Update from the HHS Office for Civil Rights

Marissa Gordon-Nguyen
Senior Advisor for Health Information Privacy Policy

December 2, 2019

Speaker Information

- **Marissa Gordon-Nguyen** is the Senior Advisor for Health Information Privacy Policy in the Office for Civil Rights (OCR), U.S. Department of Health and Human Services (HHS). In this role, she leads OCR's administration of the HIPAA Rules through rulemaking initiatives and the development of sub-regulatory guidance, among other responsibilities.
- Marissa joined OCR's Health Information Privacy Division in 2009. She earned her Law Degree from Georgetown Law and her Master of Public Health from the Johns Hopkins Bloomberg School of Public Health.

Policy

Request for Information on Modifying the HIPAA Rules to Improve Coordinated Care

- Published December 14, 2018
- Comments closed February 12, 2019
- More than 1,330 timely comments received
- Public comments are viewable at https://www.regulations.gov/docket?D=HHS-OCR-2018-0028.

HIPAA Regulatory Sprint

RFI asked for comments on specific areas of the HIPAA Privacy Rule, including:

- Encouraging timely information-sharing for treatment and care coordination
- Addressing the opioid crisis and serious mental illness
- Changing the current signature requirement on the Notice of Privacy Practices

Health App FAQs

- A covered entity cannot withhold releasing ePHI to an individual's requested health app because of concerns about how the app will use the ePHI.

- A covered entity is not liable for the re-disclosure of ePHI by a health app if there is no business associate relationship.

- Buyer Beware: HIPAA Rules don't follow health data everywhere it goes.

https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access-right-health-apps-apis/index.html

Direct Liability of Business Associates

- HITECH Act → Omnibus HIPAA Final Rule
- Fact Sheet lists the applicable requirements of the:
  - Enforcement Rule
  - Security Rule
  - Breach Notification Rule
  - Privacy Rule

https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/factsheet/index.html

Surprise Billing

- On June 24, 2019, President Trump issued Executive Order 13877 which directed HHS to “solicit comment on a proposal to require healthcare providers, health insurance issuers, and self-insured group health plans to provide or facilitate access to information about expected out-of-pocket costs for items or services to patients before they receive care.”
- Listening sessions with clearinghouses, health plans, healthcare providers and consumers.

BREACH HIGHLIGHTS AND RECENT ENFORCEMENT ACTIVITY

General HIPAA Enforcement Highlights

- Expect to receive over 26,000 complaints this year
- In most cases, entities able to demonstrate satisfactory compliance through voluntary cooperation and corrective action
- In some cases, the nature or scope of indicated noncompliance warrants additional enforcement action
- Resolution Agreements/Corrective Action Plans
  - 66 settlement agreements that include detailed corrective action plans and monetary settlement amounts
- 6 civil money penalties

