

The Office of the National Coordinator for
Health Information Technology



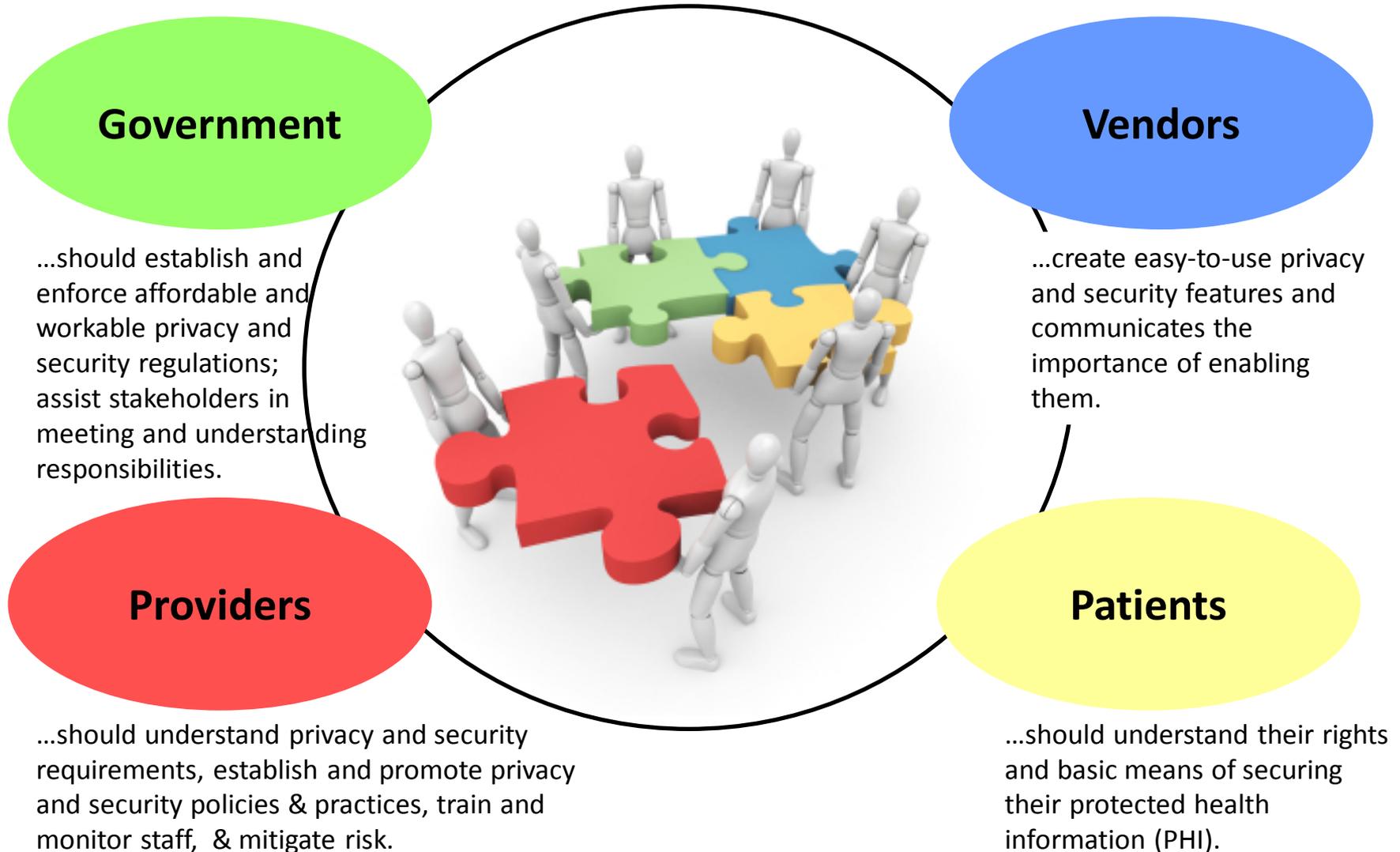
Keeping Health Information Private and Secure

New Initiatives and Tools

Office of the National Coordinator

December 12, 2012





HITECH Regulations and Enforcement

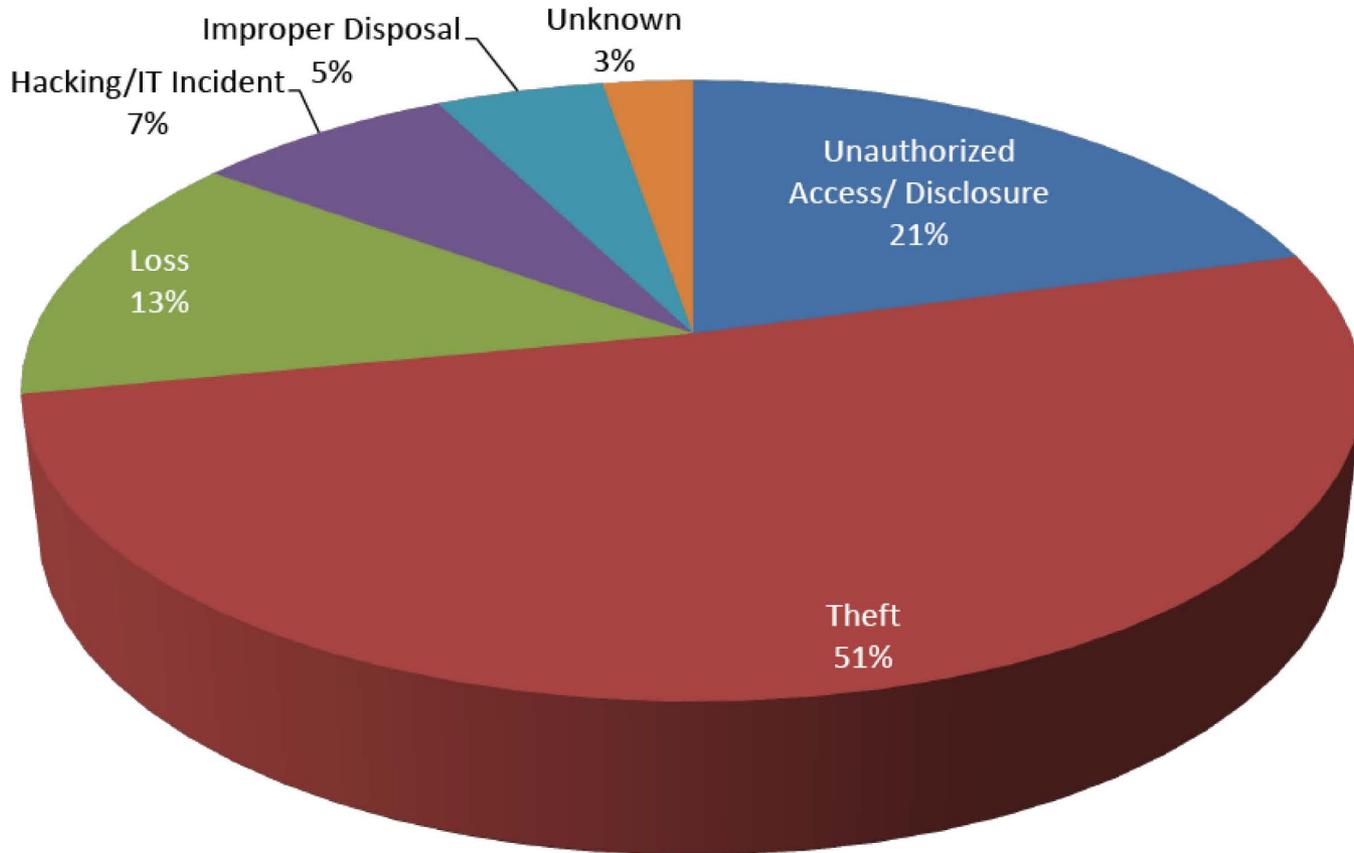
Director Leon Rodriguez
U.S. Department of Health and Human
Services
Office for Civil Rights

Breach Notification Reports

- Universe of breach notification reports
 - Over 500 reports involving 500 or more individuals, +21.4 million individuals affected and growing
 - 3,684,514 individuals affected by theft or loss of laptops or other portable electronic devices
 - Over 60,500 reports involving under 500 individuals
- Top types of large breaches
 - Theft
 - Unauthorized Access/Disclosure
 - Loss
- Top locations for large breaches
 - Paper records
 - Laptops
 - Desktop Computers
 - Portable Electronic Device

