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:"

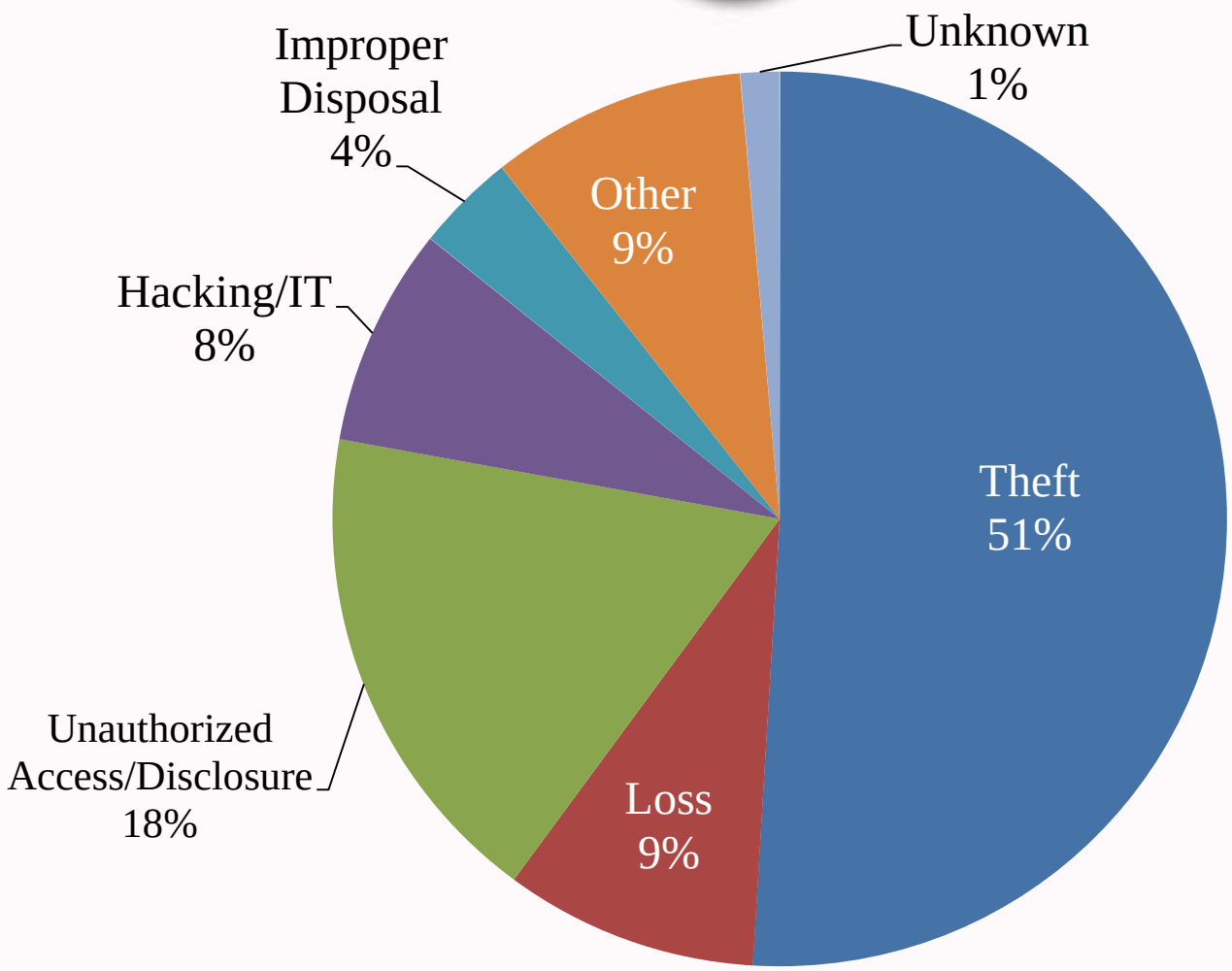
Breach Presumed UNLESS:

- "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.

