

New Frontiers In HIPAA & Privacy Enforcement:

State Courts, FTC, and OIG

Victoria L. Vance

Edward E. Taber

1. Dramatic Increase In Breaches

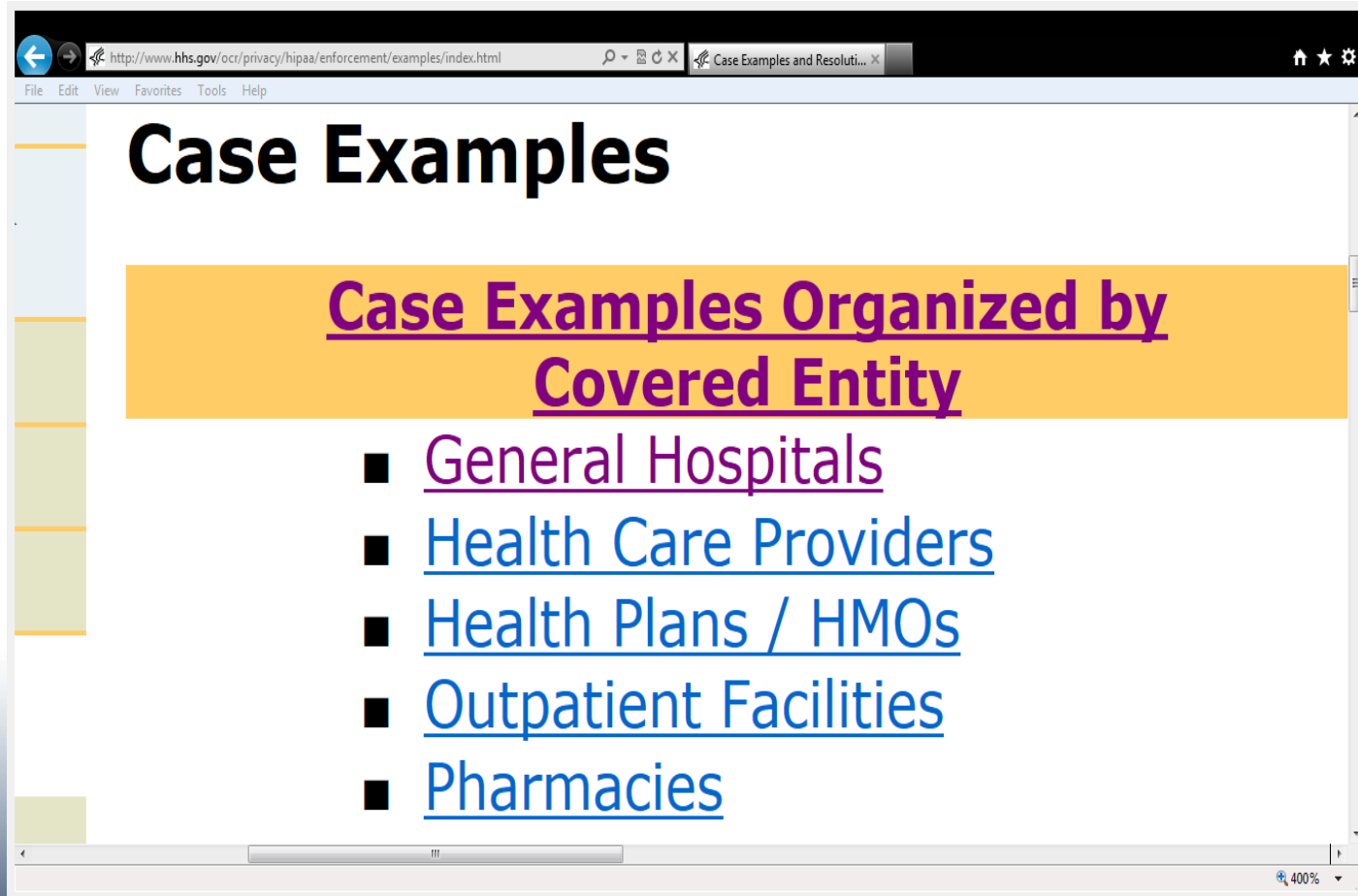


Dramatic Increase In Breaches



The screenshot shows a web browser window displaying the HHS.gov website. The address bar shows the URL: <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examp>. The page title is "Case Examples and Resoluti...". The main navigation bar includes "U.S. Department of Health & Human Services", "HHS.gov", and the tagline "Improving the health, safety, and well-being of America". Below this is a search bar and navigation links for "HHS Home", "HHS News", and "About HHS". The page is titled "Health Information Privacy" and has three tabs: "Office for Civil Rights", "Civil Rights", and "Health Information Privacy". The breadcrumb trail is: [OCR Home](#) > [Health Information Privacy](#) > [Enforcement Activities & Results](#) > [Case Examples & Resolution Agreements](#). The main content area is titled "Case Examples and Resolution Agreements" and contains the following text: "These examples show how covered entities can effectively comply with the requirements of the Privacy and Security Rules. Periodically, we update this page with case examples of the corrective actions that OCR obtains from covered entities through our enforcement efforts." Below this text are two columns of links. The left column is titled "Case Examples Organized by Covered Entity" and lists: [General Hospitals](#), [Health Care Providers](#), [Health Plans / HMOs](#), [Outpatient Facilities](#), [Pharmacies](#), and [Private Practices](#). The right column is titled "Case