Health Information Privacy & Security

The HITECH Act, Data Breach Reporting and Other Developments

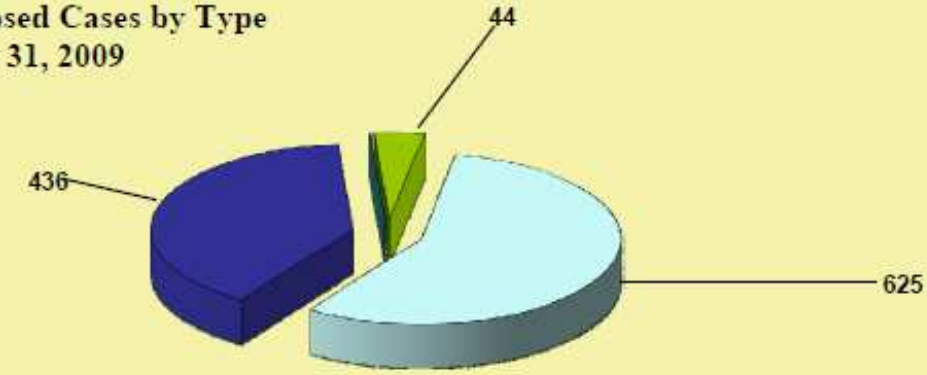
Paul T. Smith, Partner

Davis Wright Tremaine LLP

paulsmith@dwt.com

HIPAA Security Enforcement

CMS Enforcement Statistics Report
Open and Closed Cases by Type
As of July 31, 2009