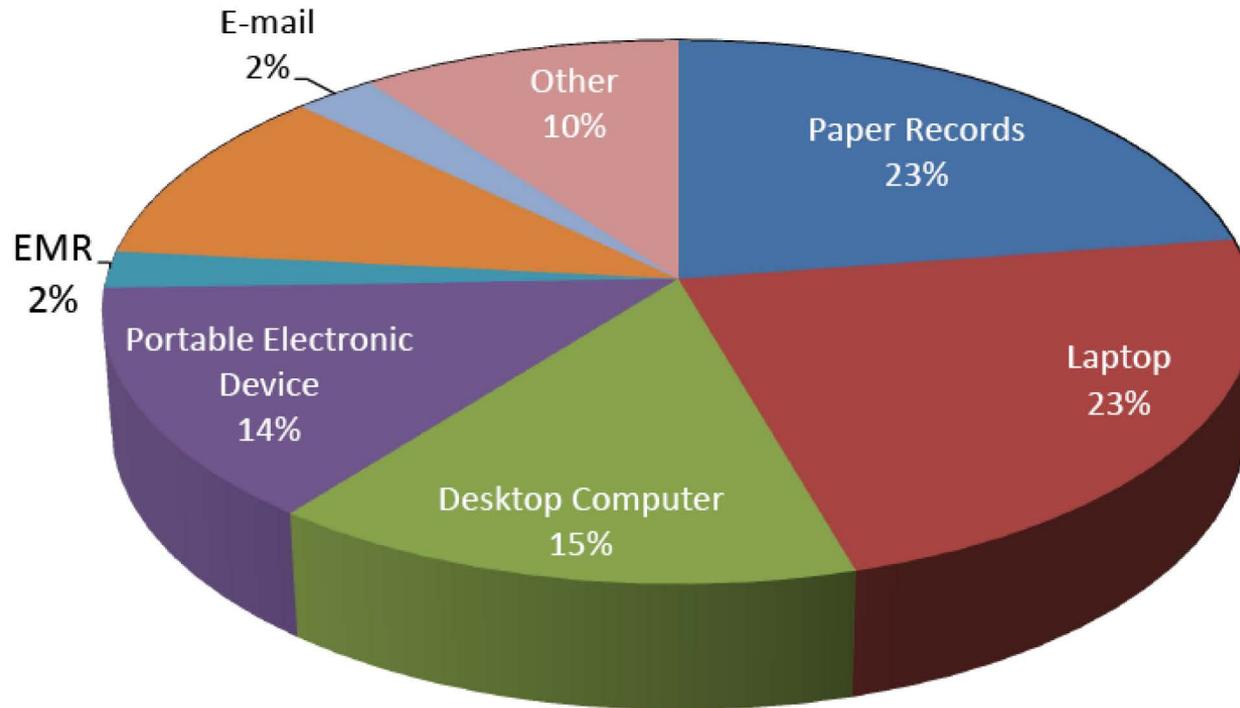
Breach Notification

500+ Breaches by Type of Breach



Breach Notification

500+ Breaches by Location of Breach



Breach Notification Reports

Recent Breaches and Highlights

- Hacking incident involving network server (780,000 affected)
- Backup tapes stored at hospital cannot be found (315,000 affected)
- Unencrypted emails sent to employee's unsecured email address (228,435 affected)
- Theft of electronic medical records from covered entity (102,153 affected)
- Theft of laptop from contractor's vehicle (66,601 affected)
- Unauthorized disclosure of protected health information (PHI) by employees (64,846 affected)
- Theft of portable electronic device from employee's vehicle (55,000 affected)

Breakdown of First 20 Auditees

Level 1 Entities - Large provider / health plan

- 11% of the first 20 auditees
- 4% with privacy audit issues
- Extensive use of HIT - complicated HIT enabled clinical /business work streams
- Revenues and or assets greater than \$1 billion

Level 3 Entities - Community hospitals, outpatient surgery, regional pharmacy / self-insured entities that do not adjudicate their claims

- 15% of the first 20 auditees
- 16% with privacy audit issues
- Some but not extensive use of HIT – mostly paper based workflows
- Revenues between \$50 - \$300 million

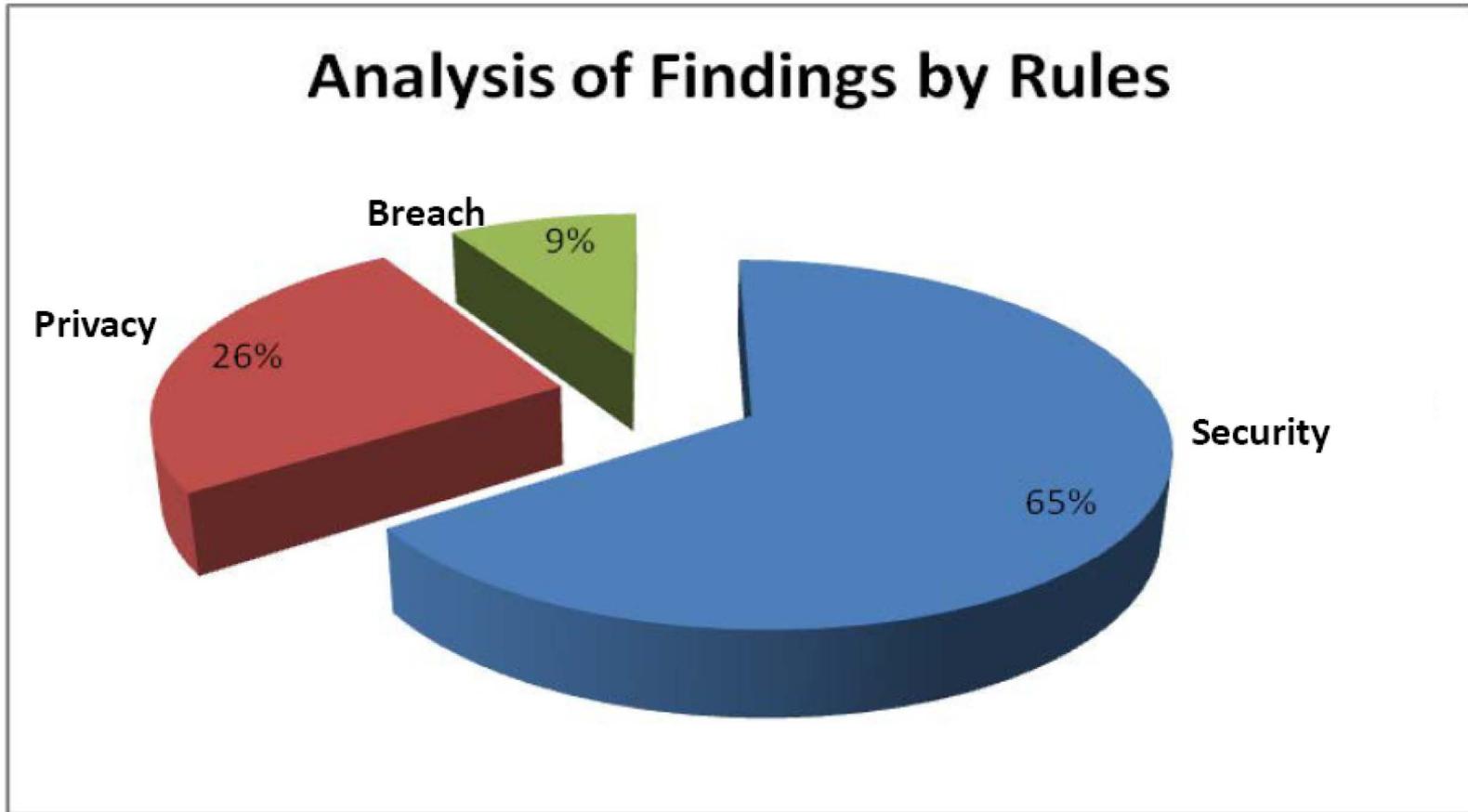
Level 2 Entities - Large regional hospital system (3-10 hospitals/region) / regional insurance company

