



Lessons Learned from Recent HIPAA Enforcement Actions, Breaches, and Pilot Audits

Iliana L. Peters, J.D., LL.M.
Senior Advisor for HIPAA Compliance and Enforcement



- What's Done:
 - Interim Final Rules
 - Enforcement penalties
 - Breach Notification
 - Omnibus Final Rule
 - HITECH provisions, including final rulemaking on IFR above
 - GINA provisions
 - Other rule changes
 - NICS NPRM
 - CLIA Final Rules
 - Access to test results directly from labs
- What's to Come:
 - From HITECH
 - Accounting of Disclosures
 - Methods for sharing penalty amounts with harmed individuals
 - NICS Final Rule



What's Done:

Omnibus Final Rule

- De-identification
- Combined Regulation Text
- Sample BA provisions
- Refill Reminder
- Factsheets on Student immunizations and Decedents

Model Notice of Privacy Practices in English and Spanish

Guide to Law Enforcement

Permitted Mental Health Disclosures

Letters from Leon

- Dear Provider – duty to warn, serious and imminent threats
- Right to access – updated for e-access requirements

What's to Come:

Omnibus Final Rule

- Breach Safe Harbor Update
- Breach Risk Assessment Tool
- Minimum Necessary
- More on Marketing
- More Factsheets on other provisions

Model Notice

- On line version

Other Guidance

- Security Rule guidance updates



Changes to the Rules:

- Security Rule: BAs (and subcontractors) now directly liable
- Privacy Rule: BAs (and subcontractors) now directly liable for:
 - impermissible uses and disclosures;
 - non-compliance with their BA Agreements; and
 - certain individual rights.



Revised Definition of “Breach:”

Breach Presumed UNLESS:

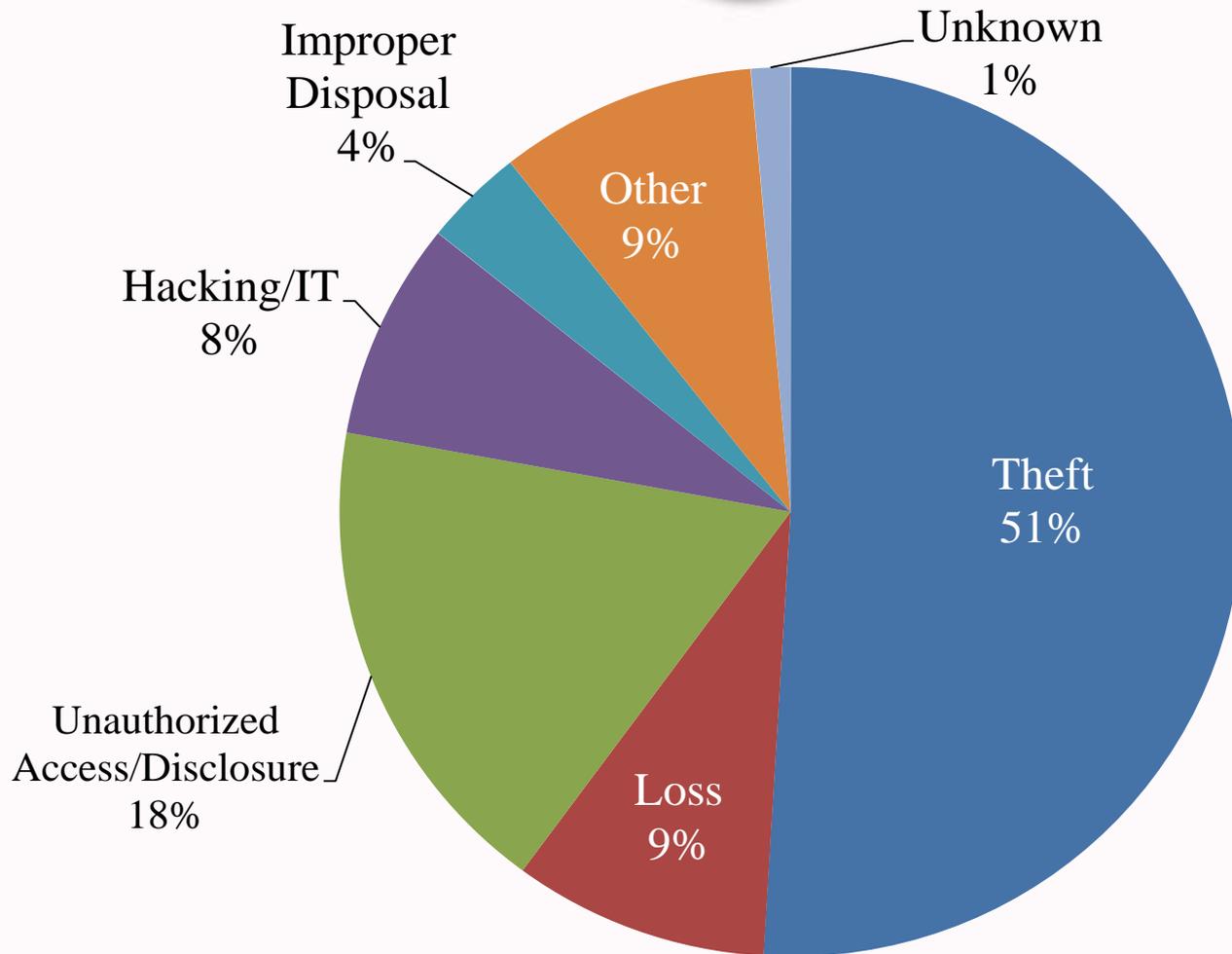
- “LoProCo:” The CE or BA can demonstrate that there is a low probability that the PHI has been compromised based on:
 - Nature and extent of the PHI involved (including the types of identifiers and the likelihood of re-identification);
 - The unauthorized person who used the PHI or to whom the disclosure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

