Grab Bag – HIPAA, BYOD, Risk Analysis, and Other Healthcare IT Issues

A Lawyer's View

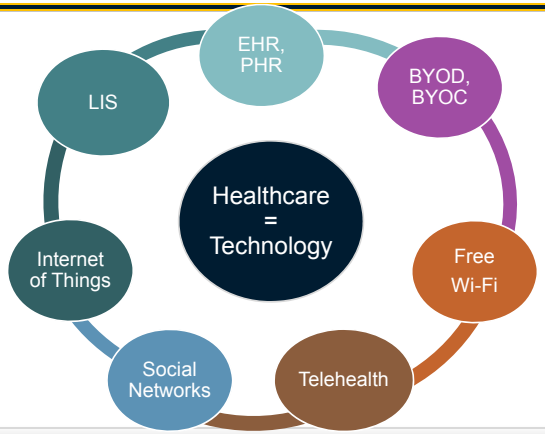
Suncoast Healthcare Executives
March 26, 2015

Tatiana Melnik
Melnik Legal PLLC
tatiana@melniklegal.com | 734-358-4201

Outline

- Why Are We Talking About Healthcare Information Technology?
- A Few Questions…
  - Communication
  - Mobile Devices
  - EHR Vendors
  - Encryption
  - Data Breaches
  - Enforcement
  - Policies and Procedures
  - Social Media & Marketing
  - Insurance
- Open Floor

Why Healthcare IT?



Communication Issues

- Email
  - Is e-mail a secure form of communication?
  - What about forms that are e-mailed from websites? Are these secure?
  - Should medical practices use personal e-mail addresses for practice communications
- eFax
  - Is eFax a secure form of communication?
- Skype and FaceTime
  - Can providers use Skype and FaceTime with patients and comply with HIPAA?
- Remote file sharing/storage systems
  - How safe/secure are programs like DropBox, Box.com, etc.?

This slide presentation is informational only and was prepared to provide a brief overview of some healthcare information technology issues. It does not constitute legal or professional advice. The healthcare regulatory environment is ever evolving. You are encouraged to consult with an attorney if you have specific questions relating to any of the topics covered in this presentation. Tatiana Melnik, Melnik Legal, PLLC, Tampa, FL

Communication Issues

- Email
  - Is e-mail a secure form of communication?
    - **Maybe**.
      - If you're using "regular" e-mail = No.
      - If you're using "secure" e-mail = Maybe.
        - **Is there a BAA in place with the e-mail provider?**
          - Microsoft will sign BAA for its Office 365 solution
          - Google will sign a BAA for its Apps for Business solution

Communication Issues

- Email
  - What about the forms that are e-mailed from websites? Are these secure?
    - **Maybe**.
      - Have you asked your webmaster?
      - What does the Privacy Policy on your website say about the forms?
      - Is there a check the box disclaimer prior to submission for each of the forms? A link to the privacy policy?

Communication Issues

- Email
  - Should medical practices use personal e-mail addresses for practice communications?
    - **No**.
      - How does the practice meet record keeping requirements?
      - Is there a BAA in place with the e-mail provider?
      - What happens when an employee leaves?
        - Is there a contract in place addressing ownership?
        - Cooperation in the event of litigation?

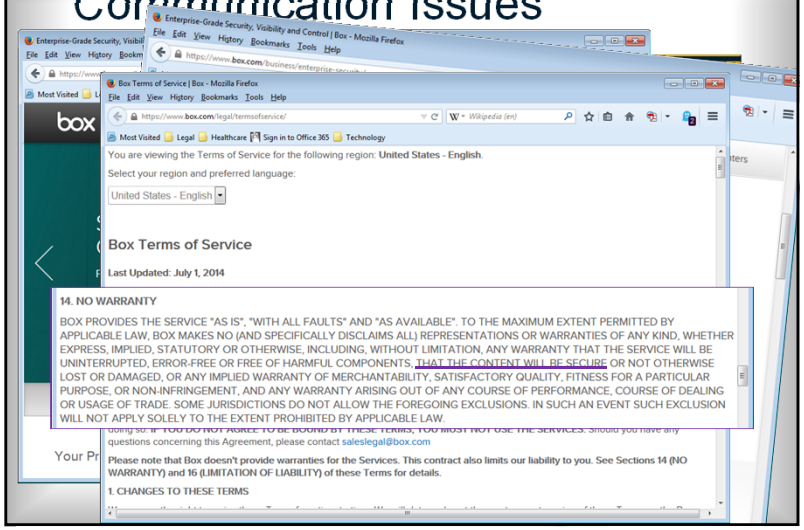
Communication Issues

- eFax
  - Is eFax a secure form of communication?
    - **Maybe**.
      - How is the fax delivered?
        - If via "regular" e-mail = No.
        - If via "secure" e-mail = Maybe.
          - Is there a BAA in place with the eFax provider?

