Massachusetts Eye and Ear

After the Breach

Heather Fowles, CISSP, CISA
Mass. Eye and Ear

HIMSS Northern New England
November 2017

Massachusetts Eye and Ear

- 41-bed nonprofit specialty hospital located in Boston
- Focused on treatment of eye, ear, nose and throat conditions
- Harvard Medical School teaching affiliate for Ophthalmology and Otolaryngology

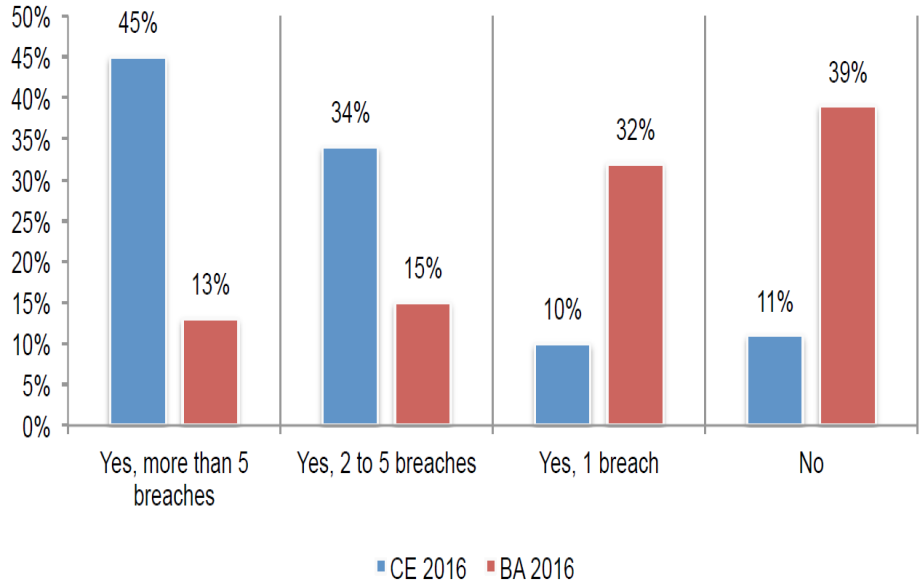
Humpty Dumpty Moments

Breaches are Common

Ponemon Institute:

- 89% of covered entities had at least one breach in last two years
  - 45% had five or more
- Not much better for business associates
- Leading causes – criminal attack, third-parties, stolen devices, employee negligence

Figure 14. Has your organization suffered a data breach involving the loss or theft of patient data in the past 24 months?



Source: ***Ponemon Institute***, *Sixth Annual Benchmark Study on Patient Privacy & Data Security (May 2016)*

Breaches are Common

Identity Theft Resource Center

- 2017 YTD, 300 publicized breaches at medical/healthcare organizations involving 4.8M records
- 27% of all reported breaches

Privacy Rights Clearinghouse – 1,073,490,127

- Records breached since 2005 (all industries)
- Medical/Healthcare: 48,073,014

Source:
Identity Theft Resource Center, *http://www.idtheftcenter.org/images/breach/2017Breaches/DataBreachReport2017.pdf*
Privacy Rights Clearinghouse, *https://www.privacyrights.org/data-breaches*