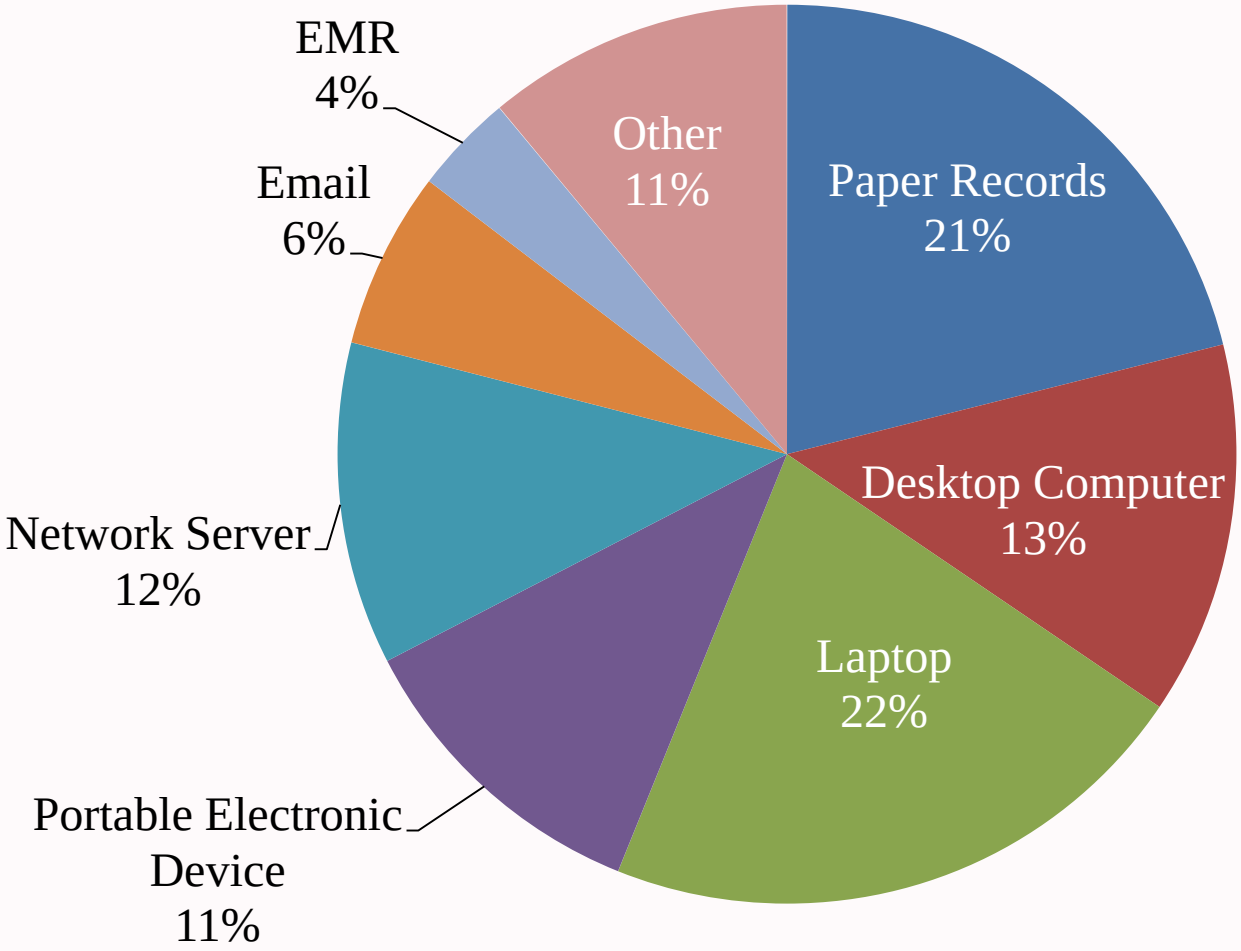
Focus on risk to the data, instead of risk of harm to the individual.

Risk Assessment must be documented.