- 8% of the first 20 auditees
- 3% with privacy audit issues
- Paper and HIT enabled work flows
- Revenues and or assets between \$300 million and \$1 billion

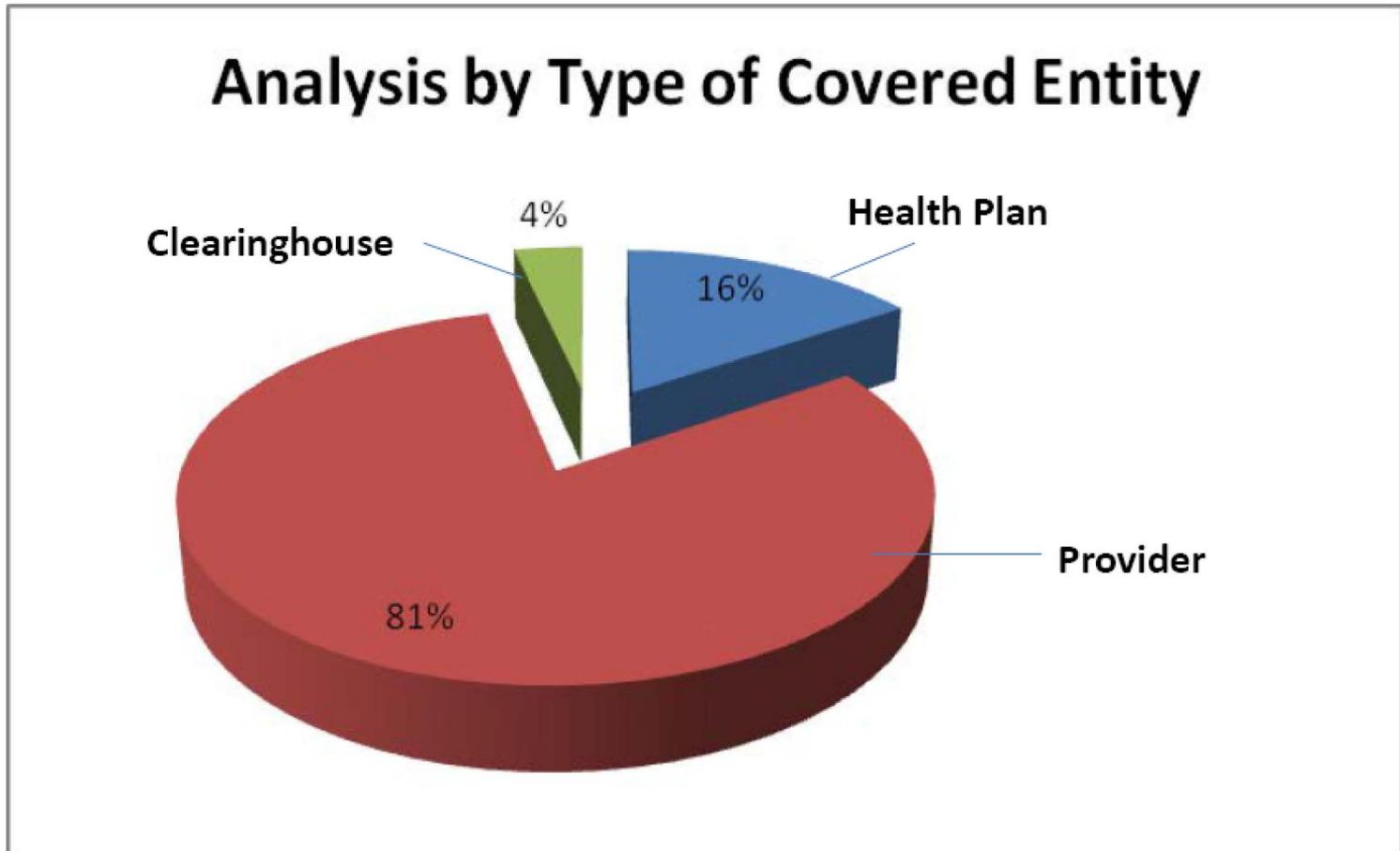
Level 4 Entities - Small providers (10 to 50 provider practices, community or rural pharmacy) 66% of the first 20 auditees

- 77% with privacy audit issues
- Little to no use of HIT – almost exclusively paper based workflows
- Revenues less than \$50 million

