Social Media and Healthcare
Legal Considerations

Mia Havel, JD
Associate
Norton, Rose, Fulbright

October 20, 2017

Legal Perspective

- Organizational vs. personal use of social media
  - Your organization must consider both!

2

Legal and Compliance Risks

- Patient privacy violations
  - HIPAA/state privacy laws
- Written authorization or de-identification
- Lawsuits
  - Invasion of privacy
  - Malpractice,
  - Negligence,
  - Breach of duty of care/confidentiality,
  - Defamation,
  - False advertising

3

Legal and Compliance Risks (continued)

- Licensing Issues
- HIPAA marketing restrictions
- Recordkeeping/security violations
- Employee privacy issues
  - NLRB
  - Privacy rights
  - Wrongful termination

4

Examples/Anecdotes

- Lawsuits
- Regulatory Investigations
- Licensing issues
- Other

5

Social Media and Marketing in Healthcare
Privacy Considerations

Alan Fong, JD, CHPC
Privacy Officer
Corporate Responsibility Program,
Catholic Health Initiatives

October 20, 2017

Social Media and HIPAA

- While social media offers a new format and medium for sharing information, ultimately, we must look to well established and familiar principles when analyzing potential privacy issues
- All workforce members should make every effort to treat their social media communications with the same care and professionalism as if they were face to face encounters

7

Social Media Policy

- Entities should:
  - **Adopt** a social media policy for your organization and workforce
  - **Communicate/educate** your staff on the policy and its requirements
  - **Enforce** the policy's requirements if/when there are violations
- <u>If you haven't already done so, develop a policy now and don't wait until after a crisis</u>

8

Effective Social Media and Marketing Policies

- Define the permissible scope of workforce members' use of social media
- Identify authority to speak on the entity's behalf
- Specify rules for use and as well as content that would violate compliance requirements or your entities' policies
- Prohibit the posting of any content that contains patient details or identifying information without the patient's written authorization. Clearly define what must be included in a valid authorization
- Establish a review process prior to posting
- Make sure your opt-out processes are clear and accessible

9

Reducing Risk

- In addition to implementing a social media policy, consider what other steps your entity can take to reduce risk
  - Establish clear lines of communication with stakeholders
  - Create a social media working group to discuss your entity's social media strategy and review relevant issues/concerns. Make sure to include your legal/privacy/security representatives
  - Provide and document a thorough, role-based training program on federal and state patient privacy regulations for your marketing staff, including examples of what not to do

10

Reducing Risk (continued)

- Define your marketing goals and ensure your social media programs are narrowly tailored to meet those goals
- Develop a robust content review and approval process prior to posting
- Supplement monitoring efforts with technological controls
- Have staff members sign confidentiality agreements and maintain a copy of the agreement in the employee's personnel file
- Develop metrics to measure program effectiveness

11

Social Media and New Vendors

- Ask whether your social media strategy is right for your industry and organization. Do the anticipated benefits justify the compliance risks?
- Ensure your legal, compliance and security representatives have a seat at the table when your organization is developing its social media plan and engaging new vendors
- Know your audience and familiarize yourself with your tools
- Take the time to conduct appropriate due diligence prior to onboarding (risk assessments, contracts, etc.)

12

Social Media and New Vendors

- Ask how the vendor plans using your data once it is in their environment (e.g. research, data mining, de-identification and repurposing, etc.)?
- Make sure your leadership team understands the resources necessary to ensure your marketing initiatives are appropriately staffed and have adequate oversight
- Track, measure and document

13

Social Media Information Security Considerations

Ram Ramadoss, MBA, CISA, CISM, CISSP, CRISC, CIPP
Vice President, Privacy, Information Security and EHR Oversight,
Corporate Responsibility Program,
Catholic Health Initiatives

October 20, 2017

Agenda

- What is considered as Social Media?
- Changing Landscape of Healthcare Organizations
- Key security threats and risks
- Mitigation controls

15

What is considered as Social Media?

16

Changing Landscape of Healthcare Organizations

- Increased number of contractors, consultants and voluntary workers
- Partnership and outsourcing activities
  - Technology companies
  - Companies based in off-shore locations
  - Sub-Contractors to your business associates
- Employee and patient level communications
- Millennials expect to have access to Social Media sites at work

17

Changing Landscape of Healthcare Organizations (contd…)

- Physicians like to access, download/upload ePHI to cloud storage sites (e.g. GoogleDocs, DropBox, Box)
- Employees could be accessing these social media sites using company computers/network, company issued mobile devices, personal computers and outside corporate network
- Productivity and network bandwidth issues – corporate network
- Using same passwords for personal and corporate use

18

Key Security Threats and Risks

- Reconnaissance
  - Hackers harvest information from social media sites
- Confidential Data Leakage (intentional & unintentional)
- Exploiting Trust and Connectivity
  - Fraudulent websites and/or malicious attachments
- Permanence and Persistency of data
- Representation and Authenticity of data

19

Key Security Threats and Risks (contd…)

- Exposure of your security controls
- Disgruntled employees/contractors
- Data Ownership
- Challenges with Forensic Investigations
- Social Media as an Investigative Tool
- Lack of visibility to social media sites outside USA

20

Common Social Media Malware/Attacks

- Low guard when using social media sites
- Spear Phishing
- Social Engineering
- Password Attacks
- Malicious Codes/Sites
- Click Jacking
- Obfuscated Links (Shortened URLs)

21

Mitigation Controls

- Strategy and Governance
  - Risk Assessment
  - Policies
- People
  - Education/Awareness to all users
  - Customers/Patients
- Process
  - Alignment with business processes
  - Change controls
- Technology
  - Technical controls (prevent/monitor browsing, download and logging)

22

Mitigation Controls (contd…)

- Acceptable Use Policies (AUP)
- Security Awareness and Training
  - Phishing Campaigns to test employee awareness
  - Social Media privacy settings
- Sanctioning of individuals violating the policy
- Exit interviews
- Application aware proxy servers and next generation firewalls
  - Web content filtering on your network
- Employee behavior monitoring
- Social Media Monitoring Tools

23

Mitigation Controls (contd…)

- Leverage Healthcare Threat Feeds/Sources
  - Pro-actively block IP addresses and domain names that control Botnets
  - Accelerate detection and containment of security incidents
- Processes and mechanisms to remove negative/offensive content
- Upfront engagement of information security team
  - Partnership with Marketing, Communications and Human Resources

24