500+ Breaches by Type of Breach as of 8/31/2014



500+ Breach by Location of Breach as of 8/31/2014



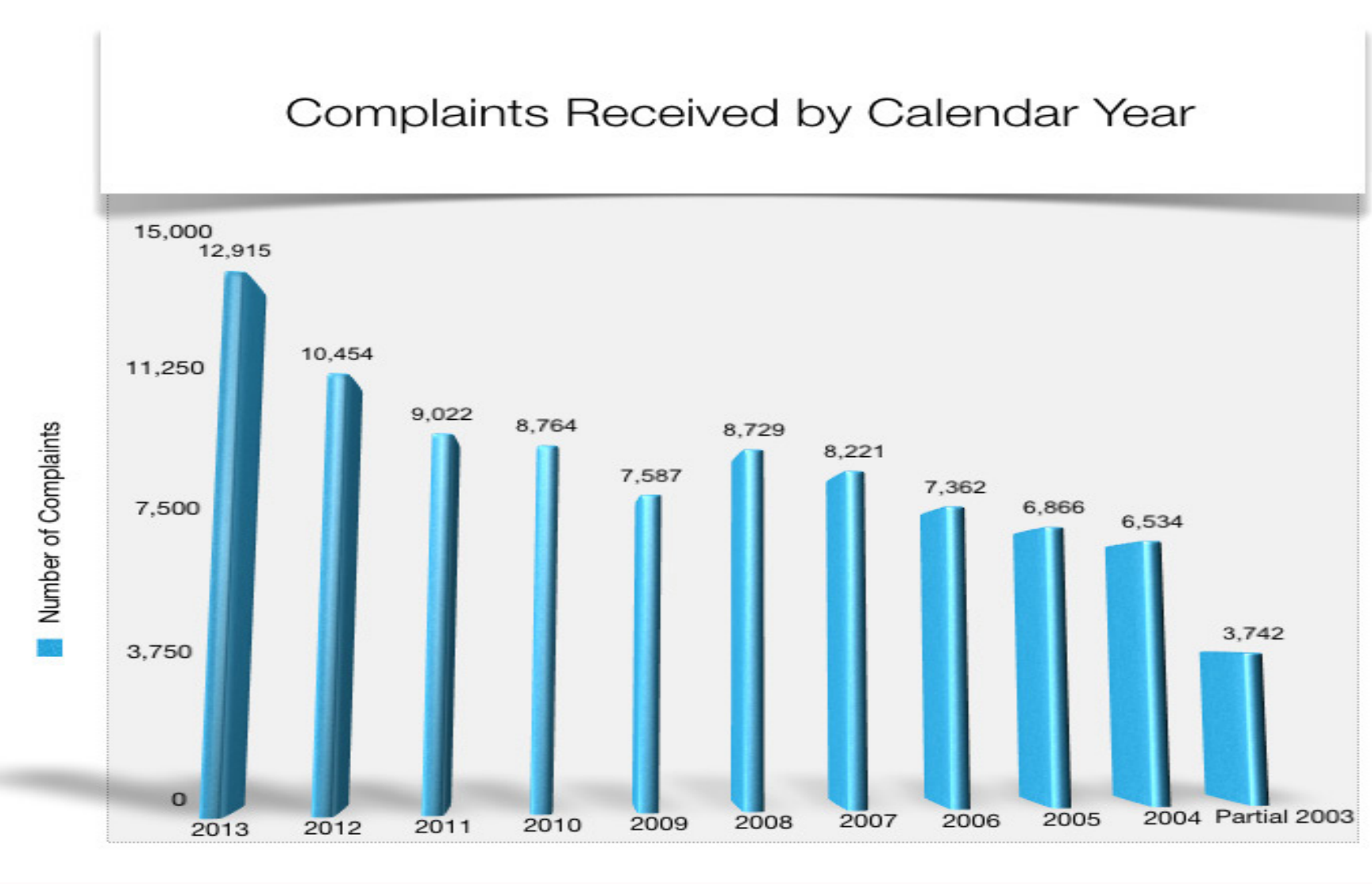
September 2009 through August 31, 2014

- 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