Initial 20 Findings Analysis Overview

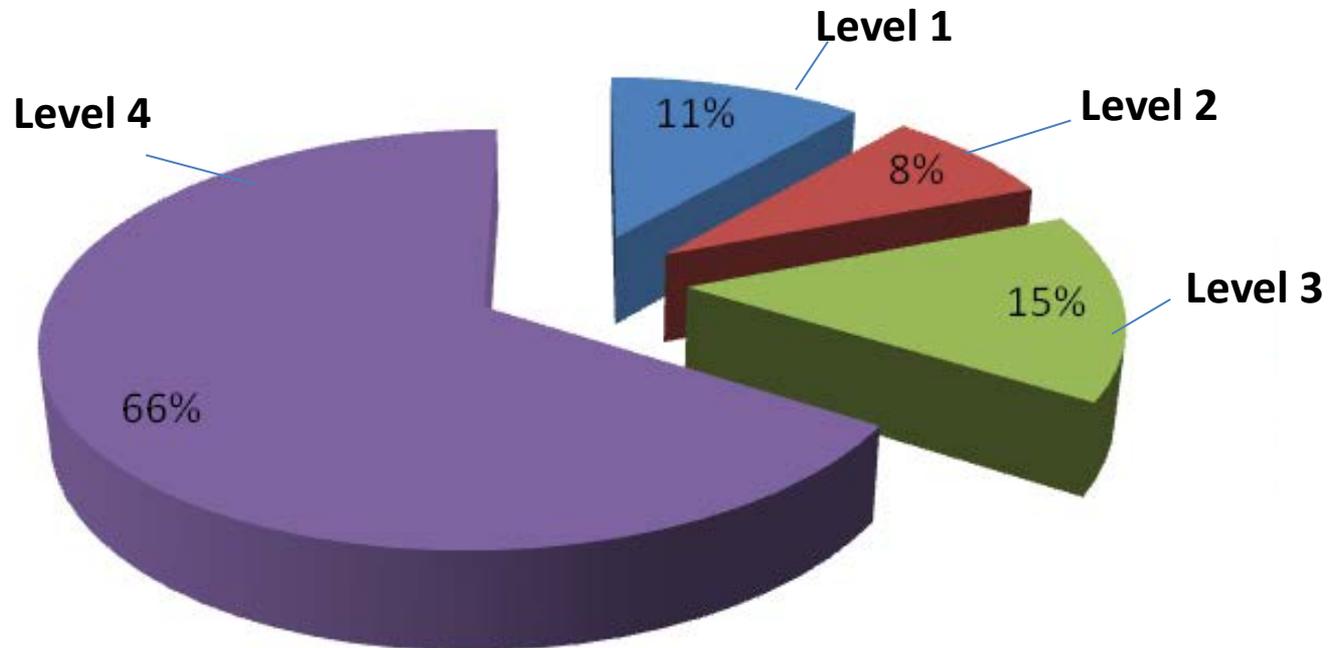


Initial 20 Findings Analysis Overview



Initial 20 Findings Analysis Overview

Analysis of Finding by Tier



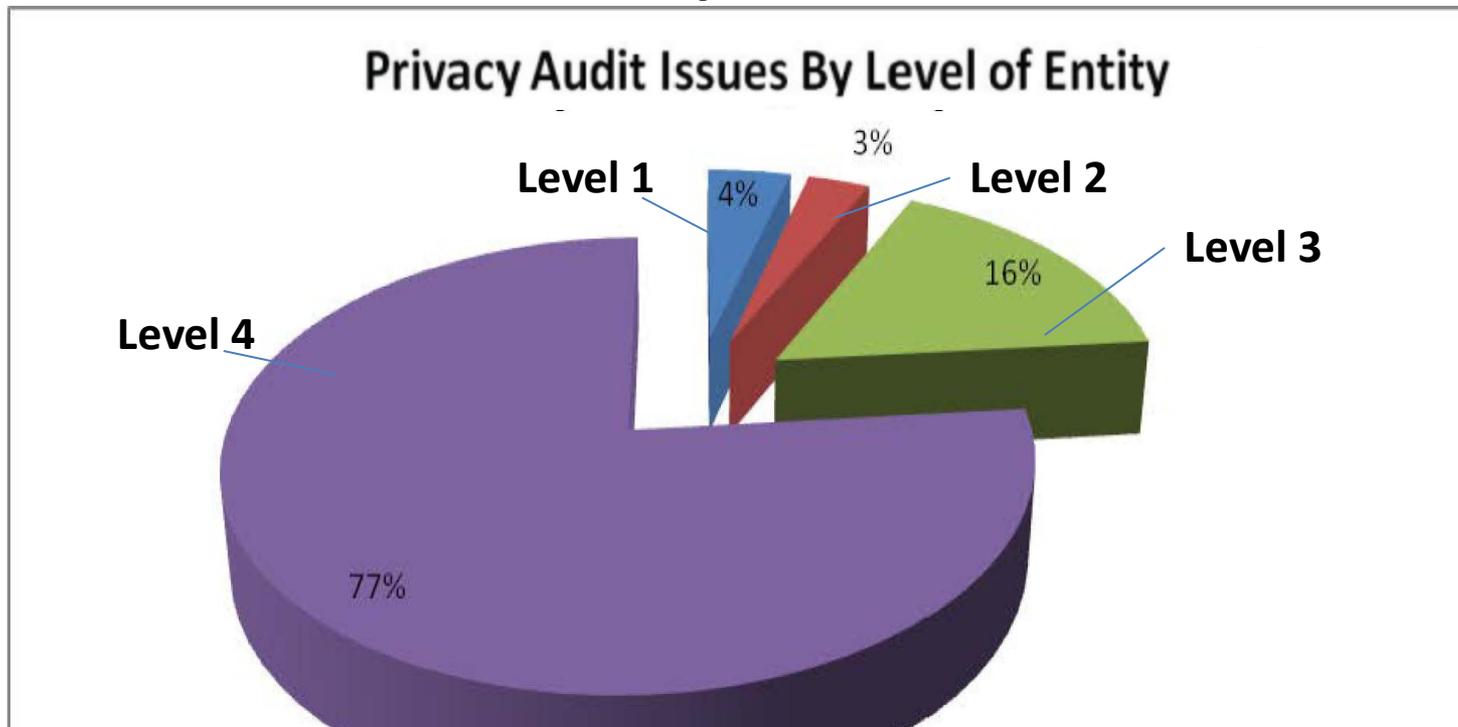
Level 1 Entities - Large Provider / Health Plan

Level 2 Entities - Large regional hospital system (3-10 hospitals/region) / Regional Insurance Company

Level 3 Entities - Community hospitals, outpatient surgery, regional pharmacy / All Self-Insured entities that don't adjudicate their claims

Level 4 Entities - Small Providers (10 to 50 Provider Practices, Community or rural pharmacy)

Initial 20 Findings Analysis Privacy Issues



Level 1 Entities - Large Provider / Health Plan

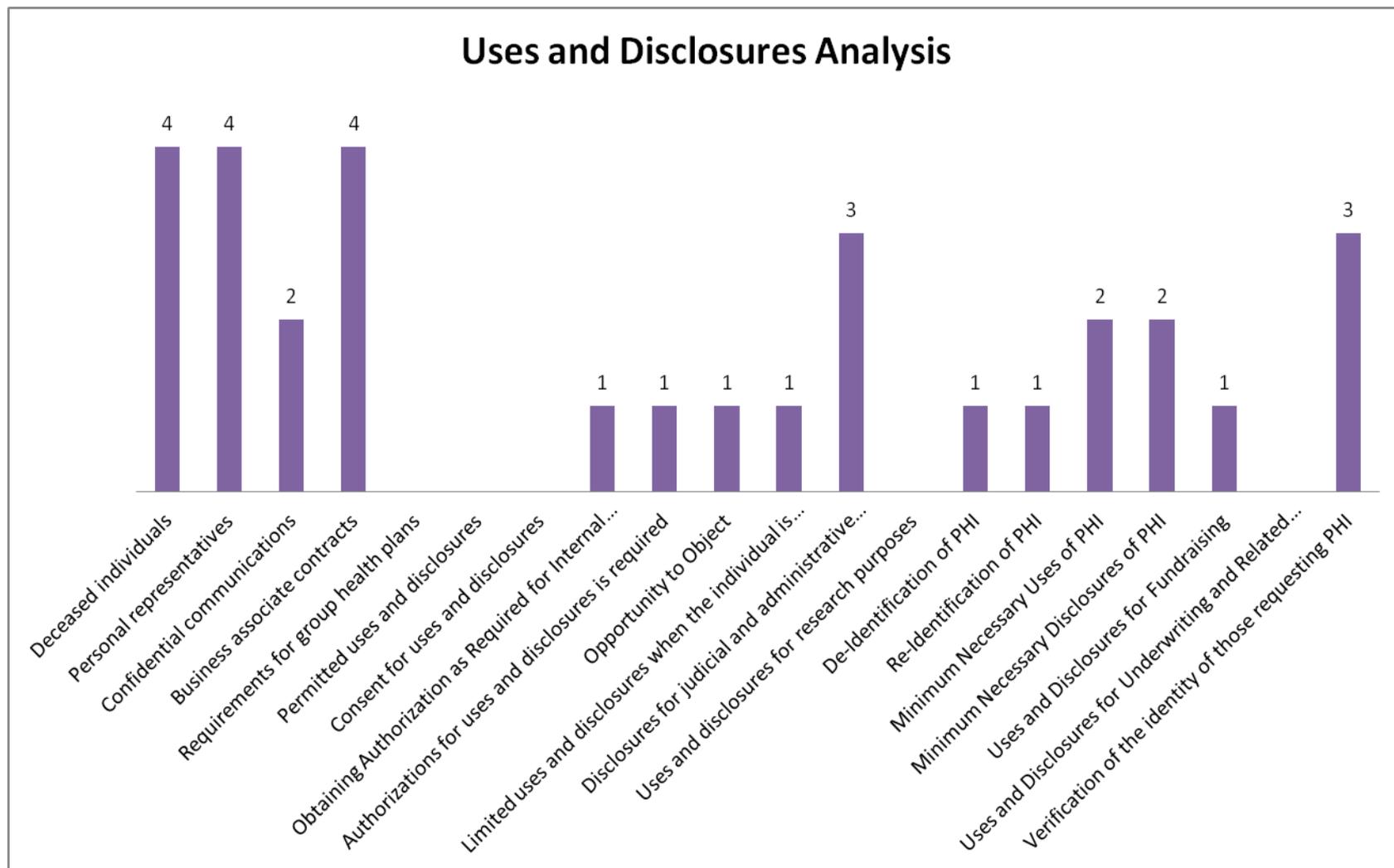
Level 2 Entities - Large regional hospital system (3 to 10 hospitals/region) / Regional Insurance Company

Level 3 Entities - Community hospitals, outpatient surgery, regional pharmacy / All Self-Insured entities that don't adjudicate their claims

Level 4 Entities - Small Providers (10 to 50 Provider Practices, Community or rural pharmacy)

