WYATT TARRANT & COMBS LLP

Legal Considerations Surrounding Cybersecurity

presented by

Erin Brisbay McMahon, Esq.
Wyatt, Tarrant & Combs, LLP

Central Kentucky Association of Health Underwriters

March 3, 2016

Lawyer's Typical Disclaimer

Nothing in this handout or presentation constitutes legal advice, nor is the content to be considered comprehensive and exhaustive on the subject matter. Consult with a lawyer before making your decisions.

Breaking News!

- Phishing attack
- Fake e-mail to HR and accounting from the CEO/CFO/managing partner
- “Send me all the W-2s for all employees immediately”
- Victims: Snapchat, many other companies
- See news story here: http://www.cbsnews.com/news/a-new-twist-on-a-w2-tax-scam/

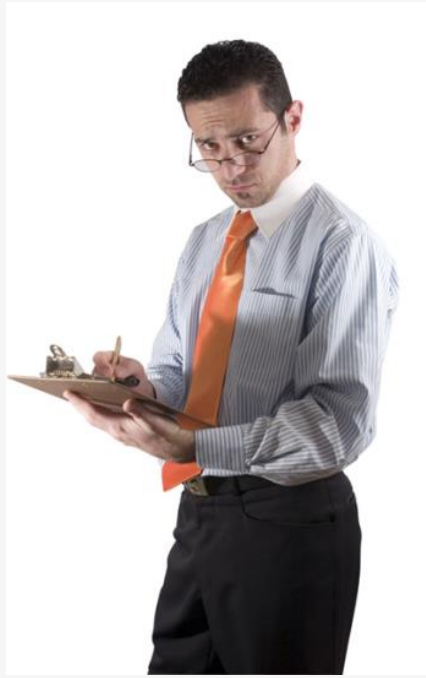
PREVENTION AND RESPONSE PLANS ARE KEY IN THIS ENVIRONMENT

Agenda

- Overview of Applicable Laws
- Business Associate Agreements
- Cyberinsurance
- What to do in case of Data Breach

Privacy Laws

- FTC - GLB (see 806 KAR 3:210), Red Flags Rule, FCRA, Section 5
- HIPAA
- State laws
  - Privacy
  - Data Breach Notification
  - Consumer Protection Acts



FTC Act

- Section 5 of the Federal Trade Commission Act (FTC Act) (15 USC 45) prohibits "unfair or deceptive acts or practices in or affecting commerce."
- What do your website page/marketing/RFPs say about your data protection policies?
- Rite Aid – 20 years of biennial audits

HIPAA Background

- 1996 – HIPAA enacted – 42 USC §§ 1320d-1320d-9
- 2003 – Privacy Rule
- 2005 – Security Rule
- 2006 – Enforcement Rule
- 2009 – HITECH enacted
  Updated Enforcement Rule and
  Breach Notification Rule
- January 25, 2013 – Final HIPAA Omnibus Rule
- September 23, 2013 – Compliance Date

HIPAA

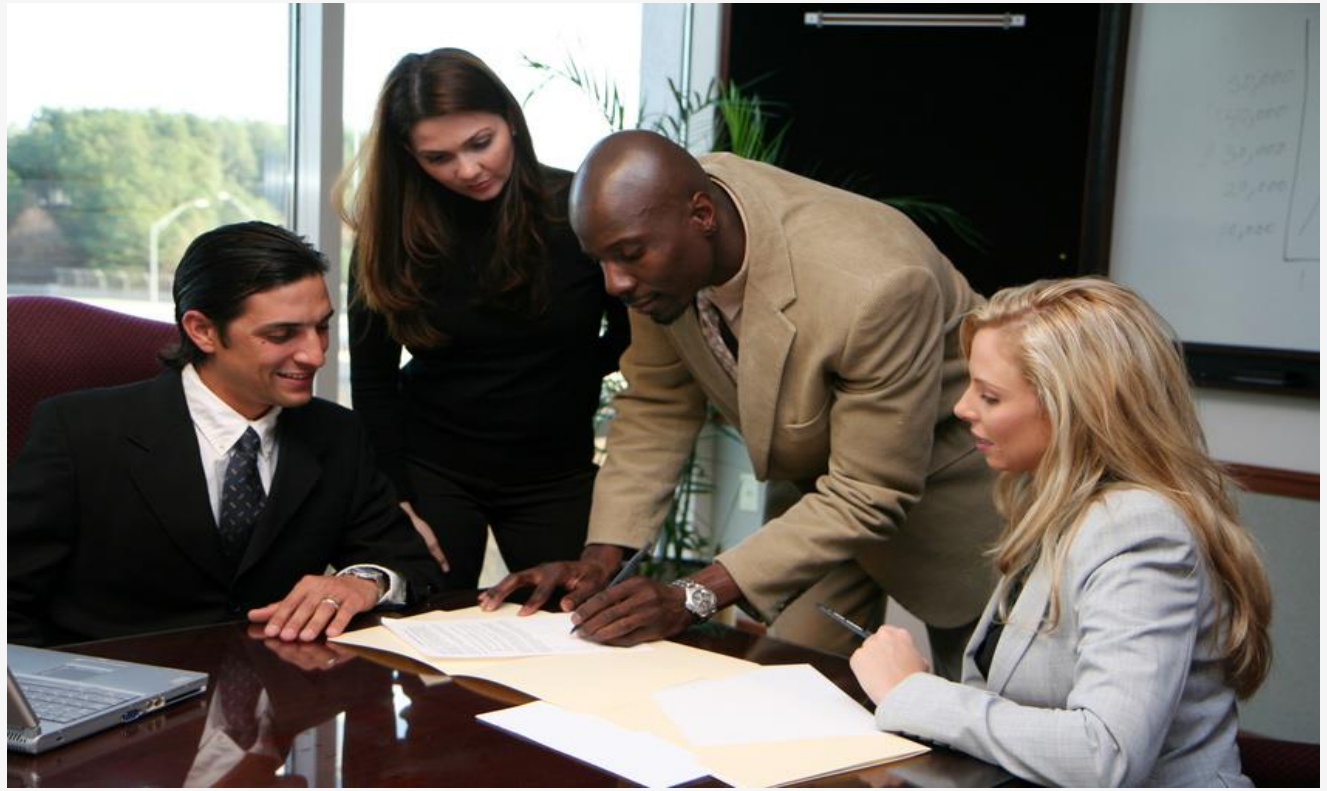
- All of the Security Rule (45 CFR 164.302-.316) applies to Business Associates, as well parts of the Data Breach Rule (45 CFR 164.400-.414) and the Privacy Rule (45 CFR 164.500-.532)

