Protected Health Information (PHI)

- PHI is individually identifiable health information
  - Including demographic information
  - That relates to the past, present or future healthcare or payment for healthcare
- HIPAA protects PHI in any form or medium
  - Electronic
  - Paper
  - Oral communication

Protected Health Information (Individual Identifiers)

1. Name
2. Any address specification (street, city, county, zip code, etc.)
3. All dates including birthdate, admission/discharge date, etc.
4. Telephone number
5. Fax number
6. Email address
7. Social security number
8. Medical record number
9. Health plan beneficiary number
10. Account number maintained by healthcare provider
11. Driver’s license number
12. License plate number
13. Medical device identifier/serial number
14. Web address
15. IP address
16. Fingerprints or other biometric identifier
17. Full face photo
18. Any other unique identifying number, characteristic or code
Social Media HIPAA Issues

- Comments about patients, even if you don’t name them
- Pictures of patients posted on social media, without authorization
- Conversations with patients about their care, even in a “private” inbox message
- Business associate relationship
- Breach notification

Social Media Marketing

- Patient Photos/Testimonials = PHI
  - Non-TPO (treatment, payment, operations) uses/disclosures require written authorization
  - Must be HIPAA compliant authorization
  - Be aware of state and other laws for use of an individual’s likeness or statements for marketing purposes
Required Elements for Authorization for Marketing Purposes

- Description of the information to be used or disclosed
- Who will use or disclose the information
- Who the information will be disclosed to
- Description of each purpose of the requested use or disclosure
- The following statements:
  - Individual’s right to revoke the authorization with a description of how to do so
  - Information may be subject to re-disclosure
  - Treatment will not be conditioned on signing the authorization
  - Individual may inspect or copy the PHI to be used or disclosed
  - Individual may refuse to sign the authorization
  - Covered entity will receive payment for the disclosure, if that it is the case
- An expiration date or event
- Signature of the individual and date

Authorization Settlements

Unauthorized Filming for "NY Med" Results in $2.2 Million Settlement with New York Presbyterian Hospital

Today, the Department of Health and Human Services, Office for Civil Rights (OCR), announced that it has reached a $2.2 million settlement with New York Presbyterian Hospital (NYPH) for the inappropriate disclosure of health information (PHI) to an unscrupulous media company. The settlement is the result of an OCR investigation of NY Med, an ABC News television series, which filmed and broadcast unauthorized protected health information (PHI) in the case of a patient with end-stage cancer who was also a patient of a famous New York City doctor. The surveillance footage provided a close-up view of the patient’s medical condition and daily activities, even after a medical professional urged the crew to stop recording.

Physical therapy provider settles violations that it impermissibly disclosed patient information

Complete P.T., a physical therapy practice located in Los Angeles, has agreed to settle violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule with the U.S. Department of Health and Human Services’ Office for Civil Rights (OCR). Complete P.T. is a physical therapy practice located in Los Angeles, California. The settlement agreement is an admission of liability by Complete P.T., requiring payment of $25,000, adoption and implementation of a corrective action plan, and annual reporting of compliance efforts for a year.
AMA Code of Ethics: Social Media

“If they interact with patients on the internet, physicians must maintain appropriate boundaries…”

“To maintain appropriate boundaries physicians should consider separating personal and professional content online.”

Social Media

http://www.huffingtonpost.com/2013/02/06/amy-dunbar-obgyn_n_2630823.html

Reputation Management

AMA Code of Ethics: Reputation Management

“Physicians must recognize that actions online and content posted may negatively affect their reputations among patients and colleagues, they have consequences for their medical careers (particularly for physicians-in-training and medical students) and can undermine public trust in the medical profession.”
Reputation Management

- Don't engage any patient online, take the conversation offline
- Ask the patient to remove the post
- Ask other patients to post good reviews
- Potentially use a professional reputation management service
- If the patient persists, consider legal counsel

Breach Notification

- HITECH Act/Omnibus Rule
  - Breach Notification Requirement
  - Unauthorized access, use or disclosure of PHI considered a Breach unless “a low probability of the information being compromised” is proven

Patient Notification Process

- Written notice no later than 60 days after discovery
- Must be sent by first class mail or email, if requested
Notice to Others

- Less than 500
  - Report annually to HHS
- 500 or more
  - Report to HHS within 60 days
  - Local media

Breaches of 500+ will be investigated by OCR

1656 Breaches
Over 168 million individuals

HIPAA Security Rule

Focus of the Security Rule

- Security Rule only focuses on electronic PHI (e-PHI)
- Protect the confidentiality, integrity, and availability of all e-PHI that is created, received, maintained, or transmitted
- Required Risk Analysis and the establishment of administrative, physical and technical safeguards
Communicating Electronically

- Email/text messaging is not specifically prohibited by HIPAA
- However, HIPAA requires appropriate physical, administrative and technical safeguards for all PHI
- Any device used to store, transmit or receive PHI must be included in Security Risk Analysis (laptops, smartphones, tablets, USB drives, external hard drives)