Initial 20 Findings Analysis

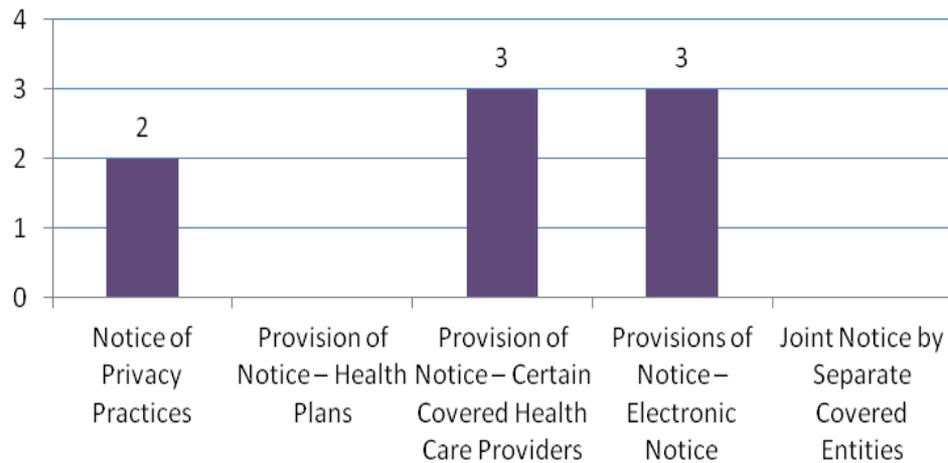
Privacy: Uses and Disclosures



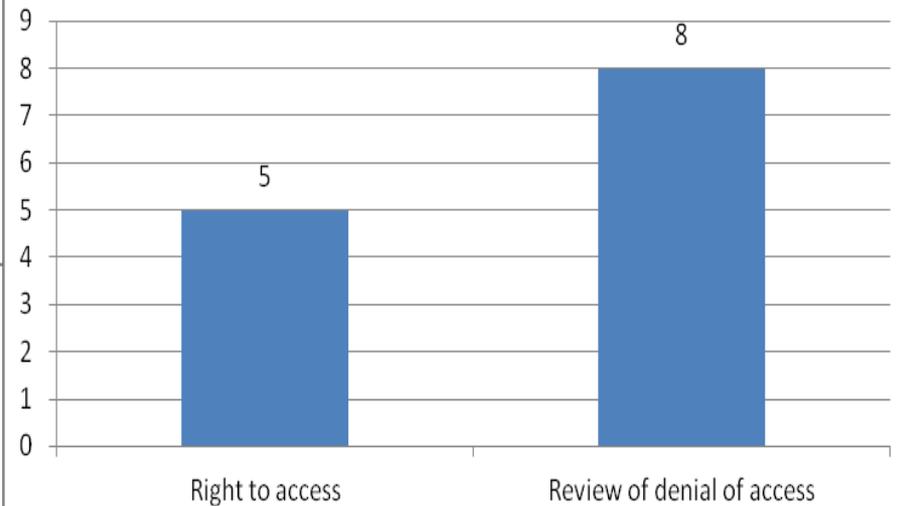
Data as of June 2012

Initial 20 Findings Analysis Privacy: Notice and Access

**Notice of Privacy Practices for PHI –
\$164.520**



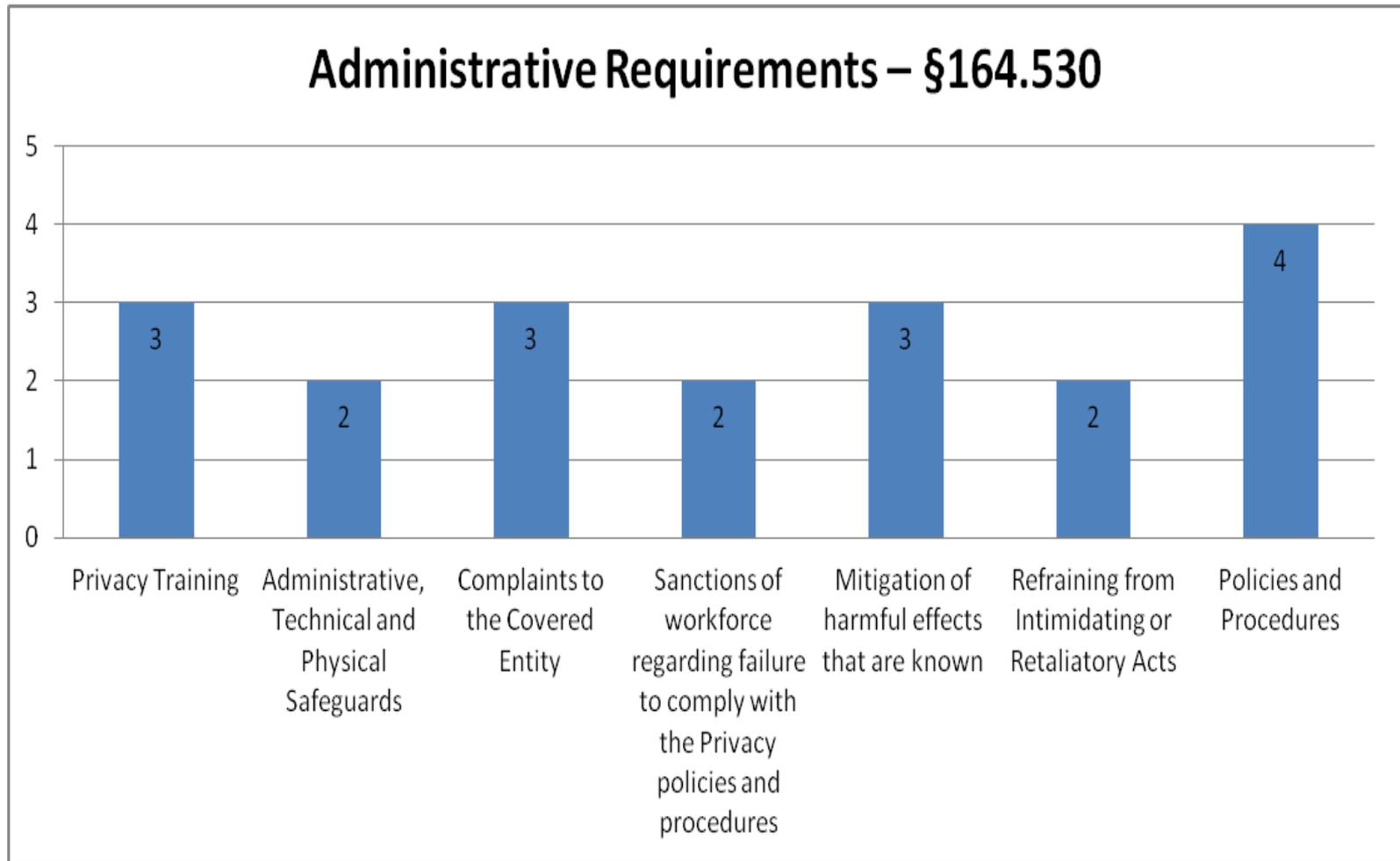
**Access of Individuals to PHI –
\$164.524**



Data as of June 2012.

Initial 20 Findings Analysis

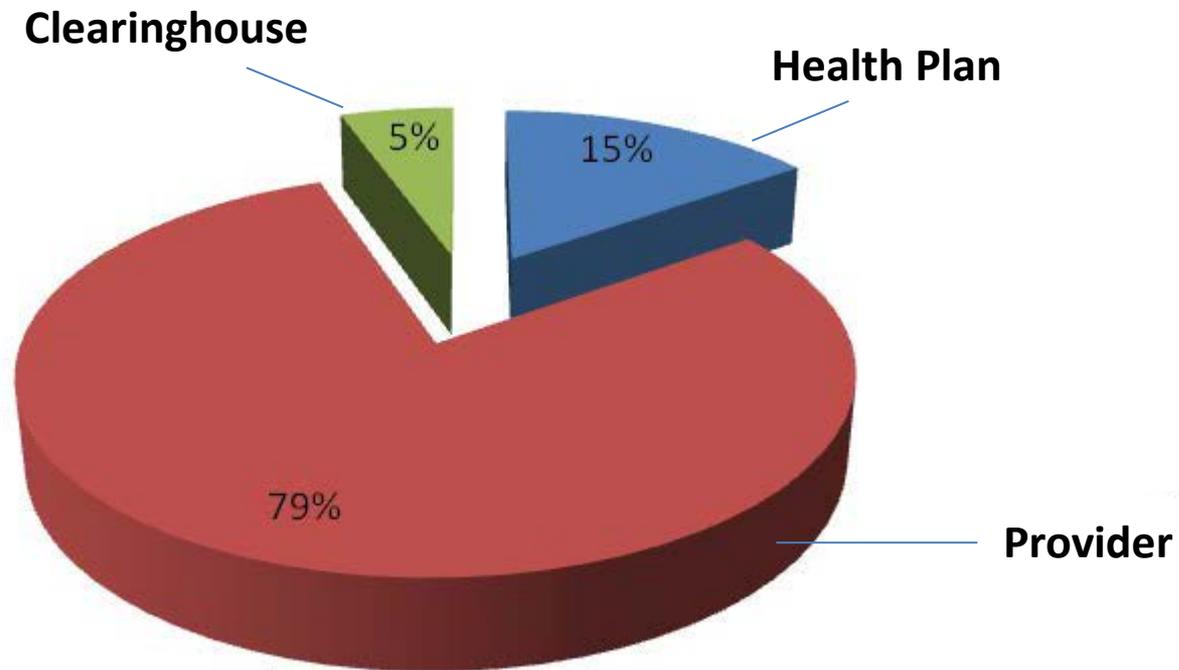
Privacy: Administrative Requirements



Data as of June 2012.

