# Lessons Learned from Recent HIPAA Breaches

HHS Office for Civil Rights

"Breach:" Impermissible acquisition, access, use, or disclosure of PHI (paper or electronic), which compromises the security or privacy of the PHI.

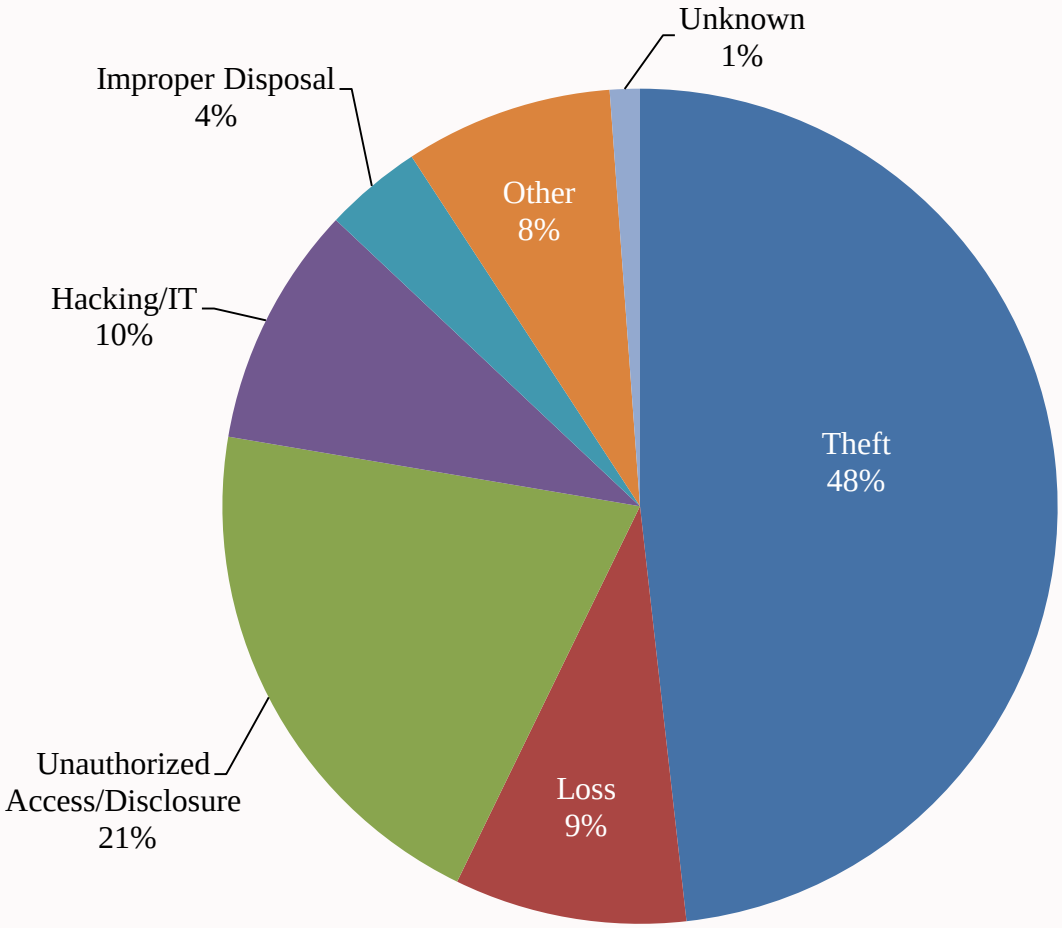
Safe Harbor: If the PHI is encrypted or destroyed.

Breach is Presumed and Must Be Reported, UNLESS:

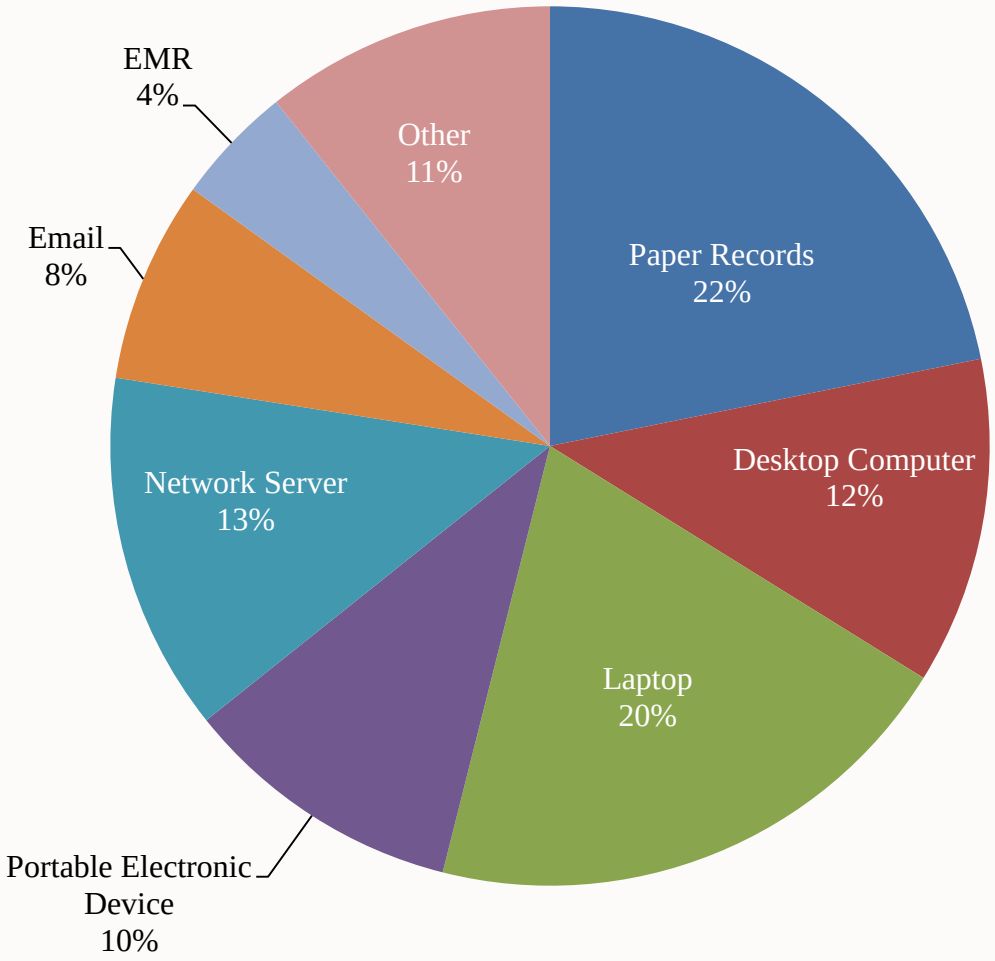
- The CE or BA can demonstrate (through a documented risk assessment) that there is a low probability that the PHI has been compromised based on:
  - Nature and extent of the PHI involved (including the types of identifiers and the likelihood of re-identification);
  - The unauthorized person who used the PHI or to whom the disclosure was made;
  - Whether the PHI was actually acquired or viewed; and
  - The extent to which the risk to the PHI has been mitigated.

Focus on risk to the data, instead of risk of harm to the individual.

# 500+ Breaches by Type of Breach as of 8/28/2015



# 500+ Breaches by Location as of 8/28/2015



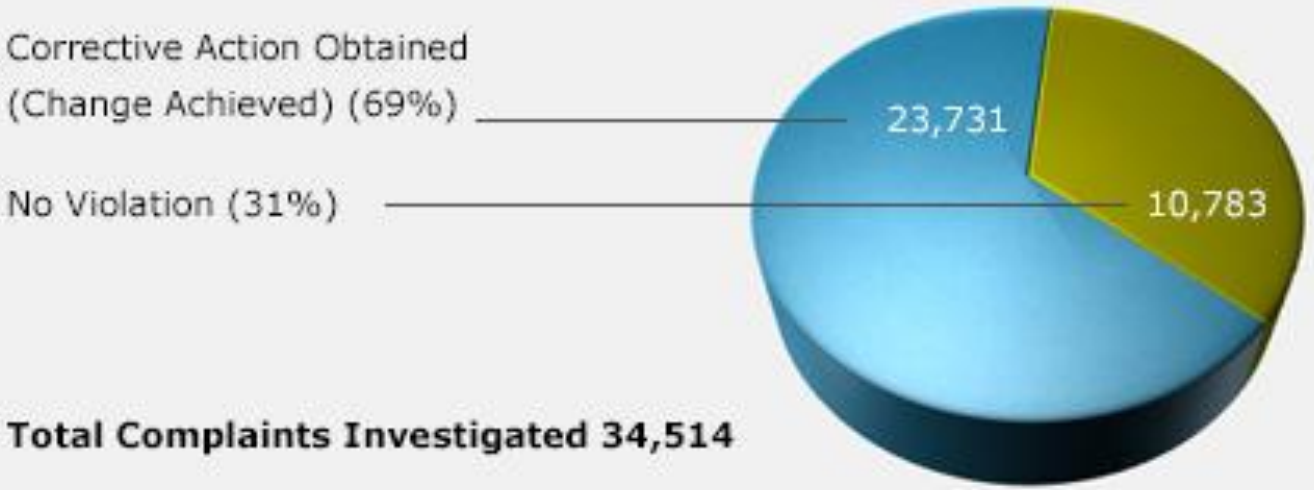


September 2009 through August 28, 2015

- Approximately 1,310 reports involving a breach of PHI affecting 500 or more individuals
  - Theft and Loss are 57% of large breaches
  - Laptops and other portable storage devices account for 30% of large breaches
  - Paper records are 22% of large breaches
- Approximately 179,000+ reports of breaches of PHI affecting fewer than 500 individuals