Examples Organized by Issue" and lists: [Access](#), [Authorizations](#), [Business Associates](#), [Conditioning Compliance with the Privacy Rule](#), [Confidential Communications](#), [Disclosures to Avert a Serious Threat to Health or Safety](#), [Impermissible Uses and Disclosures](#), [Minimum Necessary](#), [Notice](#), and [Safeguards](#). At the bottom of the page, there is a section for "Resolution Agreements" with a small image of a scale. The browser's status bar at the bottom shows "100%".

Dramatic Increase In Breaches



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

Case Examples

Case Examples Organized by Covered Entity

- General Hospitals
- Health Care Providers
- Health Plans / HMOs
- Outpatient Facilities
- Pharmacies

400%

Recently Reported Breach Incidents

- The MetroHealth System (May 15, 2015) – malware discovered on three Cardiac Cath Lab computers; a BA had disabled antivirus software on the computers during a software upgrade.
- Hattiesberg Clinic (April 2, 2015) – former employer (O.D. provider) accessed patient demographics to notify them of his new employer and practice location.
- Aspire Indiana (February 10, 2015) – several unencrypted laptops stolen, containing PHI and SSN, and identifying information; 45,000 patients and employees affected.

Major Care Insurers Affected

- Anthem (February 5, 2015) – 79 million subscribers affected.
- Premera Blue Cross (March 17, 2015) – 11 million customers.
- CareFirst (May 20, 2015) – 1.1 million customers
- FBI investigating; health care organizations are “soft targets”

Also At Risk . . .

- Dozens of health care companies and corporate deal advisers (including law firms).

