AMERICAN COLLEGE OF LEGAL MEDICINE

Physician's Guide to HIPAA Compliance

MOBILE HEALTHCARE DELIVERY PLATFORMS AND DEVICES

ACLM 55th Annual Meeting
The Cosmopolitan of Las Vegas
February 26 – March 1, 2015

Presented by:
Karin M. Zaner, J.D.
Kane, Russell, Coleman & Logan, P.C.
1601 Elm Street, Suite 3700
Dallas, Texas 75201
(214) 777-4203
E-mail: kzaner@krcl.com

KRC&L
ATTORNEYS & COUNSELORS
DALLAS • HOUSTON

GENERAL CONCERNS WITH MOBILE DEVICES

- Mobile devices (iPhones, iPads, Blackberrys, Androids) store and retain data **including ePHI**
  - within the device's onboard memory;
  - within the memory chip or SIM ("smart") card.
- Small and portable (subject to loss and theft).
- May not restrict user access to data through encryption software or authentication features.
- Employer-issued mobile devices may be compliant.
- BUT use of personal devices raises concern.
- How to navigate mobile delivery platforms and devices?

GENERAL HIPAA DEFINITIONS AND CONCEPTS

- See Physician's Guide to HIPAA for basics:
- WHAT IS PROTECTED HEALTH INFORMATION?
- WHAT EXACTLY CAN CONSTITUTE PHI?
- WHO IS A COVERED ENTITY?
- WHO IS A BUSINESS ASSOCIATE?
- WHAT IS A BUSINESS ASSOCIATE AGREEMENT?
- WHAT IS A PHI "BREACH"?

WHAT IS A PHI "BREACH"?

- Any impermissible disclosure of PHI is a breach unless "low probability that PHI was disclosed."
- Common pitfalls with **MOBILE DELIVERY DEVICES**—
- Forwarding to unsecured e-mail addresses such as gmail, hotmail, yahoo (anything that is free is not HIPAA compliant);
- Accessing and viewing PHI (electronic trail remains);
- Disclosing PHI on social media (e.g., Facebook, but also possibly sites like Sermo, Medscape, Quantia MD,).
- Stolen or lost mobile devices.
- Non-HIPAA Compliant texting.

HIPAA CONDUIT EXCEPTION

- Is cell phone texting HIPAA Compliant?
- **Logic for Conduit Exception**– If PHI made it from Point A to Point B and the conduit did not look at substance, then not a PHI breach.
- No breach of PHI if the conduit entity
  - only transmits the encrypted PHI; and
  - never has access to the encryption key.
- Exceptions for entities such as—
  - US Postal Service, Federal Express, UPS;
  - Certain Internet Service Providers (but not gmail, hotmail, yahoo and otherwise "free" accounts);
  - Cell Phone providers generally (but which ones?).
- Does this omit important information from medical record?

MOBILE DEVICES POSE SPECIAL RISK

- Physicians and all covered entities should **strictly observe** certain protocols
- www.healthit.gov/mobiledevices
- For any mobile devices that contain PHI,
- Maintain physical control at all times;
- Use encryption and passwords;
- Installing firewall and remote disabling software;
- Use adequate security when using public Wi-Fi networks;
- Deleting all PHI before discarding any device.
- Sign a "Bring Your Own Device" agreement?

MOBILE DELIVERY DEVICE APPS

- **Closed networks that are specifically HIPAA compliant** (e.g., HIPAA chat)
  - allows physicians, nurses, employees to disclose general patient conditions;
  - solicit input from fellow employed physicians and colleagues;
  - Implemented by a 3rd party and paid for by provider.
- **Third party services that store medical records** ("Universal Health Record" such as NextGen Patient Portal, My Charts by FollowMyHealth--)
  - Obtains and stores online a patient's medical records from a provider;
  - Requires authorization from a patient just like a paper medical record;
  - Keeps records encrypted, de-identified, and individually stored in separate "container" in the "intranet cloud";
  - Patient can access by password and authorize provider access.
  - But are these covered entities/BAs or just conduits?

MOBILE DELIVERY DEVICE APPS, contd.

- **Other physician networks** (such as Sermo and Quantia MD)
  - virtual doctor's lounges, sharing of opinions and advice;
  - who is allowed access?
  - Invites specific details, x-rays, photographs (even facial areas);
  - may violate HIPAA and patient privacy laws;
  - is disclosure of PHI is legal or allowed?
- **Beware of Facebook, Twitter, and Other Open Networks**
  Example– N.J. physician vented details of tough day at ER that revealed details of patient care on Facebook. This allowed 3rd party to identify patient; physician got fired and in trouble with state licensing board.

COMPLIANCE: WHERE DOES A PHYSICIAN START?

- **HIPAA Risk Assessment**—outside vendors can provide;
- **HIPAA Compliance** (Initial and Ongoing)—
  - Appoint a HIPAA Compliance Officer;
  - Storage/destruction of paper and electronic PHI;
  - Data encryption;
  - Facility access and security measures;
  - Employee training within 60 days of hire and again at least once every two years (employees to sign verification of attendance);
  - Mobile device safeguards (passwords, remote wipes, timed lock-outs, wi-fi protection);
  - **And the list goes on. . .**
  - Typically, duties set forth in a Business Associate's Agreement.

WHAT POLICIES SHOULD EXIST?

- Physical office security policies;
- Document retention policies;
- Work station log on and access;
- Network authorization parameters;
- E-mail and calendaring policies;
- Remote access safeguards;
- Protocols for use of mobile devices;
- "Bring Your Own Device" agreements;
- Cloud storage and/or document sharing agreements;
- Portal access agreements;
- Policies for storage, re-use, and disposal of devices.

PENALTIES FOR VIOLATION OF HIPAA

- Criminal penalties only be imposed when there is proof beyond a reasonable doubt that covered entity and/or business associate knowingly, violated HIPAA or any of its regulations.
- Criminal penalties include fines ($100 to $50,000) and/or prison term (1 year to 10 years).
- Civil monetary penalties (a hearing may be requested)
  (1) $100/violation to $50,000 for an unknown violation in spite of due diligence,
  (2) $1,000/violation to $50,000 for a violation due to "reasonable cause," or
  (3) $10,000/violation to $50,000 for a corrected violation due to "willful neglect."
  (4) $50,000/violation for an uncorrected violation due to "willful neglect."
- Court challenge after final HHS Appeals Board decision available.

HIPAA V. STATE LAWS

- HIPAA preempts contrary states laws; **HIPAA is a floor.**
- States can do more– as shown by Texas HB 300 drastically changing the definition of a "covered entity."
- HIPAA does not preempt state laws that relate to privacy and security of PHI.
- Thus, still need to comply with both the federal laws and any state law that offers more protection for health information.
- Government sources for compliance abound– access them!
- For example, Security Rule Guidance– www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html
- **Questions? Comments? Thank you for this opportunity!**