# CLOSED INVESTIGATED CASES

## Total Investigated Resolutions
April 14, 2003 - July 31, 2015




**Total Complaints Investigated 34,514**



- 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

# RECENT ENFORCEMENT ACTIONS

- St. Elizabeth's Medical Center (electronic)
- Cornell Prescription Pharmacy (paper)
- Anchorage (electronic)
- Parkview (paper)
- NYP/Columbia (electronic)
- Concentra (electronic)
- QCA (electronic)
- Skagit County (electronic and paper)

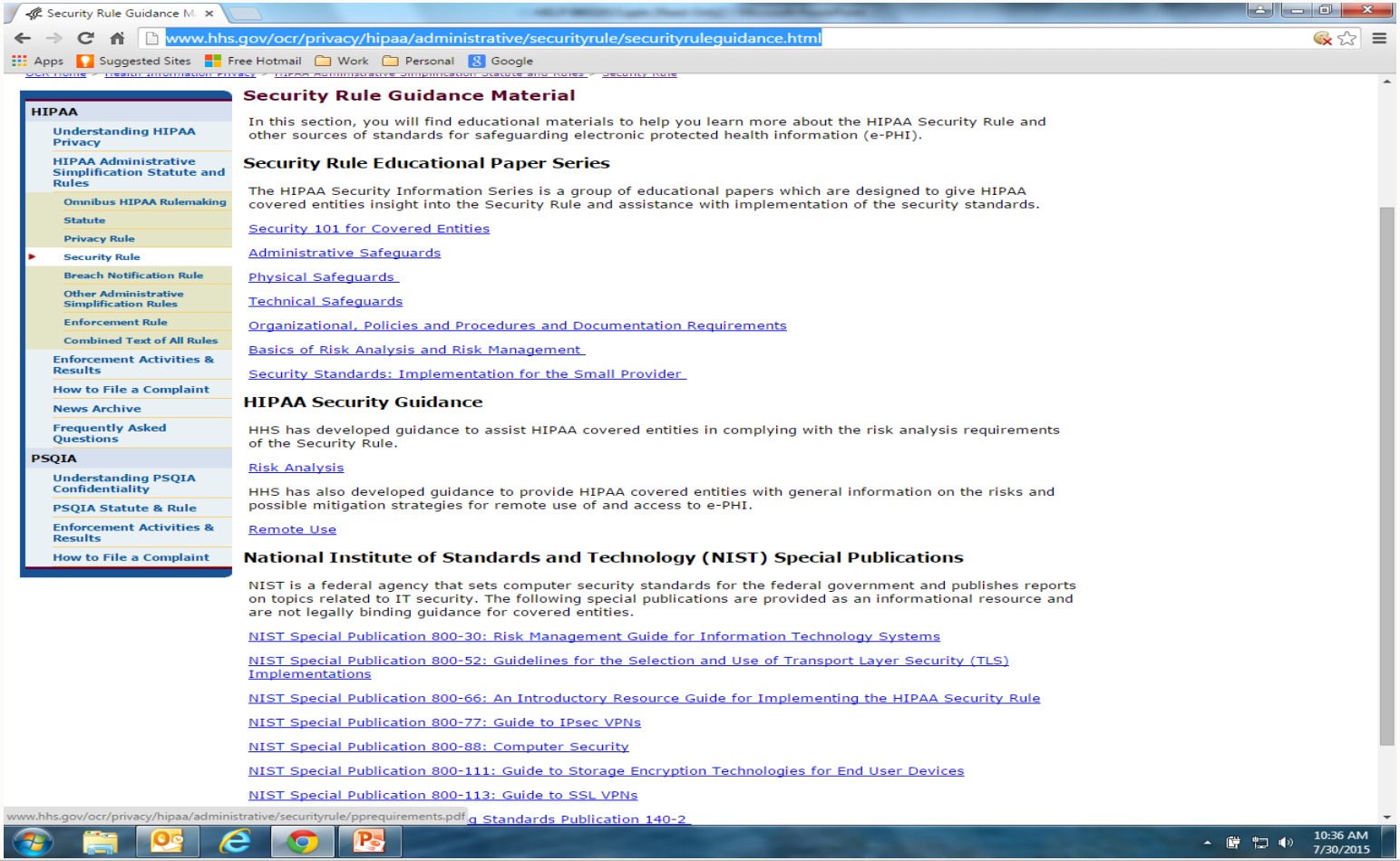
http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html