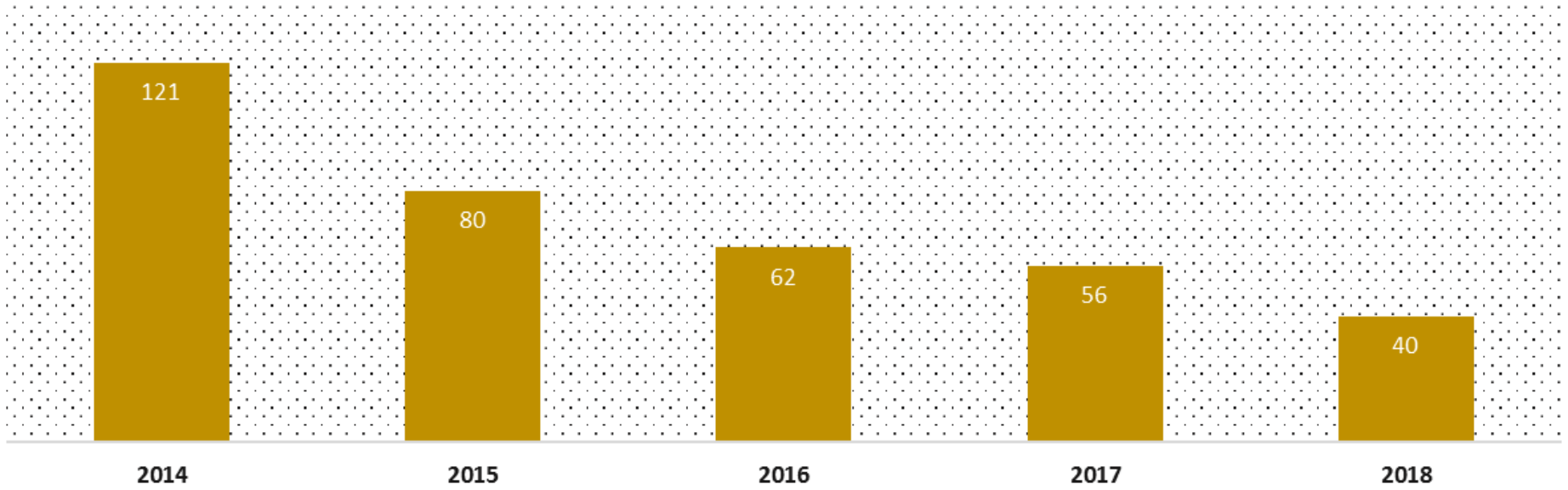
OCR's Right of Access Initiative

Common Compliance Issues:

- Untimely Access
- Unreasonable Fees
- Form and Format
- Identity Validation Burdens

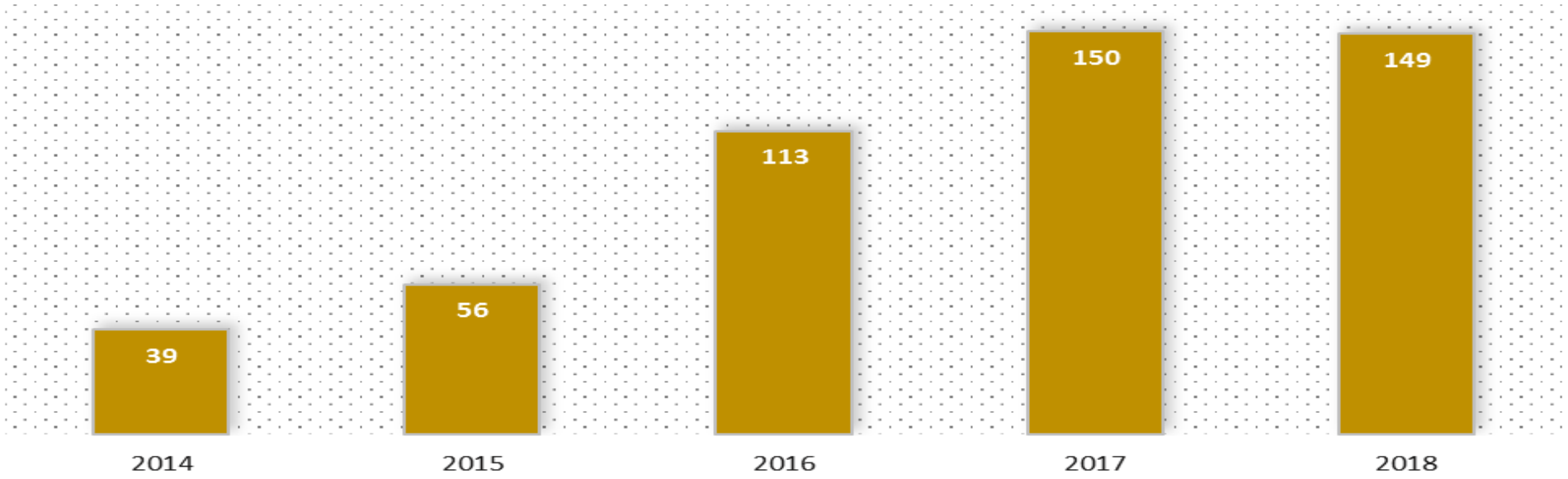
Breaches Affecting 500 or more Individuals
Reports Received Involving the Theft of PHI