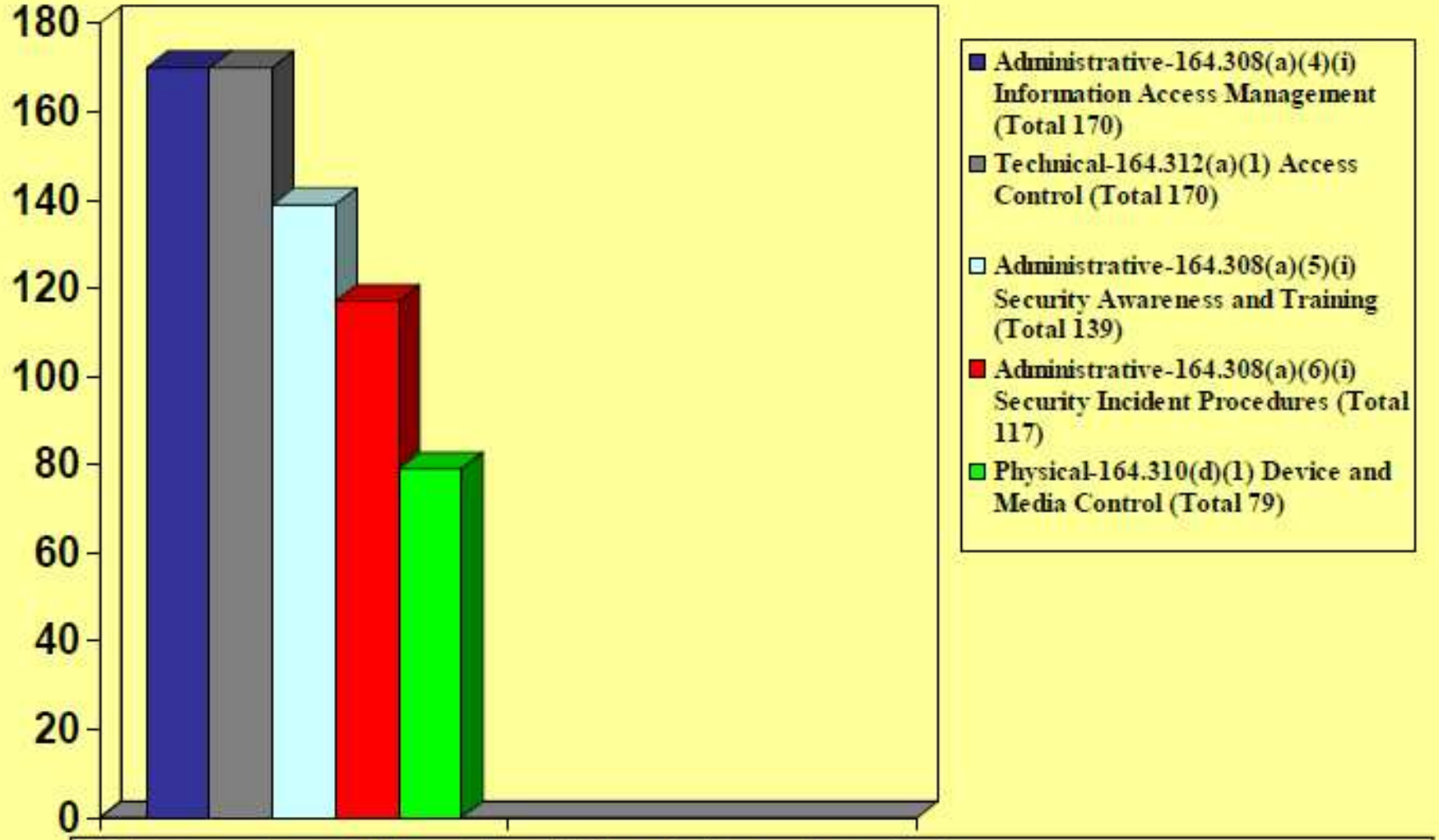


Complaint Type	Total	Open	Closed
Transactions and Code Sets (TCS)	625	38	587
Security	436	77	359
National Provider Identifier (NPI)	44	2	42
Total	1,105	117	988

Open – Outstanding issues remain. Entity may be under a corrective action plan or additional information from either the complainant, the filed against entity, or both is being sought.

Closed – No further action required. All issues have been sufficiently resolved. Please note that 47 of the 359 security cases have been closed via corrective action plans.

Summary of Most Commonly Violated Security Provisions



-A single security complaint can allege violations of all the provisions listed.
-The number of provisions listed do not correlate to the total number of security complaints.
-The total number of Administrative provisions represented on this slide, 426; Technical 170, and Physical 79.

OIG Report

October, 2008

http://www.oig.hhs.gov/oas/reports/region4/40705064.pdf

"CMS had taken limited actions to ensure that covered entities adequately implement the HIPAA Security Rule. These actions had not provided effective oversight or encouraged enforcement of the HIPAA Security Rule by covered entities. Although authorized to do so by Federal, regulations as of February 16,2006, CMS had not conducted any HIPAA Security Rule compliance reviews of covered entities. To fulfill its oversight responsibilities, CMS relied on complaints to identify any noncompliant covered entities that it might investigate. As a result, CMS had no effective mechanism to ensure that covered entities were complying with the HIPAA Security Rule or that ePHI was being adequately protected."

OCR Security Enforcement

- The authority to administer and enforce the Security Rule was transferred to OCR on July 27, 2009.
- Since OCR began reporting its Security Rule enforcement results in October 2009, HHS has received approximately 48 complaints alleging a violation of the Security Rule. During this period, we closed 32 complaints after investigation and appropriate corrective action. As of February 28, 2010, OCR had 112 open complaints and compliance reviews.

http://www.hhs.gov/ocr/privacy/hipaa/enforcement/highlights/index.html

OCR Privacy Enforcement

- OCR has investigated and resolved over 10,050 cases by requiring changes in privacy practices and other corrective actions by the covered entities.
- In 5,191 cases, investigations found no violation had occurred.
- In 28,635 cases OCR determined that the complaint did not present an eligible case for enforcement of the Privacy Rule

http://www.hhs.gov/ocr/privacy/hipaa/enforcement/highlights/01312010.html

HIPAA Enforcement

U.S. Department of Health & Human Services

HHS.gov *Improving the health, safety, and well-being of America*

Search | Search OCR All HHS

HHS Home | HHS News | About HHS | Font Size | Print | Download Reader

Health Information Privacy

Office for Civil Rights | Civil Rights | Health Information Privacy

OCR Home > Health Information Privacy > HIPAA > Enforcement Activities & Results > Case Examples

