Connecting California to Improve Patient Care

ARRA/HITECH & New Federal Privacy and Security Rules

Allen Briskin
allenbriskin@dwt.com

July 10, 2009

Davis Wright Tremaine LLP

DEFINING SUCCESS TOGETHER

Revised and Expanded Privacy and Security Rules under HIPAA

- ***American Recovery and Reinvestment Act of 2009*** ("ARRA" or "the Stimulus Bill") signed into law on February 17, 2009
- ARRA's amendments to HIPAA are found in Subtitle D of the ***Health Information Technology for Economic and Clinical Health Act*** ("HITECH Act")

Davis Wright Tremaine LLP

Overview of New Privacy and Security Rules

- Direct regulation of business associates
- New patient privacy rights
- Breach notification (different from California law)
- Guidance on the “minimum necessary” standard
- Prohibitions on sale of protected health information (“PHI”)
- Increased enforcement and penalties

Direct Regulation of Business Associates

- Before ARRA
  - Business Associates ("BA") were not directly covered by HIPAA; Covered Entities ("CE") were required to enter into contracts with their BAs, which imposed contractual duties
  - BAs were subject to contract remedies noncompliance
- Under ARRA
  - Legal requirements apply directly to BAs
  - BAs are subject to civil and criminal penalties for noncompliance

Direct Regulation of Business Associates

- Business associates must comply with:
  - HITECH privacy and security provisions
  - HIPAA security standards, BA privacy requirements
  - Obligation to respond to breaches by the CE (*i.e.,* if CE does not cure the breach, BA must terminate contract if feasible, or notify Secretary if not feasible)
- Requirements are effective 2/17/2010
- Regulations are expected

Direct Regulation of Business Associates

- HIPAA requirements that apply directly to BAs
  - BAs may only use and disclose PHI as described in the Privacy Rule
  - If BA learns of material breach by the CE, the BA is required to
    - take action to cure breach or end violation, or
    - if that is not feasible, terminate its contract with the covered entity
    - if neither is feasible, report the breach to HHS
- Whether to amend existing business associate agreements; most are awaiting guidance

New Patient Privacy Rights: Patient Restrictions

- Patients may direct providers not to disclose protected health information to a health plan for purposes of payment or health care operations
  - Information must pertain solely to item or service for which provider is paid in full out of pocket
  - Provider may (but need not) disclose PHI for other purposes, e.g., treatment
- Requirements are effective 2/17/2010
- Regulations are expected to provide guidance

New Patient Privacy Rights: Provision of Electronic Records

- Patients may demand protected health information be provided in electronic format if covered entity maintains information in electronic health record
- Patient may direct covered entity to transmit information electronically to another
- Covered entity may charge fees no greater than labor costs
- Limited to information patient has right to obtain
- Requirements are effective 2/17/2010
- Regulations are expected to provide guidance

Davis Wright Tremaine LLP

New Patient Privacy Rights: Accounting of Disclosures

- Covered entity must give patient accounting of disclosures for treatment, payment and operations made through an electronic health record
- EHR is any electronic record created, gathered, managed or consulted by clinician or staff (prescription databases, PACS, devices)
- Accounting must cover the 3 years prior to request
- Accounting includes disclosures by business associates, or covered entity may direct patient to business associate(s)

Davis Wright Tremaine LLP

New Patient Privacy Rights: Accounting of Disclosures

- Effective Date for accounting of disclosure requirements
  - 1/1/2014 for EHR acquired prior to 1/1/2009
  - 1/1/2011 for EHR acquired after 1/1/2009
- Regulations are expected to provide guidance

Davis Wright Tremaine LLP

Notification of Breach

- Before ARRA
  - Covered entities/business associates not required to obligation to notify individuals or HHS of privacy or security breaches
  - Obligation to mitigate breach may have included notice
- After ARRA
  - Covered entities required to give notice of breach to patient, etc.; business associates required to notify covered entity

