Recent HIPAA High-Points: What to know and what to do!

Iliana L. Peters, JD, LLM, CISSP
October 12, 2018

OCR Regional Offices

- New England Region – (Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island, Vermont): Susan Rhodes, Regional Manager
- Eastern and Caribbean Region – (New Jersey, New York, Puerto Rico, Virgin Islands): Linda Colón, Regional Manager
- Mid-Atlantic Region – (Delaware, District of Columbia, Maryland, Pennsylvania, Virginia, West Virginia): Barbara Holland, Regional Manager
- Southeast Region – Atlanta (Alabama, Florida, Georgia, Kentucky, Mississippi, North Carolina, South Carolina, Tennessee): Timothy Noonan, Regional Manager
- Midwest Region – (Illinois, Indiana, Iowa, Kansas, Michigan, Minnesota, Missouri, Nebraska, Ohio, Wisconsin): Steven Mitchell, Acting Regional Manager
- Southwest Region – (Arkansas, Louisiana, New Mexico, Oklahoma, Texas): Marisa Smith, Regional Manager
- Rocky Mountain Region – (Colorado, Montana, North Dakota, South Dakota, Utah, Wyoming): Andrea Oliver, Regional Manager
- Pacific Region – (Alaska, American Samoa, Arizona, California, Commonwealth of the Northern Mariana Islands, Federated States of Micronesia, Guam, Hawaii, Idaho, Marshall Islands, Nevada, Oregon, Republic of Palau, Washington): Michael Leoz, Regional Manager
  - Customer Response Center: (800) 368-1019
    - Fax: (202) 619-3818
    - TDD: (800) 537-7697
    - Email: ocrmail@hhs.gov

OCR ListServs

Privacy List Serv

- Visit the OCR-PRIVACY-LIST for a summary of archived announcements: https://list.nih.gov/cgi-bin/wa.exe?A0=OCR-PRIVACY-LIST

-OR-

- Subscribe, delete or update your subscription to the OCR Privacy Listserv

Security List Serv

- Visit the OCR-SECURITY-LIST for a summary of archived announcements: https://list.nih.gov/cgi-bin/wa.exe?A0=ocr-security-list

-OR-

- Subscribe, delete or update your subscription to the OCR Security Listserv

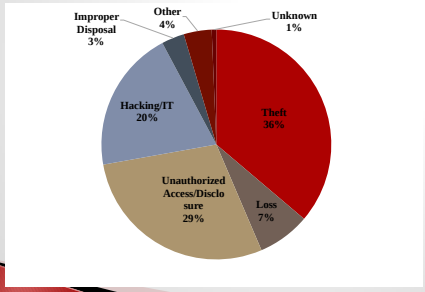
HIPAA Breach Highlights

September 2009 through June 30, 2018

- Approximately 2,363 reports involving a breach of PHI affecting 500 or more individuals
  - Theft and Loss are 43% of large breaches
  - Hacking/IT now account for 20% of incidents
  - Laptops and other portable storage devices account for 24% of large breaches
  - Paper records are 21% of large breaches
  - Individuals affected are approximately 263,666,592
- Approximately 351,753 reports of breaches of PHI affecting fewer than 500 individuals

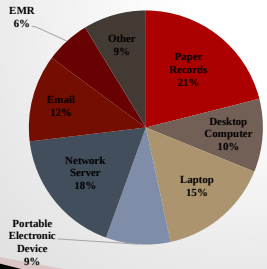
HIPAA Breach Highlights

500+ Breaches by Type of Breach
April 14, 2003 – June 30, 2018



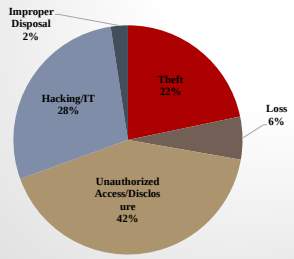
HIPAA Breach Highlights

500+ Breaches by Location of Breach
April 14, 2003 – June 30, 2018



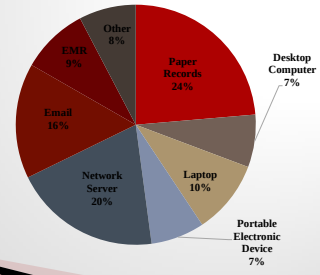
HIPAA Breach Highlights

500+ Breaches by Type of Breach
7/1/2015 – 6/30/2018



HIPAA Breach Highlights

500+ Breaches by Location of Breach
7/1/2015 – 6/30/2018



Breach Investigations

- OCR posts breaches affecting 500+ individuals on OCR website (after verification of report)
  - Public can search and sort posted breaches
- OCR opens investigations into breaches affecting 500+ individuals, and into number of smaller breaches
- Investigations involve looking at:
  - Underlying cause of the breach
  - Actions taken to respond to the breach (including compliance with breach notification requirements) and prevent future incidents
  - Entity's compliance prior to breach