HIPAA
- Understanding HIPAA Privacy
- HIPAA Administrative Simplification Statute & Rules
- Enforcement Activities & Results
  - Enforcement Process
  - Enforcement Highlights
  - Enforcement Data
  - Case Examples
- How to File a Complaint
- Frequently Asked Questions
- News Archive

Patient Safety Act
- Understanding Patient

Resolution Agreement

HHS, Providence Health & Services Agree on Corrective Action Plan to Protect Health Information

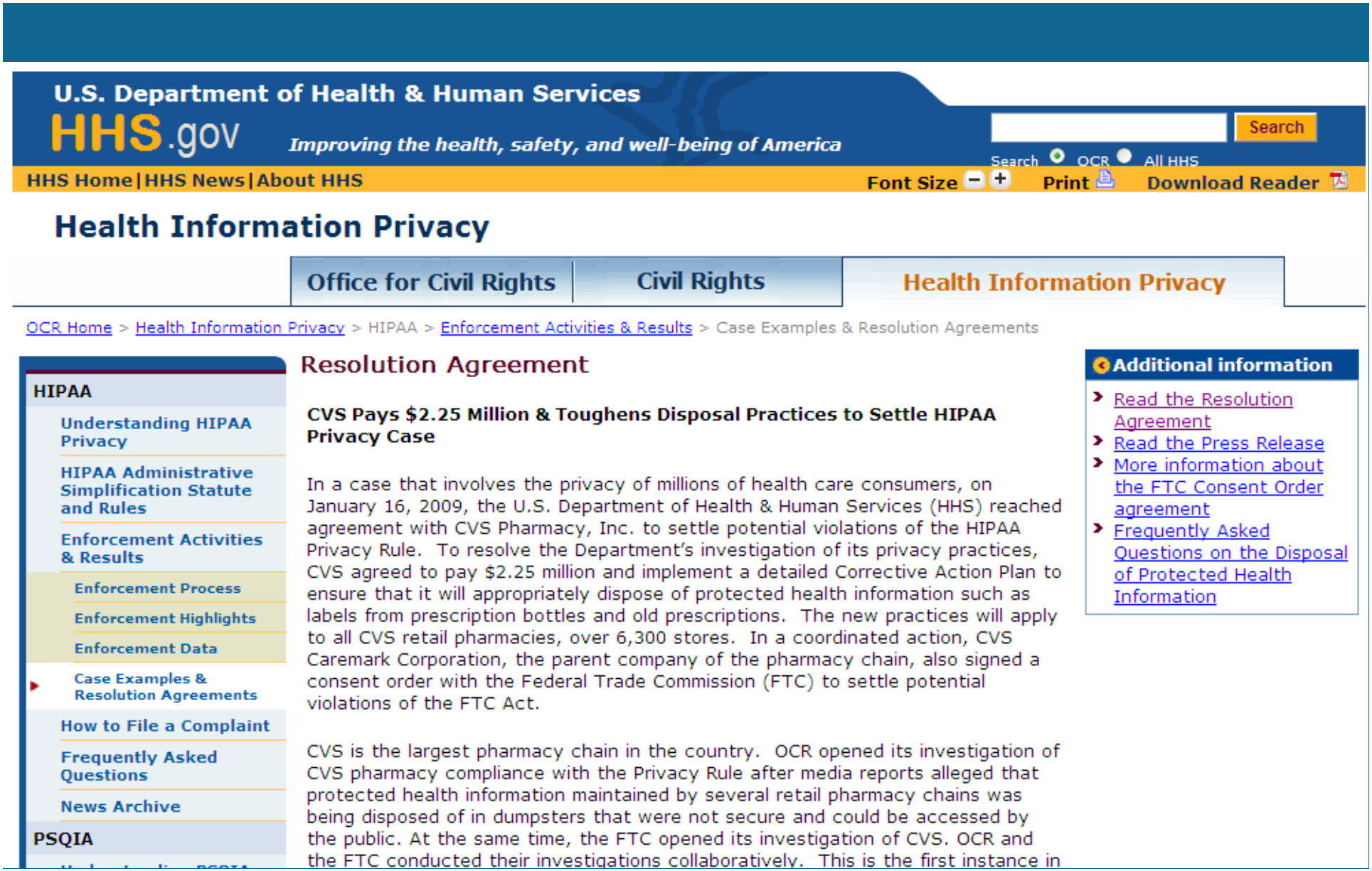
On July 16, 2008, the U.S. Department of Health & Human Services (HHS) entered into a Resolution Agreement with Seattle-based Providence Health & Services (Providence) to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules. Read the Press Release.

