



Lessons Learned from Recent HIPAA Breaches

HHS Office for Civil Rights



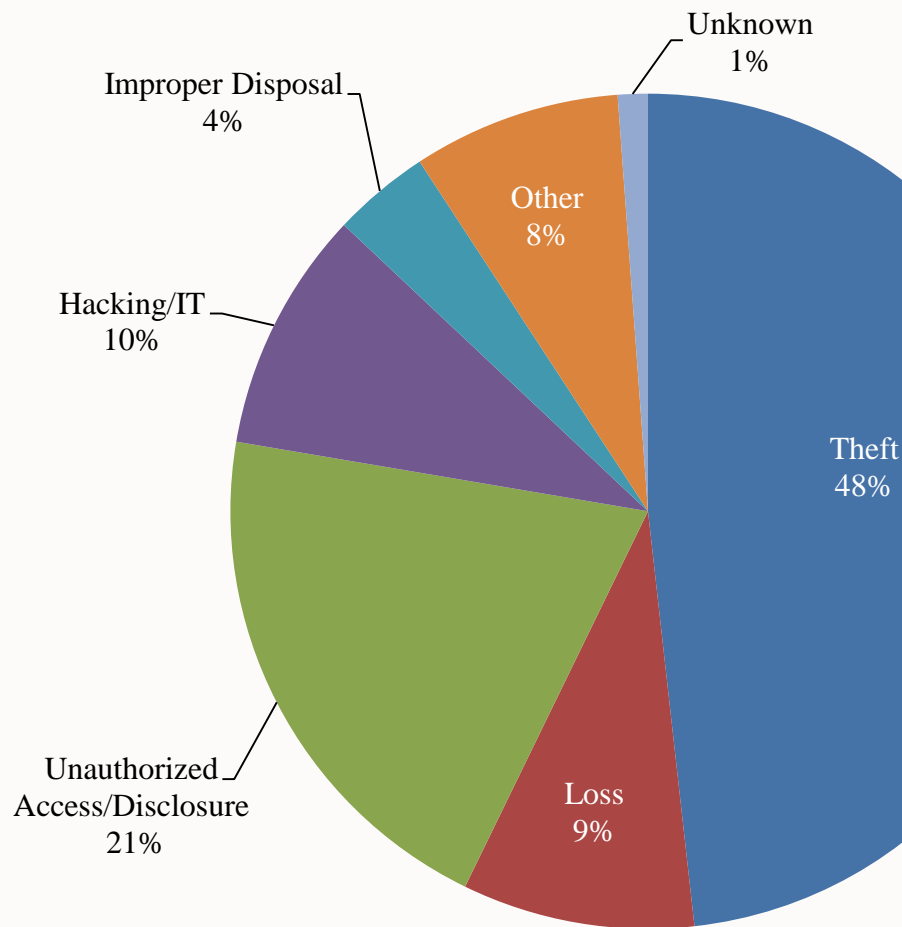
“Breach:” Impermissible acquisition, access, use, or disclosure of PHI (paper or electronic), which compromises the security or privacy of the PHI.

Safe Harbor: If the PHI is encrypted or destroyed.

Breach is Presumed and Must Be Reported, UNLESS:

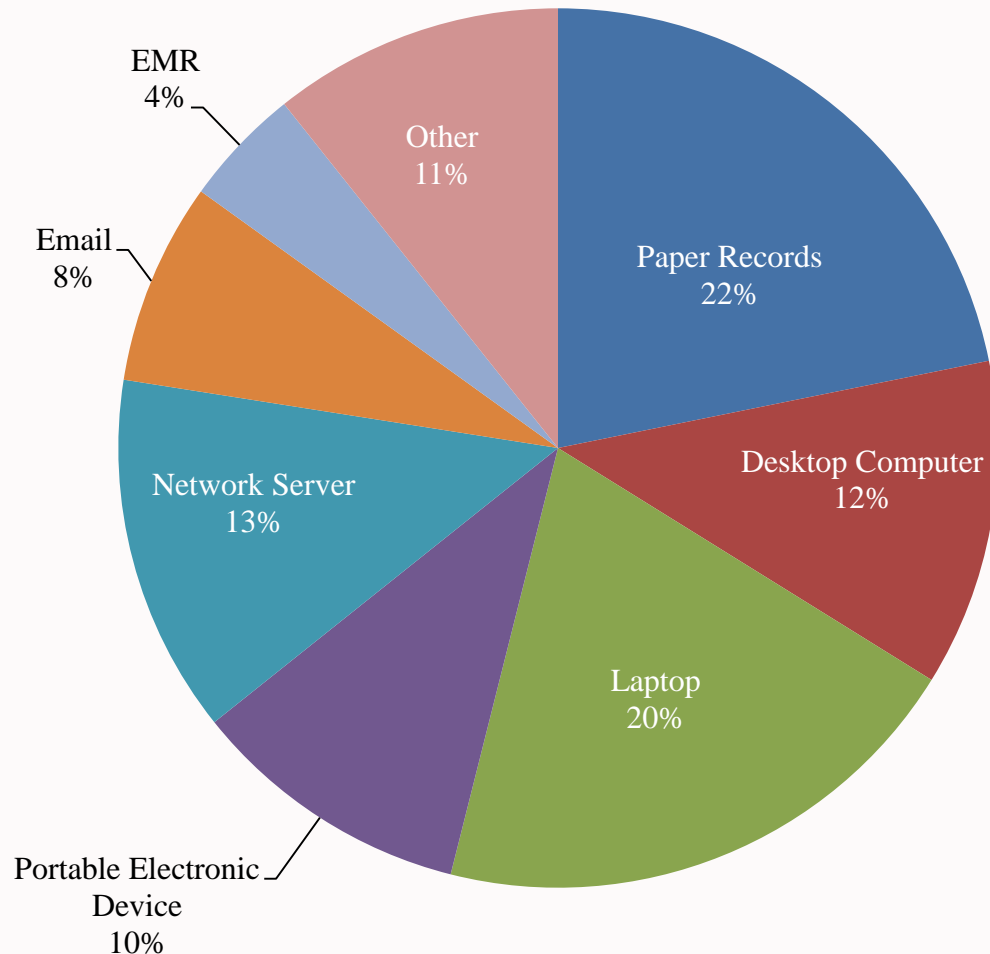
- The CE or BA can demonstrate (through a documented risk assessment) that there is a low probability that the PHI has been compromised based on:
 - Nature and extent of the PHI involved (including the types of identifiers and the likelihood of re-identification);
 - The unauthorized person who used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





