Safeguarding Your HIPAA and Personal Health Information Data

Robert Hess, Office of General Counsel
Steve Cosentino, Stinson Morrison Hecker
Overview

» Patient information confidentiality
  › Grant requirements
  › HIPAA

» Data breach notification laws

» Protecting intellectual property and trade secrets

» President’s Task Force on Cybersecurity

» Questions and Answers
Accountability and oversight

- Patients/research subjects
- University (see BPM-1201-1205)
- Granting agencies
- Office of Civil Rights – HIPPA
- Department of Justice – False Claims Act
- Qui tam relators – False Claims Act
HIPAA requirements

» Privacy rule
  › Covered entities must protect confidentiality of Protected Health Information

» Security Rule (applies to EPHI)
  › Administrative safeguards
  › Physical safeguards
  › Technical safeguards
HIPAA enforcement

» Civil money penalties
  › $100 - $50,000+ per violation
  › $1,500,000 per calendar year cap

» Criminal penalties for knowing violations
  › Fines of $50,000 up $250,000 depending on circumstances
  › Prison sentences of 1-10 years depending on circumstances
Examples

» UCLA – July 7, 2011
  › Employees inappropriately accessed patient records over 4-5 years
  › $865,500 settlement and corrective action plan

» Blue Cross and Blue Shield of Tennessee – March 9, 2012
  › 57 unencrypted hard drives were stolen
  › $1,500,000 settlement and corrective action plan
Examples, cont.

» Alaska Department of Health and Social Services – June 26, 2012
  › Unencrypted USB drive was stolen
  › $1,700,000 settlement and corrective action plan

» Affinity Health Plan, Inc. – August 14, 2013
  › Photocopiers returned to vendors with PHI of approximately 350,000 individuals
  › $1,215,780 settlement and corrective action plan
HIPAA Data Breach Requirement

» Section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act

» Requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information
HIPAA Data Breach Requirement

» Definition of Breach

› impermissible use or disclosure that compromises the security or privacy of the protected health information such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual
Exceptions to Definition of Breach

- Unintentional acquisition, access, or use of protected health information by a workforce member acting under the authority of a CE or BA.
- Inadvertent disclosure of protected health information from a person authorized to access protected health information at a CE or BA to another person authorized to access protected health information at the covered entity or business associate.
Exceptions to Definition of Breach

- In both cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule.
- The final exception to breach applies if the covered entity or business associate has a good faith belief that the unauthorized individual, to whom the impermissible disclosure was made, would not have been able to retain the information.
Breach Notification Requirements for CE’s

- Notify affected individuals following the discovery of a breach.
- Provide this individual notice in written form by first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically.
HIPAA Data Breach Requirement

» Breach Notification Requirements for CE’s

› If CE has insufficient or out-of-date contact information for 10 or more individuals, provide substitute individual notice by either posting the notice on the home page of its web site or provide notice in major print or broadcast media where the affected individuals likely reside.
HIPAA Data Breach Requirement

» Breach Notification Requirements for CE’s

› If the CE has insufficient or out-of-date contact information for fewer than 10 individuals, the covered entity may provide substitute notice by an alternative form of written, telephone, or other means.

› The final exception to breach applies if the covered entity or business associate has a good faith belief that the unauthorized individual, to whom the impermissible disclosure was made, would not have been able to retain the information.
Missouri Data Breach Requirement

Scope of Missouri Law

First name/initial and last name with unencrypted:

- **Medical information**, (any information regarding medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional).
- **Health insurance information** (health insurance policy number or subscriber ID number, any unique identifier used by a health insurer to identify individual).
Missouri Data Breach Requirement

» Scope of Missouri Law

» In addition to common elements of first name or initial and last name in combination with unencrypted SSN, DL, or account number, MO also includes unencrypted:

› **Other Financial Information**: Unique electronic identifier or routing code, in combination with any required security code, access code, or password that would permit access to an individual’s financial account.
Missouri Data Breach Requirement

» Notice

› Some discretion.

› If the entity conducts an appropriate investigation and determines that the risk of identity theft or fraud to the affected individual is not reasonably likely to occur as a result of the breach, no notice is required.

› However, the entity must maintain documentation supporting this determination for five years.
Missouri Data Breach Requirement

» Notice

› Methods for Notice.
  › Telephone, electronic means, in writing
  › Substitute notice email, posting on the entity's website, or notice to major statewide media.
  › If an entity maintains info but does not own it, they must notify the owner of the info
  › if breach impacts more than 1,000 Missouri residents at one time, notice must be provided to the State AG office
  › Civil penalties for violating the statute may reach up to $150,000 per breach of the security of the system.
Protecting Trade Secrets

- Trade Secrets are a common alternative to Patent
- Defined:
  - Information, process, formula, method, technique
  - Derives value from not being publically known; and
  - Is subject to reasonable efforts to maintain secrecy.
- Key Point – it doesn’t matter how an alleged trade secret becomes public.
  - *Religious Technology Center v. Netcom*
    - religious group lost trade secret claim because trade secrets acquired through improper means were posted on the internet
President Obama’s Cybersecurity Executive Order

› Calls for a “Framework” for cybersecurity intelligence sharing between government and the private sector
› Framework will allow intelligence to be gathered on cyberattacks and cyberthreats
President Obama’s Cybersecurity Executive Order

› Framework will focus on Areas for Improvement
  › Authentication
  › Automated Indicator Sharing
  › Conformity Assessment
  › Data Analytics
  › International Aspects, Impacts and Alignment
  › Privacy
  › Supply Chains and Interdependencies