Breach Prevention and Management: A HIPAA Perspective

Nicholas P. Heesters, Jr., JD, CIPP
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:

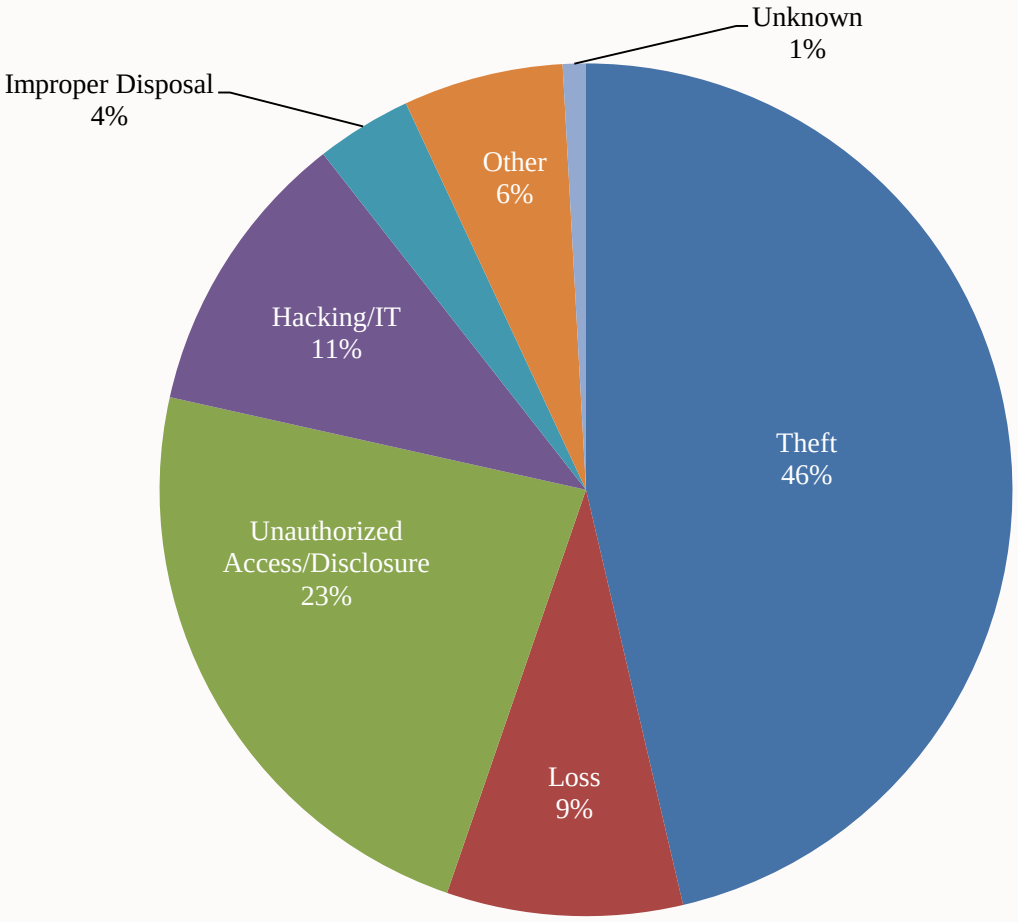
- The CE or BA can demonstrate (through a documented risk assessment) that there is a low probability that the PHI has been compromised based on:
  - Nature and extent of the PHI involved (including the types of identifiers and the likelihood of re-identification);
  - The unauthorized person who used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