Office for Civil Rights





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



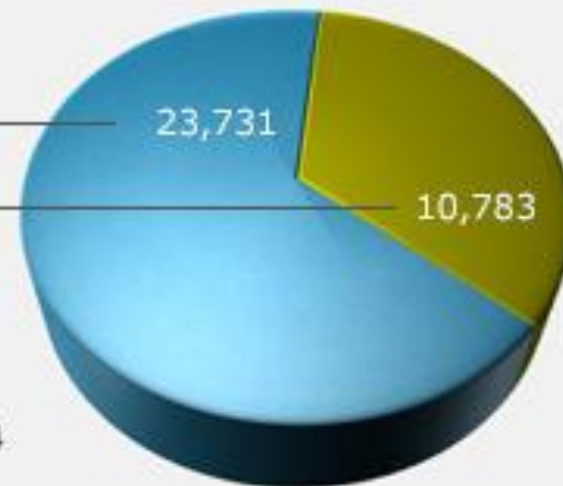
Total Investigated Resolutions

April 14, 2003 - July 31, 2015

Corrective Action Obtained
(Change Achieved) (69%)

No Violation (31%)

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



- 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>

A screenshot of a web browser displaying the HHS.gov website. The browser's address bar shows the URL: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html. The page header includes the U.S. Department of Health & Human Services logo and the text "Improving the health, safety, and well-being of America". Below the header, there is a navigation bar with links to "HHS Home", "HHS News", and "About HHS". The main content area is titled "Health Information Privacy" and includes a sub-header "Business Associate Contracts". The page is divided into three columns. The left column contains a sidebar with links to "HIPAA", "PSQIA", and "Enforcement Activities & Results". The middle column contains the main text, which includes a "SAMPLE BUSINESS ASSOCIATE AGREEMENT PROVISIONS" section and an "Introduction" section. The right column contains a "Guidance Materials for Covered Entities" section with links to "Summary of the Privacy Rule", "Guidance on Significant Aspects of the Privacy Rule", "Fast Facts for Covered Entities", "Provider Guide: Communicating With a Patient's Family, Friends, or Other Persons", "Guidance on the Application of FERPA and HIPAA to Student Health Records", "Sample Business Associate Contract", "Misleading Marketing Claims", and "Sign Up for the OCR Privacy Listserv". The bottom of the screenshot shows the Windows taskbar with various application icons and the system clock displaying 10:28 AM on 8/27/2015.



- <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>

The screenshot shows a web browser displaying the HealthIT.gov website. The address bar shows the URL <http://www.healthit.gov/providers-professionals/your-mobile-device-and-health-inform>. The page title is "Mobile Health Security: Mo...". The website header includes the HealthIT.gov logo and navigation links such as "Blog", "Federal Advisory Committees (FACAs)", "Contact", "Get Email Updates", "Newsroom", "Help Center", and "Multimedia". A search bar is also present. The main navigation bar includes "Providers & Professionals", "Patients & Families", and "Policy Researchers & Implementers". Below this, there are tabs for "Benefits of EHRs", "How to Implement EHRs", "Privacy & Security", "EHR Incentives & Certification", "Health Information Exchange (HIE)", and "Success Stories & Case Studies". The "Privacy & Security" tab is selected, leading to the "Your Mobile Device and Health Information Privacy and Security" page. This page features a video titled "Worried About Using a Mobile Health Device for Work?" with a list of "MOBILE DEVICE RISKS": 1) Lost mobile device, 2) Stolen mobile device, 3) Downloaded virus, 4) Shared mobile device, and 5) Unsecured Wi-Fi network. Below the video, there are two sections: "Read and Learn" with links to "How Can You Protect and Secure Health Information When Using a Mobile Device?", "You, Your Organization and Your Mobile Device", and "Five Steps Organizations Can Take To Manage Mobile Devices"; and "Watch and Learn" with links to "Worried About Using a Mobile Device for Work? Here's What To Do!", "Securing Your Mobile Device is Important!", and "Dr. Anderson's Office Identifies a Risk". The Windows taskbar at the bottom shows the date and time as 2:16 PM on 10/22/2013.