Breach By The Numbers

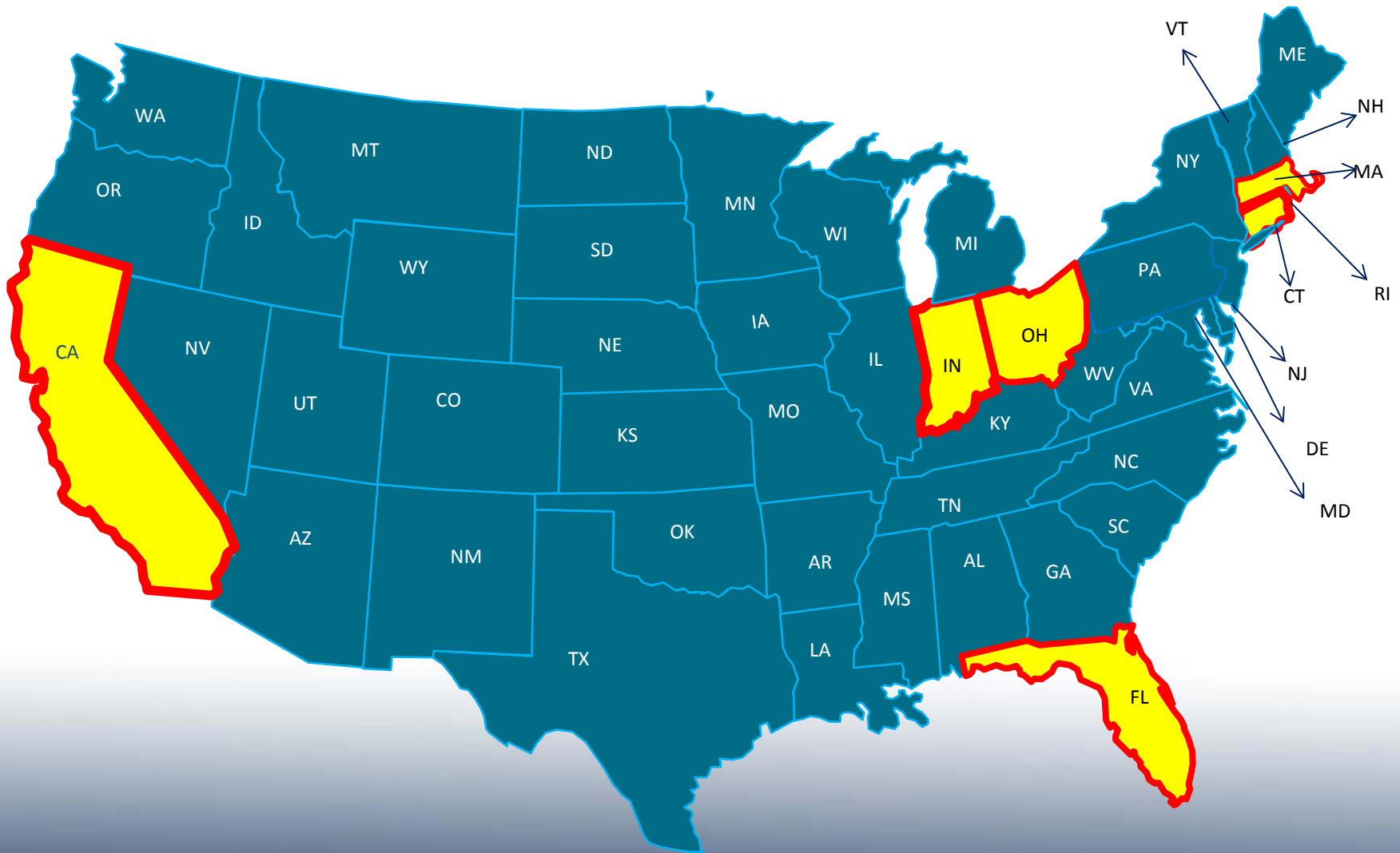
- Since 2009:
- 1,100 health data breaches
- 120 million individuals affected
https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
- Ponemon Institute's 2015 survey shows **91%** of healthcare organizations and **59%** of Business Associates have experienced a data breach
<http://www.ponemon.org/blog/criminal-attacks-the-new-leading-cause-of-data-breach-in-healthcare>

Staggering Costs:

- HITECH violation fines up to **\$1.5M**
- Breach costs **\$5.6B** in 2015
- Economic impact of medical identity theft **\$30.9B** annually

<http://www.experian.com/data-breach/healthcare-data-breach.html>

2. States Are Stepping In



Connecticut – *Byrne v. Avery Ctr. For Ob & Gyn* (Nov. 11, 2014)

- HIPAA lacks a private right to action. But . . .
- HIPAA regulations may be used to set the Standard of Care for state negligence claims.
- Negligence and Emotional Distress Claims allowed.
- Predict: Increase suits against Covered Entities and Business Associates.



Indiana – *Walgreen Co. v. Hinchy* (Nov. 14, 2014)

- Landmark Decision: Walgreen liable under state negligence law for employee's misconduct.
- \$1.4 M verdict upheld.



Florida – *Murphy v. Dulay* (Oct. 10, 2014)

- Expansive presuit PHI disclosure (records and physician interviews) not preempted by HIPAA.



California

- New California statute regulating medical software companies and privacy



Ohio

***Biddle v. Warren Gen. Hosp.* 1999**

***Gomcsak v. Dawson* 2002**

***Hageman v. Southwest* 2008**

***Med. Mut. v. Schlotterer* 2009**

***Turk v. Oiler* 2010**

**Med mal cases: Plaintiffs use
HIPAA to resist discovery**



Additional Agency Enforcement Actions

- Mass. AG (Nov. 24, 2014): Beth Israel Deaconess Med. Center pays fine and accepts Consent Judgment to Settle State Consumer Protection Act and Data Security Act violations. (Fourth data breach enforcement action by Mass. AG.)
- Indiana AG enforced HIPAA for first time (Jan. 2015).

