Dealing with the Use of Social Networking and Communications Vehicles in the Healthcare Environment: Twitter, Facebook, MySpace, IM and P-2-P

Chris Apgar, CISSP
President, Apgar & Associates, LLC

Overview

- Social Networking Review
- Use and Risks
- New Legal Consequences – HITECH Act, Red Flag Rule & Legal Risk
- What Individuals May do With Their PHI
- Reasonable Steps to Protect Against Privacy & Security Breaches
- Summary and Discussion

Social Networking Review

- Social networking is ever expanding for personal and business purposes
- Vast amounts of data are transmitted relating to the convenience of new “instant” data sharing tools
- Social networking tools and related communication vehicles now represents one of the more significant risks to privacy and security of health information

Social Networking Review

- What are those new (and sometimes old) communication tools?
  - Smartphone and mobile phone text messaging
  - Smartphone based e-mail messaging
  - Instant messaging
  - Web mail
  - Twitter
  - Facebook
  - MySpace
  - Skype
  - Go To Meeting and WebEx

Social Networking Review

- All of these communication vehicles are generally unencrypted and subject to interception by the wrong person
- Not all are necessarily a significant threat to inappropriate release of PHI or other confidential information
- It is time to ask the question – How are these tool currently being used by workforce members for both business and on-the-job personal use

Use and Risks

- The Center for Medicare and Medicaid Services (CMS) recently announced as part of their security audit process that all PHI sent over the Internet must be encrypted
- Most social networking or quick communication tools do not meet this requirement
- If unencrypted and used for business, organizations are exposed to potential interception of unencrypted PHI and privacy/security breaches

Use and Risks

- The use of Web mail poses a different type of threat:
  - Emailing PHI to unauthorized individuals
  - Theft of PHI
  - Emailing confidential or proprietary data to an individual or even to one's personal Web email account
- All data or messages sent via Web mail while at work becomes personal property and the organization has no way to audit or access what is sent

Use and Risks

- Text messaging is commonly used in many organizations and is seen as a tool to improve communication and share needed information quickly
- Text messaging is usually not encrypted unless sent between two workforce members using, say, an organization's mobile carrier who can provide a secure environment for calls and texting

Use and Risks

- If workforce members use their own smart or mobile phones and their own carriers, the organization has little control over what is communicated and the security of that communication
- Even if using an organization designated secure mobile carrier and organization owned smart or mobile phones, text messages are often sent to colleagues and others with different carriers meaning the text is no longer secure

Use and Risks

- Twitter, like text messaging represents an unsecure form of instant communication
- It may be popular but even short messages including PHI can be intercepted
- Twitter has become the new fad for instant communication and opens the door to inappropriate release of PHI
- Organizations generally cannot monitor what is sent or received via Twitter – like web mail, there is no audit trail to find out about inappropriate use

Use and Risks

- Facebook and MySpace users are no longer primarily high school, college age and young adults
- Especially Facebook is more and more becoming a significant international social networking tool for adults over the age of 50
- The potential that PHI or other confidential information may be posted from a worksite is increasing

Use and Risks

- Even mobile to mobile calls represent a potential risk if not handled appropriately
- Example: A surgeon is at a conference and contacts her office to discuss an upcoming surgical procedure via mobile phone. The surgeon makes the call in the hotel coffee shop which is crowded. Even though what others would overhear is one sided, the chance for inappropriate disclosure of the patient's PHI is high.

Use and Risks

- Mobile wireless or wireless hot spot use can also result in inappropriate disclosure of PHI
- If the wireless network is not secured and data is transmitted across an open network unsecured, it can be intercepted
- Also, if login to the organization's electronic health record, as an example, occurs in a public place social engineering (often called "shoulder surfing") represents risk of inappropriate disclosure

New Legal Consequences – HITECH Act, Red Flag Rule & Legal Risk

- The HITECH Act was made a part of the American Recovery and Reinvestment Act (ARRA) and included significant privacy and security requirement changes
- Inappropriate disclosure due to intercepted text messages, instant messaging, use of Twitter, etc. would be considered a breach
- A breach would require notification of the patient or health plan member, reporting to the Office for Civil Rights (OCR), etc.

