Duke Medicine

Social Media Policy

Tina R. Tyson, JD
Chief Compliance Officer
Duke University School of Medicine

March 2012
Agenda

- Social Media Policy
- Context - HITECH – new HIPAA requirements
Social Media Policy

• **Effective: March 22, 2012**

• Helps workforce understand appropriate ways to use communication technologies and to communicate on social media sites

• Applies to communications potentially viewable by the public when individuals are representing themselves as Duke workforce members
Take Aways

• No Duke email addresses used for social media unless it is a Duke social media site.
• No Duke Medicine equipment used to access or participate in social media sites for personal use.
• At discretion of department manager, a departmental computer may be designated to permit the workforce to access social media sites during non-work time.
• Use of personal devices to access social media for personal use may be used during non-work time outside public view.
• Duty to report if you see inappropriate information posted on social media sites.
Take Aways, cont.

• On personal social media sites, if an individual identifies themselves as a Duke workforce member:
  – Must maintain PROFESSIONALISM
  – No friending Duke research subjects or patients with whom you developed a relationship when person was patient or subject at Duke.
  – DO NOT post pictures of Duke patients or research subjects
  – If a patient or subject has taken a picture of you, remove the tags on the pictures so these do not show up on your page.
  – Do not discuss job responsibilities or specific activities that include Protected Health Information (PHI).
  – Do not discuss or share confidential or proprietary business information:
    • Research Protocol
    • Contracts
    • Financial information
    • Data
    • Employee/student information
  – Penalties up to and including termination
Frequently Asked Questions

- **What constitutes “Professional” for this purpose?**
  - Represent yourself as a professional, competent employee of Duke Medicine. Do not state anything disrespectful to fellow employees, faculty, supervisors, vendors, or competitors.
  - Be truthful
  - Avoid anger, sarcasm, criticism and any language that could be offensive, discriminatory, or defamatory.
  - No negative comments about groups of research subjects, patients, employees, etc.
Frequently Asked Questions, cont.

• **Ask yourself:**
  – Does it diminish my role as a Duke workforce member?
  – Would it reflect negatively on co-workers, colleagues, (comments on short staffing, etc.)?
  – Does it conflict with our culture, vision or values?
  – Would it reveal PHI?
  – Could it directly or indirectly identify a patient?
  – Would it place the individual or institution at risk?

Examples:
  • Joint Commission is here, I hope they do not come to my Unit.
  • FDA is here doing an audit. I hope they never come to look at my protocol.
Frequently Asked Questions, cont.

• If you already have a “Friend” that would violate the new policy, defriend and send them an encrypted email message explaining that you cannot friend patients or subjects.

• On a friend’s page, you cannot ask how a Duke patient is doing even if that person is someone with whom you had a previous relationship outside of Duke because you could be viewed as eliciting them to reveal PHI.
Regulatory Context? HITECH (Health Information Technology for Economic and Clinical Health Act 2009)

- Extends the reach of HIPAA & the Privacy & Security Rules
- Imposes breach notification requirements on HIPAA covered entities and business associates
- Limits certain uses & disclosures
- Increases individual’s rights re: PHI
- Increases enforcement and penalties
Expanded definition of PHI

• Under this policy, PHI includes:
  – Individually identifiable health information in any form (paper, oral, electronic) that is transmitted and/or stored that relates to the past, present or future health of an individual, the provision of health care, or payment for health care that is linked to a patient; and
  – Identifying or personal information, including any name or number that may be used in conjunction with any other information to identify a specific person, such as social security number, credit card number(s), or passwords.
What happens if there has been a breach?

- When an individual commits, observes, or becomes aware of an unauthorized or inappropriate access, use, or disclosure of protected health information, s/he is responsible for *promptly* reporting the potential breach. This report can be addressed to:
  - Immediate supervisor
  - Manager or department head
  - SOM Compliance Office
  - DUHS Compliance Office
  - Human Resources
  - Integrity Line 1-800-826-8109
When do I report?

• As soon as possible.
  – HHS has placed timeframes on reporting. The notification (to HHS) of a breach should be “without reasonable delay and in no case later than 60 calendar days after the discovery of the breach” [ARRA at § 13402(d)(1)]
  – A breach is deemed to be discovered as of the first day that the breach is known, or reasonably should have been known.
What will happen?

- Compliance Office, in collaboration with department manager and HR, will lead investigation

- Investigation may include:
  - Auditing user access (eBrowser, NetAccess, Meditech, IDX, WellSoft, etc.)
  - Interviewing staff
  - Reviewing telephone logs
Outcome

• If the breach is substantiated, Compliance Office will
  – Review the findings with the department Business Manager and/or Chair
  – Review the findings with HR
  – Collaborate with the department Business Manager and/or Chair and HR to determine the plan for corrective action
Level 1: Carelessness

- Discussing patient information or leaving a copy of patient information in a public area;
- Leaving a computer screen open and unattended
- Faxing PHI to the wrong fax number
- Emailing PHI to a wrong email address

- 1st offense: documented counseling session
- 2nd offense: final written warning
- 3rd offense: termination of employment, ineligible for rehire
Level 2: Reckless Disregard

- Sharing user ID and/or password with other staff or permitting another to access PHI through one’s computer or access
- Inappropriate disposal of PHI, e.g., failure to shred labels or records
- Sending electronic communication without encryption or saving unencrypted PHI on a portable device
- Removing PHI from DHE premises for other than provision of clinical care
- Permitting unauthorized third party to use a Duke computer or system
- Releasing PHI to a third party without proper verification of the person’s identification

- 1st offense: written warning
- 2nd offense: final written warning & 2 week unpaid suspension
- 3rd offense: termination of employment, ineligible for rehire
Level 3: Willful Disregard

- **Posting or participating in communication containing PHI on social networking/open source sites**
- Accessing another’s PHI outside the workforce member’s area of responsibility
- Sharing PHI with the media without authorization from the patient
- Sharing PHI obtained from a third party that is not necessarily a workforce member’s responsibility

- **1st offense**: final written warning & 2 week unpaid suspension
- **2nd offense**: termination of employment, ineligible for rehire
Level 4: Willful Disregard with Malicious Behavior

- Inappropriately and repeatedly accessing, using, or disclosing individual screen(s) or information from individual or multiple patient records
- Disclosing PHI for personal gain
- Theft or sale of PHI
- Disclosing PHI to cause harm to patient or any third party

**1st offense:** termination of employment, ineligible for rehire
Resources

• The breach policy is located on the Intranet [http://staff.dukehealth.org](http://staff.dukehealth.org) in the Policy Manual at

• DUH disclosure database
  – [https://clinapp1.duhs.duke.edu:8081/PHIDisclosureTracking/Login.asp](https://clinapp1.duhs.duke.edu:8081/PHIDisclosureTracking/Login.asp)

• HIPAA website

• SOM Compliance Office website
Questions?