From The Healthcare Attorney’s Desk

Avoid These Landmines
So Many Issues, So Little Time

• Current security landscape filled with many traps
  • Must stay ahead of issues
  • Seek help and do not try do it alone
• Often find clients or other trying to “play” lawyer
  • Issues can seem obvious, but undercurrents
Security Misconceptions

- Misunderstandings and myths common place
- Can lead to:
  - Complacency
  - Interference with organizational responsibilities and/or individual rights
  - Potential creation of liability
  - Patient/consumer dissatisfaction
Top Issues I (a healthcare lawyer) See

• Cybersecurity or other insurance provides all necessary protection
• Risk analysis is easy and of no concern
• Social media and technology is not for healthcare
• Just sign and ignore Business Associate Agreements
• HIPAA Compliant or HIPAA Certified means a product or vendor is a perfect fit
What’s Wrong With Statements

• Never good to assume everything is all set
• Do not take anything by its surface appearance, always dig deeper
• Misapplication of law should not be permitted
• Fear of consequences should not hold back decision, just become informed
Cyber Liability Insurance - Problems

- I don’t need separate cybersecurity insurance, I have coverage as part of my [fill in other type of insurance]
- The questionnaire when applying is not that important, my responses do not need to be accurate
- My policy will cover any fine, penalty, cost or action that I need to take if a breach happens
Cyber Liability Insurance – Don’t Need Policy

• Standalone coverage is likely essential
• If included with general liability, professional liability, or other type likely not comprehensive or may be wrong in assumption
• Evaluate risks, helps determine appropriate coverage to acquire
• Specific cyber liability policy contemplate specific cyber liability issues
  • For example: breach response, data recovery, compliance, protection for patients/customers
Cyber Liability Insurance - Applying

• Accuracy in questionnaire responses essential
• Misleading or inaccurate statements can be used to deny coverage
• Responses may impact premiums, exceptions to coverage and other applications of the coverage
• Can responses be updated?
  • Is change material? Was response fundamental to coverage?
  • No clear answer, require situation by situation assessment
Cyber Liability Insurance – Scope of Coverage

- Not set standard for what policies cover
- Pay attention to specific terms, conditions and riders to policy obtained
- Presentation of claim influences coverage decisions
- Be wary of contractual commitments (indemnification) that could invalidate coverage
Risk Analysis - Problems

- I can do a risk analysis by myself
- All of an organization’s risk are low
  - Some “justifications” can be do not handle much PHI, small organization, individual performing not an in-depth knowledge of systems
- Wrong tools used
- Conducted infrequently, letting too much time pass
Risk Analysis – Improving Conduct

• Starting point: essential building block for complying with HIPAA Security Rule
  • Never forget risk analysis is a required element
• Outsourcing vs. insourcing
  • Resolution depends upon resources and capability
  • Likely end up with a blend
• Be honest when reviewing systems and activities
  • No organization should ever end up with all low level threats and low likelihood of occurrence
Risk Analysis – Improving Conduct

- What tools can be used?
  - OCR provided two free tools for use
  - Regulations provide some framework
  - NIST
  - Ask colleagues and others in same position
- Think about elements laid out in rule:
  - Risks and vulnerabilities
  - Impacting confidentiality, integrity and availability
Social Media - Problems

- Social media connects directly with individuals and do not want that relationships with patients
- No one uses social media
- Social media use is not permitted by HIPAA
- No individual in the organization wants to use social media
- If information is shared, the organization is just creating liability
Social Media - Considerations

- Opportunity to provide useful, generalized information
- Means of distinguishing
- Use can be varied
- If not using social media, missing basic component of modern communication
- Have a plan, do not go in haphazardly
Social Media - Examples

- Live streaming surgery
  - Phoenix Children’s and team-based approach
- Education and Engagement
  - Mayo Clinic – created training program, including “residency” and “fellow program”
- Support
  - Not always about outward facing uses
Business Associate Agreements (BAA) - Problems

• Every BAA is signed without being read because no one actually looks at it again
• Every contracting party is given a BAA because that is a good assurance
• Including indemnification will provide protection if an issue happens
• State based data breach issues should be included
BAAs – Getting to the Heart

• BAA should never be signed without reviewing
  • Often, many terms beyond basic requirements of regulations
  • Need to know what getting into as well for required response times
• Only use when appropriate, otherwise creating contractual complications
• Additional Terms
  • Indemnification/Reimbursement
  • Insurance
  • Restrictions on use
BAAs and State Law

• What is proper scope for a BAA?
• How cohesive is state law with HIPAA?
• How aware is business associate of state law?
• No restriction on including, seeing more frequently
• Be wary of conflicting, overlapping, duplicative, and sometimes contradictory requirements
HIPAA Compliant or Certified - Problems

- Vendor says its product is HIPAA Certified to meet all privacy and security needs
- Different vendor says its product is HIPAA Compliant and fits into an organization’s compliance plan
- In either scenario, the statement is about “HIPPA”
HIPAA Compliant or Certified – Don’t Buy It

• Government and no private organization provides certification program, nor can compliance be guaranteed
• Products cannot be compliant, but are part of an organization’s compliance
• Perform due diligence on a vendor
  • Ask questions
  • Develop set list of items to present to all vendors
• Never rely solely upon basic representation
• If see HIPAA misspelled, consider it a warning sign
Takeaways

- HIPAA blamed, unfairly, for many problems in healthcare
- Take time to carefully consider problems and break each problem down to core issues
- Do not be afraid to ask questions and seek assistance
- You are not alone, others have same questions
  - Corollary – no question is bad, every question leads to person asking becoming more knowledgeable