Notification of Breach

- Covered Entity must provide notice if security of unsecured PHI is breached
- Notice must be given without unreasonable delay and within 60 days after discovery of breach
- "Breach" means unauthorized acquisition, access, use or disclosure of PHI that compromises the privacy or security of such information, unless recipient cannot reasonably retain the information
- "Breach" *does not* mean
  - Unintentional acquisition or use in good faith in the course and scope of employment, or
  - Inadvertent disclosure within the same CE or BA
  - AND the Information is not further acquired, accessed, used, disclosed

Davis Wright Tremaine LLP

Notification of Breach

- Notice goes to
  - Affected individual, at last known address, though special rules apply if misuse is imminent or the individual's address is unknown.
  - Website posting, conspicuously on home page, if more than 10 are affected and lack contact info
  - Major media outlets, if the breach involves more than 500 individuals in state or jurisdiction
  - HHS, immediately, if breach involves more than 500 individuals, and HHS will identify the breach on HHS website; or annually, if breach fewer than 500 individuals

Notification of Breach

- Notification requirements apply to breaches of unsecured PHI only
- Unsecured PHI is not secured through use of a technology or methodology identified by HHS as rendering the information unusable, unreadable or indecipherable to unauthorized persons
- Creates a "safe harbor," encouraging covered entities to adopt practices that will excuse them from notification requirements
- HHS Guidance issued 4/27/2009; updated guidance will follow annually; HHS has solicited comments

Notification of Breach

- HHS guidance is prescriptive, not examples
- Two methods
  - Encryption
    - Data at rest per NIST Special Publication 800-111
    - Data in motion per FIPS 140-2
  - Destruction
    - Hard copy media by shredding or destruction so that PHI cannot be read or reconstructed
    - Electronic media per NIST Special Publication 800-88 such that media cannot be retrieved

Notification of Breach

- State law also applies, and may be more strict
- Regulations expected by 8/17/2009
- Compliance required 30 days after publication
- ARRA also requires personal health record or “PHR” vendors to provide notice of breach, under rules issued by Federal Trade Commission

Notification of Breach

- Notice must contain
  - Brief description of what happened, date of breach, date of discovery of breach
  - Description of type(s) of unsecured PHI involved (*e.g.*, name, social security number, date of birth, address, account number, etc.)
  - Steps patient should take to protect against potential harm
  - description Covered Entity's investigation and mitigation efforts, how Covered Entity will protect against further breaches
  - Covered Entity's contact information

Minimum Necessary Standard

- Under HIPAA, a Covered Entity's use and disclosure of, and requests for, protected health information are to be limited to the minimum necessary to accomplish the Covered Entity's intended purpose
- Before ARRA, there was no explicit definition of "minimum necessary"
- HHS is to issue guidance as to meaning of "minimum necessary" by 8/2010
- Between 2/17/2010 and when HHS guidance is issued, Covered Entities are to use, disclose, or request limited data set information, or if more information is needed, in compliance with the minimum necessary standard

Prohibitions on Sale of PHI

- Covered Entities and Business Associates may not receive remuneration, directly or indirectly, for PHI, unless the patient has given a valid authorization specifically addressing sale
- Exceptions:
  - For public health activities
  - For research (cost of data prep and transmittal)
  - For treatment
  - For health care operations related to sale or transfer
  - To pay business associates for services
  - To provide an individual with his/her PHI
- Requirements effective 2/17/2009
- Regulations are expected to provide more guidance

Increased Enforcement and Penalties

- HHS is to conduct periodic audits of Covered Entities and Business Associates even if no complaint filed.
- HHS is required to conduct an audit if preliminary investigation of complaint indicates “willful neglect.”
- HHS is required to impose monetary penalties for violations due to willful neglect
- HHS to develop mechanism for individuals to share in penalties received
- HHS to develop education initiative
- State Attorneys General may prosecute HIPAA and HITECH violations, in addition to state law claims

- 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.

Davis Wright Tremaine LLP