Communication Issues

- Remote file sharing/storage systems
  - How safe/secure are programs like DropBox, Box.com, etc.?
    - **What do their terms and conditions say?**
      - Does the marketing match the contracts?
      - Who is operating the companies?
      - How do the companies make money (advertising vs. services)?
      - Have they been independently audited? Can you get a copy of those reports? How were the auditors?

Communication Issues



Communication Issues

- Skype and FaceTime
  - Can providers use Skype and FaceTime with patients and comply with HIPAA?
    - **No**.
      - Are Microsoft and Apple Business Associates with respect to these applications?
      - HIPAA requires that providers enter into a Business Associate Agreement with each of their BAs.
        - Microsoft will not sign a BAA for Skype
        - Apple will not sign a BAA for FaceTime
      - Option: Cisco Webex – Cisco will sign a BAA for Webex

Mobile Device Issues

- Can doctors text with their patients?
  - **Yes, but…**
    - Is texting secure?
    - Patient authorization? Disclaimers? Disclosures?
    - What are the protocols to ensure that information is getting into the medical record?
- Should all staff members sign a BYOD Agreement?
  - **Yes**
    - Erasing data upon termination, appropriate use, reporting in case of loss, etc.
    - Spoliation

EHR Vendor Issues

- Can my EHR vendor really sell my patients' information?
- Can my EHR vendor advertise to my patients?
- What's with all of these interface costs?
- My EHR vendor charged me for PQRS submission, but their tools didn't work and I submitted via Registry. Can I get my money back?

EHR Vendor Issues

- Can my EHR vendor really sell my patients' information?
  - **Yes, if you gave the vendor permission.**
    - What does your agreement say?
    - What rights did you grant to the EHR vendor?
    - How long is the indemnification period vs. data breach risks?
    - Consider whether the arrangement now qualifies as a "sale" under HIPAA

EHR Vendor Issues

- Can my EHR vendor advertise to my patients?
  - **Yes, if you gave the vendor permission.**
    - What does your agreement say?
    - Are you monitoring the ads?
    - Do you need to give your patients notice regarding the ads and provide disclaimers?

EHR Vendor Issues

- What's with all of these interface costs?
  - Everyone is angry, including Congress…
  - MU Stage 3 Proposed Rule (March 20)
    - CMS has proposed, for example, to include API functionality to permit data exchange –

"From the provider perspective, using this option would mean the provider would not be required to separately purchase or implement a 'patient portal,' nor would they need to implement or purchase a separate mechanism to provide the secure download and transmit functions for their patients because the API would provide the patient the ability to download or transmit their health information to a third party." (CMS-3310-P, p. 92)

EHR Vendor Issues

- My EHR vendor charged me for PQRS submission, but their tools didn't work and I submitted via Registry. Can I get my money back?
  - **Maybe.**
    - What does your agreement say?

Encryption Issues

- Do I need to encrypt ALL of my laptops?
- Can I just password protect the files?
- Can I just password protect a directory or a drive?
- Is there a specific form of encryption that should be used?

Encryption Issues

- Do I need to encrypt ALL of my laptops?
  - **No… but Yes.**
    - Encryption is an addressable standard under HIPAA. But, "addressable" ≠ optional.
    - FIPA requires the use of "reasonable measures to protect and secure data in electronic form".
    - If encrypted, then out of the breach notification requirements.

Encryption Issues

- Can I just password protect the files?
  - **Yes… but...**
    - Whether this is the best option depends on why you are using this option . . .
      - Is this the primary means to secure information stored on a laptop, desktop, server, etc.?
      - Or is the file being password protected because it needs to be shared?
    - Is there a password policy? How is it being enforced?