In the agreement, Providence agrees to pay $100,000 and implement a detailed Corrective Action Plan to ensure that it will appropriately safeguard identifiable electronic patient information against theft or loss. The Resolution Agreement relates to Providence's loss of electronic backup media and laptop computers containing individually identifiable health information in 2005 and 2006.

A Resolution Agreement is a contract signed by HHS and a covered entity in which the covered entity agrees to perform certain obligations (e.g., staff training) and make reports to HHS for a period of years, typically three years. During the period, HHS monitors the compliance of the covered entity with the obligations it has agreed to perform.

With respect to the HIPAA Privacy and Security Rules, this is the first time HHS has required a Resolution Agreement from a covered entity. Providence's cooperation with OCR and CMS allowed HHS to resolve this case without the need to impose a civil money penalty.

HIPAA Enforcement



U.S. Department of Health & Human Services

HHS.gov *Improving the health, safety, and well-being of America*

Search | Search ◉ OCR ○ All HHS

HHS Home | HHS News | About HHS | Font Size − + | Print | Download Reader

Health Information Privacy

Office for Civil Rights | Civil Rights | Health Information Privacy

OCR Home > Health Information Privacy > HIPAA > Enforcement Activities & Results > Case Examples & Resolution Agreements

HIPAA
- Understanding HIPAA Privacy
- HIPAA Administrative Simplification Statute and Rules
- Enforcement Activities & Results
  - Enforcement Process
  - Enforcement Highlights
  - Enforcement Data
  - Case Examples & Resolution Agreements
- How to File a Complaint
- Frequently Asked Questions
- News Archive

PSQIA

Resolution Agreement

CVS Pays $2.25 Million & Toughens Disposal Practices to Settle HIPAA Privacy Case

In a case that involves the privacy of millions of health care consumers, on January 16, 2009, the U.S. Department of Health & Human Services (HHS) reached agreement with CVS Pharmacy, Inc. to settle potential violations of the HIPAA Privacy Rule. To resolve the Department's investigation of its privacy practices, CVS agreed to pay $2.25 million and implement a detailed Corrective Action Plan to ensure that it will appropriately dispose of protected health information such as labels from prescription bottles and old prescriptions. The new practices will apply to all CVS retail pharmacies, over 6,300 stores. In a coordinated action, CVS Caremark Corporation, the parent company of the pharmacy chain, also signed a consent order with the Federal Trade Commission (FTC) to settle potential violations of the FTC Act.

