Davis Wright Tremaine LLP

Healthcare Privacy and Security Issues in HIT, EHR and RHIO Initiatives

Fifteenth National HIPAA Summit
Summit Day II - December 13 – 2:30 p.m.

Gerry Hinkley
gerryhinkley@dwt.com

Davis Wright Tremaine LLP

Overview

- What's driving public opinion?
- Surveys and reports
- Privacy principles
- Legal baselines
  - HIPAA
  - State laws
  - On the horizon
- HIE policies and procedures
- RHIO participation agreement
- Implications for networks of networks

What's driving public opinion?

- May 2006: VA Disability ratings stolen along with names and Social Security numbers
- June 2006: CMS reports health information of 17,000 Americans whose insurance plans are provided by Humana, Inc. was at risk because of unsecured computer data
- September 2006: New York City's public hospital system suspends 39 employees without pay for peeking at the private medical records of 7 year old Nixzmary Brown
- September 2006: Medical identities of 42 Virginia Mason Clinic patients stolen and used by two employees since May 2005

Davis Wright Tremaine LLP

What's driving public opinion?

- November 2006: Richard Yaw Adjei of Bear, Delaware pleaded guilty in federal court on November 16 to aggravated identity theft and three counts of fraud for his part in a widespread criminal scheme that used information from a hospital billing service to steal the identities of more than 400 people
- November 2006: The personal health information of more than 200 people was discovered by TV investigators in unlocked garbage dumpsters outside Houston area Walgreens, CVS and other pharmacies
- March 2007: The California state Department of Health Services inadvertently revealed the names and addresses of up to 53 people living with enrolled in an AIDS drug assistance program to other enrollees by putting benefit notification letters in the wrong envelopes

Davis Wright Tremaine LLP

Surveys and reports

- September 2005: CHCF survey shows 52% of respondents concerned that employers may use health information to limit job opportunities; 61% concerned about privacy of their health information; one in four consumers is aware of recent privacy breaches
- September 2006: GAO survey finds almost half of all responding Medicare Advantage contractors admitted to recent breaches of privacy of health records
- November 2006: Medicare Advantage providers “mostly compliant” with HIPAA decreases from 91% in 2005 to 85% in 2006
- April 2007: Mathematica survey finds nearly all low income racial and ethnic minority groups mistrust the security of electronic health records systems, driving them out of the system

Davis Wright Tremaine LLP

Privacy Principles (Thanks to Connecting for Health)

- **Openness and Transparency**

  There should be a general policy of openness about developments, practices, and policies with respect to personal data. Individuals should be able to know what information exists about them, the purpose of its use, who can access and use it, and where it resides

- **Purpose Specification and Minimization**

  The purposes for which personal data are collected should be specified at the time of collection, and the subsequent use should be limited to those purposes or others that are specified on each occasion of change of purpose

- **Collection Limitation**

  Personal health information should only be collected for specified purposes, should be obtained by lawful and fair means and, where possible, with the knowledge or consent of the data subject

Davis Wright Tremaine LLP

Privacy Principles (Thanks to Connecting for Health)

- **Use Limitation**

  Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified

- **Individual Participation and Control**

  Individuals should control access to their personal information:

  - Individuals should be able to obtain from each entity that controls personal health data information about whether or not the entity has data relating to them
  - Individuals should have the right to:
  - Have personal data relating to them communicated within a reasonable time (at an affordable charge, if any), and in a form that is readily understandable;
  - Be given reasons if a request (as described above) is denied, and to be able to challenge such denial; and
  - Challenge data relating to them and have it rectified, completed, or amended

Davis Wright Tremaine LLP

Privacy Principles (Thanks to Connecting for Health)

- **Data Integrity and Quality**

  All personal data collected should be relevant to the purposes for which they are used and should be accurate, complete, and current

- **Security Safeguards and Controls**

  Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure

- **Accountability and Oversight**

  Entities in control of personal health data must be held accountable for implementing these information practices