Initial 20 Findings Analysis Security Issues

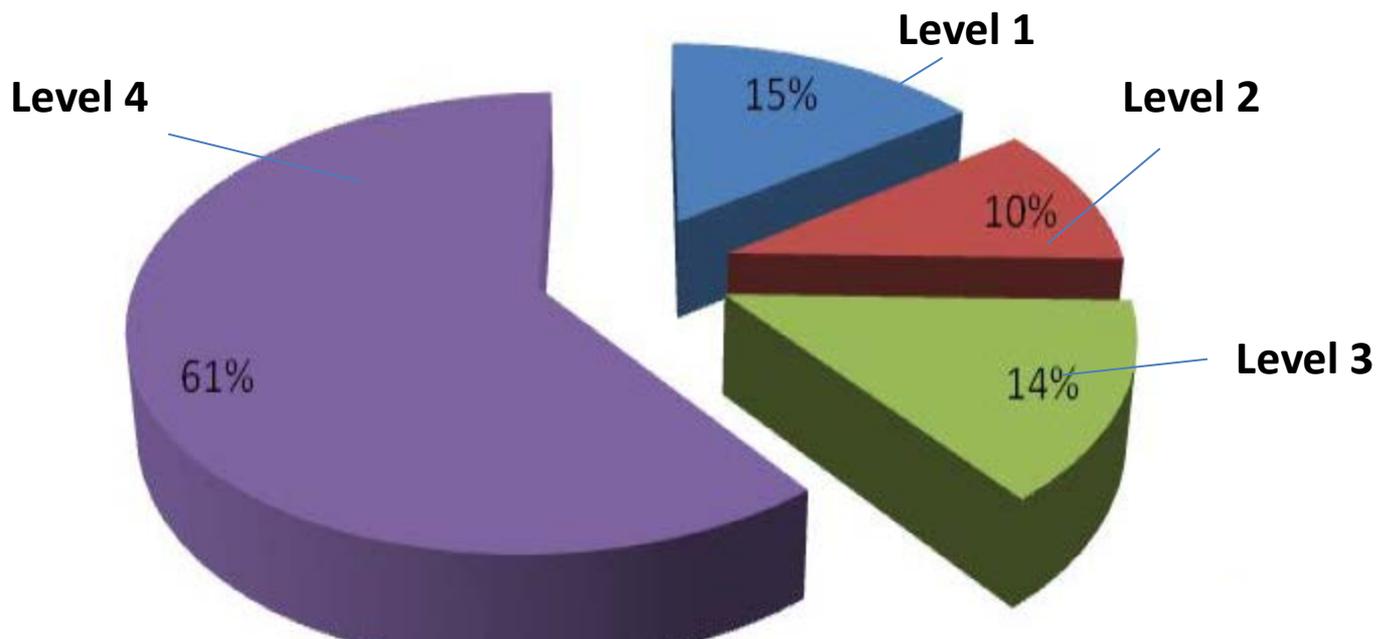
Security Audit Issues by Type of Entity



Data as of June 2012.

Initial 20 Findings Analysis Security Issues

Security Audit Issues by Level of Entity



Level 1 Entities - Large Provider / Health Plan

Level 2 Entities - Large regional hospital system (3 to 10 hospitals/region) / Regional Insurance Company

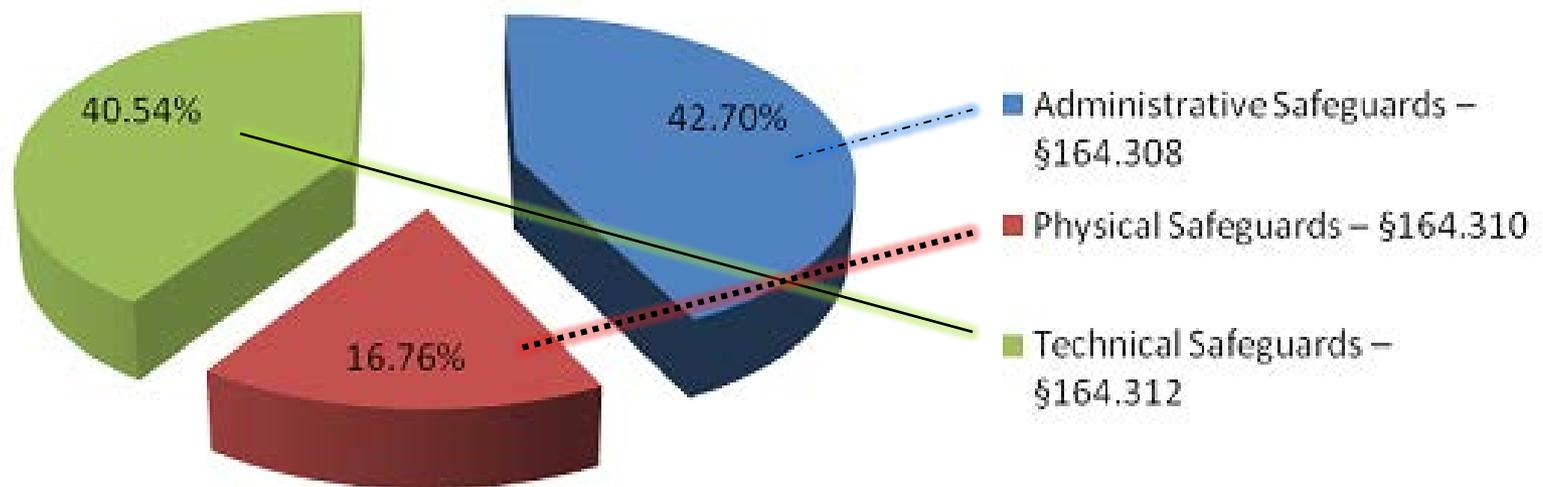
Level 3 Entities - Community hospitals, outpatient surgery, regional pharmacy / All Self-Insured entities that don't adjudicate their claims

Level 4 Entities - Small Providers (10 to 50 Provider Practices, Community or rural pharmacy)

Data as of June 2012.

