A Breach Is Just the Beginning: Privacy and Security Enforcement Trends

HCCA Washington D.C. Regional Conference
March 10, 2017

Adam Greene, JD, MPH
Partner, Davis Wright Tremaine

Davis Wright Tremaine LLP

Agenda

- The HIPAA Audit Program
- Increased OCR Enforcement Actions
- Data Breach Class Action Lawsuits

HIPAA Audit Program

Current Phase 2 Audit Dates

- March 21, 2016 – OCR sends first e-mail verifications
- April 4, 2016 – OCR sends first pre-screening questionnaires
- May 20, 2016 – OCR sends largest batch of e-mail verifications
- July 11, 2016 – OCR sends desk audit requests to 167 covered entities (CEs)
- July 13, 2016 – OCR presents webinar for auditees
- ~ November 30, 2016 – OCR's sends desk audit requests to 45 business associates
- ~ Feb. 23, 2017 – Some CE draft audit reports are sent out
- 2017 [?] – Onsite audits to begin

Initial Desk Audit Subjects: Covered Entities

Privacy/Breach	Security
• Notice of Privacy Practices • Right of Access • Timeliness of Breach Notification • Content of Breach Notification	• Risk Analysis • Risk Management

Sample Data Requests

- Upload policies and procedures regarding the entity's risk analysis process.
- Consistent with 164.316(b)(2)(i), upload documentation demonstrating that policies and procedures related to the implementation of this

documentation related to the implementation of this implementation specification is available to the persons responsible for implementing this implementation specification

persons responsible for implementing this implementation specification and that such documentation is periodically reviewed and, if needed, updated.

- Upload documentation of the current risk analysis and the most recently conducted prior risk analysis.
- Upload documentation of current risk analysis results.

Sample Audit FAQ

Q: What would be an example of proof that the risk analysis was available to the workforce members?

For example, to show that individuals or groups requiring electronic access to risk analysis documentation (i.e., IT teams, security teams, management, legal counsel, etc.) screen shots could be used to show the availability of the risk analysis documentation by showing document properties, mapped drive permissions, etc.

counsel, etc.) screen shots could be used to show the availability of the risk analysis documentation by showing document properties, mapped drive permissions, etc. that indicate that the individuals or groups required to have access to such documents have such access.

Desk Audit Tips

- Ensure "@hhs.gov" e-mails are not blocked (including OSOCRAudit@hhs.gov)
- Going forward, start collecting additional information from BAs and maintaining centralized list.
- Confirm policies and procedures and supporting documentation is in place for likely future audit areas:
  - Device and media controls
  - Transmission security
  - Privacy safeguards
  - Privacy training
  - Encryption and decryption of data at rest
  - Facility access controls

Onsite Audits

- Onsite, comprehensive audits will use the revised audit protocol available at http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/
- "Some desk auditees may be subject to a subsequent onsite audit."
- Will include an entrance conference and a three- to five-day site visit.
- Entities will have ten business days to respond to draft report.

Onsite Audit Tips

- Use the revised audit protocol to prepare.
- Treat preparation as a significant project and allocate resources accordingly.
- Don't get onsite audit tunnel vision – breach preparedness may be more important compliance priority.

Increased OCR Enforcement Actions

Enforcement Highlights

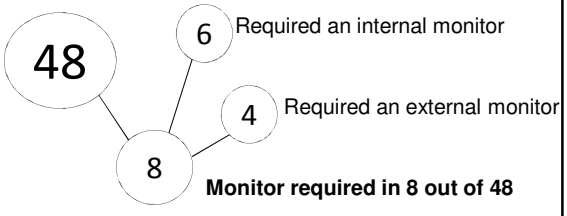
45	OCR Settlements

$58,455,200
In settlements and CMPs

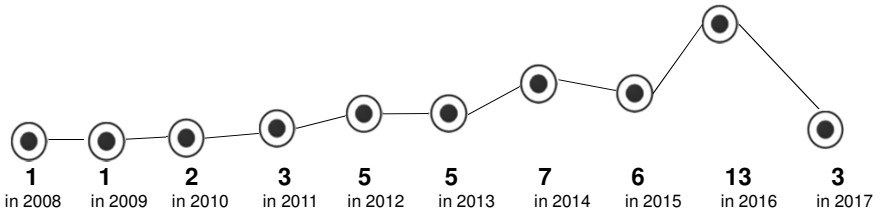
3	Civil Monetary Penalty Actions

$1,299,004
Average settlement amount

31 of **48**
enforcement actions arose from breach reports to HHS



Enforcement Highlights



1	1	2	3	5	5	7	6	13	3
in 2008	in 2009	in 2010	in 2011	in 2012	in 2013	in 2014	in 2015	in 2016	in 2017

(as of February 1, 2017)

Average minimum length of a corrective plan:
APPROXIMATELY 2 YEARS

Average attorney general enforcement action:
$347,909*

*may represent financial settlements associated with claims unrelated to HIPAA violations

