Updates on OCR's HIPAA Enforcement and Regulations

Hospital Council of Western Pennsylvania

June 21, 2012

Topics

- HIPAA Privacy and Security Rule Enforcement
- HITECH Breach Notification
- OCR Audit Program
- Regulations and Compliance Tools for 2012

HIP Enforcement Results

Complaints and Compliance Reviews by Year	2011	2010
Opened	9032	8770
Closed	8370	9189
Closed After Corrective Action	2595	2709
Investigation Found No Violation	1303	1529
Resolved After Intake & Review	4472	4951

Security Rule Enforcement Results

Complaints and Compliance Reviews by Year	2011	2010
Closed	203	128
Closed After Corrective Action	158	70
Investigation Found No Violation	15	18
Closed Without Investigation	30	40

Enforcement Highlights

- **April 2012 – Phoenix Cardiac Surgery**
  - $100,000 RA/CAP
  - Failed to secure appointment calendaring app
  - Failed to have risk analysis and risk management processes under Security Rule
- **Lessons Learned**
  - Small providers must comply
  - Pay attention to fundamentals of security – standards are flexible and scalable
  - Security in the “Cloud”

Enforcement Highlights

- **March 2012 – BlueCross/BlueShield of TN**
  - $1.5 million RA/CAP
  - Theft of servers affecting over 1 million individuals
  - Failure to assess and remediate changes in security risk to ePHI due to relocation
- **Lessons Learned**
  - Security applies to all ePHI
  - Revise the risk analysis/risk management plan to address changes in security environment
  - Security is entity's responsibility – don't rely on 3d parties without a business associate agreement