Risk Assessment must be documented.

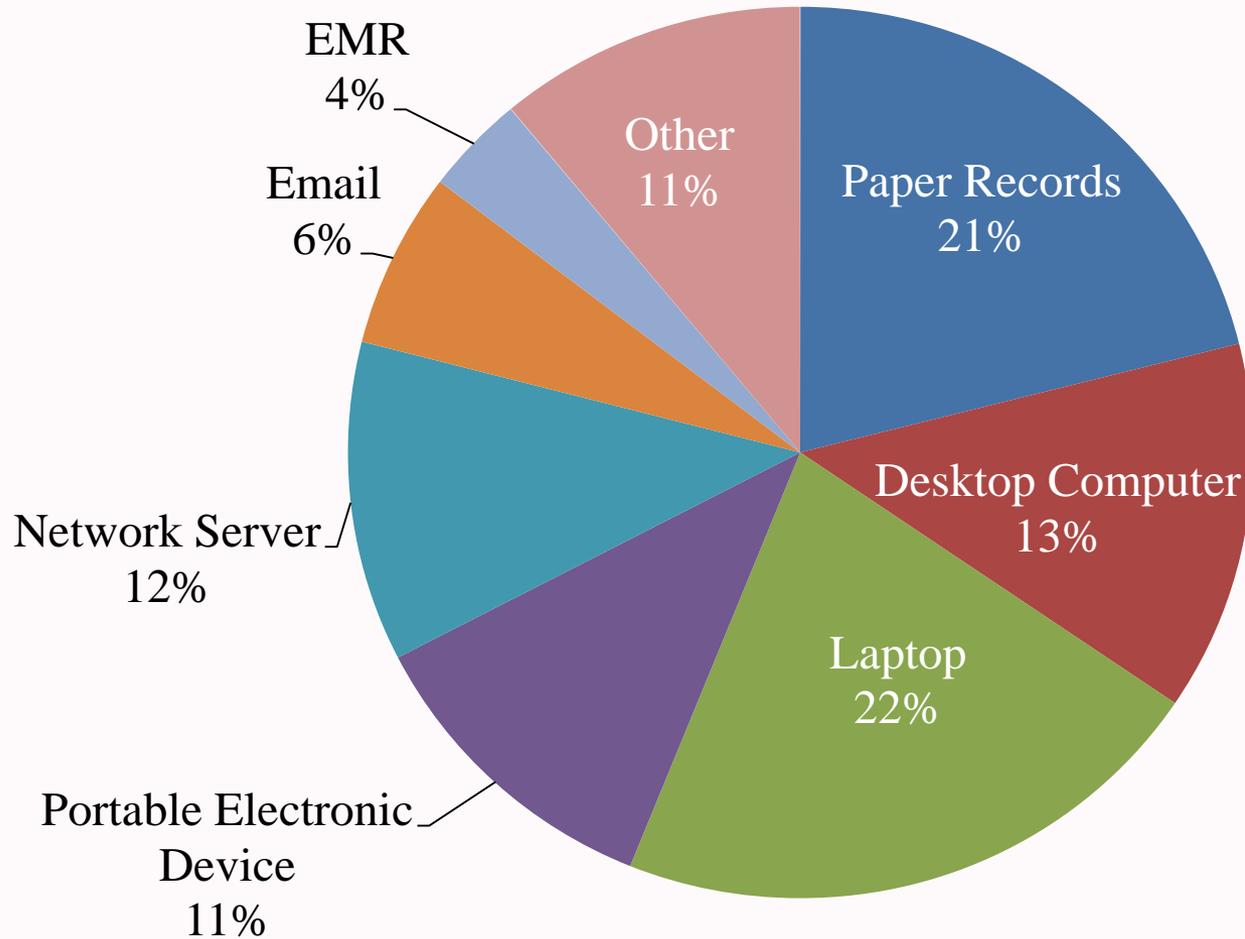


Office for Civil Rights





Office for Civil Rights





September 2009 through August 31, 2014

- Approximately 1176 reports involving a breach of PHI affecting 500 or more individuals
 - Theft and Loss are 60% of large breaches
 - Laptops and other portable storage devices account for 33% of large breaches
 - Paper records are 21% of large breaches
- Approximately 122,000+ reports of breaches of PHI affecting less than 500 individuals

