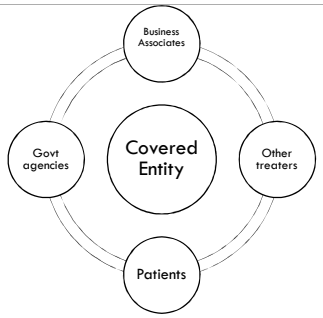
HIPAA:
Considerations for Business Associate Relationships

Slides created by Jennifer L. Cox, J.D.
Cox & Osowiecki, LLC
Hartford, Connecticut

Key HIPAA Relationships

2



HIPAA Roles: Threshold Questions

3

- HIPAA must apply to use HIPAA rules
- Understand the role of each entity involved
- Definitions and role identification are important for sharing permissions
- Keep in mind that a covered entity might also sometimes be a business associate, depending on the relationship and tasks being performed

The Point of a BAA

4

- Each CE-BA relationship needs to have a written BA arrangement in place for compliance
  - Failure to have written arrangements immediately takes you out of compliance with several HIPAA rules
- But ***just signing a piece of paper*** is not the only essential feature for establishing and maintaining a successful CE-BA relationship
- Understanding roles, permissions, obligations, and scope of use is also critical
- Having a clear communication plan between CE-BA in the event of a breach is essential

Entity Status

5

- Do not deputize yourself a Covered Entity if you are not one
  - Self appointment of status when the rules do not support that status will result in mistakes for sharing and handling of sensitive information and PHI
- Do not deputize vendors as Business Associates if they do not fit the rule
  - Consider this a Goldilocks issue: **it needs to be just right**
  - Avoid the urge to make every vendor a BA – you need to do the work to be sure the vendor fits the rule

BAA Terms

6

- You cannot fall below the minimum rule BA requirements for Privacy, Security, and Breach
- You cannot contract out of the Enforcement Rule (no matter how hard you try)
- The OCR template is very useful to identify what is required in a BAA
- It does not matter who drafts the BAA, but you need to have a "meeting of the minds"
- Threshold question: what functions and services are being performed
  - Services can be set forth in a separate contract, these terms do not need to be repeated in the BAA

Optional Terms and Add-Ons

7

- Indemnity clauses: how much does this actually help, and consider that incorrectly drafted, they can they hurt you
- Insurance clauses should be reasonable
- Be sure that indemnity and insurances clauses do not accidentally make it harder to rely on otherwise available insurance (happens often)
- If you exceed the minimum HIPAA rules, are you doing it for a good reason?
  - The BA probably has other customers who have their own list of issues; if you over-customize are you just making it unnecessarily hard to use that vendor

Your Brother's Keeper

8

- The HIPAA Rules do not make the CE the overlord of the BA's activities, but…
  - CE cannot ignore a BA's blatantly poor HIPAA compliance
- You need a comfort level that the BA understands its core obligations – chief among these is that the BA must comply fully with the Security Rule