CVS is the largest pharmacy chain in the country. OCR opened its investigation of CVS pharmacy compliance with the Privacy Rule after media reports alleged that protected health information maintained by several retail pharmacy chains was being disposed of in dumpsters that were not secure and could be accessed by the public. At the same time, the FTC opened its investigation of CVS. OCR and the FTC conducted their investigations collaboratively. This is the first instance in

Additional information
- Read the Resolution Agreement
- Read the Press Release
- More information about the FTC Consent Order agreement
- Frequently Asked Questions on the Disposal of Protected Health Information

CMS Security Compliance Reviews

- Piedmont Hospital, Atlanta 2007
- CMS hired PWC to conduct 10 compliance review in 2008
- Compliant driven, or self-reported or publicized incidents
- Information Request for Onsite Compliance Review

http://www.cms.hhs.gov/Enforcement/Downloads/InformationRequestforComplianceReviews.pdf

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

CMS Security Compliance Reviews

- Risk analysis and management
- Security training
- Physical security of facilities and mobile devices
- Off-site access and use of ePHI from remote locations
- Storage of ePHI on portable devices and media
- Disposal of equipment containing ePHI
- Business associate agreements and contracts
- Data encryption
- Virus protection
- Technical safeguards in place to protect ePHI
- Monitoring of access to ePHI.

- http://www.cms.hhs.gov/SecurityStandard
- 2004-2007
- Basic guides covering --
  - Security 101
  - Administrative safeguards
  - Physical safeguards
  - Technical safeguards
  - Organizational policies
  - Basics of risk management
  - Small providers

NIST Introductory Resource Guide for Implementing the HIPAA Security Rule

- http://www.cms.hhs.gov/SecurityStandard
- May, 2008
- Intended to assist federal agencies in—
  - Understanding information security terms and security concepts in the HIPAA Security Rules
  - Directing agencies to other resources
- Describes a risk management framework for selecting, specifying, and implementing security controls

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

CMS Security Guidance for Remote Access

- http://www.cms.hhs.gov/SecurityStandard
- December, 2006
- Describes strategies for managing security risks in
  - Portable media (e.g., flash drives)
  - Laptops, PDAs
  - Home computers

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

The HITECH Act

- Title XIII of the American Recovery and Reinvestment Act of 2009
- Enacted February 17, 2009
- Most provisions effective February 17, 2010

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

The HITECH Act

- Promotion of HIT, with a view to universal EMRs by 2014
  - Standards and certification criteria
  - Testing
  - Financial incentives for adoption
- Health information privacy and security
  - Strengthens HIPAA
  - Creates new data breach notification requirements

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

The HITECH Act - Enforcement

- Increases penalties for HIPAA violations (effective immediately)
- Penalties tiered, based on fault & whether corrected
- $100 per violation for innocent violations
- Up to $50,000 per violation for violations due to willful neglect that are not corrected

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

The HITECH Act - Enforcement

- Permits states' attorneys general to bring civil suits under HIPAA to recover penalties and attorneys' fees
- Clarifies that individuals who are not covered entities can be prosecuted criminally under HIPAA
- Beginning 2012, requires formal CMP investigations for violations involving willful neglect
- Requires HHS to conduct periodic HIPAA compliance audits

HIPAA Enforcement

Featured Story Dec. 9, 2009

Two Data Security Breaches Give State Attorneys General a Chance to Exercise Their New HIPAA Powers

Reprinted from REPORT ON PATIENT PRIVACY, the industry's most practical source of news on HIPAA patient privacy provisions.

In a sign that state attorneys general may be flexing the HIPAA enforcement muscle granted by the HITECH Act provisions in the Recovery Act, the Connecticut and Arizona attorneys general are investigating health plans that recently experienced data breaches that they failed to disclose for several months.

Typically, state attorneys general prosecute only violations of state laws, but they now have authority to investigate and levy fines for violations of HIPAA and the HITECH Act, which requires mandatory notifications within two months of knowledge of a breach.