Information Technology Trends

- Consumerization
- Mobility
- Cloud
- IoT

Healthcare Trends

- Digitization
- Data Sharing
- Cost Containment

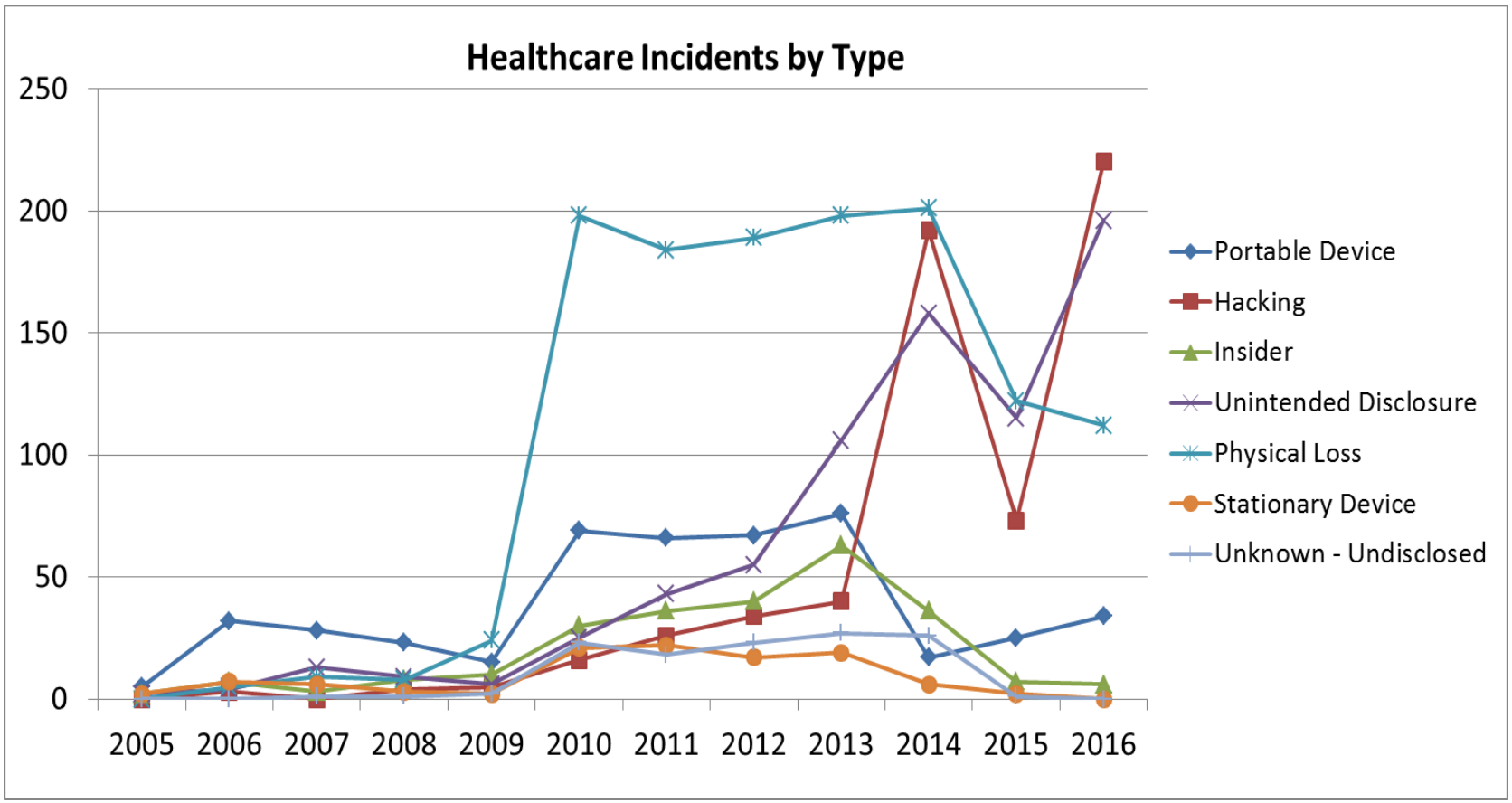
Regulatory

- HIPAA
- HITECH
- PCI-DSS
- State Breach Laws

New Threat Actors & Risks

- Cybercriminals
- Nation States/APTs
- Ransom Attacks

Shift in Breach Causes?



Source: Privacy Rights Clearinghouse, *https://www.privacyrights.org/data-breaches*

Breach Consequences

- **Response costs**
- **Reputational harm**
- **Regulatory / legal**
- **Interruption to operations & patient care**

Ponemon estimate: data breaches cost the U.S. healthcare industry over $6B annually

