manatt

Heightened Data Privacy Risks for Healthcare Organizations

Robert Belfort
Manatt, Phelps & Phillips, LLP
212.830.7270
rbelfort@manatt.com
April 7, 2010

Causes of Heightened Data Privacy Risks

manatt

- Increased HIPAA Civil Penalties
- More Aggressive HIPAA Civil Enforcement by HHS
- New Role of State Attorneys General
- Clearer Authority for HIPAA Criminal Enforcement
- Direct Regulation of Business Associates
- Breach Notification Obligations
- Expanded Role of FTC in Privacy Enforcement

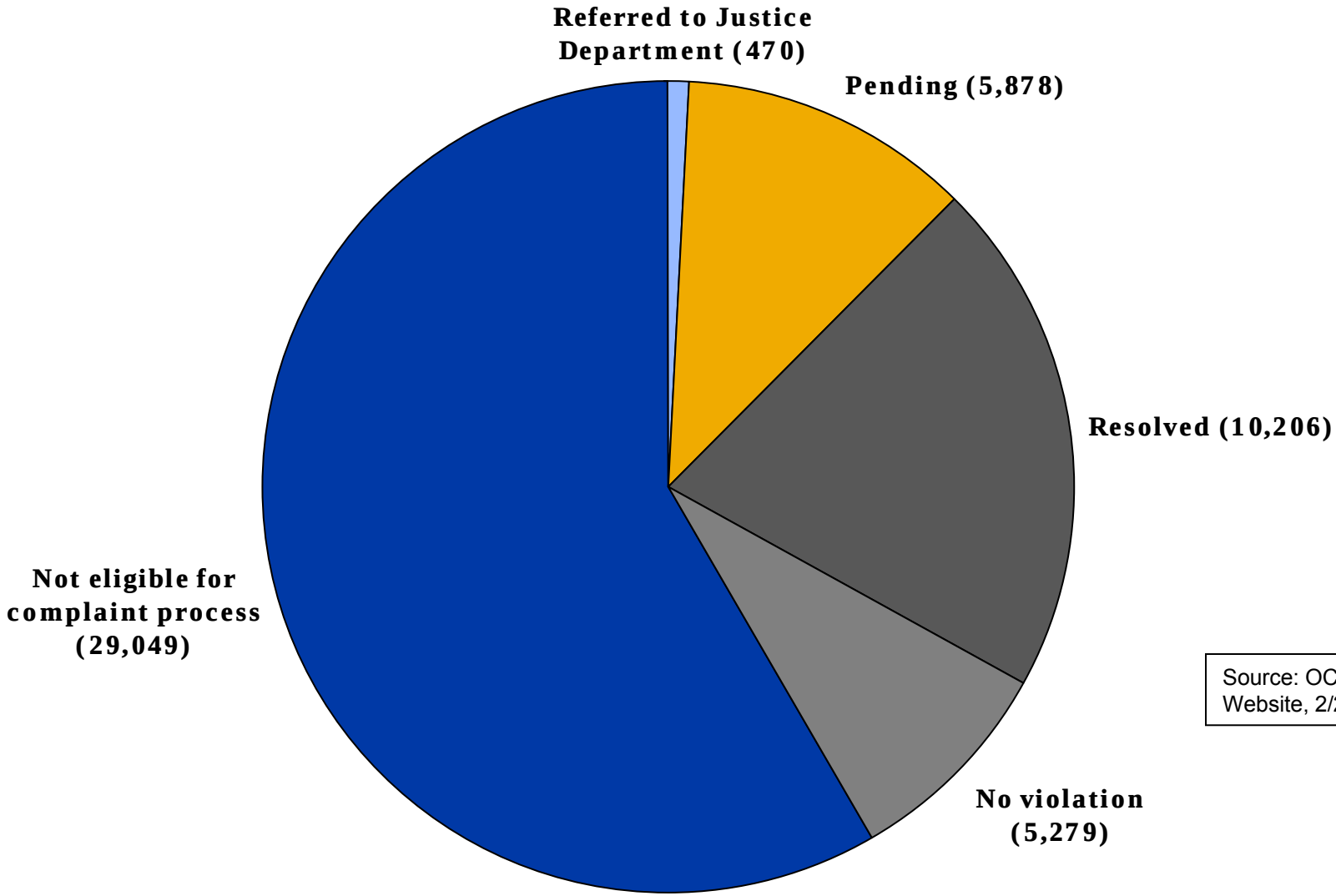
Increased HIPAA Civil Penalties

manatt

Level of Culpability	Minimum/Maximum Civil Penalty Par Violation	Maximum Annual Penalty for Type of Violation
Entity did not know and could not have reasonably known of the violation	$100/$50,000	$1,500,000
Violation due to reasonable cause but not willful neglect	$1,000/$50,000	$1,500,000
Violation based on willful neglect but corrected upon notice from HHS	$10,000/$50,000	$1,500,000
Violation based on willful neglect and not corrected upon notice from HHS	$50,000	$1,500,000

History of HIPAA Civil Enforcement: Disposition of Privacy Complaints

manatt



Source: OCR Website, 2/28/10

HIPAA "Resolution Agreements"

manatt

Covered Entity	Date of Settlement	Alleged Violation	Monetary Payment	Other Remedies
Providence Health	7/16/08	Lost laptops and tapes containing unencrypted PHI	$100,000	• Corrective action plan • 3-year monitoring
CVS	1/16/09	Disposal of prescription labels in publicly accessible dumpster	$2.25 million	• Corrective action plan • 3-year monitoring

Other Potential Effects of HITECH

manatt

- Mandatory civil penalties for violations involving willful neglect (effective 2/17/11)
- Mandatory GAO report by 8/17/10 on methodology for sharing civil penalties with affected individuals (becomes effective 2/17/12)
- Directive for HHS to conduct "periodic audits"
  - No privacy audits to date
  - CMS began security audits in 2008 after OIG's audit of Piedmont Hospital and public criticism of CMS