OCR Security Rule Resource Center:

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

HIPAA

- Understanding HIPAA Privacy
- HIPAA Administrative Simplification Statute and Rules
- Omnibus HIPAA Rulemaking Statute
- Privacy Rule
- Security Rule
- Breach Notification Rule
- Other Administrative Simplification Rules
- Enforcement Rule
- Combined Text of All Rules
- Enforcement Activities & Results
- How to File a Complaint
- News Archive
- Frequently Asked Questions

PSQIA

- Understanding PSQIA Confidentiality
- PSQIA Statute & Rule
- Enforcement Activities & Results
- How to File a Complaint

Security Rule Guidance Material

In this section, you will find educational materials to help you learn more about the HIPAA Security Rule and other sources of standards for safeguarding electronic protected health information (e-PHI).

Security Rule Educational Paper Series

The HIPAA Security Information Series is a group of educational papers which are designed to give HIPAA covered entities insight into the Security Rule and assistance with implementation of the security standards.

- [Security 101 for Covered Entities](#)
- [Administrative Safeguards](#)
- [Physical Safeguards](#)
- [Technical Safeguards](#)
- [Organizational, Policies and Procedures and Documentation Requirements](#)
- [Basics of Risk Analysis and Risk Management](#)
- [Security Standards: Implementation for the Small Provider](#)

HIPAA Security Guidance

HHS has developed guidance to assist HIPAA covered entities in complying with the risk analysis requirements of the Security Rule.

- [Risk Analysis](#)

HHS has also developed guidance to provide HIPAA covered entities with general information on the risks and possible mitigation strategies for remote use of and access to e-PHI.

- [Remote Use](#)

National Institute of Standards and Technology (NIST) Special Publications

NIST is a federal agency that sets computer security standards for the federal government and publishes reports on topics related to IT security. The following special publications are provided as an informational resource and are not legally binding guidance for covered entities.

- [NIST Special Publication 800-30: Risk Management Guide for Information Technology Systems](#)
- [NIST Special Publication 800-52: Guidelines for the Selection and Use of Transport Layer Security \(TLS\) Implementations](#)
- [NIST Special Publication 800-66: An Introductory Resource Guide for Implementing the HIPAA Security Rule](#)
- [NIST Special Publication 800-77: Guide to IPsec VPNs](#)
- [NIST Special Publication 800-88: Computer Security](#)
- [NIST Special Publication 800-111: Guide to Storage Encryption Technologies for End User Devices](#)
- [NIST Special Publication 800-113: Guide to SSL VPNs](#)
- [NIST Special Publication 140-2](#)



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

disposalfaq.pdf - Adobe Reader

File Edit View Window Help

1 / 4 130% Fill & Sign Comment

DEPARTMENT OF HEALTH & HUMAN SERVICES - USA

THE HIPAA PRIVACY AND SECURITY RULES

OCR

OFFICE FOR CIVIL RIGHTS

Frequently Asked Questions About the Disposal of Protected Health Information

U.S. Department of Health and Human Services • Office for Civil Rights

- What do the HIPAA Privacy and Security Rules require of covered entities when they dispose of protected health information?**

The HIPAA Privacy Rule requires that covered entities apply appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information (PHI), in any form. See 45 CFR 164.530(c). This means that covered entities must implement reasonable safeguards to limit incidental, and avoid prohibited, uses and disclosures of PHI, including in connection with the disposal of such information. In addition, the HIPAA Security Rule requires that covered entities implement policies and procedures to address the final disposition of electronic PHI and/or the hardware or electronic media on which it is stored, as well as to implement procedures for removal of electronic PHI from electronic media before the media are made available for re-use. See 45 CFR 164.310(d)(2)(i) and (ii). Failing to implement reasonable safeguards to protect PHI in connection with disposal could result in impermissible disclosures of PHI.

Further, covered entities must ensure that their workforce members receive training on and follow the disposal policies and procedures of the covered entity, as necessary and appropriate for each workforce member. See 45 CFR 164.306(a)(4), 164.308(a)(5), and 164.530(b) and (i). Therefore, any workforce member involved in disposing of PHI, or who supervises others who dispose of PHI, must receive training on disposal. This includes any volunteers. See 45 CFR 160.102 (definition of "workforce").

8.50 x 11.00 in

10:23 AM 8/27/2015



QUESTIONS?