Legal Issues in Medical Office Use of Social Media

James F. Doherty, Jr.
Pecore & Doherty, LLC
Columbia, Maryland

Legal Issues in Social Media for Physician Practices

- HIPAA/State Confidentiality laws
- State Medical Practice Act/Licensure
  - Standard of Care
  - Advertising
  - Confidentiality
- Medical Malpractice
- Defamation (plaintiff or defendant)
- False Advertising (state, FTC)

HIPAA

- Applies to “Protected Health Information” (“individually identifiable health information”) ***in any medium***
- Fines, civil and criminal penalties for unauthorized disclosure/breach
- No private cause of action but federal investigations, patient state law suits for breach of privacy, etc.
- Particularly sensitive to PHI containing information on sexual or reproductive issues, mental health substance abuse or personal financial information

HIPAA II

- HITECH Changes, HIPAA 2.0
- Omnibus Final Rule Compliance required as of September 23, 2013
- New breach notification standard
- Patient access to electronic records
- Increased penalties
- “Mere conduits” or digital couriers are not included as BAs, but entities storing PHI, even without intent to view it, are included.
- Cloud Models are implicated (open box vs. sealed box)

“Social Media”

- Twitter
- Facebook
- Blogs
- Wikis
- LinkedIn
- Google+
- Smartphone apps

Online Stupidity Olympics

- Physician Tweeting during his medical malpractice trial
- Nurse who posted funny patient photo and chart on Facebook, including comments on patient's sexual health concerns
- Physician who treated patient over Twitter
- ER personnel posting pictures of patient with fatal stab wounds on the Internet
- Doctor who asked a patient on a date after seeing her online dating profile
- Physician fired by hospital and reprimanded by Medical Board for posting blog about a hard day at work with employer complaints and patient details

Stupidity Olympics II

- Group of nurses using Facebook to provide unauthorized shift change updates to their co-workers, no use of patient names, but enough specifics about patients so that the incoming nurses could prepare for their shift
- Paramedic who treated a sexual assault victim posted information about the assault on his MySpace page. No disclosure of the victim's name, but enough information for news reporters to discover the identity of the victim and then search for her at her home.
- Medical office staffer who offered female patients with substance abuse problems drugs from the sample cabinet in exchange for sex
- Hospital staff taking selfies in front of patient assignment boards

Breach Notification

- Elimination of “harm” standard (substantial risk of financial, reputational or other harm”)
- ***Rebuttable presumption*** that unauthorized disclosure is a reportable breach
- Risk analysis:
  - Nature and extent of PHI involved
  - Identity of person who made disclosure or received PHI
  - Whether PHI was actually acquired or viewed
  - Extent to which risk has been mitigated

Breach Notification II

- Exclusions from definition of Breach remain the same:
  - Within the Scope of Authority
  - Inadvertent disclosure
  - Recipient is unable to retain PHI

Breach Notification III

- Maryland Personal Information Protection Act (MPIPA):
  - If there is a breach of patient personal information that could lead to identity theft or other financial harm, MPIPA notice is required.
  - May overlap with HIPAA breach notification
  - Applies even if no health information is released (SSNs, address, driver's license, phone numbers, account numbers, policy numbers, etc.).
  - Breach notice must be submitted to Maryland Attorney General ID Theft Unit in advance (http://www.oag.state.md.us/idtheft/)

Patient Access

- If PHI is maintained electronically, patient may request electronic copy
- Must be offered in any format readily producible, otherwise in readable format agreed by provider and patient
- Provider may charge for cost of media (CD, USB, other portable media) and labor for responding to request

Notice of Privacy Practices

- New OCR templates available
- Update to include email, social media?
- Must now include:
  - Sale or marketing of PHI
  - Other purposes that require patient authorization
  - For providers engaging in fundraising, opt out statement
  - Health Plan restrictions
  - Right to receive breach notifications

Penalties

- **Covered Entity did not know** (and it would not have been reasonable for them to know):
  - $100 to $50,000 per violation; $1.5 Million maximum per standard violated per year.
- **Due to reasonable cause** (and not willful neglect):
  - $1,000 to $50,000 per violation; $1.5 Million maximum per standard violated per year.
- **Due to willful neglect (corrected within 30 days):**
  - $10,000 - $50,000 per violation; $1.5 Million maximum per standard violated per year. At least $50,000 if not corrected within 30 days