New Legal Consequences – HITECH Act, Red Flag Rule & Legal Risk

- The HITECH Act included a significant increase in the amount of civil penalties that may be levied for violations such as sending PHI unencrypted over the Internet
- The US Department of Health and Human Services (HHS; likely through OCR) can choose to levy fines up to $50,000 per violation with a maximum fine of $1.5 million per calendar year for the same type of violation

New Legal Consequences – HITECH Act, Red Flag Rule & Legal Risk

- Civil penalty amounts that can be levied per violation were tiered with higher violations related to willful neglect BUT…
- The HITECH Act allowed levying higher tier penalties for all violations, no matter the cause and whether or not related to willful neglect
- State attorney generals were given the power to pursue violations in US District Court

New Legal Consequences – HITECH Act, Red Flag Rule & Legal Risk

- A formal audit program is now required of HHS which means there will be a higher likelihood privacy compliance audits will occur beginning 2Q 2010 (security compliance audits are already occurring)
- Also, if willful neglect is suspected, HHS must investigate

New Legal Consequences – HITECH Act, Red Flag Rule & Legal Risk

- All enforcement activity related to the HIPAA Security and Privacy Rules now belongs to OCR
- CMS recently announced encryption is mandatory even though the Security Rule lists encryption as an addressable implementation specification
- What must be encrypted doesn't just relate to the exchange of email that includes PHI

New Legal Consequences – HITECH Act, Red Flag Rule & Legal Risk

- CMS also announced over a year ago when the CMS HIPAA Security Rule compliance program was launched one of the key audit criteria would be whether or not the covered entity (and now business associate) adhered to CMS' published remote access guidelines
- This would cover remote access from the infamous coffee shop, mobile phone conversations in the wrong places, use of Twitter from a smart phone, etc.

New Legal Consequences – HITECH Act, Red Flag Rule & Legal Risk

- The Red Flag Rule was effective August 1, 2009 (not enforced for the healthcare industry until November 1, 2009)
- The new rule, enforced by the Federal Trade Commission (FTC), requires "creditors" (many health care providers) to implement identity and medical identity theft protection programs
- This would include paying attention to those new social networking tools and sending PHI unencrypted

New Legal Consequences – HITECH Act, Red Flag Rule & Legal Risk

- In addition to increased penalties, increased likelihood of audits and new announced security requirements, inappropriate disclosure of PHI can and has led to very expensive law suits
- While HIPAA provides no private right of action, it does not prevent civil suits where individuals claim damages due to inappropriate disclosure or breach of their PHI

New Legal Consequences – HITECH Act, Red Flag Rule & Legal Risk

- Other risks related to new networking tools and inappropriate disclosure include:
  - Damage to reputation
  - Unfriendly headlines
  - Increased likelihood of audit (CMS audits were based on complaints and headlines)
  - Loss of business related to patient or health plan member lack of trust

What Individuals May do With Their PHI

- Facebook and MySpace have been used to post personal health information about individuals with Facebook and MySpace accounts (often posted by the individual who the information relates to)
- If an individual is provided an electronic copy of his or her medical or claims record and the individual posts information from the record on Facebook or MySpace, that lies outside the area of covered entity and business associate responsibility

What Individuals May do With Their PHI

- While in the care of covered entities and business associates, PHI must be protected but once released to a third party (as long as appropriate authentication has occurred), any further release and privacy protection is the responsibility of the third party
- A covered entity or business associate cannot prevent an individual from posting even his or her whole medical record on Facebook or MySpace

What Individuals May do With Their PHI

- Even if the individual indicated he or she intended to post parts or all of the record on the Web, the covered entity cannot refuse to provide the individual a copy of his or her medical or claims record
- On the other hand, the covered entity would not be responsible if the individual elected to do so and damages occurred related to the posting