Connecticut Attorney General Richard Blumenthal (D) has emerged as possibly the first AG to take on a HIPAA investigation, and Arizona's AG may also be pursuing a similar course. The larger of the two breaches that have come to the AGs' attention was experienced by Health Net, Inc., which lost a portable external hard drive containing seven years of data for 446,000 Connecticut residents. The lost data came from 1.5 million individuals in total, who also hailed from New Jersey and New York.

Health Net reported the loss to the Connecticut AG on Nov. 19, and on the same day Blumenthal issued a scathing statement demanding answers and promising action. He specifically said he was investigating whether Health Net may have violated "federal laws," as well as his state's own data protection laws.

Consumer Security Breach Notification Law

- No explicit HIPAA requirement for notification of data breaches
- California's consumer breach notification law requires businesses and agencies that own or license "computerized data that includes personal information . . . to disclose any breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

Civil Code 1798.82

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

Consumer Security Breach Notification Law

- Personal information includes name with any of the following:
  - SSN
  - DL or CA ID card no.
  - Account or credit or debit card number with any required access code
  - Medical information
  - Health insurance information

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

Consumer Security Breach Notification Laws

- "Good faith" exception:

  CC 1798.82(d): Good faith acquisition of personal information by an employee or agent for the purposes of the business is not a breach if the information is not used or subject to further unauthorized disclosure

SB 541 – Focus on Facilities

- SB 541 created new obligations for *health facilities* to maintain the confidentiality of medical information and to report violations of this confidentiality to both the Department of Public Health (DPH) and to the patient.
- Failure to prevent or to report unlawful or unauthorized access/use/disclosure of patient information results in fines.

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

Prevent

- *Health facilities* must prevent unlawful or unauthorized access to, or use or disclosure of, patient medical information (SB 541)
  - DPH: Prevent = establish and implement appropriate administrative, technical and physical safeguards to protect the privacy of medical information; reasonably safeguard from unauthorized access or unlawful access, use or disclosure (AB 211)

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

Self-Report

- Facilities must report any unlawful or unauthorized access/use/disclosure of, patient medical information *to DPH* and *to the affected patient*
  - Must report within *five business days* after detection of the unlawful or unauthorized access, use or disclosure
  - SB 337 (2009) allows delay up to 120 days upon request by law enforcement official if disclosure likely to impede law enforcement activities

Who's Covered?

- Reporting obligations apply to:
  1. General acute care hospitals, acute psychiatric hospitals, skilled nursing facilities and other licensed facilities
  2. Licensed clinics
  3. Home health agencies and hospices
- Not included: health plans, individual providers (physicians, etc.), businesses that maintain medical information for providers or individuals

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

Report What?

- Must report unlawful or unauthorized access to, or use or disclosure of, patient medical information
  - "Unauthorized":
    - inappropriate access, review, or viewing
    - without a direct need for medical diagnosis, treatment, or other lawful use (as permitted by the CMIA or other law governing access, use, or disclosure of medical information

Report What?

- DPH AFL 09-03 (July 29, 2009)
- Misdirected internal paper records, email, or fax transmissions to another health care worker within the same facility or health care system for the purpose of coordinating care or delivery of services do not need to be reported to the department.
- In these circumstances, the health facility should review internal policies and procedures to determine if changes are necessary to strengthen patient privacy protections and prevent similar occurrences in the future.

Content of Report

DPH AFL 09-03 (July 29, 2009)

- Date and time of reported incident
- Facility name
- Facility address/location
- Facility contact person
- Name of patient(s)
- Name of the alleged violator(s)
- General information about the circumstances surrounding the breach
- Any other information needed to make the determination for an onsite investigation

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

Report What?