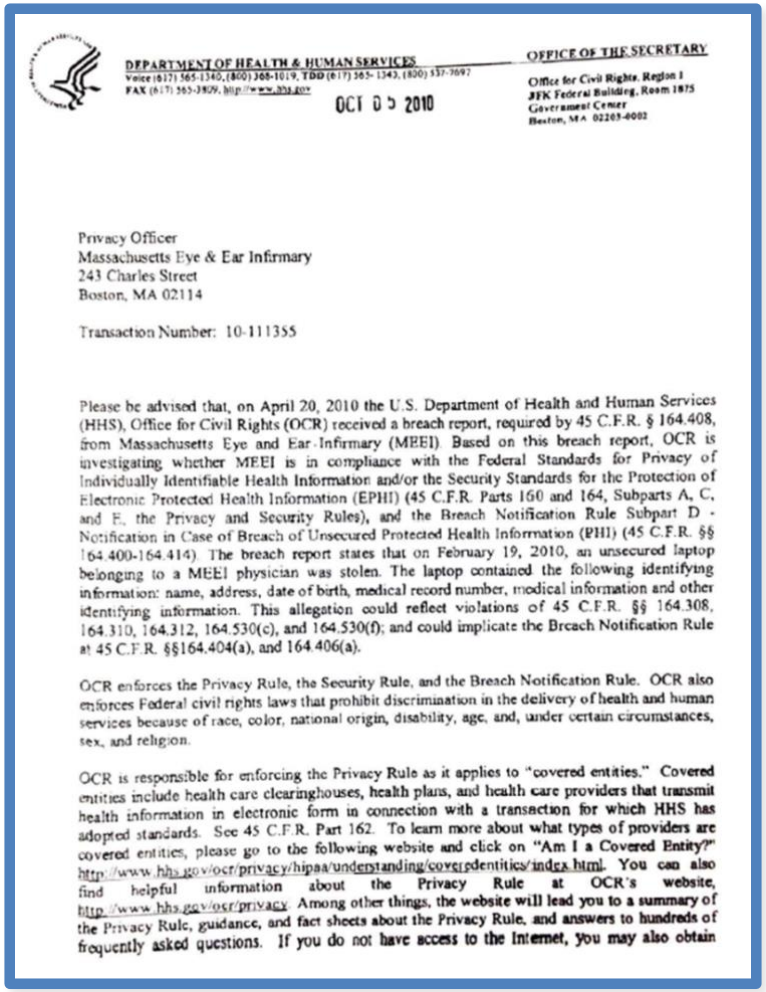
Source: ***Ponemon Institute***, *Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data (May 2016)*

Case Study - Stolen Laptop

- **February 2010:**
  - Laptop stolen overseas
- **March 2010:**
  - Theft reported to Mass. Eye and Ear IT and Privacy Office
- **April 2010:**
  - Incident reported to OCR
  - Statutory notices and offer of credit monitoring/identity theft insurance to affected patients

Stolen Laptop

- **October 2010:**
  - Letter initiating OCR investigation
  - Broad scope
  - Mass. Eye and Response to OCR



DEPARTMENT OF HEALTH & HUMAN SERVICES
Voice (617) 565-1340, (800) 368-1019, TDD (617) 565-1343, (800) 537-7697
FAX (617) 565-3809, http://www.hhs.gov

OFFICE OF THE SECRETARY
Office for Civil Rights, Region I
JFK Federal Building, Room 1875
Government Center
Boston, MA 02203-0002

OCT 05 2010

Privacy Officer
Massachusetts Eye & Ear Infirmary
243 Charles Street
Boston, MA 02114

Transaction Number: 10-111355

Please be advised that, on April 20, 2010 the U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR) received a breach report, required by 45 C.F.R. § 164.408, from Massachusetts Eye and Ear Infirmary (MEEI). Based on this breach report, OCR is investigating whether MEEI is in compliance with the Federal Standards for Privacy of Individually Identifiable Health Information and/or the Security Standards for the Protection of Electronic Protected Health Information (EPHI) (45 C.F.R. Parts 160 and 164, Subparts A, C, and E, the Privacy and Security Rules), and the Breach Notification Rule Subpart D - Notification in Case of Breach of Unsecured Protected Health Information (PHI) (45 C.F.R. §§ 164.400-164.414). The breach report states that on February 19, 2010, an unsecured laptop belonging to a MEEI physician was stolen. The laptop contained the following identifying information: name, address, date of birth, medical record number, medical information and other identifying information. This allegation could reflect violations of 45 C.F.R. §§ 164.308, 164.310, 164.312, 164.530(c), and 164.530(f); and could implicate the Breach Notification Rule at 45 C.F.R. §§164.404(a), and 164.406(a).

OCR enforces the Privacy Rule, the Security Rule, and the Breach Notification Rule. OCR also enforces Federal civil rights laws that prohibit discrimination in the delivery of health and human services because of race, color, national origin, disability, age, and, under certain circumstances, sex, and religion.

