

HIPAA and Social Media

Best Practices for Hospitals

July 21, 2015

Presented by:

Stacy Harper, JD, MHSA, CPC

for



Disclaimer

The information provided is for educational purposes only and is not intended to be considered legal advice or create an attorney-client relationship.

Opinions expressed are those of the speaker and do not represent the opinions or position of Kansas Hospital Association, the Kansas Association of Health Care Communicators or Lathrop & Gage LLP.

Agenda

- An overview of the HIPAA privacy rule;
- Identifying risks and compliance obligations associated with social media;
- Analyze specific case examples sent in by Kansas hospitals; and
- Discuss options available to leverage the social media opportunity.

Statutory Background

- **Health Insurance Portability and Accountability Act of 1996** (Administrative Simplification Provisions) – August 21, 1996
- **Health Information Technology for Economic and Clinical Health Act of 2009** – February 17, 2009

Regulatory Background

- **HIPAA Electronic Transaction Standards** – August 17, 2000
- **HIPAA Privacy Standards** – December 28, 2000 & August 14, 2002
- **HIPAA Unique Employer Identifier Standard** – May 31, 2002
- **HIPAA Security Standards** – February 20, 2003
- **HIPAA/HITECH Breach Notification Standards** – August 24, 2009
- **Omnibus HIPAA Regulatory Modifications** – January 25, 2013

Basic Structure of HIPAA

HIPAA Privacy

- Applies to all protected health information
- Determines when PHI can be used/disclosed
- Minimal Safeguard Requirements
- Provides Patients Rights to Information

HIPAA Security

- Applies to electronic protected health information
- Additional layers of safeguards for ePHI

HIPAA Breach Notification

- Spans Privacy and Security
- Adds transparency to the process

If state law differs from HIPAA, the more restrictive law applies

Enforcement

	Tier 1	Tier 2	Tier 3	Tier 4
	Violation not known or reasonably known	Violation due to reasonable cause, but not willful neglect	Violation due to willful neglect, if corrected	Violation due to willful neglect, if not corrected
Old HIPAA	None	\$100 per violation, \$25,000 max for identical violations in calendar year	\$100 per violation, \$25,000 max for identical violations in calendar year	\$100 per violation, \$25,000 max for identical violations in calendar year
New HIPAA	At least \$100 per violation, \$1.5 million max for identical violations in calendar year	At least \$1,000 per violation, \$1.5 million max for identical violations in calendar year	At least \$10,000 per violation, \$1.5 million max for identical violations in calendar year	At least \$50,000 per violation, \$1.5 million max for identical violations in calendar year

HIPAA Provisions Implicated by Social Media

Protected Health Information

- Individually identifiable health information that is transmitted in electronic media, maintained in electronic media, or transmitted or maintained in any other form, but not including education records covered by FERPA, certain higher education records, employment records held by a covered entity in its role as employer, and regarding a person who has been deceased more than 50 years.
- Health information means any information, including genetic information, that is created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school or university, or healthcare clearinghouse and relates to past, present, or future physical or mental health or condition of an individual, provision of health care, or past, present or future payment for the provision of health care
- Individually identifiable means information that identifies an individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual

HIPAA Provisions Implicated by Social Media

De-Identification

Performed by consultant or remove:

- Names;
- All geographic subdivisions smaller than a State,
- All elements of dates (except year) for dates directly related to an individual;
- Telephone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints;
- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic, or code

HIPAA Provisions Implicated by Social Media

The Basic Rule:

You must have written authorization of the individual prior to using or disclosing PHI for:

- Marketing
- Sale of PHI
- Psychotherapy Notes
- Any use or disclosure not specifically permitted under HIPAA

HIPAA Provisions Implicated by Social Media

Marketing:

- Except as provided below, marketing means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service.
- Marketing does not include a communication made:
 - To provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, only if any financial remuneration received by the covered entity in exchange for making the communication is reasonably related to the covered entity's cost of making the communication.
 - Financial remuneration means direct or indirect payment from or on behalf of a third party whose product or service is being described. Direct or indirect payment does not include any payment for treatment of an individual.

HIPAA Provisions Implicated by Social Media

- Marketing exceptions, continued
 - For the following treatment and health care operations purposes, except where the covered entity receives financial remuneration in exchange for making the communication: (A) For treatment of an individual by a health care provider, including case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual;(B) To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits; or (C) For case management or care coordination, contacting of individuals with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment.

HIPAA Provisions Implicated by Social Media

Authorization Core Element Requirements

- A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion.
- The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure.
- The name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure.
- A description of each purpose of the requested use or disclosure. The statement “at the request of the individual” is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose.
- An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. The statement “end of the research study,” “none,” or similar language is sufficient if the authorization is for a use or disclosure of protected health information for research, including for the creation and maintenance of a research database or research repository.
- Signature of the individual and date. If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must also be provided.

HIPAA Provisions Implicated by Social Media

Authorization Required Statements:

- The individual's right to revoke the authorization in writing, and either:
 - The exceptions to the right to revoke and a description of how the individual may revoke the authorization; or
 - To the extent that the information in paragraph (c)(2)(i)(A) of this section is included in the notice required by § 164.520, a reference to the covered entity's notice.
- The ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization, by stating either:
 - The covered entity may not condition treatment, payment, enrollment or eligibility for benefits on whether the individual signs the authorization when the prohibition on conditioning of authorizations in paragraph (b)(4) of this section applies; or
 - The consequences to the individual of a refusal to sign the authorization when, in accordance with paragraph (b)(4) of this section, the covered entity can condition treatment, enrollment in the health plan, or eligibility for benefits on failure to obtain such authorization.
- The potential for information disclosed pursuant to the authorization to be subject to re-disclosure by the recipient and no longer be protected by this subpart.
- If third party payment is involved, the amount of payment

Resources

Online at www.kha-net.org, click on communications, social media

- Template Consent Form
- Sample Social Networking Policy
- A Hospital Leadership Guide to Digital and Social Media – AHA
- #kansashospitals



Stacy Harper

Lathrop & Gage LLP

sharper@lathropgage.com

913-451-5125