- Inappropriate access, review, or viewing by whom?
  - What if a facility becomes aware of wrongful access, use or disclosure by a business associate?
- No “good faith” exception
  - CC 1798.82(d): Good faith acquisition of personal information by an employee or agent for the purposes of the business is not a breach if the information is not used or subject to further unauthorized disclosure

And If I Don't

- For failure to prevent unlawful/unauthorized access/use/disclosure, DPH may assess administrative penalties:
  - *Up to* $25,000 *per patient,* and
  - *Up to* $17,500 per subsequent violation of that patient's medical information
- DPH shall consider:
  - history of compliance
  - other laws
  - extent to which facility detected violations and took prompt action, and
  - factors outside the facility's control

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

And If I Don't

- For failure to report privacy violations to DPH and to the affected patient within 5 days, DPH may assess a penalty:
  - $100 for each day not reported as required
- Total combined penalties (for breach and failure to report) shall not exceed $250,000 "per reported event"
  - "Reported event" means all breaches included in any single report that is made to DPH, regardless of the number of breach events contained in the report

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

HealthLeaders Media May 15, 2009

Kaiser Fined $250,000 for Disclosing Octo-Mom Medical Record

Comment Email Print RSS News Widget ShareThis

Cheryl Clark, for HealthLeaders Media, May 15, 2009

Kaiser Permanente Bellflower Hospital in Los Angeles has been assessed a $250,000 fine because 23 employees at a number of Kaiser facilities with access to electronic medical records unlawfully breached the privacy of a patient who gave birth to octuplets earlier this year.

It is the first fine of its kind under a new state law that went into effect Jan. 1 designed to protect patient privacy, state officials said today.

Under another state law, the 23 individuals who engaged in the breach were referred for investigation and other charges could be filed by another state agency, the Office of Health Information Integrity. There also is the possibility that those responsible could see the loss or suspension of their medical licenses.

"As a byproduct of that investigation, Kaiser terminated one employee, 14 resigned, and eight received disciplinary action," said Kathleen Billingsley of the California Department of Public Health, Center for Health Care Quality.

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

LA Times June 16, 2009

Kaiser Bellflower is fined $187,500 for privacy breach [Updated]

July 16, 2009 | 11:43 am

The Kaiser Permanente hospital in Bellflower has been hit with a $187,500 fine for failing for a second time to prevent unauthorized access to confidential patient information, state pubic health officials said today.

[**Updated at 3 p.m.:** A spokesman for the hospital said the fine was part of the ongoing investigation into employees improperly accessing the medical records of Nadya Suleman and her children. Disciplinary action has been taken against the employees, said Jim Anderson, a hospital spokesman. All the incidents occurred in January; a previous post said they had occurred in April and May.]

State officials said Kaiser Permanente Bellflower Medical Center compromised the privacy of four patients when eight employees improperly accessed records. This is the second penalty against the hospital, officials said.

The hospital was fined $250,000 in May for failing to keep employees from snooping in the medical records of Nadya Suleman, the woman who set off a media frenzy after giving birth to octuplets in January.

The fine was the first penalty imposed and largest allowed under a new state law enacted last year after the widely publicized violations of privacy at UCLA Medical Center involving Farrah Fawcett, Britney Spears, California First Lady Maria Shriver and other celebrities.

"We are very concerned with violations of patient confidentiality and their potential harm to the residents of California," said Dr. Mark Horton, director of the California Department of Public Health. "Medical privacy is a fundamental right and a critical component of quality medical care in California."

--Ruben Vives

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

Can I Fight It?

- Facilities can dispute penalty assessments for breach and failure to report
  - Request a hearing w/in 10 days of receipt of penalty assessment
  - Hearings are held in Sacramento before an administrative law judge selected by DPH
    - Same process as for appealing immediate jeopardy penalties

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

Can I Fight It? 75% Solution

- In lieu of disputing a determination the facility can pay ***75%*** of the penalty w/in 30 days of receipt of the penalty assessment

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

The HITECH Act – Breach Reporting

- Requires HIPAA covered entities and personal health record providers to report breaches of "unsecured protected health information"
- FTC published final rule for PHR providers August 25, 2009
  http://www.dwt.com/LearningCenter/Advisories?find=126206
- HHS published interim final rule for covered entities August 24, 2009
  http://www.dwt.com/LearningCenter/Advisories?find=130345
  - Effective September 23, with 60-day comment period
  - HHS will delay enforcement 180 days