- http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidance.html
- http://scap.nist.gov/hipaa/
- http://www.healthit.gov/providers-professionals/security-risk-assessment

http://www.healthit.gov/mobiledevices

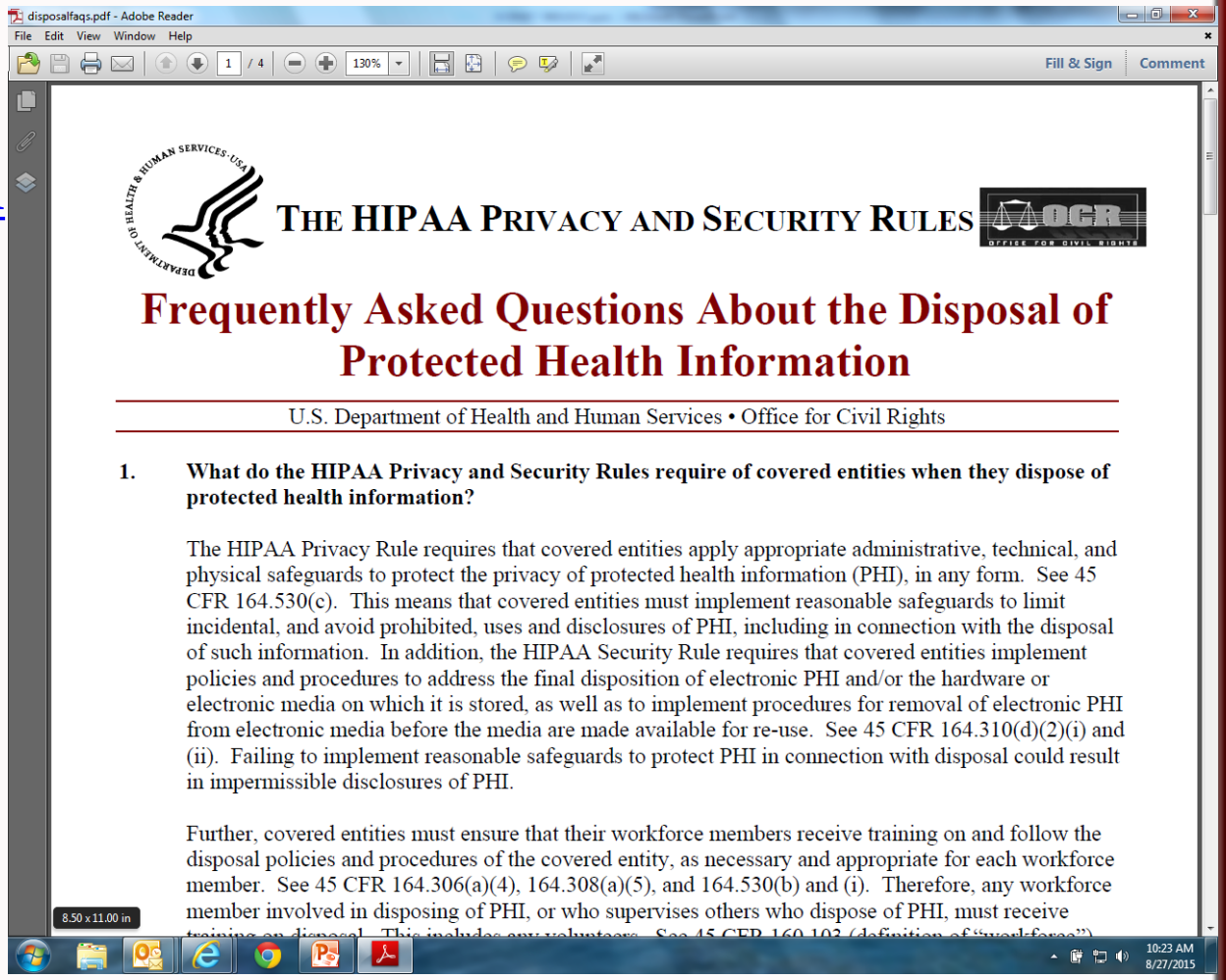
# OCR Security Rule Resource Center:

http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html



# DISPOSAL

http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html



# QUESTIONS?