Initial 20 Findings Analysis Security Issues

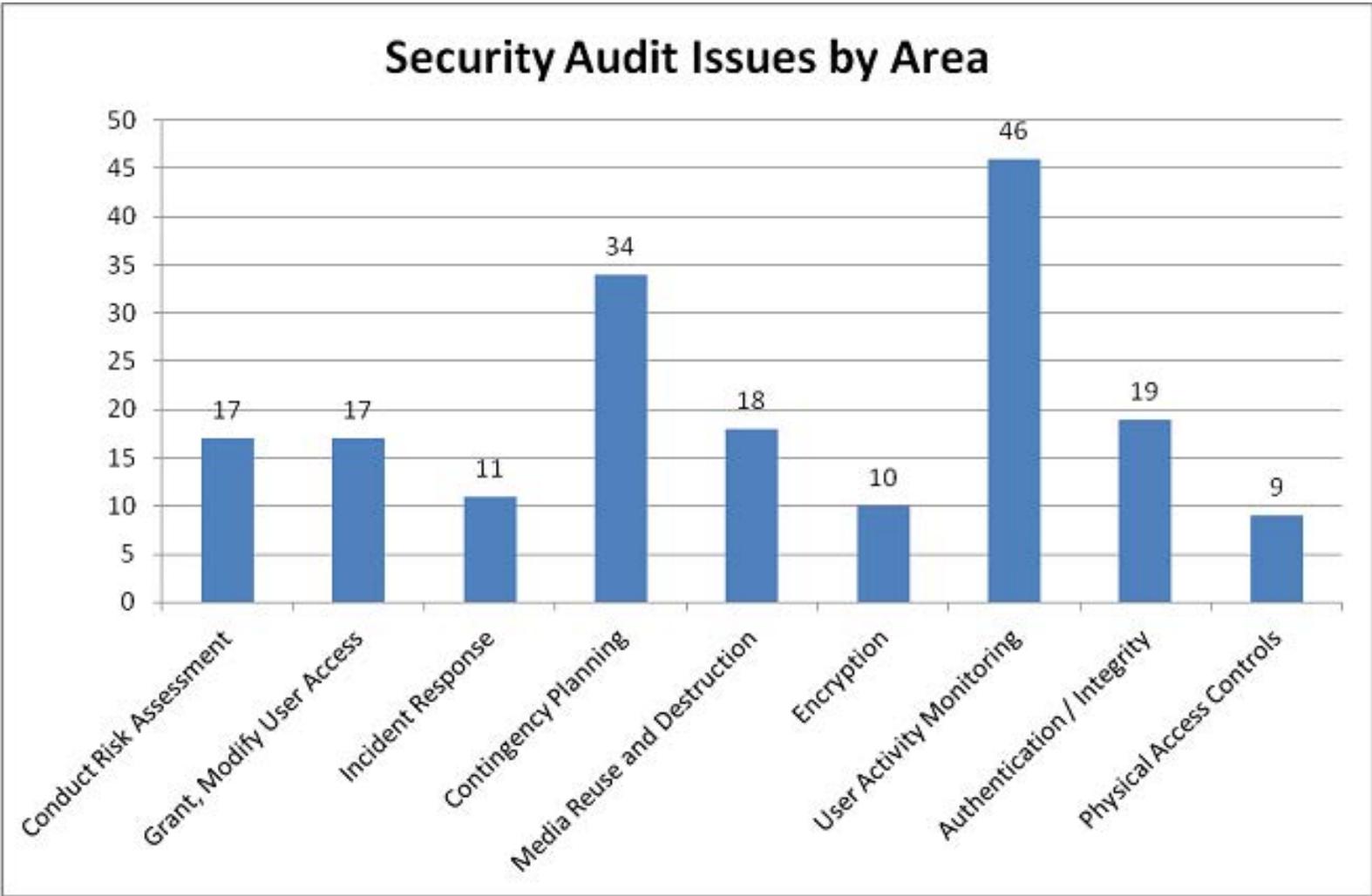
Security Audit Issues by Area of HIPAA Security Rule



Data as of June 2012.

Initial 20 Findings Analysis

Security Top Issues



Data as of June 2012.

Initial 20 Findings

Preliminary Observations

- Policies and procedures
- Priority HIPAA compliance programs
- Small providers
- Larger entities security challenges
- Conduct of risk assessments
- Managing third party risks
- Privacy challenges widely dispersed throughout protocol
- No clear trends by entity type or size

HIPAA Compliance and Enforcement

Covered Entity	Amount	Date
Massachusetts Eye and Ear Infirmary	\$1.5 Million	September 17, 2012
Alaska Department of Health and Social Services	\$1.7 Million	June 26, 2012
Phoenix Cardiac Surgery	\$100,000	April 13, 2012
Blue Cross Blue Shield of Tennessee	\$1.5 Million	March 13, 2012
University of California at Los Angeles Health System	\$865,500	July 6, 2011
Massachusetts General Hospital	\$1 Million	February 14, 2011
Cignet Health of Prince George's County, MD (Civil Money Penalty)	\$4.3 Million (Summary Judgment by U.S. District Court for \$4,782,845.43)	February 4, 2011 (August 28, 2012)
Management Services Organization of Washington, Inc.	\$35,000	December 13, 2010
Rite Aid Corporation	\$1 Million	July 27, 2010
CVS Pharmacy, Inc.	\$2.25 Million	January 16, 2009
Providence Health & Services	\$100,000	July 16, 2008

Total Complaints filed (since 2003): 74,554 **Total Cases Investigated: 26,513** **Total Cases with Corrective Action: 17,767**
 Data as of December 31, 2011.

HIPAA Compliance and Enforcement Issues and Results (2008 – present)

Covered Entity	Issue	Results of OCR Investigation
+ Massachusetts Eye and Ear Infirmary (MEEI) September 17, 2012 \$1.5 Million	Breach report submitted by MEEI reporting the theft of an unencrypted personal laptop containing electronic protected health information (ePHI) of MEEI patients and research subjects.	<ul style="list-style-type: none"> • Failure to conduct a risk analysis. • Failure to implement security measures for portable devices. • Failure to implement policies and procedures to restrict access to ePHI. • Failure to implement policies and procedures regarding security incident identification, reporting, and response.
+ Alaska Department of Health and Social Services (DHSS) June 26, 2012 \$1.7 Million	Breach report submitted by Alaska DHSS indicating that a portable electronic storage device (USB hard drive) possibly containing electronic protected health information (ePHI) was stolen from the vehicle of an Alaska DHSS employee.	<ul style="list-style-type: none"> • Failure to complete a risk analysis. • Failure to implement risk management measures. • Failure to complete security training. • Failure to implement device and media controls. • Failure to address device and media encryption.
Phoenix Cardiac Surgery April 13, 2012 \$100,000	<ul style="list-style-type: none"> • Physician practice posted clinical and surgical appointments for its patients on an Internet-based calendar that was publicly accessible. • Implemented few policies and procedures to comply with the HIPAA Privacy and Security Rules. • Limited safeguards in place to protect patients' electronic protected health information (ePHI). 	<ul style="list-style-type: none"> • Failure to implement adequate policies and procedures. • Failure to document training. • Failure to identify a security official and conduct a risk analysis. • Failure to obtain business associate agreements with Internet-based email and calendar services where the provision of the service included storage of and access to its ePHI.

+ = OCR resolution agreements resulting from investigations initiated after a covered entity's reporting of a breach incident.

* = Findings of noncompliance were made in a Notice of Proposed Determination on October 25, 2010.

HIPAA Compliance and Enforcement Issues and Results (2008 – present), continued

Covered Entity	Issue	Results of OCR Investigation
+ Blue Cross Blue Shield of Tennessee (BCBST) March 13, 2012 \$1.5 Million	Breach notice submitted by BCBS Tennessee to HHS in which it was reported that 57 unencrypted computer hard drives containing protected health information (PHI) of over 1 million individuals had been stolen from a leased facility in Tennessee.	<ul style="list-style-type: none"> • Failure to implement appropriate administrative safeguards. • Failure to perform the required security evaluation following operational changes. • Failure to implement appropriate facility access controls.
University of California at Los Angeles Health System (UCLA HS) July 6, 2011 \$865,500	Unauthorized employees repeatedly looked at the electronic protected health information (ePHI) of numerous UCLA HS patients.	<ul style="list-style-type: none"> • Failure to conduct Privacy and Security trainings. • Did not implement sanctions policy. • Failure to implement security measures to reduce the risks of impermissible access to ePHI.
Massachusetts General Hospital February 14, 2011 \$1 Million	Loss of protected health information (PHI) of 192 patients of Mass General's Infectious Disease Associates outpatient practice, including patients with HIV/AIDS.	<ul style="list-style-type: none"> • Impermissible disclosure of PHI. • Failure to implement safeguards to protect PHI when removed from Massachusetts General's premises.
* Cignet Health of Prince George's County, MD (Cignet) (Civil Money Penalty) February 4, 2011 \$4.3 Million	Violated the right to access medical records of 41 patients.	<ul style="list-style-type: none"> • Failure to provide copies of the patient's records. • Failure to respond to OCR's investigation.

+ = OCR resolution agreements resulting from investigations initiated after a covered entity's reporting of a breach incident.

* = Findings of noncompliance were made in a Notice of Proposed Determination on October 25, 2010.