OCR is responsible for enforcing the Privacy Rule as it applies to "covered entities." Covered entities include health care clearinghouses, health plans, and health care providers that transmit health information in electronic form in connection with a transaction for which HHS has adopted standards. See 45 C.F.R. Part 162. To learn more about what types of providers are covered entities, please go to the following website and click on "Am I a Covered Entity?" http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html. You can also find helpful information about the Privacy Rule at OCR's website, http://www.hhs.gov/ocr/privacy. Among other things, the website will lead you to a summary of the Privacy Rule, guidance, and fact sheets about the Privacy Rule, and answers to hundreds of frequently asked questions. If you do not have access to the Internet, you may also obtain

Stolen Laptop

- **September 2012:**
  - Resolution Agreement with OCR
    - No admission / no concession
    - 3-year Corrective Action Plan (CAP)
    - Six areas of “covered conduct”
    - Pay $1.5M settlement to OCR
  - CAP requirements
    - Policies and procedures
    - Re-train workforce
    - Independent CAP Monitor
    - Additional controls, especially re portable devices

Stolen Laptop

- **January 2013:**
  - Mass. Eye and Ear submits revised policies and proposed Monitor to OCR for approval
  - OCR approves Monitor (PwC)
- **February - April 2013:**
  - Monitor plan development
- **March 2013:**
  - OCR approves policies and procedures
  - Implementation and workforce re-training begin

Stolen Laptop

- **May 2013:**
  - OCR approval of initial Monitor Plan
- **May 2013 – May 2016**
  - Monitoring
    - 6 Monitoring Periods
    - Scheduled audit every 6 months for ~2 weeks
    - Unannounced audit visits at any time to departments at main hospital and satellite practice locations

Stolen Laptop

- **CAP in retrospect:**
  - Significant financial impact to organization
  - Extensive investment in security program
    - User training and policy certification
    - Access administration
    - Network access control
    - Outsourced SOC/monitoring
    - Encryption of portable devices
    - Inventory management
    - Anti-phishing program

Stolen Laptop

- **Takeaways:**
  - You may be responsible for more than you think you are
  - Train staff to report incidents promptly
  - “Contain first” IR strategy
  - If you must report a breach
    - Don’t wait to address known weaknesses
  - If you receive a regulatory investigation letter
    - Put best team and effort into initial response
    - Don’t expect investigation to focus narrowly on breach
    - Be prepared to show compliance over time

Stolen Laptop

- **Takeaways:**
  - If you must enter into a CAP with monitoring
    - Better the devil you know
    - Agree up front on standards
    - Monitor opinion vs. report of issues
      - Audit rigor vs. audit transparency trade-offs
    - Negotiate the details

Stolen Laptop

- **Takeaways:**
  - Know organization's limits
    - Be realistic about resources
    - Go outside for commodity services
    - Don't underestimate effort for communication and process changes

Case Study – Credential Compromise

- **April 2016:**
  - Several employees report tax identity fraud
  - Initial investigation - do we have a problem?

- **May 2016:**
  - Log review and identification of compromise
  - Containment
  - New login restrictions / enhanced authentication

Credential Compromise

- **May 2016:**
  - Cyber-insurance claim
  - “Breach coach” and forensic investigators
  - Document retention order
  - Designated internal team
    - Security, IT, legal, communications, HR, executive management

Credential Compromise

- **May – June 2016:**
  - Forensic investigation
    - What and whose data was breached?
      - HR System logs
    - How did it happen?
      - Network/MSSP logs
      - Workstation data collection
      - Home computer data collection

Credential Compromise

- **June 2016:**
  - Management decisions
    - Credit monitoring and identity theft insurance
    - Call center and mailing services
    - Communication
  - Statutory notices
    - Requirements vary by state
      - Notice to affected employees
      - Notice to regulators
  - Reported to law enforcement

Credential Compromise

- **Incident in Retrospect:**
  - Cost to Mass. Eye and Ear
    - Insurance retention
    - Resource time
  - Impact on staff and dependents/beneficiaries
  - Further investment in security program
    - Expanded use of multi-factor authentication
    - Limits on access to system from Internet
    - Shift from security compliance to security risk orientation
  - Enhanced staff acceptance of need for security controls

Credential Compromise

- **Takeaways:**
  - You may be responsible for more than you think you are, part II
    - Vendors / business associates
    - Do you know where your PHI/PII is?
  - Train staff to report incidents promptly
  - “Contain first” IR strategy
  - If you must report a breach
    - Don’t wait to address known weaknesses

Credential Compromise

- **Takeaways:**
  - Put together the right team
    - Right for the organization
    - Right for the incident
    - Don’t forget communications
    - Consider outside services where appropriate
  - Cyber-insurance – get protected

Questions?