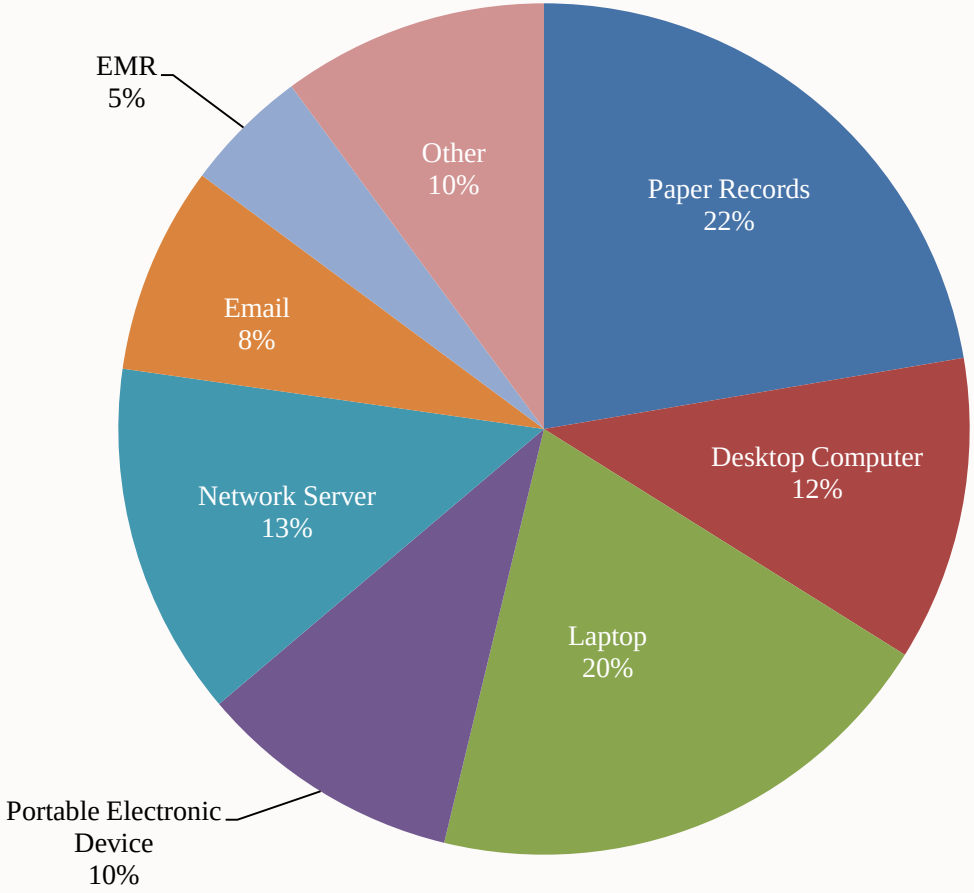
September 2009 through March 31, 2016

- Approximately 1,516 reports involving a breach of PHI affecting 500 or more individuals
  - Theft and Loss are 55% of large breaches
  - Hacking/IT now account for11% of these incidents
  - Laptops and other portable storage devices account for 30% of large breaches
  - Paper records are 23% of large breaches
- Approximately 222,512+ reports of breaches of PHI affecting fewer than 500 individuals

500+ Breaches by Type of Breach



500+ Breaches by Location



Frequent Breach Related Issues:

- Web application / data leakage
- Lost or stolen devices (workstations, laptops, servers, electronic media, medical devices)
  - Files containing PHI
- Known vulnerabilities exploited due to use of unpatched or obsolete software
  - Open source software
  - Firmware
- Malware/Ransomware
- Advanced Persistent Threat (APT) style attacks
- Excessive permissions / lack of access controls

Breach Prevention:

- Security awareness and training
  - Processes are in place to detect/guard against malicious software
  - How to detect and report malicious software
- Risk analysis
  - Identify the risks and vulnerabilities to the confidentiality, integrity, and availability of all ePHI entities create, receive, maintain, or transmit
- Risk management
  - Implement security measures sufficient to reduce identified threats and vulnerabilities to a reasonable and appropriate level
- Access controls
  - Ensure access rights granted are not excessive
- Business Associate Agreements
  - Define processes, including responsibilities, to prevent, manage and report security incidents and breaches

Breach Recovery:

- Security incident response
  - Prepare for security incidents ahead of time
    - Define teams and activities
  - Detect and conduct initial analysis of incident
    - Identify scope of incident
    - Determine origination (who/what/where/when)
    - Determine if incident has concluded or is ongoing
    - Determine how incident occurred
  - Contain the impact and propagation of the incident
  - Eradicate the incident and vulnerabilities which may have permitted its ingress and/or propagation
  - Recover from incident (restore lost data, return to business as usual)
  - Post-incident activities which could include responding to regulatory and/or contractual obligations as a result of breach

Breach Recovery:

- Contingency plans
  - Data backup plans
  - Disaster recovery plans
  - Emergency operations mode plans
  - Testing and revision procedures
    - Conduct test restorations to verify the integrity of backed up data and provide confidence in data restoration capabilities
    - Testing contingency plans to ensure organizational readiness and provide confidence that contingency plans would be effective
    - Revise contingency plans if tests show areas which would be ineffective
  - Application and data criticality analysis
    - Ensure all critical applications and data are accounted for as part of the contingency plans

QUESTIONS?