Email

- Encrypted = secure email
- Beware of free email
  - Typically not “secure”
  - Never use personal email to transmit PHI
- Email provider may be business associate

Patient Request for Unencrypted Email

- Patient may request that PHI be delivered by email
- Must accommodate request, even if encryption is not available
- Patient must be informed that email is not secure and may be accessible by unauthorized individuals, before PHI is emailed to patient
- Sample form available at SVMIC.com

HIPAA Violation Involving Email

- Phoenix Cardiac Surgery
  - Posted over 1,000 entries of PHI on Google calendar (surgery schedule)
  - Emailed PHI to workforce members' personal email
- Patients discovered their information was online and filed complaints with the Office of Civil Rights

OCR Investigation Revealed

- No documented training of workforce (ever)
- Lack of administrative & technical safeguards, no security official, no risk assessment completed
- No business associate agreements with Google

OCR stated in Resolution Agreement...“Covered Entity failed to obtain satisfactory assurances in business associate agreements from the Internet-based calendar and from the Internet-based public email providers that these entities would appropriately safeguard the ePHI received from Covered Entity.”

Final Outcome

Corrective Action Plan
- Implement written policies/procedures for administrative & technical safeguards
- Conduct risk assessment
- Identify business associates and implement agreements
- Train existing & new members of the workforce on policies/procedures
- Pay $100,000 settlement

Email Best Practices

- Include the use of email in Security Risk Analysis
- Consult IT professional to implement encryption
- Educate your workforce on how/when to use encrypted email
- Never use free/personal email for transmitting PHI
- Educate patients and staff on what information is appropriate to relay in an email and how to safely use email as a means of communication
Texting

Are you texting PHI?

Yes

High Risk of HIPAA Liability Issues

No

Probably Okay

SMS Text Messaging

- No authentication (Required by the Security Rule)
  - Is the intended recipient the only one who receives the message?
  - Did you text the right person/number?
- Unauthorized access
  - Does recipient share the same cloud with family members?
  - Does someone else have their phone?

More Texting Issues

- Business Associates
  - Messages stored in the “cloud” may trigger BA relationship
  - HIPAA requires a written agreement with all Business Associates
- Joint Commission’s opinion on texting
Joint Commission Says “No” to Texting Orders

Standards FAQ Details:

Record of Care, Treatment, and Services (RC) (Ambulatory Health Care)

Texting Orders

Is it acceptable for physicians and licensed independent practitioners (and other practitioners allowed to write orders) to text orders for patients to the hospital or other healthcare setting?

No it is not acceptable for physicians or licensed independent practitioners to text orders for patients to the hospital or other healthcare setting. This method provides no ability to verify the identity of the person sending the text and there is no way to keep the original message as validation of what is entered into the medical record.


Joint Commission: UPDATE
April 29, 2016

- Orders may be sent by “Secure text messaging platform” that includes the following:
  - Secure sign-on process
  - Encrypted messaging
  - Delivery and read receipts
  - Date and time stamp
  - Customized message retention time frames
  - Specified contact list for individuals authorized to receive and record orders

- Organizations need to consider documentation of text in electronic health record

http://www.jointcommission.org/assets/1/6/Update_Texting_Orders.pdf

What the OCR Says About Texting

Phoenix Cardiac Surgery-Corrective Action Plan

- Risk management plan must include security measures sufficient to reduce risks and vulnerabilities to ePHI in text messages that are transmitted or stored on portable devices
- Technical measures to protect PHI sent via text message
- Training regarding text messages

Alternatives to Texting

- Patient portal
- Encrypted email
- Secure messaging applications (Search “secure messaging for healthcare”)
Encrypting iPhones

- **iOS 8/9**
  - Go to Settings
  - Touch ID & Passcode
  - Change “Require passcode” option to “Immediately”
  - Disable “Simple Passcode”
  - Use a passcode longer than 6 digits
  - Turn on “Erase Data”

Encrypting Android Devices

To start, users will want to go into settings by tapping the gear-shaped icon in the notification bar, or finding the settings app in your application tray.

- Once you are in settings scroll down to Security, and then add a password, pin, or lock screen security of choice.
- If you did set a pin or password, write it down or remember it. You’ll need this to turn on and use your encrypted and protected device. Otherwise you’ll have to do a factory data reset to use your phone or tablet, which will erase all user data.
- The next step is the important one. You will need your phone to be fully charged, and also plugged in to encrypt the device. This often takes over an hour, so have time set aside to let this complete. If you interrupt the process or unplug your device, you may lose important data.
- Once the process (which can take over an hour) is done, your device will reboot and, if you added a password, you will be asked to enter it to continue using your device. You’ll need the password or PIN every time you use/turn on your phone.
Questions

Loretta Duncan, FACMPE
Senior Medical Practice Consultant
LorettaD@svmic.com
501-864-7454