  - CMS published October 2008 report of security audit findings

Civil Enforcement Authority of State Attorneys General

manatt

- Damages are capped at $100 per violation/$25,000 for all identical violations per year
- Attorney fees may be payable
- AGs can request injunctive relief

Connecticut Attorney General HealthNet Case

manatt

- Lost disk drive containing unencrypted PHI (including SSNs) of 446,000 individuals
- 6-month delay in notifying individuals of breach
- AG claims in January 2010 action:
  - Failure to maintain adequate safeguards under HIPAA
  - Failure to notify affected individuals under CT law
- AG remedies:
  - Civil penalties under HIPAA and CT law
  - Mandatory encryption

Lessons Learned from HealthNet Case

manatt

- Heightened vulnerability of portable media and devices. Did PHI (including SSNs) of 446,000 people have to be maintained on disk drive?
- Although not a "required" standard under the HIPAA Security Rule, encryption is effectively becoming mandatory for data maintained on portable media and devices.
- Preferable not to adopt policy rather than ignore policy that was adopted.
- Absence of log file delayed assessment of breach.

Pre-HITECH HIPAA Criminal Liability Language

"(a) A person who knowingly and in violation of this part

(1) uses or causes to be used a unique health identifier

(2) obtains individually identifiable health information relating to an individual; or

(3) discloses individually identifiable health information to another person,

shall be punished as provided in subsection (b) of this section."

42 U.S.C. § 1320d-6

HITECH Language on HIPAA Criminal Penalties

manatt

"For purposes of the previous sentence, a person (including an employee or other individual) shall be considered to have obtained or disclosed individually identifiable health information in violation of this part if the information is maintained by a covered entity . . . and the individual obtained or disclosed such information without authorization."