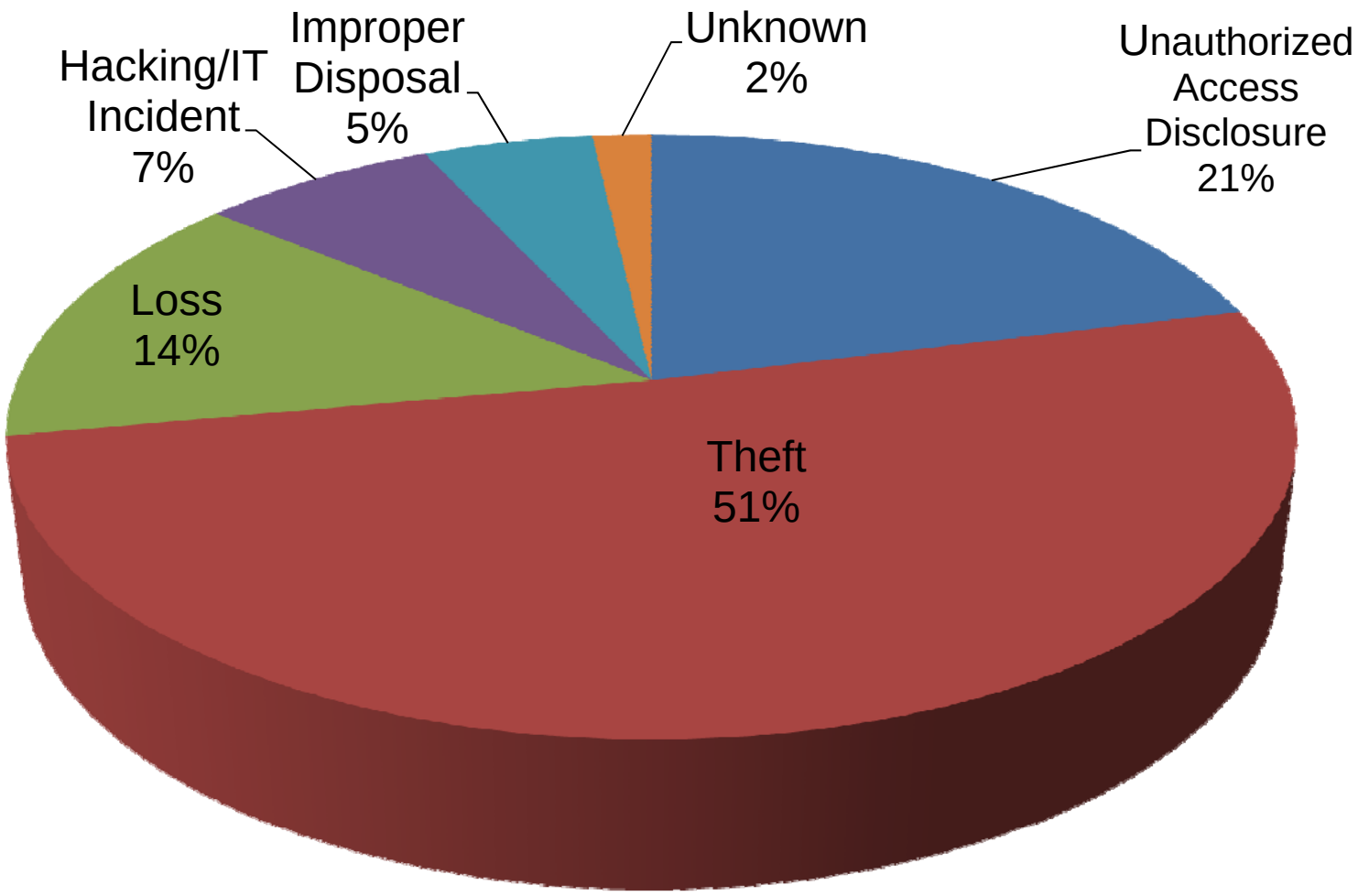
Breach Notification Highlights

September 2009 through May 31, 2012

- 435 reports involving a breach of over 500 individuals
  - Theft and Loss are 65% of large breaches (about 70% of these incidents involved ePHI)
  - Laptops and other portable storage devices account for 38% of large breaches
  - Paper records are 24% of large breaches
- 57,000+ reports of breaches of under 500 individuals

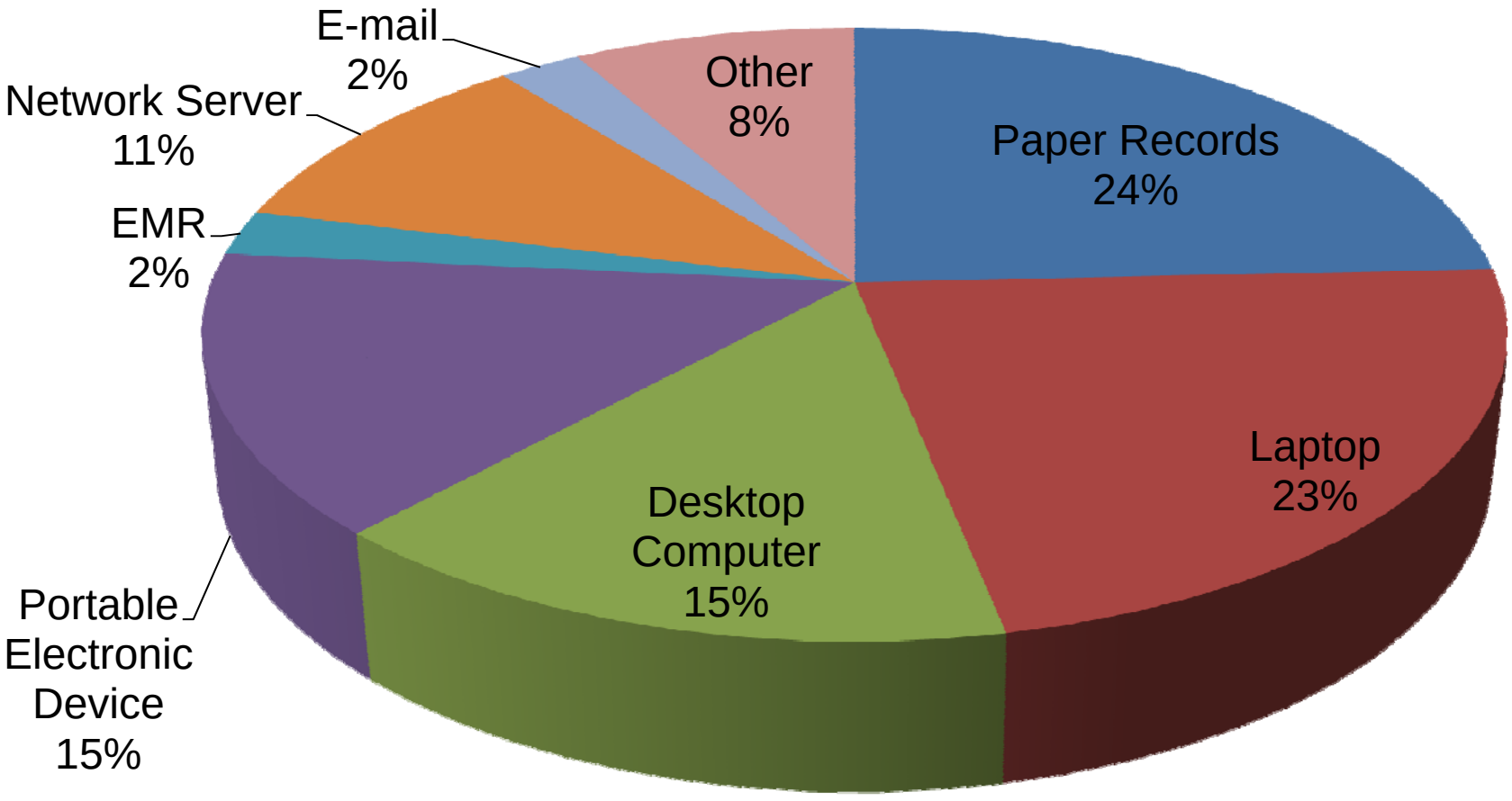
Breach Notification:

500+ Breaches by Type of Breach



Breach Notification:

500+ Breaches by Location of Breach



Risks in Storing & Transporting e-PHI

- Back-up tapes stolen from BA employee car – 4.9 million affected
- Lost back-up tapes in office renovation – over 1 million affected
- Desktop computer stolen from health care provider's office -- 943,000 affected
- Theft of laptop and hard drive of BA – 71,000 affected (patients of 1 plan & 6 providers)
- Improper disposal of computer damaged in flood -- 55,000 affected

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
  - Train workforce members on how to effectively safeguard data and timely reporting of incidents

Audit

- All audits in pilot to end December 2012
- KPMG final report will highlight themes, consistent findings, possible root causes, leading practices
- Evaluation contract to conduct analysis
- Pilot experience and reports will feed into decisions re ongoing audit program
  - Structure, focus, size

Background

- Section 13411 of the HITECH Act requires HHS to provide for periodic audits to ensure covered entities and business associates are complying with the HIPAA Privacy and Security Rules and Breach Notification standards
- OCR is piloting a program to perform up to 115 audits by 12/2012 of covered entities to assess HIPAA privacy and security performance

Program Objective

- Audits present a new opportunity to:
  - Examine mechanisms for compliance
  - Identify best practices
  - Discover risks and vulnerabilities that may not have come to light through complaint investigations and compliance reviews
  - Encourage renewed attention to compliance activities

Who Will be Audited?

- Every covered entity is eligible for an audit
- OCR seeks to audit as wide a range of types and sizes of covered entities as possible which includes:
  - Health plans of all sizes
  - Health care clearinghouses
  - Individual and organizational providers
- Business Associates in later audit wave

First 20 Auditees by Entity Type

	Level 1	Level 2	Level 3	Level 4	Total
Health Plans	2	3	1	2	8
Healthcare Providers	2	2	2	4	10
Healthcare Clearinghouses	1	1	0	0	2
Total	**5**	**6**	**3**	**6**	**20**

REGULATIONS AND OTHER COMPLIANCE TOOLS FOR 2012

Omnibus HITECH/GINA/HIPAA

- Final Rulemaking Combining:
  - July 2010 NPRM on HITECH changes to HIPAA
  - October 2009 NPRM on GINA changes to HIPAA
  - August 2009 IFR on Breach Notification
  - October 2009 IFR on Enforcement Rule
- Compliance Dates: 180 days from effective date

HIPAA/HITECH/GINA Omnibus Rule

- **HITECH NPRM Content:**
  - Business associates
  - Enforcement
  - Electronic access
  - Marketing
  - Fundraising
  - No sale of PHI
  - Right to request restrictions
- **HITECH IFR Content:**
  - Breach Notification Rule
  - Enforcement Rule
- **GINA NPRM Content:**
  - Genetic information is protected health information
  - Prohibit the use or disclosure of genetic information for underwriting
- **HIPAA NPRM Content**:
  - Harmonize research authorizations
  - Share student immunization records
  - Share decedent information

GINA

- Genetic Information Non-discrimination Act
  - Requires “genetic information” be treated as protected health information under HIPAA
  - Prohibits the use or disclosure of genetic information for underwriting purposes by health plans
  - Terms and definitions track regulations prohibiting discrimination in provision of health insurance based on genetic information

ComplianceTools

- Risk Analysis Guidance
  - OCR website July 2010
- NIST Security Rule Tool
- Small Provider Guidance
- ONC/OCR Mobile Device Roundtable
  - March 19
- De-identification Guidance
  - Target date – Summer 2012

NIST HIPAA Security Rule Toolkit

- A toolkit to help covered entities and their business associates
  - better understand the requirements of the HIPAA Security Rule
  - implement those requirements
  - assess those implementations in their operational environments
  - A self-contained, desktop based application that can support various operating environments (e.g. Microsoft Windows, Apple OS-X, Linux)
- **http://scap.nist.gov/hipaa**

Want More Information?

The OCR website, http://www.hhs.gov/ocr/privacy/ offers a wide range of helpful information about health information privacy including educational information, FAQ's, rule text and guidance for the Privacy, Security, and Breach Notification Rules.