Securing Individually Indentifying Health Information

Todd Ferris, MD

Director, Informatics Services

Associate CIO – IT Services

Privacy Officer

Information Resources and Technology

Stanford University School of Medicine

STANFORD SCHOOL OF MEDICINE

irt INFORMATION PRIVACY & SECURITY

Overview

- New California State Laws
  - AB211 and SB541
- CalPSAB
- HITRUST

New California State Laws

- Senate Bill 541 (SB541)
  - 541 authorizes the California Department of Public Health (CDPH) to investigate unlawful or unauthorized access to, or viewing, use or disclosure of, patient information
- Assembly Bill 211 (AB211)
  - Authorized a new California state office, the Office of Health Information Integrity (OHII), to investigate and enforce existing medical privacy laws and to investigate individuals and assess penalties against individuals for unauthorized access to or viewing, use or disclosure of patient information

SB 541

- Unauthorized access must be reported to the California Department of Public Health within five (5) days of detection of breach
- Fines for hospitals failing to prevent unauthorized access are up to $25,000 per patient whose medical information was breached

SB 541

- Mandates that hospitals monitor and report any unauthorized activity
- As part of the reporting, hospitals must provide the full names of all people involved. The state then may report those names to licensing boards and to CalOHII for investigation.
- Effective January 1, 2009

AB 211

- Authorizes new California state office, Office of Health Information Ingerity (OHII):
  - Will investigate and enforce existing medical privacy laws
  - Will investigate INDIVIDUALS for unauthorized access
  - Will assess penalties against individuals for unauthorized access to or viewing, use or disclosure of patient information

AB 211

- Patient has private right of action; can sue for damages, either actual or nominal
- Became effective January 1, 2009

What does this mean?

- If you use patient information, you are now personally responsible for unauthorized activities
- Regardless of whether it was mal-intended or not, you are personally responsible
- Patient whose information was breached has the right to sue you personally; does not have to be for actual damages

Kaiser Bellflower Incident

- Kaiser Permanente's Bellflower hospital was where Nadya Suleman delivered her octuplets on Jan 26th, 2009
- An internal investigation found 23 employees improperly accessed Suleman's records
  - One worker fired, fourteen resigned, eight disciplined
  - Incident reported to DHHS on February 5th
- On May 15th, California Department of Public Health announced an administrative penalty of $250k after a determination that the facility failed to prevent unauthorized access to confidential patient medical information

How?

California Privacy and Security Advisory Board (CalPSAB)

- Established by Secretary of the California Health and Human Services Agency October 2007
- Mission:
  - Develop and recommend privacy and security standards for California Health Information Exchange that promote quality of care, respect the privacy and security of personal health information, and enhance trust.

CalPSAB Structure

- Advisory board made up of members representing public and private health care industry stakeholders
- Advisory board oversees five committees:
  - Privacy
  - Security
  - Legal
  - Education
  - Health Information Organizations (HIO)

More Information on CalPSAB

- Products
  - Integrated Privacy and Security Policy Framework
  - Proposal for Baseline Security Guidelines
  - Business Associate Agreements Guidance
  - Proposal for Patient Consent
- http://www.ohi.ca.gov/calohi/

HITRUST

- Health Information Trust Alliance (HITRUST) is a private, independent company created to establish a common security framework that will allow for more effective and secure access, storage and exchange of personal health information

Common Security Framework (CSF)

- Leverages existing, globally recognized standards
- Scales according to type, size and complexity of an implementing organization
- Provides prescriptive requirements to ensure clarity
- Follows a risk-based approach offering multiple levels of implementation requirements determined by risks and thresholds
- Allows for the adoption of alternate controls when necessary
- Evolves according to user input and changing conditions in the healthcare industry and regulatory environment

More Information

- Sample Implementation Guide
  - http://www.hitrustalliance.net/HITRUST%202009%20CSF%20Implementation%20Manual%20Sample.pdf
- HITRUST website

  www.hitrustalliance.net

Thank you

References

- CDPH press release http://www.cdph.ca.gov/Pages/NR2009-44.aspx
- SF Chronicle Article http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2009/05/15/BU3S17L7DM.DTL
- HITRUST http://www.hitrustalliance.net/