HITECH, Section 13409

HIPAA Criminal Cases

manatt

Case	Alleged Facts	Disposition
U.S. v. Gibson	Employee of Seattle Cancer Care Alliance used PHI to fraudulently obtain credit cards.	Guilty plea on August 19, 2004.
U.S. v. Ramirez	Employee of medical practice sold PHI to FBI agents posing as drug traffickers.	Guilty plea on March 6, 2006.
U.S. v. Williams	Employee of billing company sold PHI to co-conspirator.	Guilty plea on April 26, 2006.
U.S. v. Ferrer and Machado	Employee of Cleveland Clinic (FL) gave PHI to co-defendant to submit fraudulent Medicare claims.	Guilty verdict after trial on April 27, 2007.

HIPAA Criminal Cases

manatt

Case	Alleged Facts	Disposition
U.S. v. Smith	Clinic nurse disclosed PHI to husband for use in legal proceeding against patient.	Guilty plea on December 4, 2008.
U.S. v. Howell	Employee of counseling center gave PHI to co-conspirators for credit card fraud.	Guilty plea on August 22, 2008.
U.S. v. Zhou	Former UCLA Medical Center researcher viewed PHI of celebrities without valid purpose.	Guilty plea on January 13, 2010.
U.S. v. Jackson	Administrative employee at UCLA Medical Center sold PHI about celebrities to National Inquirer.	Defendant died before trial.

Lessons Learned from Criminal Cases

manatt

- No covered entities convicted
- Absence of criminal (or civil) enforcement against institutions likely due to fact that:
  - Improper conduct was carried out by low level personnel
  - Covered entities had reasonable policies and employee training in place
  - Covered entities did not benefit from improper conduct
- Risk of organizational criminal liability highest if disclosure occurs as part of authorized company activity

Direct Regulation of Business Associates

manatt

- Security rule administrative, physical and technical standards apply to business associates "in the same manner" as applicable to covered entities
- Business associates must comply with business associate agreement and HITECH privacy provisions
- Business associates must seek cure and terminate/report covered entities for pattern of activity or practice that constitutes material breach of business associate agreement
- Business associates subject to civil penalties for violating any of the above requirements
- Clarification of criminal liability of business associates

Emerging Issues in Breach Notification

manatt

- Uncertainty caused by the "risk of harm" standard
  - When is it triggered?
  - Will it be revised?
  - Will states interpret their breach notification laws' "compromise the security" language in the same manner?
- Business associate as "agent" for calculating 60-day notice period
- Credit monitoring as emerging de facto requirement?
- Growing use of breach notification vendors
- Acquisition of breach insurance

Observations From First Publication of Reported Braches by HHS

manatt

- 41 breaches on HHS list
- Number of affected individuals ranges from 501 to 500,000
- Wide variety of covered entities affected
- 10 cases appear to involve breaches by business associates
- Majority of breaches involve theft of paper records, physical medium (CD or tape) or device (laptop)
- Only 2 relate to hacking, phishing or other external technical penetration

New Obligations of PHR Vendors

manatt

- No "risk of harm" standard in breach notification rule
- Confusion about when PHR vendors interfacing with health care providers or health plans are business associates
- Special challenges in contacting consumers who have not provided street address
- Potential for regulation beyond breach notification
  - California's expanded definition of "health care provider" covers entities whose primary purpose is maintaining medical information for patients or providers
  - HITECH directive to study expanded regulation of non-covered entities

Expanded Role of FTC in Privacy Enforcement

manatt

- Initial claims of "deceptive" acts or practices under FTC Act based on misrepresentation of policies or safeguards, not violation of substantive privacy standards
- More recent claims also rely on "unfairness" prong of FTC Act
- Major FTC health care privacy cases:
  - CVS (2009)
  - Eli Lilly (2002)
  - Online pharmacy case (2000)
- New authority for overseeing breach notification by PHR vendors

Thank You

Robert Belfort
Manatt, Phelps & Phillips, LLP
7 Times Square
New York, NY 10036

212.830.7270
rbelfort@manatt.com