Calendar Years 2014 - 2018

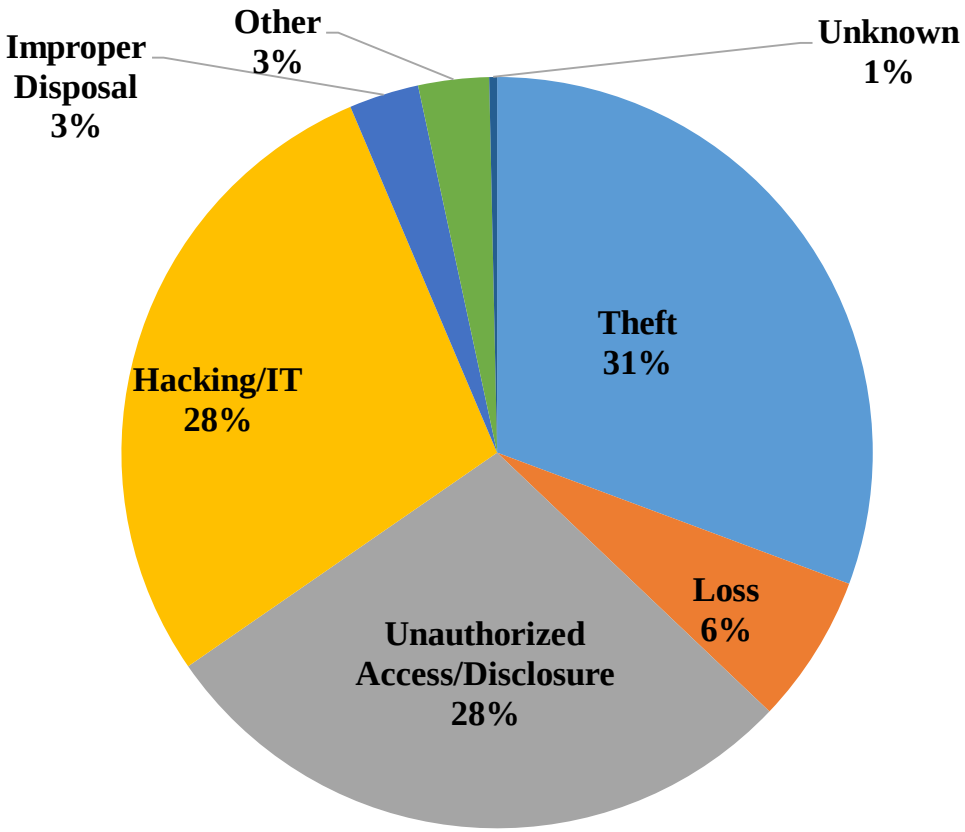


Breaches Affecting 500 or more Individuals
Reports Received Involving
Hacking/IT Incidents

