Use of Social Media by Healthcare Providers:

HIPAA and Other Risk Management Concerns

J. Kevin West

Parsons, Behle & Latimer

OUM

Treated Fairly

Underwritten by a ProAssurance Company

Types of Social Media

- Social networking (Facebook, MySpace, Twitter)
- Professional networking (LinkedIn)
- Media sharing (YouTube, Flickr)
- Content production (blogs & microblogs)
- Knowledge/information aggregation (Wikipedia)

HIPAA: How Did We Get Here?

- Health Insurance Portability and Accountability Act of 1996
- HIPAA Privacy Rule (2003)
- HIPAA Security Rule (2005)
- HITECH Act (2010)

The HIPAA Privacy Rule (2003)

- Extensive rules regarding privacy of patient health information (PHI)
- A “minimum floor” of privacy protections
- New patient rights
- Applies to all health information (oral, paper, electronic)

The HIPAA Security Rule (2005)

- Applies only to electronic health information (ePHI)
- Imposed new standards for protecting, transmitting and maintaining ePHI

The HITECH Act (2010)

- Authorized HHS to issue rules amending HIPAA:
  - ➢ Breach notification
  - ➢ New patient rights
  - ➢ Stricter enforcement

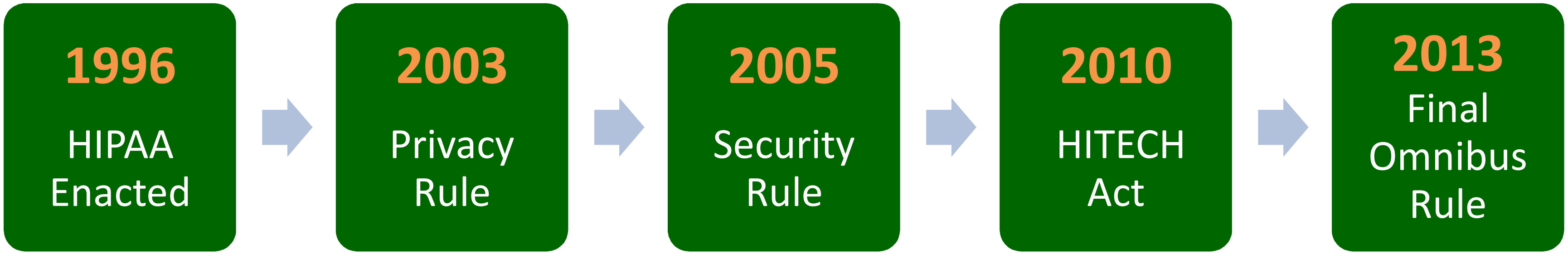
- Rule making process stretched from 2010 to late 2012

Final Omnibus Rule Of 2013

- Implements requirements of the HITECH Act

- Amends HIPAA Privacy and Security Rules

- Compliance required as of 09/23/13



1996
HIPAA Enacted

2003
Privacy Rule

2005
Security Rule

2010
HITECH Act

2013
Final Omnibus Rule

Some Statistics …

67% of physicians use social media in some form

33% of physicians who use social media have received “friend” requests from patients

11% of blogs by healthcare professionals contain product endorsements

Some Statistics …

- In a recent study of 271 medical blogs:

→42% described individual patients

→17% provided sufficient information to identify the patient

HIPAA Basics Re : Social Media

Protected health information (“PHI”):

- “Individually identifiable health information” (i.e., that could be used to identify individual)
- Concerns physical or mental health, health care or payment
- Created or received by covered entity
- Maintained in any form or medium

General Rule for Use and Disclosure
Use and Disclosure Rules

- Cannot use or disclose protected health information unless –
  - There is a valid written authorization (release)

    - OR -
  - Permitted by HIPAA Rules

Requirements of a Valid HIPAA Release

- ✓ Written in plain language
- ✓ Describe info to be disclosed
- ✓ Identify entity authorized to make disclosure
- ✓ Identify entity to whom disclosure made
- ✓ Describe purpose of disclosure
  - "at request of individual" if patient initiates
- ✓ Include expiration date or event
- ✓ Dated and signed by patient or representative
- ✓ State authority of personal representative
- ✓ CMS requires attach document of authority

Seven Types of Permitted Uses/Disclosures of PHI

1. Treatment or payment
2. Serious threat to health/safety
3. Public Health reporting
4. Adult or child abuse
5. Health oversight activities
6. Judicial actions
7. Law enforcement

NOTE: Patients may not be asked to waive their HIPAA rights

HIPAA Concerns Re: Social Media

- Understanding the technology
- Some do’s and don’ts

Understand The Technology

- Social Media
  - An umbrella term that encompasses several different types of technology
  - These different technologies provide combination of media storage, display and communication applications
  - Each one allows a single person to communicate to a broadly identified group
  - Different technologies pose different risks and must be addressed thoughtfully
  - Policies and education should be focused on the communication made, not the brand name

Facebook

- Ubiquitous photo, messaging and mail service
- Technology similar to MySpace, LinkedIn, Sales Force Chatter, etc.
- 1.11 billion users as of May 1, 2013
- Personal information
- Connections by consent
- Updates pushed by “friends”
- Messages – mail, chat, the “Wall”
- “Tagging” photos and locations in other friend’s photos

Facebook (con't)