What Individuals May do With Their PHI

- As with financial transactions, consumers are moving more towards convenience versus strict privacy controls (this does not mean privacy concerns will quickly go away)
- This means consumers are more willing to:
  - Text their doctor and include PHI
  - Send unencrypted e-mail messages to their provider or health plan
  - Review their medical or claims information from an Internet café
  - Post health information on the Web

What Individuals May do With Their PHI

- Covered entities cannot force consumers to use secure methods of communication but covered entities must not use non-secure methods when responding to patients or health plan members
- Covered entities cannot ask an individual to sign a waiver accepting the risk of sending unencrypted PHI over the Internet
- This relates to the Privacy Rule prohibition against requiring individuals waive any of their privacy rights

Reasonable Steps to Protect Against Privacy & Security Breaches

- Documentation and formal policies are a must
- Also, training on and enforcement of those policies are required
- A risk analysis should be conducted at least annually or when any major business or systems changes occur and this should include evaluating the use of text messaging, Twitter, remote access, etc.

Reasonable Steps to Protect Against Privacy & Security Breaches

- Where feasible, organizations should require workforce members use company owned laptops, smartphones and mobile phones to be used for business or clinical purposes
- Search for a mobile provider who offers an encrypted mobile network (keeping in mind this will not protect PHI sent to smart and mobile phones outside that carrier's secure network)

Reasonable Steps to Protect Against Privacy & Security Breaches

- Prohibit/block the use of Web mail and access to social networking sites
- Implement a related policy and require remote users and smartphone users to adhere to the policy (often difficult to enforce)
- Monitor Internet use and sites visited where PHI could be disclosed and block as necessary

Reasonable Steps to Protect Against Privacy & Security Breaches

- Prohibit the use of text messaging or at least evaluate the risk associated with the use of text messaging
- If text messaging is allowed for business purposes, documenting the risk was evaluated and accepted is required
- Follow the same process for determining if the use of Twitter will be allowed
- Require the use of encrypted transmission for all forms of electronic PHI (email, FTP, etc.)

Reasonable Steps to Protect Against Privacy & Security Breaches

- Encrypt laptop hard drives (company owned) and require encryption of hard drives or folders used to store PHI if personal portable device use for business purposes is allowed
- Evaluate the risk of allowing workforce members to access non-secure wireless networks when remotely accessing the organization's network, applications, email, etc.

Reasonable Steps to Protect Against Privacy & Security Breaches

- Access may be through an encrypted web site but that doesn't necessarily prevent laptop hijacking or external access to the remote device
- If the risk is considered acceptable, document
- Reasonably ensure anti-malware software is kept up to date and regularly run
- This can be set up as part of the configuration of company owned devices but may be difficult to enforce if personal devices are used

Reasonable Steps to Protect Against Privacy & Security Breaches

- Implement and require the use of a virtual private network (VPN) if feasible for all remote access
- Require workforce members use portable devices appropriately and only in secure locations
- Implement appropriate controls related to portable media
- Encrypt portable media where feasible

Reasonable Steps to Protect Against Privacy & Security Breaches

- Use of GoToMeeting and WebEx should not be used when PHI will be disclosed such as with internal staff training that requires the use of PHI for training purposes or for consultation purposes
- If GoToMeeting, WebEx or a related on-line meeting tool is used and PHI is exchanged, upgrade (at a cost) to encrypted meeting sessions

Summary

- The brave new world of instant and international Web based communication and data sharing poses significant challenges to the healthcare industry
- New legal requirements increase risk to covered entities and business associates who do not pay attention to these new challenges
- The consumer will often not follow proper privacy/security practices
- Be prepared, implement controls and document

Question & Answer

Chris Apgar, CISSP
President

10730 Southwest 62nd Place | Portland, Oregon 97219
503-977-9432 | 503-245-2626 Fax | www.ApgarAndAssoc.com