HIPAA Compliance and Enforcement Issues and Results (2008 – present), continued

Covered Entity	Issue	Results of OCR Investigation
Management Services Organization of Washington December 13, 2010 \$35,000	Disclosure of electronic protected health information for marketing purposes.	Did not have in place or implement appropriate and reasonable administrative, technical, and physical safeguards to protect the privacy of the protected health information.
Rite Aid Corporation July 27, 2010 \$1 Million	Protected health information (PHI) disposed of in dumpsters that were not secure and could be accessed by the public.	<ul style="list-style-type: none"> • Failure to implement adequate policies and procedures to safeguard PHI during the disposal process. • Failure to adequately train employees on the disposal process. • Did not maintain and implement a workforce sanctions policy.
CVS Pharmacy, Inc. January 16, 2009 \$2.25 Million	Protected health information (PHI) disposed of in dumpsters that were not secure and could be accessed by the public.	<ul style="list-style-type: none"> • Failure to implement adequate policies and procedures to safeguard PHI during the disposal process. • Failure to adequately train employees on the disposal process. • Did not maintain and implement a workforce sanctions policy.
Providence Health & Services July 16, 2008 \$100,000	Loss and theft of electronic backup media and laptop computers containing individually identifiable health information.	Failure to implement policies and procedures to safeguard individually identifiable health information.

† = OCR resolution agreements resulting from investigations initiated after a covered entity's reporting of a breach incident.

* = Findings of noncompliance were made in a Notice of Proposed Determination on October 25, 2010.

Consumer Videos



<http://www.youtube.com/watch?v=JY1I5s8ED5c>

Visit the HHS OCR youtube channel at [youtube.com/user/USGovHHSOCR](https://www.youtube.com/user/USGovHHSOCR)
or our website at [HHS.gov/OCR](https://www.hhs.gov/OCR)



The Office of the National Coordinator for
Health Information Technology



Keeping Health Information Private and Secure

Kathryn Marchesini, JD
Office of the Chief Privacy Officer



- **Data Segmentation for Privacy Initiative**
 - Demonstration Planned 1st Q 2013
- **eConsent Trial Project**
 - Pilot launched in October 2012
- **SHARPS Grants on Privacy and Security Innovations**
- **Patients' Attitudes toward Privacy and Security Survey**
- **Notice of Privacy Practices (NPP) Project**
- **Provider and Staff Security Video Games**
- **Mobile Device Portfolio**
 - mHealth Consumer/Patient Research
 - Mobile Device Provider Education



Office of the Chief Privacy Officer

The Office of the National Coordinator for
Health Information Technology

U.S. DEPARTMENT OF
HEALTH AND HUMAN SERVICES

**OFFICE FOR
CIVIL RIGHTS**

Mobile Devices:
Know the RISKS. Take the STEPS.
PROTECT and SECURE
Health Information.



Learn more at HealthIT.gov/mobiledevices

Instructional Video Series

To help illustrate risks and safeguards providers and professionals better understand how to protect and secure health information when using their mobile device, a five video series was created and is available on the HealthIT.gov/mobiledevices site.



Securing Your Mobile Device is Important!



Dr. Anderson's Office Identifies a Risk



A Mobile Device is Stolen



Can You Protect Patients' Health Information When Using a Public Wi-Fi Network?

The videos explore mobile device risks and discuss privacy and security safeguards providers and professionals can put into place to mitigate risks.



Worried About Using a Mobile Device for Work? Here's What To Do!

The Mobile Device Privacy and Security page hosts downloadable education and awareness materials including the tips and steps providers, professionals, and health care organizations can take to safeguard health information.

Online Resource Center: Tips to Protect and Secure Health Information



Use a password or other user authentication.



Keep security software up to date.



Install and enable encryption.



Research mobile applications (apps) before downloading.



Install and activate wiping and/or remote disabling.



Maintain physical control of your mobile device.



Disable and do not install file-sharing applications.



Use adequate security to send or receive health information over public Wi-Fi networks.



Install and enable a firewall.



Install and enable security software.



Delete all stored health information before discarding or reusing the mobile device.

- Fact sheets
- Posters
- Brochure



Mobile Devices: Know the RISKS. Take the STEPS.
PROTECT & SECURE Health Information.
 Find out more at HealthIT.gov/mobiledevices

10 tips to protect and secure health information when using a mobile device.

- 1 Use a **password** or other user authentication
- 2 Install and enable **encryption**
- 3 Install and activate **remote wiping** or **remote disabling**
- 4 Do not install or use **file sharing** applications
- 5 Install and enable a **firewall**
- 7 **Research** mobile applications before downloading
- 8 Always keep your device **in your possession**
- 9 Use adequate security to send or receive health information over **public Wi-Fi** networks
- 10 **Delete** all stored health information before discarding the mobile device

Providers and professionals are using mobile devices in their work. Covered entities with HIPAA Privacy and Security rules to protect and secure health information, including mobile devices. As a leader within your organization, you are responsible for implementing mobile device procedures and policies that will protect the health information entrusted to you.

Your organization can take steps to help protect mobile devices in your health care setting:

Mobile devices will be used to create, receive, transmit, or store patients' information or be used as part of your organization's internal network or systems, including electronic health record systems. This creates risks to your organization's information that you must decide to allow the use of mobile devices.

There are risks when using mobile devices to transmit the health information you hold. Conduct a risk analysis to identify threats to the information. If you are a solo provider, conduct the risk analysis yourself. If you are a large provider, the organization should conduct the risk analysis.

Mobile device risk management strategy, policy and security safeguards. An effective risk management strategy will help your organization implement mobile device safeguards to protect the information identified in the risk analysis, including the use of mobile devices and regular maintenance of the mobile devices you put in place.

4. Develop, document, and implement your organization's mobile device policies and procedures to safeguard health information. Some topics to consider when developing mobile device policies and procedures are:
 - Mobile device management
 - Using your own device
 - Restrictions on mobile device use
 - Security or configuration settings for mobile devices
5. Conduct mobile device privacy and security awareness and ongoing training for providers and professionals.



Mobile Devices: Know the RISKS. Take the STEPS.
PROTECT and SECURE Health Information.

security software and keep it date

Be a team player.
 Understand and follow your organization's mobile device policy and procedures.
It's your responsibility.
 Visit HealthIT.gov/mobiledevices

Mobile Devices: Know the RISKS. Take the STEPS.
PROTECT and SECURE Health Information.

Take the STEPS.
 Protect and Secure Health Information.

Is your information protected? Mobile devices are easily lost or stolen. Avoid losing or disclosing patient health information. Keep your mobile device with you. Learn more at HealthIT.gov/mobiledevices.



Mobile Devices: **Know the RISKS. Take the STEPS.**
PROTECT & SECURE Health Information
Find out more at HealthIT.gov/mobiledevices

The online resource center features informative videos, easy-to-download fact sheets, and posters that organizations can use to raise awareness of risks and educate their staff on safeguarding health information. HHS developed the resource center as a result of the [Mobile Device Roundtable: Safeguarding Health Information](#) and public comment period HHS hosted in March 2012.

“We hope that the steps and information we’ve posted on the online resource center can help health care providers, administrators and their staffs create a culture of privacy and security all across their organization.”

Privacy & Security References



- **The HHS Office of Civil Rights, HIPAA FAQs:** <http://www.hhs.gov/ocr/privacy/hipaa/faq/index.html>
- **ONC's Guide to Privacy and Security of Health Information:** [with http://www.healthit.gov/policy-researchers-implementers/hipaa-and-health-it](http://www.healthit.gov/policy-researchers-implementers/hipaa-and-health-it)
- **Data Segmentation for Privacy Initiative:** <http://wiki.siframework.org/Data+Segmentation+for+Privacy+Homepage>
- **SHARPS Grants on Privacy and Security Innovations:** <http://www.healthit.gov/policy-researchers-implementers/strategic-health-it-advanced-research-projects-sharp>
- **Provider and Staff Security Video Game:** <http://www.healthit.gov/providers-professionals/privacy-security-training-games>
- **Mobile Device Privacy & Security Resource Center:** www.healthit.gov/mobiledevices
- **HHS Health IT Privacy and Security Toolkit – OCR Guidance:** http://healthit.hhs.gov/portal/server.pt?open=512&objID=1174&parentname=CommunityPage&parentid=26&mode=2&in_hi_userid=10732&cached=true
- **Fast Facts about the HIPAA Privacy Rule:** <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/cefastfacts.html>