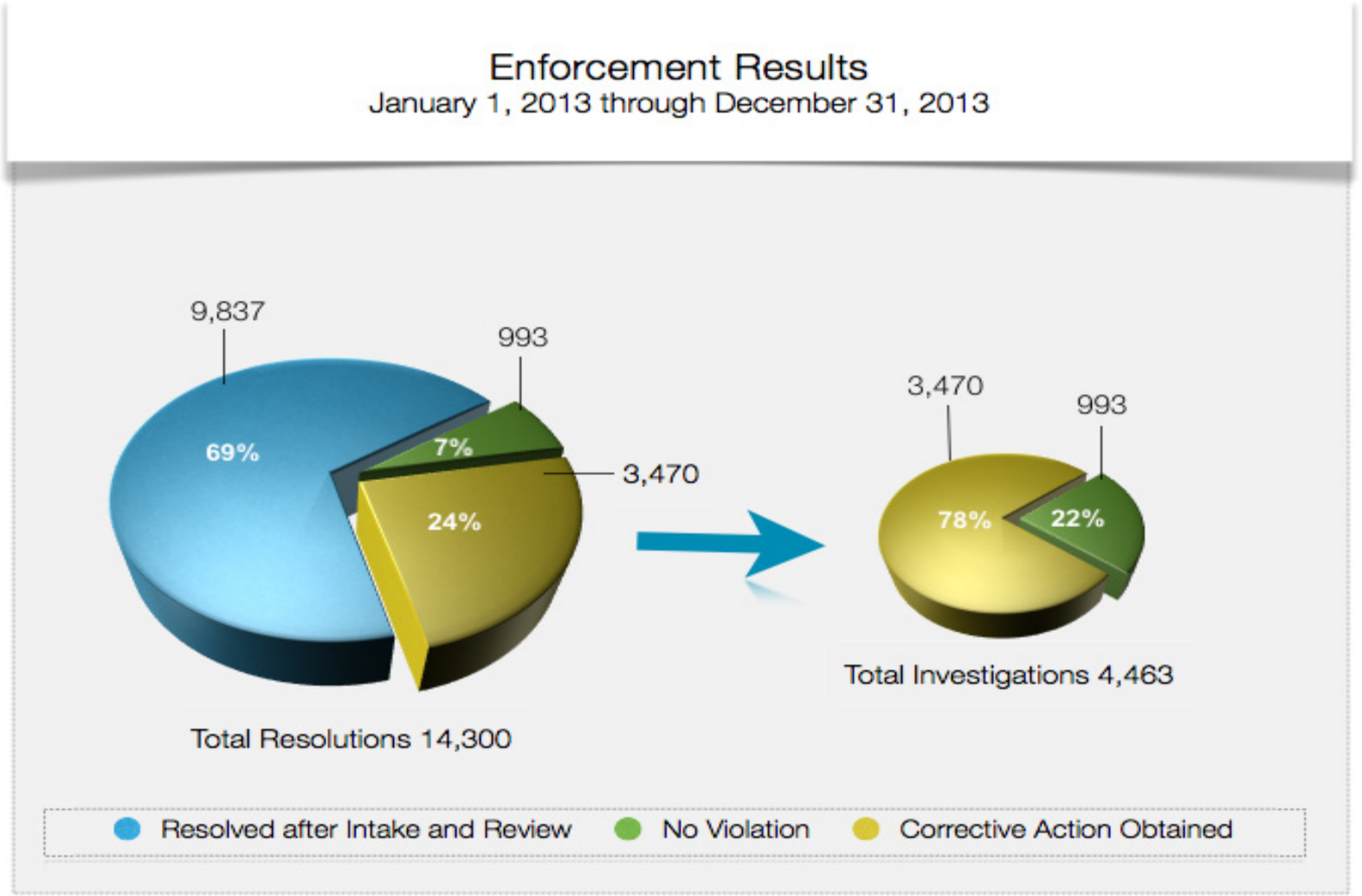
Appropriate Safeguards Prevent Breaches

- 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



2013 CLOSED CASES



RECENT ENFORCEMENT ACTIONS

- 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.