- **Remedies**

  Legal and financial remedies must exist to address any security breaches or privacy violations

Davis Wright Tremaine LLP

Legal Baseline: HIPAA

- It's not about privacy, it's about disclosure
- Patient consent not required for payment, treatment, health operations
- Notice of Privacy Practices
  - The kitchen sink of policies
  - Like drinking from a fire hose

Davis Wright Tremaine LLP

Legal Baseline: State laws

- RTI project discloses
  - a crazy-quilt of state laws
    - Sensitive information
      - HIV/AIDS
      - Mental health
      - Substance abuse
      - Genetic testing
    - All health information (NY)
  - "my own private HIPAA"

Davis Wright Tremaine LLP

On the Horizon: Wired for Health Care Quality Act

- Operator of health information data base is a HIPAA “covered entity”
- Health plans, clearinghouses and providers who transmit data must notify patients of breaches

Davis Wright Tremaine LLP

On the Horizon: Kennedy-Leahy – "the new HIPAA"

- Patient's right to
  - Privacy of health information
  - "Opt out"
  - Inspect records
  - Modify information
  - Nondisclosure if private pay
- Possessors of information must implement
  - Safeguards
  - Risk management and control
  - Accounting for disclosures
  - Opt-out procedure
  - Limited uses
  - Labeling as "PHI"

Davis Wright Tremaine LLP

On the Horizon: Kennedy-Leahy – "the new HIPAA" (2)

- Notice of privacy practices
- Prior to obtaining or disclosing PHI for treatment or payment or any other purpose must obtain signed authorization from patient
- Disclosure to next of kin, directories
- Overseas outsourcing scrutinized
- Notice of loss or corruption of data to patient
- Notice of breach to owner or licensee
- Office of Health Information Privacy

Davis Wright Tremaine LLP

On the Horizon: Kennedy-Leahy – "the new HIPAA" (3)

- Criminal penalties for violations
- Civil sanctions for violations
- Private right of action
- Enforcement by states attorneys general
- Whistleblower protections
- No pre-emption of state laws that provide greater protections, relate to police powers
- HIPAA regulations to be amended to conform

Davis Wright Tremaine LLP

On the Horizon: Independent Health Record Trust Act of 2007

- IHRT: certified by FTC; standards set by FTC with input from NCVHS
- "Privacy": as to PHI = control over acquisition, uses, and disclosures
- Affirmative consent
- Data entry: EHR users, participants; limitations on "sensitive information"
- Data access: participant specifies what is accessible; exception – law enforcement
- Violations: fines, imprisonment

Davis Wright Tremaine LLP

HIE policies and procedures: So what's a RHIO to do?

- Structure emphasizing cooperation among participants
- RHIO in supervisory and disciplinary role
- Broadly representative RHIO governing body
- RHIO Policies
  - promote efficient and consistent operation
  - promote trust among participants, trust by patients/consumers and the community
- Contracts among participants are the glue
  - Flexible arrangements permitting change as circumstances change, laws change and electronic HIE matures

Davis Wright Tremaine LLP

RHIO Participation Agreement: It's all about the contract

- Inputs
  - Legal requirements
  - RHIO policies
- Privacy-related subjects
  - Patient Consent
  - Permitted Uses of Data
  - Prohibited Uses of Data
  - Authorized Users
  - Measures to Assure Privacy and Security of Data
  - Breaches of Privacy and Security

Davis Wright Tremaine LLP

Implications for networks of networks

- Back to the Common Framework
- Patient consent commonality – a new semantic away from “opt in/opt out”
- Address the adequacy of technology
- State-level leadership
- A national dialogue toward federal leadership and direction
- In the meantime
  - Don’t erect barriers to growth and connectivity
  - Get on with it

Davis Wright Tremaine LLP

This is a publication of the Health Information Technology Group of Davis Wright Tremaine LLP with a purpose to inform and comment upon recent developments in health law. It is not intended, nor should it be used, as a substitute for specific legal advice as legal counsel may only be given in response to inquiries regarding particular situations.