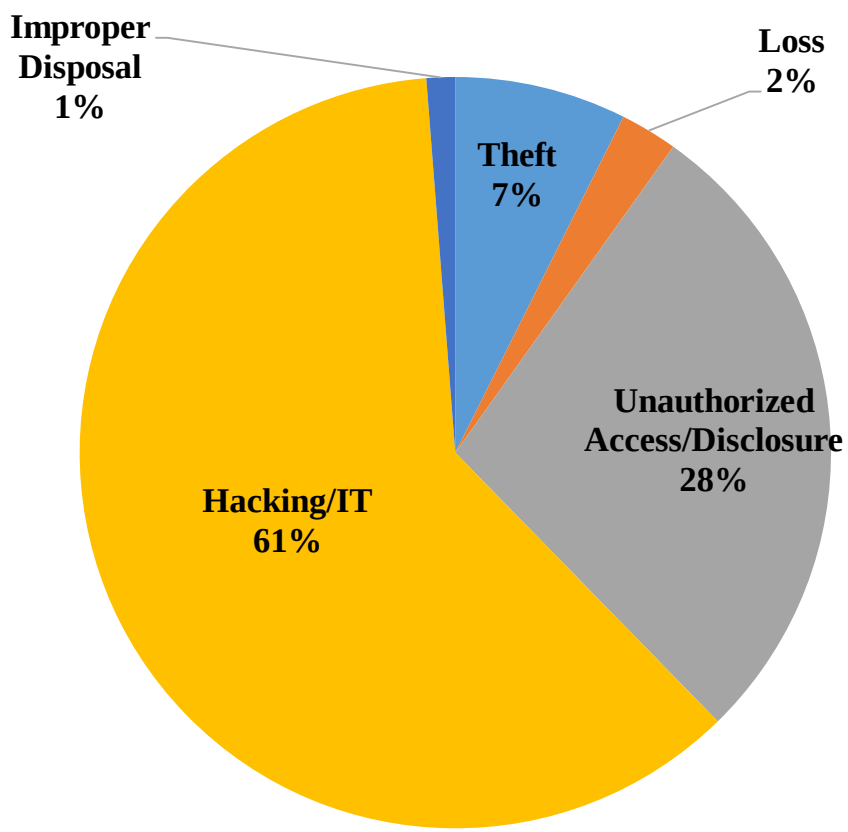
Calendar Years 2014 - 2018



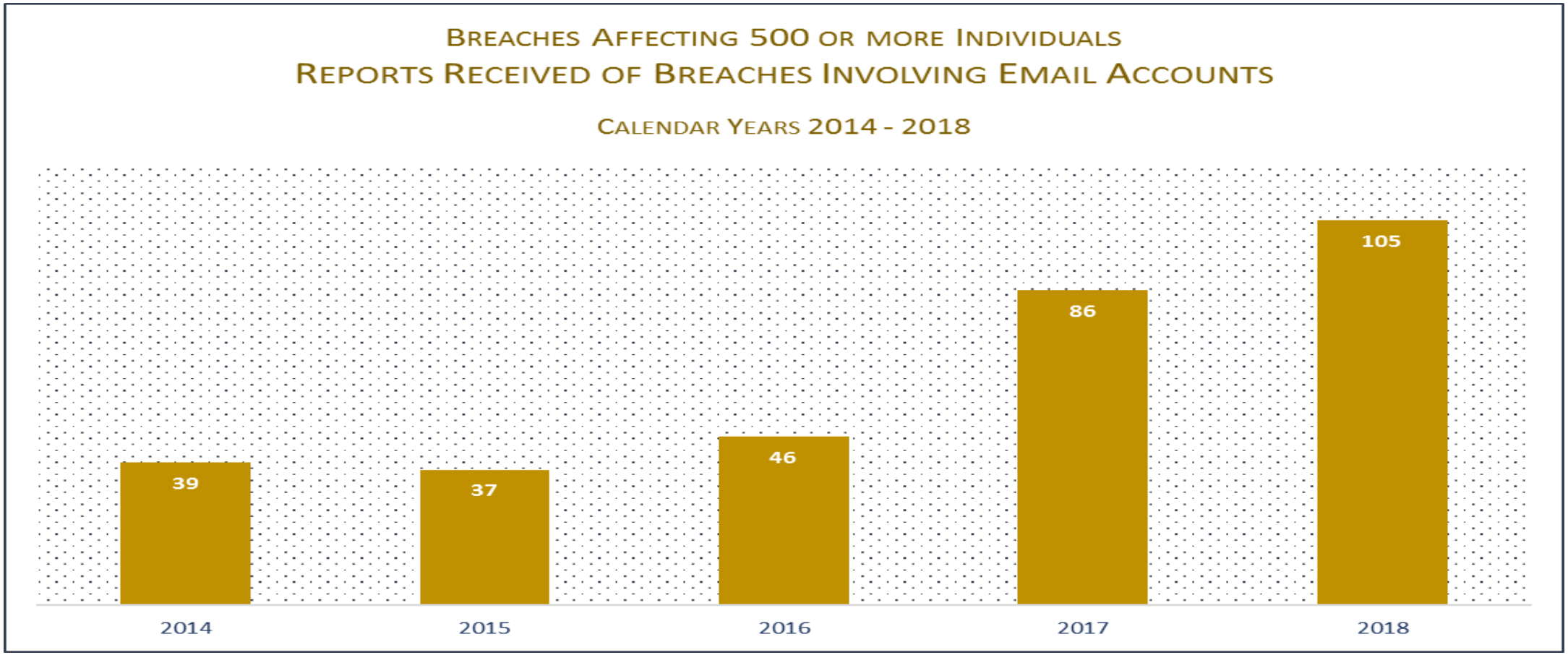
500+ Breaches by Type



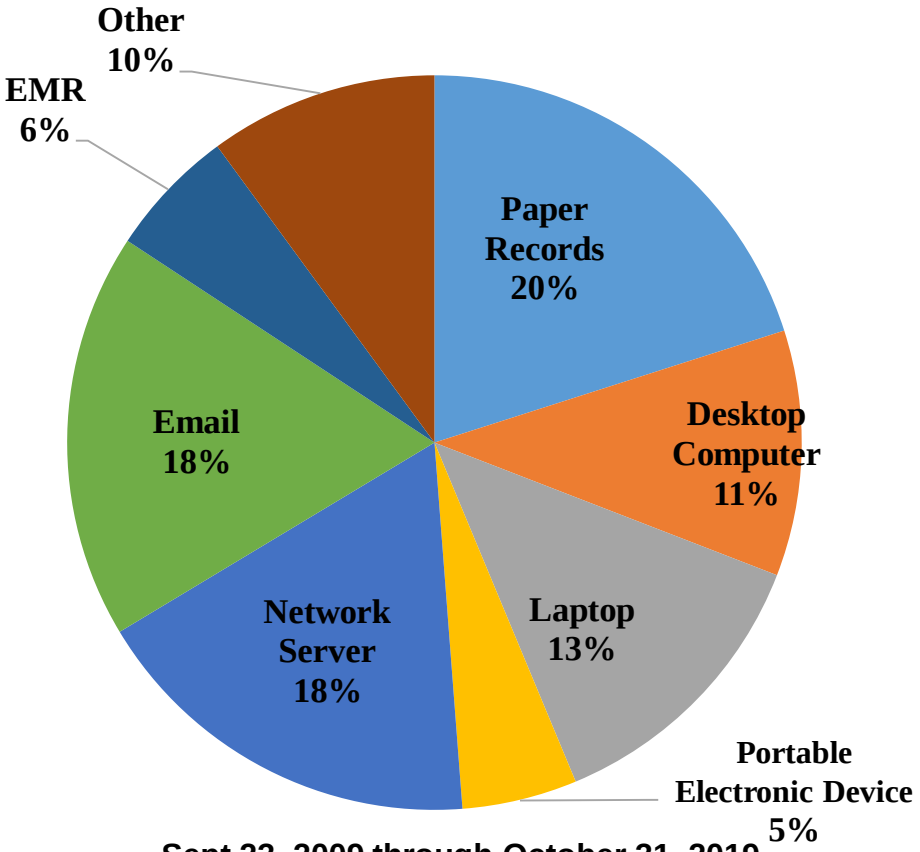
Sept 23, 2009 through October 31, 2019



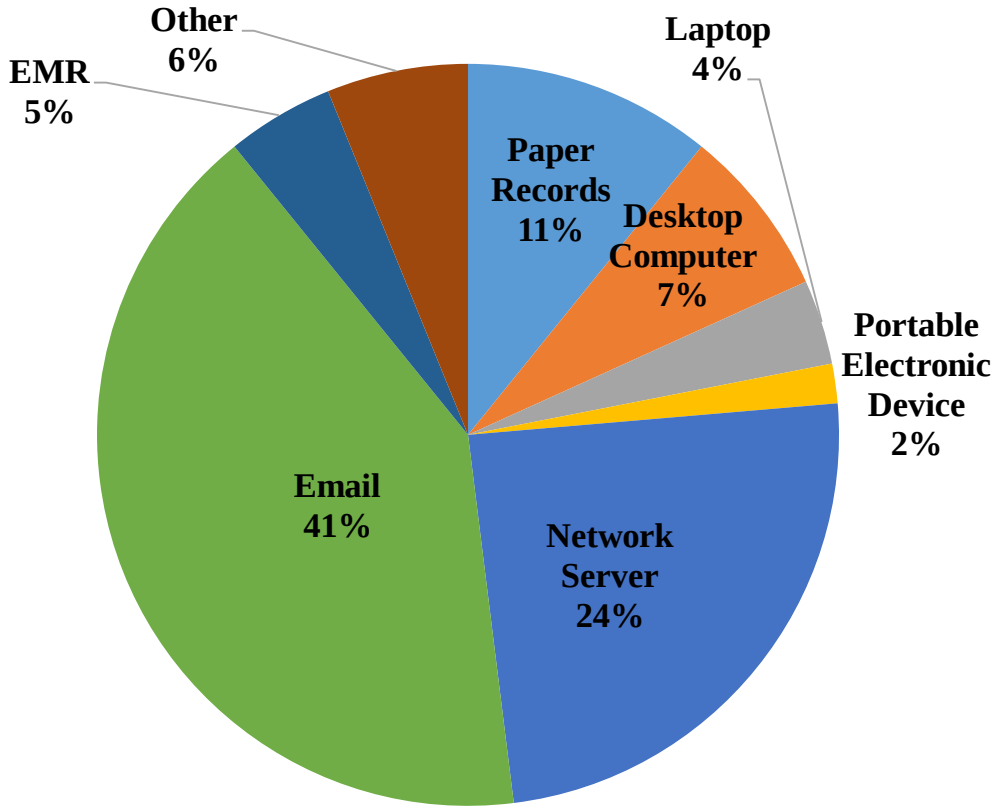
Jan 1, 2019 through October 31, 2019


Breaches Affecting 500 or more Individuals
Reports Received of Breaches Involving Email Accounts
Calendar Years 2014 - 2018
39
37
46
86
105
2014
2015
2016
2017
2018

500+ Breaches by Location



Sept 23, 2009 through October 31, 2019



Jan 1, 2019 through October 31, 2019

Cybersecurity Concerns and Trends

- Ransomware
- Phishing Attacks
- Unsecured Servers
- Lack of Encryption
- Weak Authentication
- Access Controls

OCR Cybersecurity Newsletters

- Current Topics
  - Advanced Persistent Threats and Zero Day Vulnerabilities
  - Managing Malicious Insider Threats
- Past Topics Include
  - Risk Analyses v. Gap Analyses
  - Workstation Security
  - Software Vulnerabilities and Patching
  - Guidance on Disposing of Electronic Devices and Media
  - Considerations for Securing Electronic Media and Devices

http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html

AUDIT

Audit Program

Purposes:

- Identify best practices
- Uncover risks and vulnerabilities not identified through other enforcement tools
- Encourage consistent attention to compliance

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