



Update on Administration and Enforcement of the HIPAA Privacy, Security, and Breach Notification Rules

**Office for Civil Rights (OCR)
U.S. Department of Health and Human Services**



Updates

- Breach Notification
- Enforcement
- Audit



BREACH HIGHLIGHTS AND RECENT ENFORCEMENT ACTIVITY



Breach Notification Requirements

- Covered entity must notify affected individuals, HHS, and in some cases, the media, of breach
- Business associate must notify covered entity of breach
- Notification to be provided without unreasonable delay (but no later than 60 calendar days) after discovery of breach
 - Annual reporting to HHS of smaller breaches (affecting less than 500 individuals) permitted
- OCR posts breaches affecting 500+ individuals on OCR website



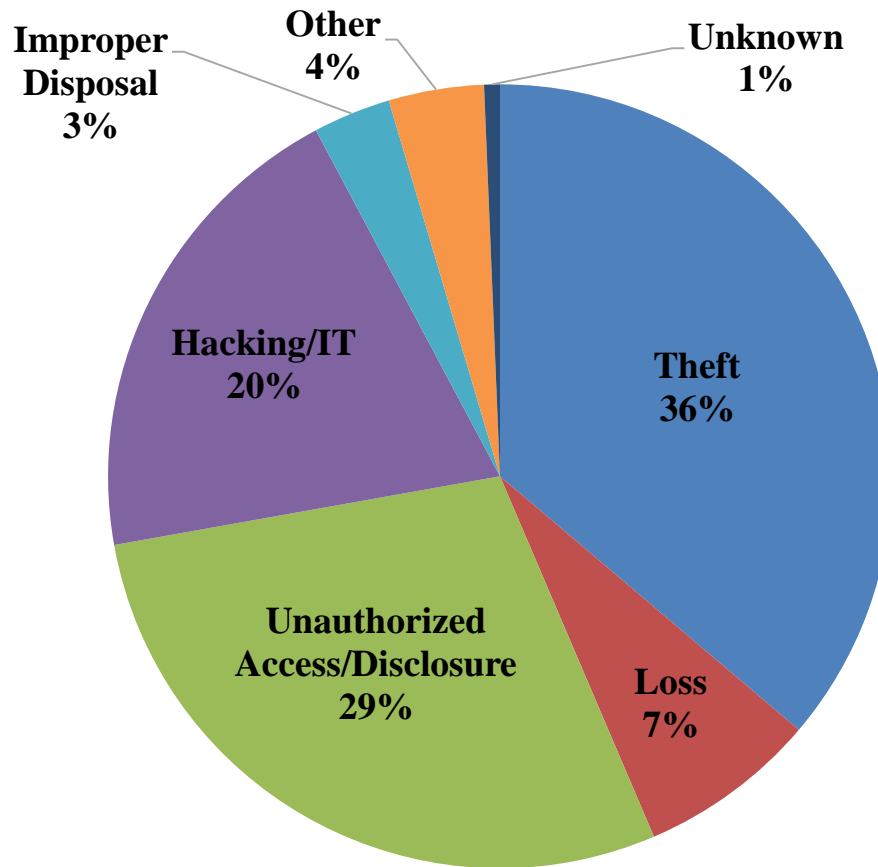
September 2009 through June 30, 2018

- 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



500+ Breaches by Type of Breach

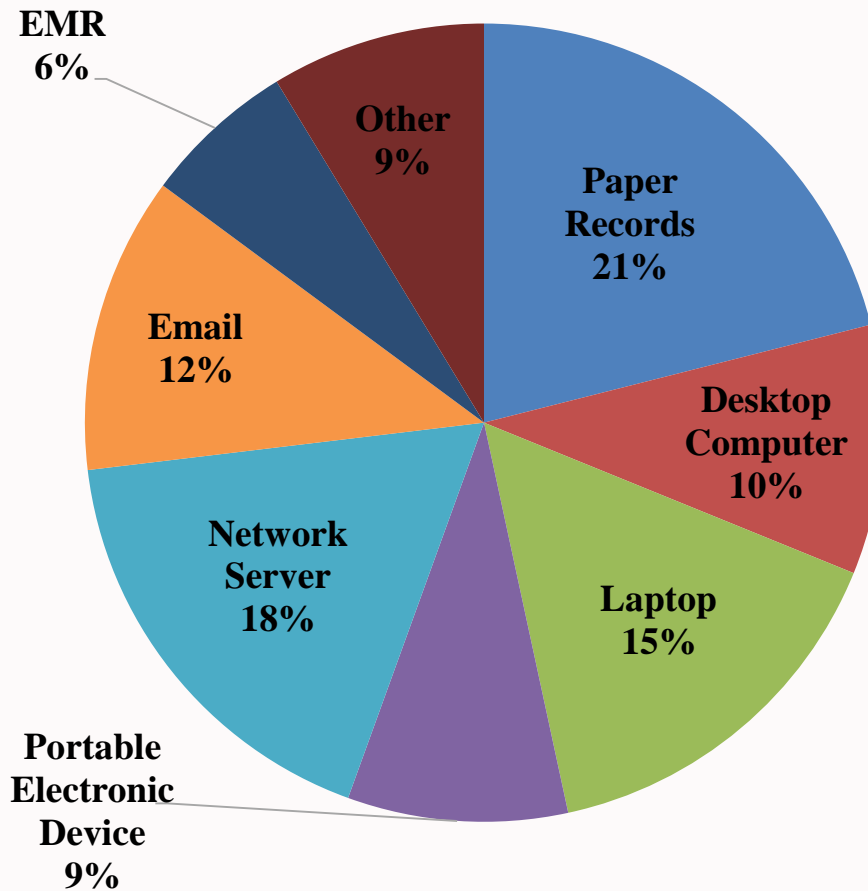
September 23, 2009 – June 30, 2018





500+ Breaches by Location of Breach

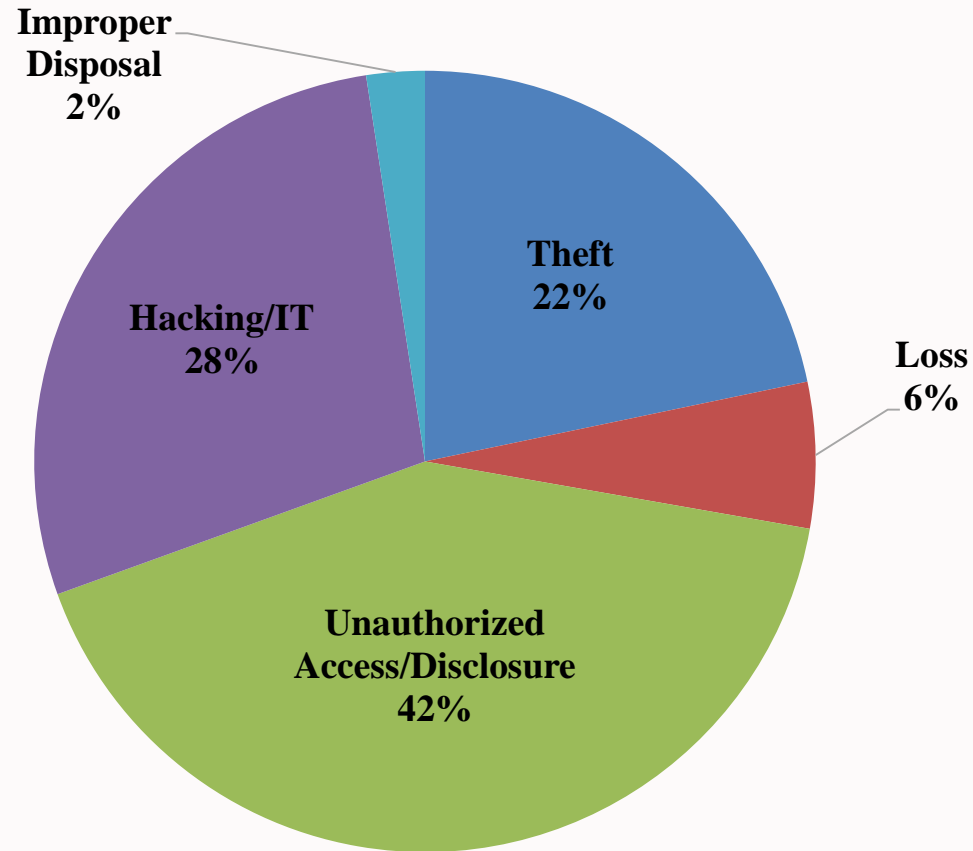
September 23, 2009 – June 30, 2018





500+ Breaches by Type of Breach

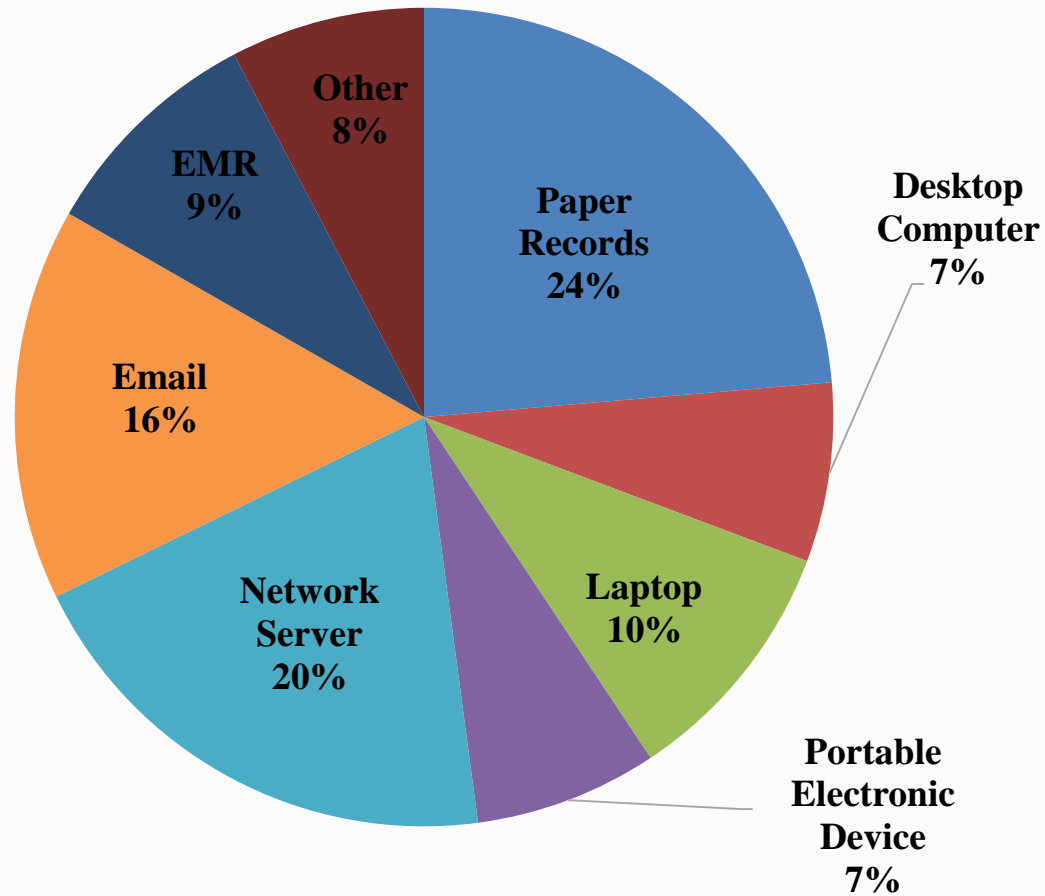
7/1/2015 – 6/30/2018





500+ Breaches by Location of Breach

7/1/2015 – 6/30/2018





- 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



General HIPAA Enforcement Highlights as of 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