Encryption Issues

- Can I just password protect a directory or a drive?
  - **Yes… but... No.**
    - Whether this is the best option depends on why you are using this option . . .

AvMed Health Plan - In 2009, *unencrypted* laptops stolen from office during a "break-in"
- Class action filed in Florida; after several years of litigation, AvMed **settled** in October 2013 for **$3M**
- In fact, AvMed *implemented encryption* – but encrypted a drive where employees were ***supposed to*** store PHI

Encryption Issues

- Is there a specific form of encryption that should be used?
  - **Yes.**
    - Under HITECH, Congress required the HHS Secretary to issue guidance to render unsecured PHI unusable, unreadable, or indecipherable to unauthorized individuals
    - The Guidance looks to NIST
      - Data at rest - NIST Special Publication 800-111
      - Data in motion - NIST Special Publications 800-52 and 800-77
      - **Bottom line**: best to use technology that is **FIPS 140-2 *validated*** (not "compliant")
        - *Includes*: Microsoft BitLocker (included on Windows 8 machines for free), Symantec PGP (the Symantec Endpoint Encryption suite is used by the IRS)
        - TruCrypt is not FIPS 140-2 validated and is no longer supported

Data Breach Issues

- Do I have to report every HIPAA Breach?
- Can an individual be held liable under the HIPAA Privacy and Security Rule?
- I keep hearing about the Office of Civil Rights, but are there others enforcing HIPAA?

Data Breach Issues

- Do I have to report every HIPAA Breach?
  - **Yes.**
    - If the security incident is a "breach" as defined in HIPAA (or FIPA), then the question is merely *when* the report is due.
      - If breach impacts *500+* individuals – report due to the
        - **HHS Secretary** "without **unreasonable delay** and in no case later than **60 calendar days** from discovery"
        - **Florida AG** "as **expeditiously as practicable**, but no later than **30 days** after the determination of the breach or reason to believe a breach occurred"
      - If breach impacts *less than* 500 individuals – report due to the Secretary "within 60 days of the end of the calendar year in which the breach was discovered"

http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html

Data Breach Issues

- Can an individual be held liable under the HIPAA Privacy and Security Rule?
  - **Yes.**
    - There are criminal and civil penalties
      - Criminal penalties – fine of $250,000 and 10 years in federal prison
      - Civil – fine of $1.5M
    - Doesn't happen often; most likely to be indicted for other federal offenses (*e.g.*, some form of fraud – mail fraud, Medicare fraud, etc.)
    - But, a Texas grand jury indicted a former employee of a covered entity for HIPAA violations in July 2014

Data Breach Issues

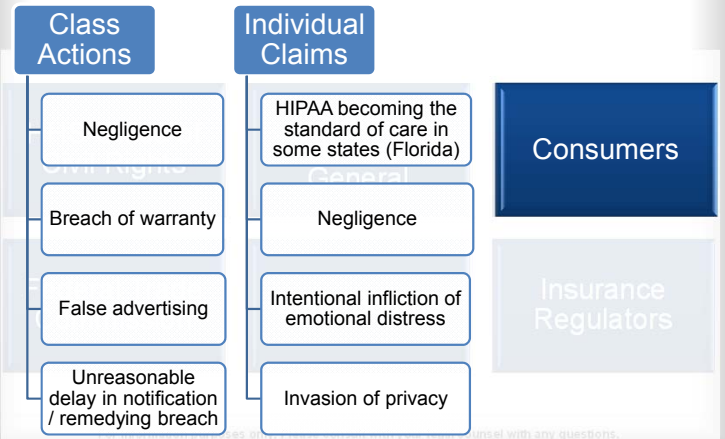
- I keep hearing about the Office of Civil Rights, but are there others enforcing HIPAA?
  - **Yes.**

Data Breach Issues

- Who are the enforcers?

