRIL 22, 2022

1

What We'll Cover

- HIPAA Requirements for Business Associates
- Pre-Contracting Diligence
- Security Assessment
- Contracting
- Monitoring Compliance
- Termination

2

HIPAA Requirements for BAs

- Business Associate Agreements
  - Under 45 CFR § 164.308, BAA required for vendors that will create, receive, maintain, or transmit PHI
  - Minimum contract terms
  - Representation of privacy/security program vs. validation testing
- CE not in compliance with HIPAA if CE knew of a pattern of activity or practice of BA that constituted a material breach or violation of the BA's obligation under the BAA, unless CE took reasonable steps to cure breach or end violation, and if unsuccessful, terminate
- Agency analysis

3

Pre-Contract Diligence

- Get privacy involved on Day 0 of lifecycle, not just to sign BAA after contract has been negotiated
  - Dealing with internal pressure to "get it done"
- Pre-contracting attestations
  - Opportunity for internal training – form as a trigger for privacy/security involvement
  - What do you want to know?
    - Offshoring PHI? FDR obligations
    - What data?
    - How will access work?

4

Security Assessment

- How do you evaluate vendor safeguards?
- Self-attestation vs. validation testing
- What do certifications mean?
- Same approach for sophisticated and unsophisticated vendors?

5

Contracting

- BAA required terms are the minimum
  - Sophistication of vendor
  - Best practice privacy/security is evolving
  - Indemnification, insurance, limitation of liability
  - Remember agency analysis considerations. How prescriptive do you want to be?
- What is the organization's risk tolerance?
- What about vendors with access to personal information (not just PHI)?
  - State law
- Leverage

6

Monitoring Compliance

- Continuous communication with vendor?
- Evolving security expectations
- Evergreen contracts
- IT / manpower to monitor

7

Contract Termination

- You need a good prenup
- Return / destroy
  - Infeasibility determination
  - What about backups?
  - Is the data actually returned / destroyed
- Triggers for privacy / security involvement
- Is access terminated?

8

Thank you.

Questions?

9