- 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
 - 52 settlement agreements that include detailed corrective action plans and monetary settlement amounts
- 3 civil money penalties

As of June 30, 2018



Recent Enforcement Actions

2017 - 2018

4/12/2017	Metro Community Provider Network	\$400,000
4/21/2017	Center for Children's Digestive Health	\$31,000
4/21/2017	CardioNet	\$2,500,000
5/10/2017	Memorial Hermann Health System	\$2,400,000
5/23/2017	St. Luke's-Roosevelt Hospital Center	\$387,200
12/28/2017	21st Century Oncology	\$2,300,000
2/1/2018	Fresenius Medical Care North America	\$3,500,000
2/13/2018	Filefax	\$100,000

Total \$11,618,200



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



Corrective Actions May Include:

- Updating risk analysis and risk management plans
- Updating policies and procedures
- Training of workforce
- Implementing specific technical or other safeguards
- Mitigation
- CAPs may include monitoring



Some Best Practices:

- Review all vendor and contractor relationships to ensure BAAs are in place as appropriate and address breach/security incident obligations
- Risk analysis and risk management should be integrated into business processes; conducted regularly and when new technologies and business operations are planned
- Dispose of PHI on media and paper that has been identified for disposal in a timely manner
- Incorporate lessons learned from incidents into the overall security management process
- Provide training specific to organization and job responsibilities and on regular basis; reinforce workforce members' critical role in protecting privacy and security



AUDIT



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 a compliance review (for example, if significant concerns are raised during an audit)
 - Learn from Phase 2 in structuring permanent 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
- Evaluation of Pilot (2013) – issuance of formal evaluation report of pilot audit program
- Phase 2 (2016-2017) - desk audits of 207 covered entities and business associates



Phase 2 - Selected Desk Audit Provisions

- For Covered Entities:
 - Security Rule: risk analysis and risk management;
 - Breach Notification Rule: content and timeliness of notifications; **or**
 - Privacy Rule: NPP and individual access right
- For Business Associates:
 - Security Rule: risk analysis and risk management **and**
 - Breach Notification Rule: reporting to covered entity
- See auditee protocol guidance for more details:
<http://www.hhs.gov/sites/default/files/2016HIPAADeskAuditAuditeeGuidance.pdf>



Status

- 166 covered entity and 41 business associate desk audits were completed in December 2017
- Website updates with summary findings will be published in 2018



<http://www.hhs.gov/hipaa>

Join us on Twitter @hhsocr