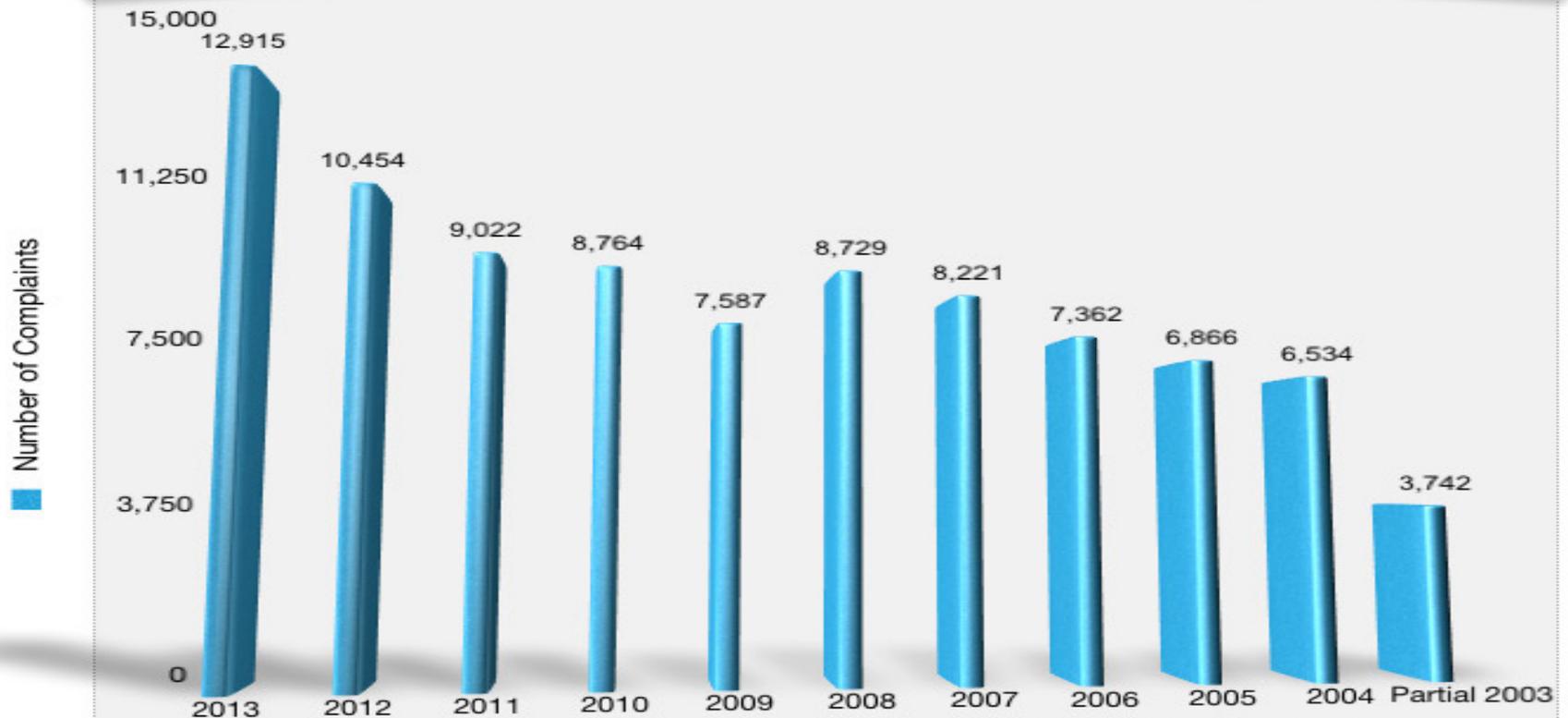


Appropriate Safeguards Prevent Breaches

- Evaluate the risk to e-PHI when at rest on removable media, mobile devices and computer hard drives
- Take reasonable and appropriate measures to safeguard e-PHI
 - Store all e-PHI to a network
 - Encrypt data stored on portable/movable devices & media
 - Employ a remote device wipe to remove data when lost or stolen
 - Consider appropriate data backup
 - Train workforce members on how to effectively safeguard data and timely report security incidents