HHS Office of Civil Rights	State's Attorneys' General	Consumers
Federal Trade Commission	State Boards	Insurance Regulators

Data Breach Issues



This slide presentation is informational only and was prepared to provide a brief overview of some healthcare information technology issues. It does not constitute legal or professional advice. The healthcare regulatory environment is ever evolving. You are encouraged to consult with an attorney if you have specific questions relating to any of the topics covered in this presentation. Tatiana Melnik, Melnik Legal, PLLC, Tampa, FL

Policies and Procedures

- Aren't all of these HIPAA policies and procedures just "forms"? Can I just pick a set off of the Internet?
  - **No and no.**
    - Polices and procedures are not aspirational; they should reflect what your practice actually does
    - The HIPAA regulations have specific requirements
    - OCR audits:

Policies and Procedures

- For every finding and observation cited in the audit reports, audit identified a "Cause."
- Most common across all entities: **entity unaware of the requirement.**
  - in 30% (289 of 980 findings and observations)
    - **39% (115 of 293) of Privacy**
    - **27% (163 of 593) of Security**
    - **12% (11) of Breach Notification**
  - Most of these related to elements of the Rules that explicitly state what a covered entity must do to comply.
- Other causes noted included but not limited to:
  - Lack of application of sufficient resources
  - Incomplete implementation
  - Complete disregard

Social Media & Marketing

- A patient complained about my practice on Yelp. Should I respond?
- A patient complained about my practice on Yelp. Can I have it removed?
- I got a cease and desist trademark infringement letter from "XYZ Practice," but the name of my practice "XYZ Practice *and More*." Do I have to change the name of my practice?

Social Media & Marketing

- A patient complained about my practice on Yelp. Should I respond?
  - **Probably not.**
    - Disclosing the fact that someone is a patient is problematic under HIPAA
- A patient complained about my practice on Yelp. Can I have it removed?
  - **Maybe…**
    - Is it defamatory? (slander = spoken; libel = written)
      - False statements that damage someone's reputation
      - Florida recognizes defamation *per se* – something so bad that the mere fact that it was spoken/written is sufficient to show damages (*e.g.*, damaged someone's business reputation, claim/disclose STD status, claim someone committed a crime, etc.)
      - Is it true? Truth is a defense.
    - Requires an individualized assessment because turns on what was actually said

Social Media & Marketing

Abigail E. Hinchy v. Walgreen Co. et al. (Indiana Superior Ct., 2013; Affirmed by Appellate Ct., 2014)

- Pharmacist improperly accessed medical records of one patient
- Patient reported the incident to Walgreens and Walgreens did not disable the pharmacist's access
- Jury awarded $1.8 million, with $1.4M of that to be paid by Walgreens

Social Media & Marketing

- I got a cease and desist trademark infringement letter from "XYZ Practice," but the name of my practice "XYZ Practice *and More*." Do I have to change the name of my practice?
  - **Maybe.**
    - It depends on a number of factors including how common XYZ is for the specific services, whether you were the first to use the name, etc.
    - Should obtain trademark clearance prior to adopting a mark
      - If you have media coverage, your insurance policy will likely require this for coverage

Insurance

- What should I look for in a data breach insurance policy?
  - Many options – work with an experienced broker and obtain legal review
    - Are government fines covered? Are there limitations (*e.g.*, actual fine vs. cost to investigate)
    - Are business associates covered? Only covered if you have "written agreements" in place?
    - Rogue employee coverage?
    - Are there encryption requirements for laptops?
    - Identity theft coverage? Include call centers and credit monitoring?
    - Coverage for forensics? Sub-limits?
    - Coverage for crisis management? Sub-limits?

Disclaimer

This slide presentation is informational only and was prepared to provide a brief overview of hot topics in healthcare. It does not constitute legal or professional advice.

You are encouraged to consult with an attorney if you have specific questions relating to any of the topics covered in this presentation, and Melnik Legal PLLC would be pleased to assist you on these matters.

This slide presentation is informational only and was prepared to provide a brief overview of some healthcare information technology issues. It does not constitute legal or professional advice. The healthcare regulatory environment is ever evolving. You are encouraged to consult with an attorney if you have specific questions relating to any of the topics covered in this presentation. Tatiana Melnik, Melnik Legal, PLLC, Tampa, FL

This slide presentation is informational only and was prepared to provide a brief overview of some healthcare information technology issues. It does not constitute legal or professional advice. The healthcare regulatory environment is ever evolving. You are encouraged to consult with an attorney if you have specific questions relating to any of the topics covered in this presentation. Tatiana Melnik, Melnik Legal, PLLC, Tampa, FL