CALIFORNIA HEALTHCARE FOUNDATION

Impact of Federal Stimulus Efforts on the Privacy & Security of Health Information in California

Deven McGraw

Director, Health Privacy Project

Center for Democracy & Technology

June 26, 2009

Sacramento, CA

Today's Program

1. Welcome & Overview – Teri Boughton & Veenu Aulakh
2. Impact of Federal Stimulus Efforts on the Privacy & Security of Health Information in California – Deven McGraw
3. California Stimulus Activities – Jonah Frohlich
4. Discussion
5. Wrap-up and Adjourn

About the Health Privacy Project at CDT

- Health IT and electronic health information exchange have tremendous potential to improve health care quality, reduce costs, and empower consumers.
- Until recently, little progress had been made on resolving the privacy and security issues raised by e-health.
- Project's aim: To develop and promote workable privacy and security policy solutions for personal health information.
- CDT (the Center for Democracy & Technology) is a nonprofit, nonpartisan policy advocacy organization in Washington, DC and San Francisco, CA.

Agenda

1. Privacy and Security Protections Before the American Recovery & Reinvestment Act of 2009 (ARRA)
2. ARRA Strengthens Protection
3. Significant Gaps Remain

Context

- Survey data show the public wants electronic access to their personal health information for themselves and their physicians.
- But a majority – 67% – also have significant concerns about the privacy of their medical records (CHCF, 2005).
- Without privacy protections, people will engage in "privacy-protective behaviors" to avoid having their information used inappropriately.
  - 1 in 6 adults withhold information from providers due to privacy concerns (Harris Interactive, 2007).
  - People in poor health, and racial and ethnic minorities, report even higher levels of concern and are more likely to engage in privacy-protective behaviors (CHCF, 2005).

Law in CA Before ARRA

- What and who are covered by the law
  - Identifiable health information
  - Specific types of health entities
  - Some “contractors” directly covered in CA; “business associates” under the Health Insurance Portability and Accountability Act (HIPAA) regulations covered only by contract
  - Others?
    - California law recently amended to extend protections to “any business organized for the purpose of maintaining medical information…”
    - Does this cover Internet companies and employers offering personal health records (PHRs)?

Law in CA Before ARRA (cont.)

- Permitted uses and disclosures of health data
  - Both CA and federal law allow entities covered by the law to use identifiable health information for a broad range of purposes without consent – the "TPO" exception
  - HIPAA also limits access, use, and disclosure to "minimum necessary" except disclosures for treatment purposes
  - Some heightened protections for more sensitive data (substance abuse records, HIV test results, psychotherapy notes)

Law in CA Before ARRA (cont.)

- Patient's Right to Know
  - Federal "audit trail" requirement is limited
- Use of information for marketing purposes
  - Authorization "required" – but exceptions diminish rule's impact
- Breach notification
  - No federal requirement
  - California first to enact law to protect computerized personal information (amended in 2008 to cover electronic health data)
  - Safe harbor for encrypted data

Law in CA Before ARRA (cont.)

- Enforcement
  - Federal enforcement lacking since HIPAA rules implemented
  - State laws confer greater enforcement power
    - State authorities may bring civil action
    - Individuals may sue for damages arising from negligent release of confidential information
  - Certain health facilities in CA also required to affirmatively prevent unauthorized access to medical information – improper access must be reported to CDPH within five days; mandatory fines
  - Cal OHI has authority to establish rules to enforce state's health privacy laws

Changes Made by ARRA

- Changes strengthened HIPAA rules
  - Now equal to or stronger than CA laws in some cases
- Stronger CA laws remain in effect
- Most changes go into effect February 18, 2010

Changes Made by ARRA (cont.)

- Who is covered
  - HIPAA business associates directly accountable for complying with key provisions of privacy and security rules (including all new ARRA provisions)
  - Regional health information organizations (RHIOs) and HIEs must be business associates
  - Vendors of PHRs must be business associates in some cases – needs interpretation by federal authorities

Changes Made by ARRA (cont.)

- Permitted uses and disclosures of health data
  - No change to baseline rules (TPO exception) – but more guidance on "minimum necessary" and encouragement to use "limited data set" (stripped of identifiers) where appropriate
  - Patients paying out of pocket can restrict disclosures to health plans
- Patient's Right to Know
  - "Audit Trail" requirement significantly strengthened – must account for all disclosures from "electronic" record
  - Strengthened right to obtain an electronic copy and have it sent directly to another individual or entity

Changes Made by ARRA (cont.)

- Use of information for marketing purposes
  - Strengthened federal protections for “remunerated” communications – federal “opt-in” required
  - Still some exceptions
  - Intersection with CA opt-out
- New prohibition on sales of identifiable health data
  - Exceptions apply – HHS to issue regulations
- Breach notification
  - New federal requirements go into effect 9/18/09
  - Safe harbor includes encryption
  - Federal law very specific re: content and timing of notice, notice to federal regulators

Changes Made by ARRA (cont.)

- Enforcement
  - Significant changes
  - State AGs now authorized to enforce HIPAA rules
  - Civil penalties increased – up to $1.5 million max – when applied by federal authorities (states can impose at previous level)
  - Criminal penalties can be assessed against individuals
  - HHS must impose penalties in cases of willful neglect
  - Business associates can be held liable
  - HHS must periodically conduct privacy and security audits

Significant Gaps Remain

- Personal health records
  - Currently not covered by HIPAA if offered by Microsoft, Google, Dossia, WebMD, and others (except if HIPAA business associate provisions apply)
  - ARRA established breach notification requirements, strengthened right to receive electronic copy of data
  - HHS (working with FTC) to provide recommendations to Congress by 2/2010 on privacy and security protections
- Application of California law?

Significant Gaps Remain – PHRs

- Need consistent regulation – but HIPAA as currently structured is not the answer
  - Treatment, payment, and operations exception makes little sense for PHRs, which should be consumer controlled
  - Reliance on authorization for marketing and business uses provides weak protection
  - Markle Common Framework for Networked Personal Health Information provides good model
  - FTC should play a role in regulating PHRs

Still Work to be Done

- Implementation of new rules will take a lot of work
  - Education about new rights, responsibilities
  - Will HHS take a more active role in privacy stewardship?
- Uses of data for marketing purposes – still too many loopholes
- Will new enforcement authority be effective?
- Lack of private right of action at the federal level

Still Work to be Done (cont.)

- Strengthening de-identification standard and establishing clear rules against, and penalties for, re-identification
  - HHS required to study current standard by next February
- Enacting limits on use of health information to discriminate in employment and insurance
  - Possibility of accomplishing in federal health reform efforts

Questions?

Thank you.

Deven McGraw

Director, Health Privacy Project

Center for Democracy & Technology

deven@cdt.org

www.cdt.org/healthprivacy