FDA: Cybersecurity Guidance for Medical Devices (Oct. 2014)

- Manufacturers should develop cybersecurity controls to assure medical device security and maintain device functionality and safety.
 - limit access to devices to authenticated users; strengthen password protection; physically lock devices (if appropriate).
 - restrict software updates to authenticated code.
 - ensure secure data transfer to/from device.
 - include features that allow security threat to be detected, logged and acted upon.
- <http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf>

FTC: Settlement With Health Billing Company (Dec. 2014)

- Billing company deceptively obtained consumer's medical information when they signed up for billing portal to track health bills violated Section 5 of FTC Act.
- Sanction: Consent Order, forced to destroy all sensitive data, ban on misleading consumers.



3. Next Wave of PHI Protections

Strict Enforcement of Business Associates

- “Senior Health Partners (N.Y. health plan) blames BA for Breach.”
- Nurse’s laptop and unencrypted mobile phone stolen (Nov. 26, 2014).
 - OCR data: 25% - 64% of HIPAA breaches involve business associates.
 - Growing mistrust of BA’s ability to handle sensitive patient information.

Criminal Exposure Increasing

- Criminal attacks are number one cause of data breaches in healthcare.
- Individuals and Covered Entities can be prosecuted.
- 42 U.S.C. § 1320d-5.

Source: Ponemon Institute, “Fifth Annual Benchmark Study on Privacy and Security of Healthcare Data” (May 2015).

OIG Work Plan 2015

- NEW! Disaster Planning: Examine hospitals' compliance with HIPAA requirement to create contingency plans to protect PHI in emergencies.
- Ongoing: Do hospitals have adequate safeguards to protect sensitive PHI on medical devices that integrate with EMRs?

4. Essential Action Steps

1. People

- Employee training
- Monitor employee compliance
- Educate personnel on criminal penalties
- Create a Zero Tolerance Culture
- Address customer (patient, family, employee) concerns

Essential Action Steps

2. Processes

- Utilize in OCR's Security Rule Risk Assessment Tool
- Stay up to date on Patches and Upgrades
- Review and Audit BA compliance with Security and Privacy Rules
- Disaster Preparedness: include safeguards for PHI

Essential Action Steps

3. Product

- Tighten up privacy policies and ensure enforcement (CEs and BAAs)
- Follow best practices for drafting BAAs
- Update Privacy/Security Breach Incident Response Programs
- Ensure adequate insurance to cover emerging negligence and tort-based risks
- Portable devices: trace, encrypt, secure medical devices: heighten awareness of manufacturer obligations for marketing secure devices

RESOURCES

RESOURCES

Statutes/Regulations

- HIPAA
 - Pub. L. 104-91; 42 USC 1320d-1320d-8
 - Privacy Rule: 45 CFR Part 160, Part 164 (Subparts A and E)
 - Security Rule: 45 CFR Part 160, Part 164 (Subparts A and C)
 - Enforcement Rule: 45 CFR Part 160 (Subparts C-E)
- HITECH Act of 2009

Cases

- *Byrne v Avery Center for Ob & Gyn PC*, Supreme Court of Conn., Case No. SC 18904 (Nov. 11, 2014)
- *Murphy v Dulay*, U.S. Ct. App. 11th Cir., Case No. 13-14637 (Oct. 10, 2014)
- *Walgreen Co. v Hinchy*, Ct. App. Of Indiana, No. 49A02-1311-CT-950 (Nov. 14, 2014)(Opinion on Rehearing, Jan. 15, 2015)

RESOURCES

Guidance

- HHS, OIG Work Plan FY 2015 (p. 22)
- FDA, Content of Premarket Submissions for Management of Cybersecurity in Medical Devices (Oct. 2, 2014)

Data

- Ponemon Institute, *Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data* (May 2015)
- Experian, *2015 Second Annual Data Breach Industry Forecast*

Questions



Thank You!

Victoria L. Vance

victoria.vance@tuckerellis.com

216.696.3360

Edward E. Taber

edward.taber@tuckerellis.com

216.696.2365