Enforcement Highlights

April 14, 2003 – June 30, 2018

- Over 184,614 complaints received to date
- Over 26,071 cases resolved with corrective action and/or technical assistance
- Expect to receive 24,000 complaints this year

Enforcement Highlights

- In most cases, entities able to demonstrate satisfactory compliance through voluntary cooperation and corrective action
- In some cases though, nature or scope of indicated noncompliance warrants additional enforcement action
- Resolution Agreements/Corrective Action Plans
  - 55 settlement agreements that include detailed corrective action plans and monetary settlement amounts
- 4 civil money penalties

Recent HHS Enforcement Actions

- May 10, 2017: Memorial Hermann Health System (MHHS)
  - $2,400,000
  - Texas health system settles potential HIPAA violations for disclosing patient information
- May 23, 2017: St. Luke's Roosevelt Hospital System Inc.
  - $387,200
  - Careless handling of HIV information jeopardizes patient's privacy, costs entity $387k
- December 18, 2017: 21st Century Oncology
  - $2,300,000
  - $2.3 Million Levied for Multiple HIPAA Violations at NY-Based Provider
- February 1, 2018: Fresenius Medical Care North America (FMCNA)
  - $3,500,000
  - Five breaches add up to millions in settlement costs for entity that failed to heed HIPAA's risk analysis and risk management rules
- February 13, 2018: Filefax, Inc.
  - $100,000
  - Consequences for HIPAA violations don't stop when a business closes
- June 18, 2018: MD Anderson
  - $4.3 Million CMP
  - Judge rules in favor of OCR and requires a Texas cancer center to pay $4.3 million in penalties for HIPAA violations
- September 20, 2018: "Boston Med"
  - $999,000
  - Unauthorized Disclosure of Patients' Protected Health Information During ABC Television Filming Results in Multiple HIPAA Settlements

HITECH Audit Program

- Purpose: Identify best practices; uncover risks and vulnerabilities not identified through other enforcement tools; encourage consistent attention to compliance
  - Intended to be non-punitive, but OCR can open up compliance review (for example, if significant concerns are raised during an audit)
  - Also hope to learn from this next phase in structuring permanent audit program

HITECH Audit Program

History

- HITECH legislation: HHS (OCR) shall provide for periodic audits to ensure that covered entities and business associates comply with HIPAA regulations. (Section 13411)
- Pilot phase (2011-2012): comprehensive, on-site audits of 115 covered entities
- 2013: issuance of formal evaluation report
- 2016 & 2017: Phase 2 – between 200-250 desk audits of covered entities and business associates

HITECH Audit Program

Phase 2 Status

- Have completed
  - 166 covered entity desk audits
  - 41 business associate audits
- After Phase 2, on-site audits will be conducted as a part of the permanent audit program.
  - On-site audits will evaluate auditees against comprehensive selection of controls in the audit protocol:
  - https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/

CE Desk Audit Ratings

		Rating					
Element #	Provision	1	2	3	4	5	N/A
P55	Notice	2	34	40	11	16	0
P58	eNotice	59	16	4	6	15	3
P65	Access	1	10	27	54	11	0
BNR12	Timeliness	67	6	2	9	12	7
BNR13	Content	14	15	24	38	7	5
S2	Risk Analysis	0	9	20	21	13	0
S3	Risk Management	2	2	15	28	16	0

BA Desk Audit Ratings

		Rating					
Element #	Provision	1	2	3	4	5	N/A
BNR17	Notice to CEs	1	2	3	3	0	32
S2	Risk Analysis	3	5	15	12	6	0
S3	Risk Management	0	5	8	21	7	0

Recurring Compliance Issues

- Business Associate Agreements
- Risk Analysis
- Failure to Manage Identified Risk, e.g. Encrypt
- Lack of Transmission Security
- Lack of Appropriate Auditing
- No Patching of Software
- Insider Threat
- Improper Disposal
- Insufficient Data Backup and Contingency Planning

Questions?

- Feel free to contact me for more information:
  - Iliana Peters: ipeters@polsinelli.com