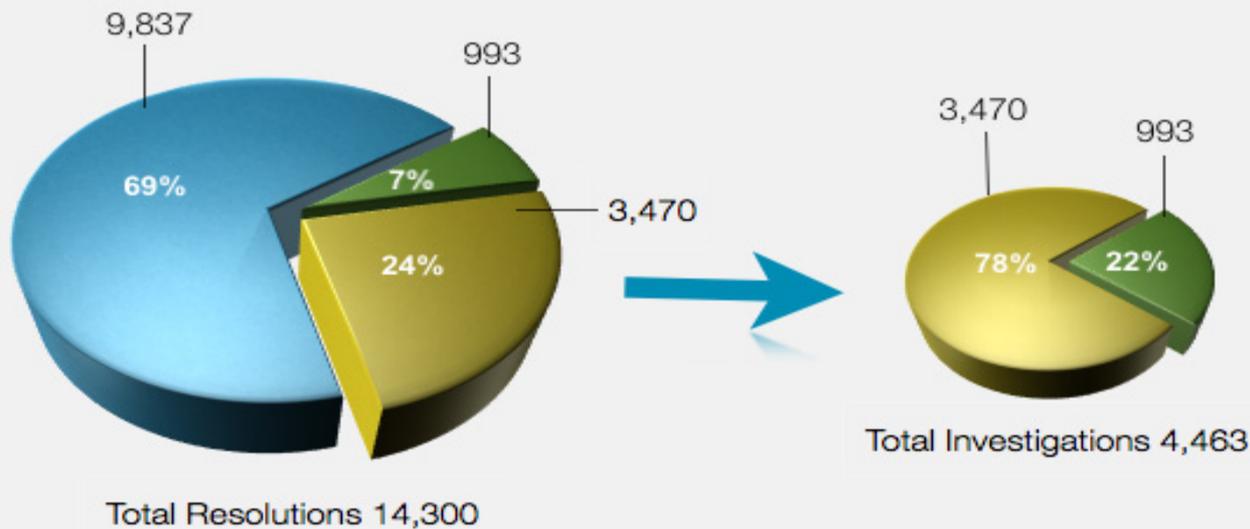


Complaints Received by Calendar Year





Enforcement Results
January 1, 2013 through December 31, 2013



● Resolved after Intake and Review ● No Violation ● Corrective Action Obtained



- Parkview
- NYP/Columbia
- Concentra
- QCA
- Skagit County
- Adult & Pediatric Dermatology, P.C.
- Affinity Health Plan, Inc.



Lessons Learned:

- HIPAA covered entities and their business associates are required to undertake a careful risk analysis to understand the threats and vulnerabilities to individuals' data, and have appropriate safeguards in place to protect this information.
- Take caution when implementing changes to information systems, especially when those changes involve updates to Web-based applications or portals that are used to provide access to consumers' health data using the Internet.
- Senior leadership helps define the culture of an organization and is responsible for knowing and complying with the HIPAA privacy and security requirements to ensure patients' rights are fully protected as well as the confidentiality of their health data.



No findings
or
observations
for 13
entities
(11%)

- 2 Providers, 9 Health Plans, 2 Clearinghouses

Security
accounted
for 60% of the
findings and
observations—
although only
28% of potential
total.

Providers
had a
greater
proportion of
findings &
observations
(65%) than
reflected by
their proportion
of the total set
(53%).

Smaller,
Level 4
entities
struggle
with all
three
areas



Internal analysis for follow up and next steps

- Creation of technical assistance based on results
- Determine where entity follow up is appropriate
- Identify leading practices