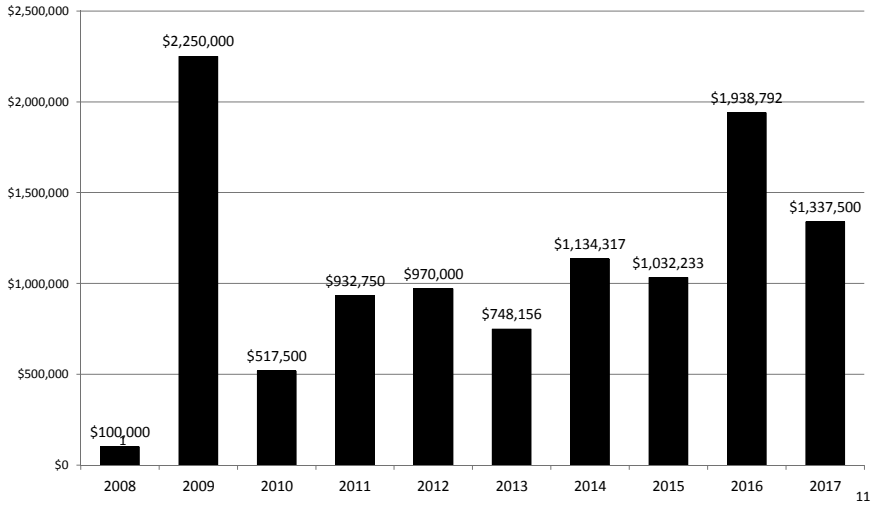
12 actions by state attorneys general/ in just over 6 years:

5 Massachusetts	2 New York	1 Vermont
2 Connecticut	1 Indiana	1 Minnesota

13

dwt.com

Average Settlement Amount

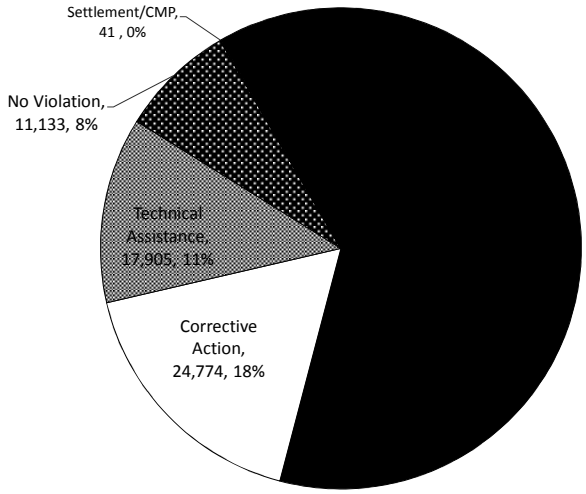


11

14

dwt.com

Enforcement Highlights (as of 12/31/16)



Data Breach Class Action Lawsuits

Class Actions – Most Dismissed Due to Lack of Standing

"The court in the related Maryland class action reached [the] same conclusion, granting the defendants' motion to dismiss for lack of subject matter jurisdiction on standing grounds. It rejected the plaintiffs' argument that the breach increased their risk of future harm because '**most courts to consider the issue 'have agreed that the mere loss of data – without any evidence that it has been either viewed or misused – does not constitute an injury sufficient to confer standing**.'' … This Court likewise concludes that Plaintiffs have not demonstrated a sufficiently substantial risk of future harm stemming from the breach to establish standing."

- *Attias v. CareFirst, Inc.*, 1:2015cv00882 - Document 40 (D.D.C. 2016)

Class Actions – Some Settlements

Limited Plaintiff Successes Absent Clear Damages

- *AvMed* $3 million settlement (1.2 million affected customers, claim of unjust enrichment based on premiums allegedly not going towards adequate information security) (2014)
- *Stanford* $4 million settlement (20,000 patients, settlement mostly paid by Stanford's vendors) (2014)

Section 5 of the FTC Act

"The central focus of any inquiry regarding unfairness is consumer injury … a finding of unfairness requires that the injury in question be 'substantial.' … We conclude that the disclosure of sensitive health or medical information causes additional harms that are neither economic nor physical in nature but are nonetheless real and substantial and thus cognizable under Section 5(n)."

- Opinion of the Commission, In the Matter of LabMD, Inc.

HITECH Act

ESTABLISHMENT OF METHODOLOGY TO DISTRIBUTE PERCENTAGE OF CMPS COLLECTED TO HARMED INDIVIDUALS.—

Not later than 3 years after the date of the enactment of this title [enacted 2/19/2009], the Secretary shall establish by regulation … a methodology under which an individual who is harmed by an act that constitutes an offense … may receive a percentage of any civil monetary penalty or monetary settlement collected with respect to such offense.

Class Actions: Welcome to California

You suffer a breach that affects 125,000 California residents.

Class Actions: Welcome to California

38. Plaintiff and the Class seek nominal damages of one thousand dollars ($1,000) per violation pursuant to California Civil Code section 56.36(b)(1), actual damages per violation pursuant to California Civil Code section 56.36(b)(2), punitive damages up to three thousand dollars ($3,000) per violation pursuant to California Civil Code section 56.35.

39. Plaintiff and the Class seek recovery of attorneys' fees of up to one thousand dollars ($1,000) per violation pursuant to California Civil Code section

7. Negligence;
8. Breach of Implied Contract; and
9. Unjust Enrichment.

Jury Trial Demanded As To Claims That Are So Triable

Defendants.

Welcome to California …

125,000 x ($1,000 + $3,000 + $1,000) =
$625M

Class Actions: Welcome to California

But courts have avoided awarding damages in several California cases:

- In *Regents of UC*, court found that "release" requires proving that confidential nature of medical information was breached, not merely the loss of possession of the information.
- Similarly, in *Sutter Health*, court held that evidence must show that medical information was actually viewed.
- In *Eisenhower Med. Ctr.*, court held that patient demographic information was not "medical information."

Yet other states may be considering "nominal damages" for breaches. Stay tuned …

For questions …

Adam H. Greene, JD, MPH

Davis Wright Tremaine LLP

adamgreene@dwt.com
202.973.4213