- Users have a wide variety of privacy functionalities and can maintain a high level of privacy
- Newer or more naïve users may not be aware of privacy functions or risks
- Privacy functionalities are constantly in flux
- User information is stored and controlled centrally. You can choose to share registration information and other information. Your date of birth allows Facebook to show you age appropriate content and advertisements
- User controls cannot override corporate decisions – posted information is "out there" forever
- Posted information can be stored or saved by other users, especially pictures

Facebook (con't)

- Facebook's response to questions regarding control of information:
  - When a person shares information on Facebook, they first need to grant a license to use that information so Facebook can show it to the other people they've asked us to share it with. Without the license, Facebook couldn't help people share the information
  - When information is shared with a friend, two copies of that information is created: one in the person's sent box and the other in their friend's inbox. Even if the account is deactivated, the friend still has a copy of that message
  - Terms have been changed to clarify but not change these issues.
  - Sharing information and also having control of the information so it can be turned off are at odds with each other
  - No system can enable sharing and then simultaneously allow control what services it is shared with

Twitter

- Short bursts of text, links or pictures to thousands, if not millions of “followers”
- As of May 7, 2013, 500 million users on Twitter; 134,000 new users/day
- 58 million tweets/day
- Messages limited to 140 characters (Tweets)
- Tweets are sent through the internet, but may originate from cell phones or text messaging services
- Applications add the ability to share links, re-post others’ “Tweets” and to share photos
- Data is centrally stored and is not user controlled. Private messages may be sent, but default is public

Twitter (con’t)

- Information sent is forever “out there” and may not be recalled.
- Shared photos may be used or sold to another entity (TwitPic).
- Accounts may be faked or hacked and Twitter shares user information with third parties
- FTC brought action to force Twitter to improve its security; settled in 2010
- FTC now has a security form for users to complete if someone believes there is a breach
- Twitter also has volunteer security researchers to look for security issues.

Blogs

- A discussion or informational site published on the World Wide Web consisting of discrete entries (posts)
- Web logs or “blogs” allow users to post an online multi-media journal on a specific topic or topics of general interest
- A majority are interactive allowing visitors to leave comments and message each other
- Considered social networking
- May be operated on a personal website or blog hosting site
- Content is almost always public
- Hosted content is subject to hosting companies terms of use, may not be entirely controlled by poster
- Greater control, but is still subject to copying and storage
- Blogs may be hacked or faked

Text Messaging

- Also known as “texting”
- Act of typing and sending a short message between two or more mobile phones over a phone network
- Inherently insecure
- Texts are generally stored on a central server of the cellular provider (or more than one) as well as on both the sending and receiving devices
- Also referred to as Short Message Service or SMS.

Social Media Summary

- Social Platforms were created to help people connect with one another, broadcast their ideas, and create stores of personal information online
- Services like Facebook, Twitter, YouTube were built for sharing public information, not for confidential information

Six Do's & Don'ts

First, don't discuss patients in a way that might identify them

Six Do’s & Don’ts

Second, don’t “friend” patients

Six Do’s & Don’ts

Third, don’t post patient testimonials, pictures, etc. without a proper HIPAA release

Six Do’s & Don’ts

Fourth, don’t respond to patient complaints, or comments online

Six Do’s & Don’ts

Fifth, do promote your practice and your services without violating patient privacy

Six Do’s & Don’ts

Sixth, do adopt a written social media policy for your office/staff

- Limits on who speaks for the Practice
- Guidelines as to content of postings
- Prohibitions against discrimination
- Disciplinary action for failure to adhere

Top Ten Risk Management Concerns with Social Media

1. Lack of professionalism in social media content and tone

   - Posing with weapons or alcohol
   - Use of discriminatory language
   - Sexually suggestive images/photos
   - Taking photos/videos of medical procedures

Top Ten Risk Management Concerns with Social Media

2. Blurring of boundaries between doctor and patient

- "Friending" patients
- Inappropriately intimate conversations, posts, etc…

Top Ten Risk Management Concerns with Social Media

3. Failure to maintain a separate professional and private persona online

- Often difficult to segregate one’s personal and professional activities

Top Ten Risk Management Concerns with Social Media

4. Creating a “shadow medical record” online

  - Interactions with patients or comments about their care can be used as evidence
  - Difficulty in keeping online interactions as part of the “chart”

Top Ten Risk Management Concerns with Social Media

5. Responding online to patient complaints and comments about your Medicare care

- See HIPAA concerns
- See item #1 above
- See item #4 above
- May result in licensure board discipline

Top Ten Risk Management Concerns with Social Media

6. Unauthorized practice of medicine

    - Interacting with patients living in other states
    - Use caution in responding to patient-specific questions

Top Ten Risk Management Concerns with Social Media

7. Misrepresentation of credentials, false advertising and scope of practice issues

- Common for your competitors to report you to licensure boards
- Common for licensure boards to identify issues
- Use care with claims of the efficacy of treatment, your qualifications, etc…

Top Ten Risk Management Concerns with Social Media

8. Conflicts of interest in promoting products and services (i.e., without disclosing compensation)

Top Ten Risk Management Concerns with Social Media

9. Looking up information about patients online

    - Could be viewed as a boundary violation

Top Ten Risk Management Concerns with Social Media

10. Don’t post it if you would not want to see it in the newspaper

Remember

- Social Platforms are created to help people connect with each other, broadcast their ideas, and create stores of personal information online.
- Services like Facebook, Twitter and YouTube were built for sharing, not for confidential or private matters.