Protocol Updates

- Revise CE Protocol to reflect Omnibus Rule
- Develop BA Protocol

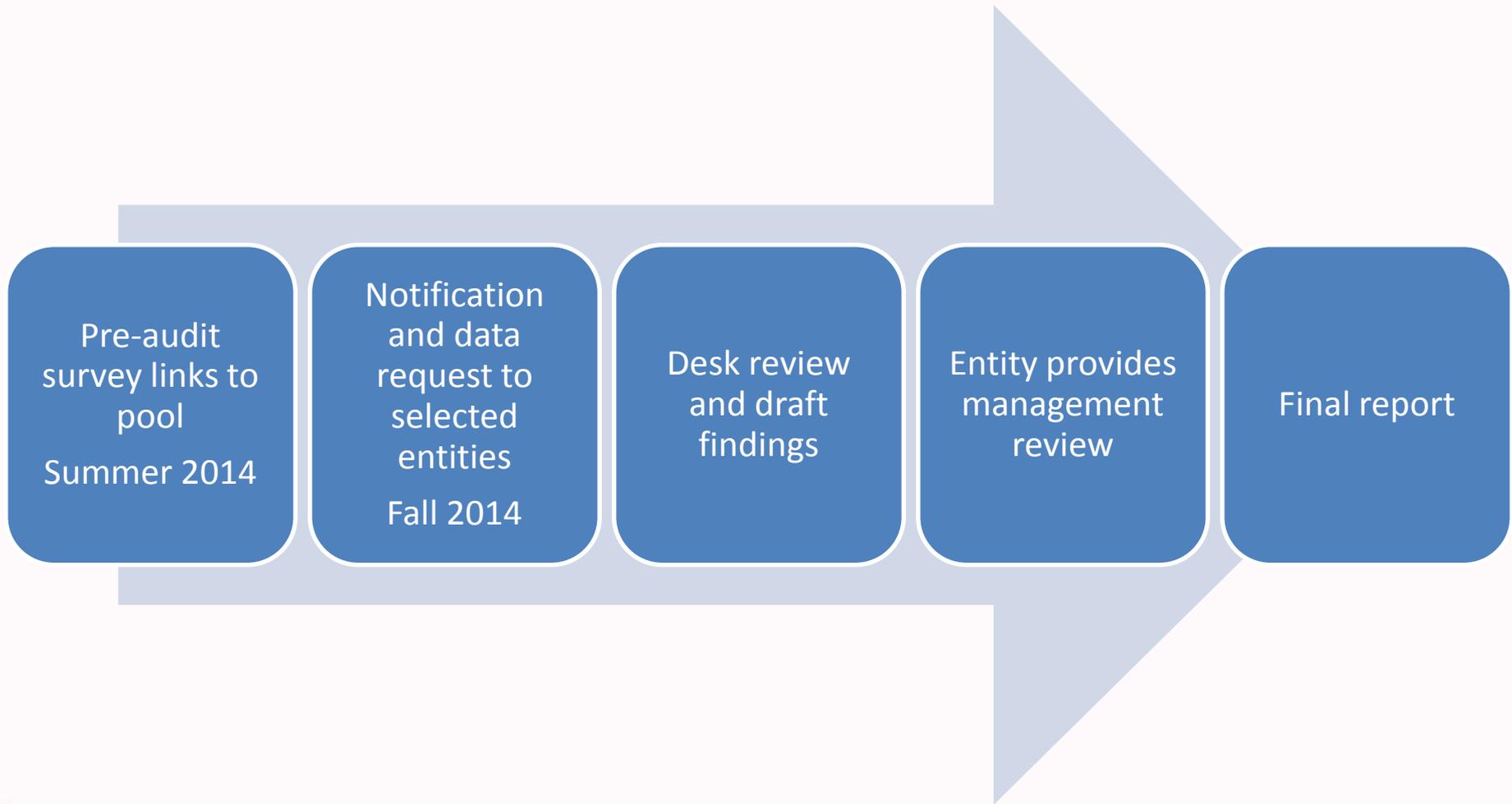


Future program design and focus

- Business Associates: Identify the population.
- Identify areas of focus for future audits.
- Accreditation /Certification correlations?



- Primarily internally staffed
- Selected entities will receive notification and data requests
- Entities will be asked to identify their business associates and provide their current contact information
- Will select business associate audit subjects for first wave from among the BAs identified by covered entities
- Desk audits of selected provisions
- Comprehensive on-site audits as resources allow





Office for Civil Rights

Data request will specify content & file organization, file names, and any other document submission requirements

Only requested data submitted on time will be assessed.

All documentation must be current as of the date of the request.

Auditors will not have opportunity to contact the entity for clarifications or to ask for additional information, so it is critical that the documents accurately reflect the program.

Submitting extraneous information may increase difficulty for auditor to find and assess the required items.

Failure to submit response to requests may lead to referral for regional compliance review



New Guidance:



The HIPAA Omnibus Rule
<https://www.youtube.com/watch?v=mX-QL9PoePU>



Consumer Awareness:



Your New Rights Under HIPAA

- Consumers

https://www.youtube.com/watch?v=3-wV23_E4eQ

**Over 262,000 views since
September 4, 2013**



Mobile Devices:

<http://www.healthit.gov/mobiledevices>

The screenshot shows a web browser displaying the HealthIT.gov website. The page title is "Privacy & Security" and the main heading is "Your Mobile Device and Health Information Privacy and Security". The page features a video player with the title "Worried About Using a Mobile Health Device for Work? Here's What To Do!" and a list of "MOBILE DEVICE RISKS":

- 1) Lost mobile device
- 2) Stolen mobile device
- 3) Downloaded virus
- 4) Shared mobile device
- 5) Unsecured Wi-Fi network

Below the video, there are two sections: "Read and Learn" and "Watch and Learn".