State laws

- Privacy
- Data Breach Notification
- Consumer Protection Acts

WYATT TARRANT & COMBS LLP

BUSINESS ASSOCIATE AGREEMENTS



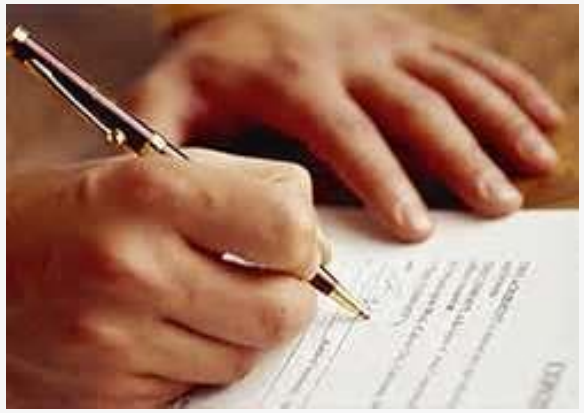
Who Is a Business Associate?

1) Creates, receives, maintains or transmits PHI for or on behalf of a Covered Entity (payment or health care operations purposes)

2) Provides certain identified services to a Covered Entity that require the disclosure of PHI (e.g., claims processing, legal, accounting, consulting, etc.)

Business Associate Agreements

- Sample provisions: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html
- Beyond OCR's website –
  - insurance provisions
  - indemnity provisions



Indemnity Provisions

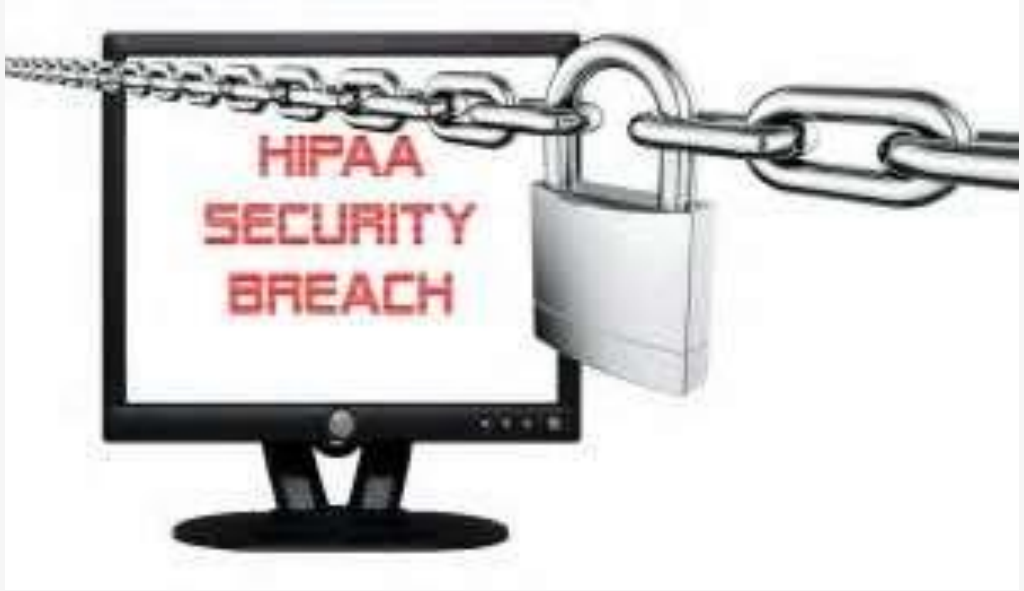
- What are you promising?
  - Beware the dreaded “any and all” clause (including attorneys’ fees)
  - Does your cybersecurity insurance let you make those promises without suffering an exclusion?