Recent Enforcement Actions

- Hospice of North Idaho: **$50,000 settlement** for theft of laptop affecting less than 500 individuals (Jan. 2013)
- Phoenix Cardiac Surgery: **$100,000 settlement** for clinical appointment calendar that was publicly accessible on internet (April 2012)
- Mass Eye & Ear: **$1.5 million settlement** for theft of laptop (Sept. 2012)
- Alaska Medicaid: **$1.7 million settlement** for theft of portable USB hard drive (June 2012)
- BCBST: **$1.5 million settlement** for theft of 56 unencrypted hard drives (March 2012)
- UCLA Health System: **$865,000 settlement** for employees' improper access of celebrity patients' EMRs (July 2011)

Recent Enforcement Actions II

- Concentra Health Services, $1.7 Million fine for theft of an unencrypted laptop
- Mass. Gen. Hospital: **$1 million settlement** for failure to safeguard PHI containing SSNs and HIV/AIDS left on subway (Feb. 2011)
- Cignet Health: **$4.3 million civil monetary penalty** for failure to provide access to medical records and failure to cooperate with investigation (Feb. 2011)
- Dramatically increased enforcement expected in the next 12 months

Medical Malpractice

- Inadvertent creation of physician patient relationship online (Facebook, Twitter, etc.)
- Third party reliance on posted advice
- Allegation of inadequate examination or treatment
- Inadequate response time to online inquiry
- Online communication could be construed as evidence of relationship and medical record of interaction
- Treat as a “cocktail party consult”

Medical Malpractice II

- Risk Management:
  - Use of disclaimers
  - Offline response to specific inquiries
  - In-person evaluation or evaluation that meets Maryland web site telemedicine guidelines
  - Use of Privacy Settings
  - Avoid unsecured Wi-Fi networks
  - Check with your liability carrier for guidelines and best practices

Defamation

- Untrue or unsupported statements that harm a person's reputation, financial interests
- State court actions for libel (written) or slander (oral) defamation.
- Action if physician is defamed on social media:
  - Contact web site and request takedown
  - Cite violation of specific terms of service
  - Civil action

Maryland Telemedicine Regulations

- COMAR 10.32.05
- Permissible interaction modalities, two-way audio visual (not phone call or email)
- Mandatory payor reimbursement
- **Mandatory telemedicine website disclosures**:
  - Licensure status and physician number
  - Physician ownership
  - Fees for services offered
  - HIPAA Notice of Privacy Practices
  - Identity verification procedures
  - Prevention of unauthorized access
  - Expected response time

AMA Social Media Guidelines 2010

- Optimal use of privacy settings
- Routinely monitor your own Internet presence, posted by you or by third parties for accuracy and appropriateness
- Maintain appropriate boundaries of physician patient relationship online
- Separate personal and professional online content
- Recognize risks and potential negative consequences

2012 HHS Guidance on Use of Mobile Devices

- www.healthit.gov
- Risks:
  - Lost devices
  - Stolen devices
  - Virus downloads
  - Shared devices
  - Unsecured Wi-Fi connections

Guidance on Use of Mobile Devices

- Passwords
- Encryption remote wiping/disabling
- No file sharing
- Firewall
- Security software
- Routine updates
- Careful app selection
- Physical control
- Secure use of public Wi-Fi networks
- Wipe memory prior to discard, sale or re-use of device

FDA Guidance on Mobile Medical Applications September 2013

- FDA may look at apps that:
  - Help patients (i.e., users) self-manage their disease or conditions without providing specific treatment or treatment suggestions;
  - Provide patients with simple tools to organize and track their health information;
  - Provide easy access to information related to patients' health conditions or treatments;
  - Help patients document, show, or communicate potential medical conditions to health care providers;
  - Automate simple tasks for health care providers; or
  - Enable patients or providers to interact with Personal Health Record (PHR) or Electronic Health Record (EHR) systems.

Risk Management Tips

- Don’t talk about specific patients with primary or secondary identifiers
- Talk in general terms about conditions treatment, research
- Don’t post anonymously
- Watch your tone
- If you wouldn’t say it on the elevator, don’t say it online

Risk Management Tips II

- Use separate accounts for personal and professional activity
- Fewer patient details the better
- Remember that PHI posted or sent by the patient is not a HIPAA violation
- Use HIPAA compliant consents and releases for any patient information posted (before and after photos, endorsements, etc.)
- Remote wiping programs

Risk Management Tips III

- Use HIPAA compliant cloud vendors
- Enter into Business Associate Agreements with vendors housing PHI
- Consider use of secure mobile apps:
  - Docbook MD
  - Wickr