Read and Learn

- How Can You Protect and Secure Health Information When Using a Mobile Device?
- You, Your Organization and Your Mobile Device
- Five Steps Organizations Can Take To Manage Mobile Devices

Watch and Learn

- Worried About Using a Mobile Device for Work? Here's What To Do!
- Securing Your Mobile Device is Important!
- Dr. Anderson's Office Identifies a Risk



<http://www.hhs.gov/ocr/privacy/hipaa/modenotices.html>

Instruction A: Insert the covered entity's name

Instruction B: Insert the covered entity's address, web site and privacy official's phone, email address, and other contact information.



Your Information. Your Rights. Our Responsibilities.

This notice describes how medical information about you may be used and disclosed and how you can get access to this information.
Please review it carefully.

Your Rights

When it comes to your health information, you have certain rights. This section explains your rights and some of our responsibilities to help you.

Get an electronic or paper copy of your medical record

- You can ask to see or get an electronic or paper copy of your medical record and other health information we have about you. Ask us how to do this.
- We will provide a copy or a summary of your health information, usually within 30 days of your request. We may charge a reasonable, cost-based fee.

Ask us to correct your medical record

- You can ask us to correct health information about you that you think is incorrect or incomplete. Ask us how to do this.
- We may say "no" to your request, but we'll tell you why in writing within 60 days.

Request confidential communications

- You can ask us to contact you in a specific way (for example, home or office phone) or to send mail to a different address.
- We will say "yes" to all reasonable requests.

continued on next page



Medscape Resource Center:

<http://www.medscape.org/sites/advanced/patients-rights>

Medscape MULTISPECIALTY Search Location

Today News Reference Education Discussion 0 Post

Protecting Patients' Rights

INTRODUCTION

The Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services administers and enforces the health information privacy, security, and breach notification rules issued under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act. In addition, we play an important role in ensuring that individuals' health information remains private and secure, and that individuals have a right to their health information.

Approved by the U.S. Department of Health and Human Services, Office for Civil Rights

POLLING QUESTION

Who in your practice is responsible for updating privacy and security policies?

- Office manager
- Chief privacy officer
- Chief information officer
- Quality assurance manager
- Other

LEARN ABOUT COMPLYING WITH THE HIPAA PRIVACY AND SECURITY RULES

- Your Mobile Device and Health Information Privacy and Security**
How do you ensure the secure disclosure, storage, use and protection of patients' health information?
Answer: 8/20/10
- Understanding the Basics of HIPAA Security: Risk Analysis and Risk Management**
Do you know the basics of cybersecurity, risk analysis and risk management for electronic protected health information?
Answer: 8/20/10
- Patient Privacy: A Guide for Providers**
Individuals have much control over how their data are used. Do your practice's policies protect their rights?
Last: 8/20/10
- HIPAA and You: Building a Culture of Compliance**
Health care privacy is every one's responsibility. Learn steps to safeguard patient information throughout the care environment.
Last: 8/20/10
- Examining Compliance With the HIPAA Privacy Rule**
An unsecured laptop or outdated privacy policies could lead to hefty fines. Is your practice HIPAA compliant?
Last: 8/20/10

RESOURCES FOR MEDICAL PROFESSIONALS AND BUSINESS ASSOCIATES

- Are You a Covered Entity?
- For Small Providers, Small Health Plans, and Other Small Businesses
- Summary Guidance on Significant Aspects of the Privacy and Security Rules
- Fast Facts for Covered Entities
- Business Associate FAQs
- Simple Business Associate Agreements
- Security Rule Guidance Materials
- Guidance on Risk Analysis
- Mobile Device Security
- Communicating with a Patient's Family, Friends, or Others Involved in the Patient's Care
- FAQs About the Disclosure of Protected Health Information
- Training Materials on the HIPAA Privacy Rule

RESOURCES FOR YOUR PATIENTS

- Your Health Information Privacy Rights
- Privacy, Security, and Electronic Health Records
- Understanding the HIPAA Notice
- Sharing Health Information with Family Members and Friends
- HIPAA: Voices for Consumers



Office for Civil Rights

More Guidance:

- Business Associates
- Breach Notification Rule
- Security Rule
- Individual Rights
- Other Privacy Rule Topics

More Training:

- Online Training Modules

Audit Program



QUESTIONS?