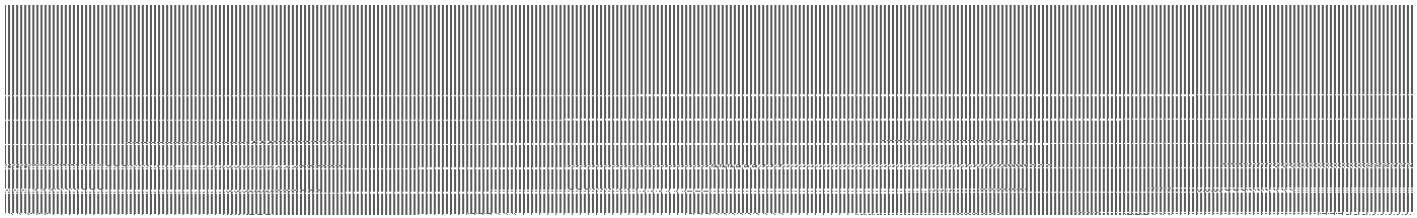
HIPAA and Son of HIPAA: Rain on Your Parade

HealthCamp Boston
April 21, 2009

David Harlow JD MPH
THE HARLOW GROUP LLC

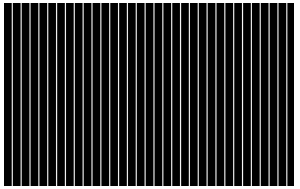


HIPAA and Son of HIPAA Meet Social Media in Health Care

- The promise of interoperable patient-centered health records, and social media . . .
- And the potential collision with “new and improved” HIPAA and related privacy rules in the HITECH Act

HITECH Act rules

- Layered on top of existing HIPAA privacy and security rules we have:
- Security breach notification requirement
  - FTC rule published last week
- Make it indecipherable requirement
  - HHS guidance published last week
    - If it's indecipherable, release is not a breach
  - Open Q: Is a fingerprint -locked flash drive secure?



PHR privacy regulated by FTC

SEC. 13407. TEMPORARY BREACH NOTIFICATION REQUIREMENT FOR VENDORS OF PERSONAL HEALTH RECORDS AND OTHER NON -HIPAA COVERED ENTITIES.

(a) In General- In accordance with subsection (c), each vendor of personal health records, following the discovery of a breach of security of unsecured PHR identifiable health information that is in a personal health record maintained or offered by such vendor, and each entity described in clause (ii), (iii), or (iv) of section 13424(b)(1)(A),** following the discovery of a breach of security of such information that is obtained through a product or service provided by such entity, shall--

(1) notify each individual who is a citizen or resident of the United States whose unsecured PHR identifiable health information was acquired by an unauthorized person as a result of such a breach of security; and

(2) notify the Federal Trade Commission.

. . . .

** (ii) entities that offer products or services through the website of a vendor of personal health records;

(iii) entities that are not covered entities and that offer products or services through the websites of covered entities that offer individuals personal health records;

(iv) entities that are not covered entities and that access information in a personal health record or send information to a personal health record;

FTC carries a big stick

- If FTC is key enforcement agency, expect a lot of activity and the very heavy enforcement of privacy law ("unfair business practice" enforcer)
- One observer:
  - "The goal is to rein it in … have some modicum of control over the Web 2.0, health IT, PHI mashup craze before it ends in a privacy and security train wreck."

BAA requirement

SEC. 13408. BUSINESS ASSOCIATE CONTRACTS REQUIRED FOR CERTAIN ENTITIES.

Each organization, with respect to a covered entity, that provides data transmission of protected health information to such entity (or its business associate) and that requires access on a routine basis to such protected health information, such as a Health Information Exchange Organization, Regional Health Information Organization, E-prescribing Gateway, or each vendor that contracts with a covered entity to allow that covered entity to offer a personal health record to patients as part of its electronic health record, is required to enter into a [Business Associate Agreement]

Business Associate obligations

- HIPAA compliance policies and procedures
- Subject to audit
- Subject to liability for unauthorized release / security breach
- Increased penalties and enforcement in hands of:
  - HHS
  - FTC
  - State AGs

What does all this have to do with social media?

Social Media meets HIPAA & Son of HIPAA

- What if a patient releases information online (in social media context)?
- What if provider releases?
- BAA required?
- When is consent given, when can it be assumed? Can it ever be assumed? (New, messier rules re: consent)
- If there is a “private” 1-on-1 conversation between a patient & a provider via an online service
  - Is the online service a Business Associate?
  - What are its obligations?
  - What protections should it have in place?

Other Issues

-
-
-
-
-

Questions, Approaches, Solutions

-
-
-
-
-

Discussion

David Harlow JD MPH
THE HARLOW GROUP LLC
www.harlowgroup.net
www.healthblawg.typepad.com
www.twitter.com/healthblawg
david@harlowgroup.net
617.965.9732