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

The HITECH Act – Breach Reporting

Unsecured protected health information is protected health information that has not been encrypted or destroyed

- Initial guidance issued April 17, 2009; updated in interim final regs
- NIST encryption standards for electronic data in use
- Shredding or destruction of hard-copy media
- NIST standards for purging or destruction of electronic media

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

The HITECH Act – Breach Reporting

Conditions for reporting

- Breach must be violation of the Privacy Rule
- Breach must pose significant risk of harm
  - To whom disclosed
  - Possibility of mitigation
  - Type and amount of information disclosed
- Risk analysis must be documented if no disclosure made

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

The HITECH Act – Breach Reporting

Exceptions to reporting:

- Good faith unintentional access by authorized person
- Inadvertent disclosure by one authorized person to another
- Unauthorized disclosure to a person who cannot reasonably retain it

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

The HITECH Act – Breach Reporting

Report must be given to—

- The individual
- Prominent media outlets if ≥500 residents of the state are affected
- HHS concurrently if ≥500 individuals are affected; otherwise annual log (including for 2009)

http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

The HITECH Act – Breach Reporting

- Report form:

http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html

- Summary of posted reports:

http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/postedbreaches.html

The HITECH Act – Breach Reporting

Notice must describe:

- What happened (including date of breach and date of discovery)
- Types of information involved
- Mitigation efforts
- Contact information

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

The HITECH Act – Breach Reporting

- Notice must be given without unreasonable delay, and no later than 60 days following discovery (i.e., when breach is known or should have been known with reasonable diligence)

- Notice must be delayed at request of law enforcement official for the period requested (but the request must be written for a delay of more than 30 days)

The HITECH Act – Breach Reporting

Notice must be given by first-class mail, except:

- Email notice is permitted if the individual has agreed to electronic notice
- Substitute notice if the CE does not have contact information
  - If < 10 individuals, by written notice, telephone or other means
  - If ≥ 10 individuals, by
    - Conspicuous posting on web site home page for 90 days, or
    - Conspicuous posting in major print or broadcast media

  With toll-free telephone number

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

The HITECH Act – Breach Reporting

Business associates—

- Required to notify CE without unreasonable delay and in any event within 60 days
- Required to provide information that the CE must include in notification (but should not delay initial notification while they collect this information)

Covered entities deemed to discover breach—

- If the BA is an agent, when the BA discovers it (or is deemed to discover it)
- If the BA is an independent contractor, when the BA notifies the CE

The HITECH Act – Breach Reporting

- Begin logging data breaches
- Assign compliance responsibility
- Prepare policies and procedures
  - Detection and investigation of breaches
  - Determining whether reportable
    - HIPAA analysis
    - Exceptions
    - Risk assessment
  - Coordinating with state reporting requirements
- Develop form of notice
- Train workforce
- Communicate with business associates
- Check security, especially portable media

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

State Security Breach Notification Laws

HIPAA pre-emption rule applies

- State laws survive unless it is impossible to comply with both, or the state law stands as an obstacle to the federal law

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

FACT Act Red Flag Rules

- "Red Flags" – reports, notices, and suspicious events that suggest possible identity theft
- RFR require written program to detect, prevent and mitigate identity theft
- Board of Directors must approve and provide oversight

FACT Act Red Flag Rules

- Identity Theft Red Flag Rules promulgated November 2007 pursuant to the Fair and Accurate Credit Transaction Act of 2003
  - "Creditors" with "covered accounts" must have identity theft prevention programs in place by June 1, 2010
  - Health care providers are "creditors" if they extend credit

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

Questions?

Speaker Contact Information:

Paul Smith

paulsmith@dwt.com, 415.276.6532

Davis Wright Tremaine LLP

DEFINING SUCCESS TOGETHER