CYBERINSURANCE

Types of Insurance

- First-party
  - Attorneys' fees
  - Forensics
  - Mailings
  - Credit monitoring
  - Crisis Management
  - Regulatory settlements/fines
- Third-party claims
- Cyberextortion
- Media liability
- Business Interruption

BREACH NOTIFICATION



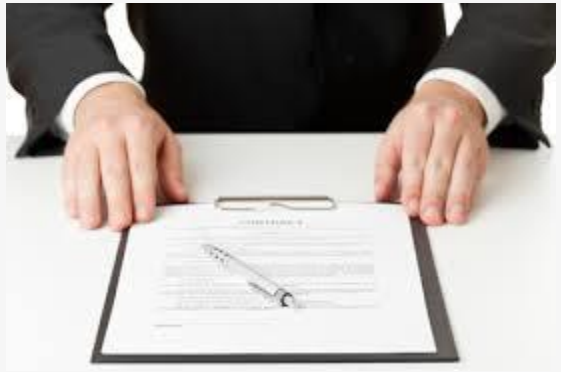
What the Rule says

- Business Associate notifies Covered Entity, then the Covered Entity notifies its patients/insureds
- Business Associate needs to notify Covered Entity within 60 days of date of discovery but without “unreasonable delay”
- Include the identification of each individual whose unsecured PHI has been, or is reasonably believed by the business associate to have been, accessed, acquired, used, or disclosed during the breach, plus.

What the Rule says

- Include:
  - What happened (incl. date of breach and date of discovery)
  - Types of PHI potentially compromised
  - Steps individuals can take to protect themselves
  - What you are doing to investigate and mitigate
  - Contact procedures

More importantly – what does your BAA say?



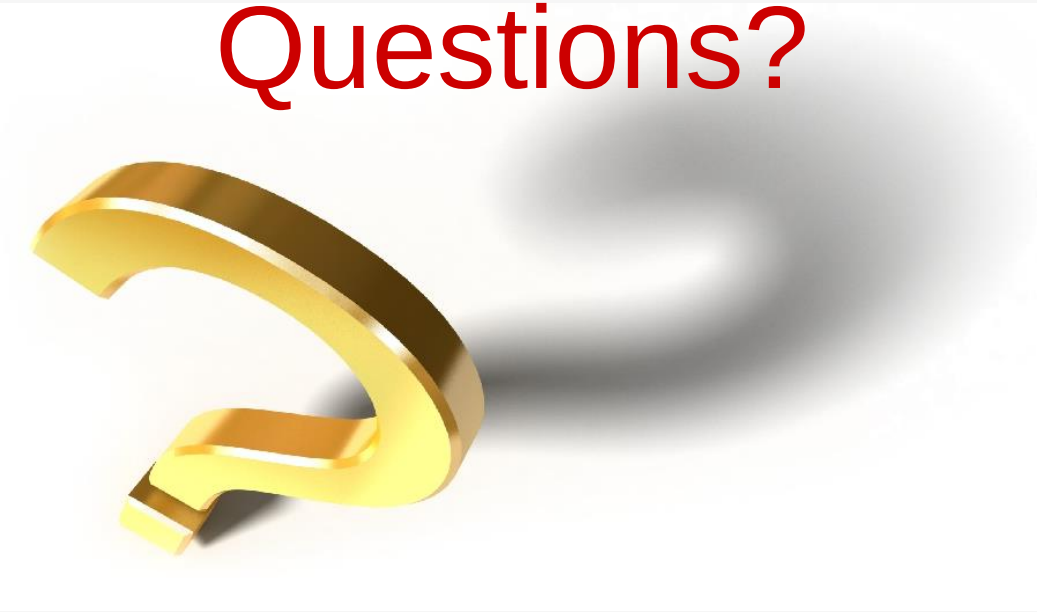
- Notifying the Covered Entity
- Who provides notices – the Covered Entity or you?
- Indemnity for costs of a Breach

WYATT TARRANT & COMBS LLP

Practical Tips to Respond to a Breach

- Breach response plan and table-top exercises
- Keep a BAA binder
- Look at the relevant BAAs if there is a potential breach – how much time do you have for notice to the affected Covered Entities?
- Call your insurer – they will dictate attorneys, forensics, mailing company, crisis management
- Litigation hold – let employees/agents know not to destroy any notes pertinent to the investigation. Disable auto-delete rules that might affect the investigation.

Questions?



Erin Brisbay McMahon, Esq.
Wyatt, Tarrant & Combs, LLP
250 West Main St.
Suite 1600
Lexington, KY 40507
emcmahon@wyattfirm.com
(859) 288-7452