AUDIT PILOT FINIDNGS AND OBSERVATIONS

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

AUDIT PROGRAM NEXT STEPS

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

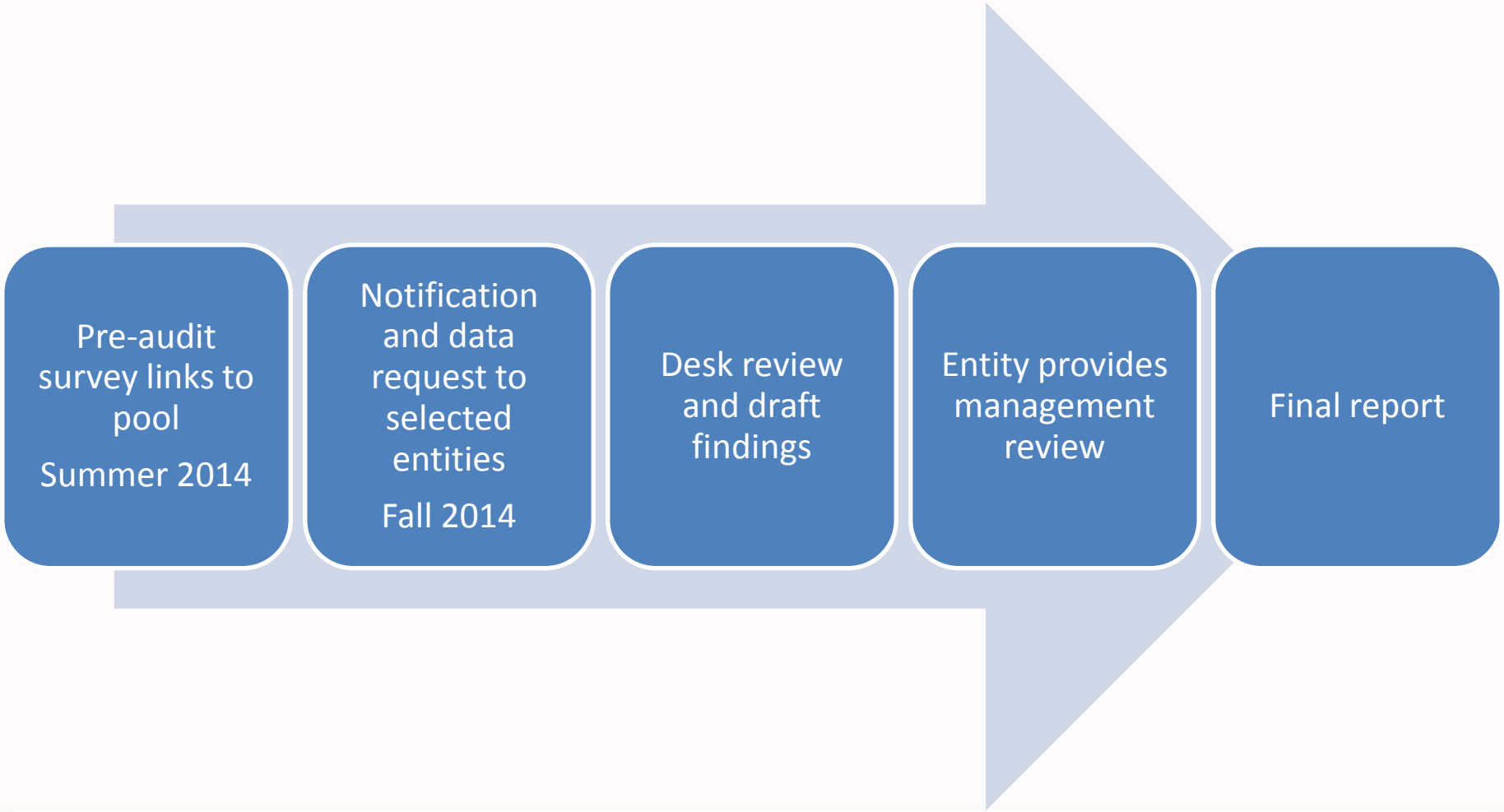
Future program design and focus

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

AUDIT PHASE 2 APPROACH

- 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

PHASE 2 DESK AUDITS



AUDITS PHASE 2 EXPECTATIONS

- 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:

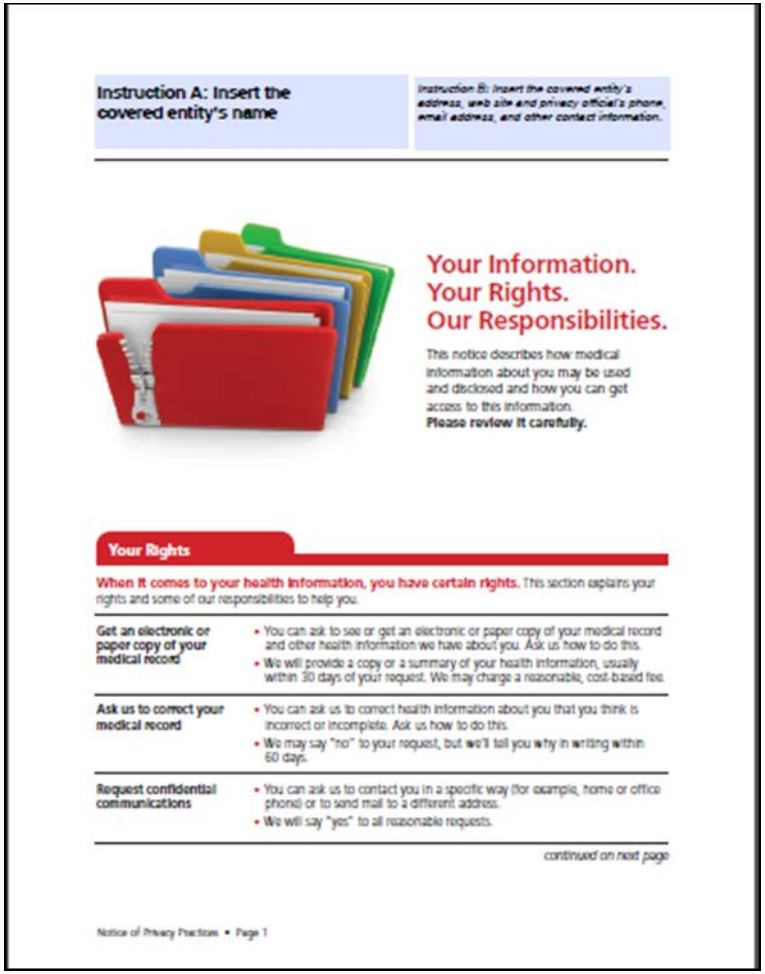
Your New Rights Under HIPAA - Consumers
https://www.youtube.com/watch?v=3-wV23_E4eQ

Over 262,000 views since September 4, 2013

Mobile Devices:

http://www.healthit.gov/mobiledevices

http://www.hhs.gov/ocr/privacy/hipaa/modelnotices.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.

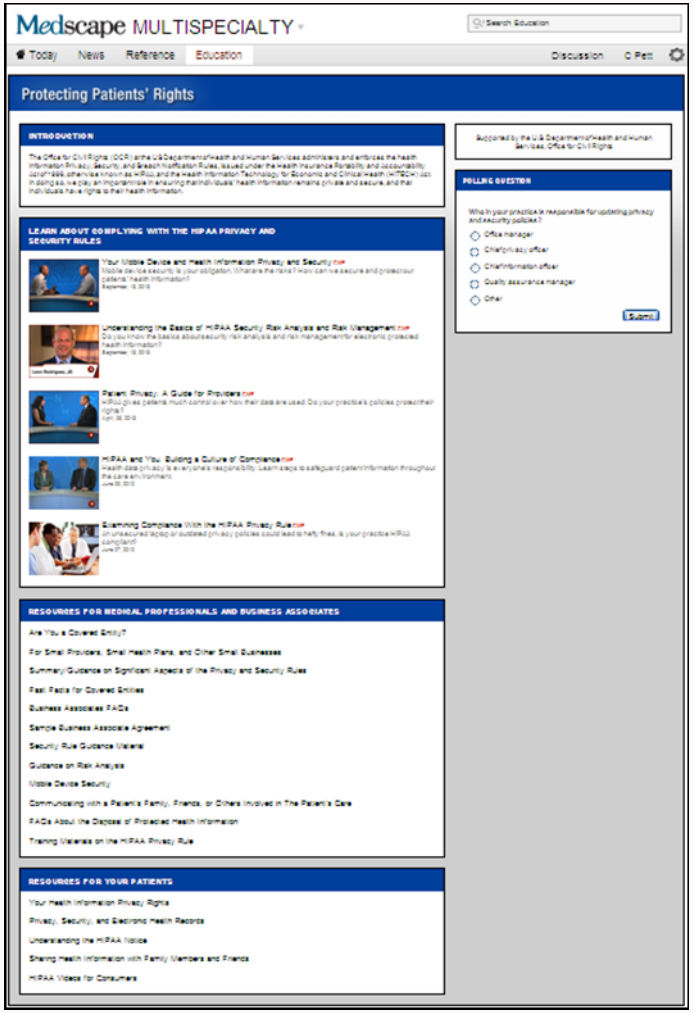
Get an electronic or paper copy of your medical record	• You can ask to see or get an electronic or paper copy of your medical record and other health information we have about you. Ask us how to do this. • We will provide a copy or a summary of your health information, usually within 30 days of your 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

Notice of Privacy Practices • Page 1

Medscape Resource Center:

http://www.medscape.org/sites/advances/patients-rights



More Guidance:

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

More Training:

- Online Training Modules

Audit Program

QUESTIONS?