United States Department of
Health & Human Services

Office of the Secretary
Office for Civil Rights (OCR)

Health Information Privacy
The Future of Enforcement

20th National HIPAA Summit

March 26, 2012

Leon Rodriguez

Director of OCR

Susan McAndrew

Deputy Director for Health Information Privacy

Topics

- Culture of Compliance
- HIPAA Privacy and Security Rule Enforcement
- HITECH Breach Notification
- OCR Audit Program
- Regulations Update

A Culture of Compliance

- OCR aggressively enforcing the HIPAA Privacy and Security Rules

- Covered entities and business associates should have robust HIPAA Privacy and Security compliance programs

- A robust compliance program includes employee training, vigilant implementation of policies and procedures, regular internal audits, and a prompt action plan to respond to incidents

Update on Enforcement of the HIPAA Privacy and Security Rules

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 (1)

- March 2012 – BlueCross/BlueShield of TN
  - $1.5 million RA/CAP
  - Theft of servers containing ePHI
  - Failure to assess and remediate changes in security risk to ePHI due to relocation
  - Reported as Breach affecting over 1 million individuals

Enforcement Highlights (2)

- July 2011 – UCLA Health Systems
  - $865,000 RA/CAP
  - Unauthorized access by employees to patient records
  - Stronger policies & procedures to limit, detect, and sanction unauthorized access by employees and better training on minimum necessary and access policies

Enforcement Highlights (3)

- February 2011 – Massachusetts General Hospital
  - $1 million RA/CAP
  - Sensitive PHI left on subway by employee returning to work
  - Institution-wide policies and procedures to control when PHI is removed from premises by employees and stronger safeguards for all PHI -- paper and electronic -- off-premises

HITECH Breach Notification Rule Reports and Trends

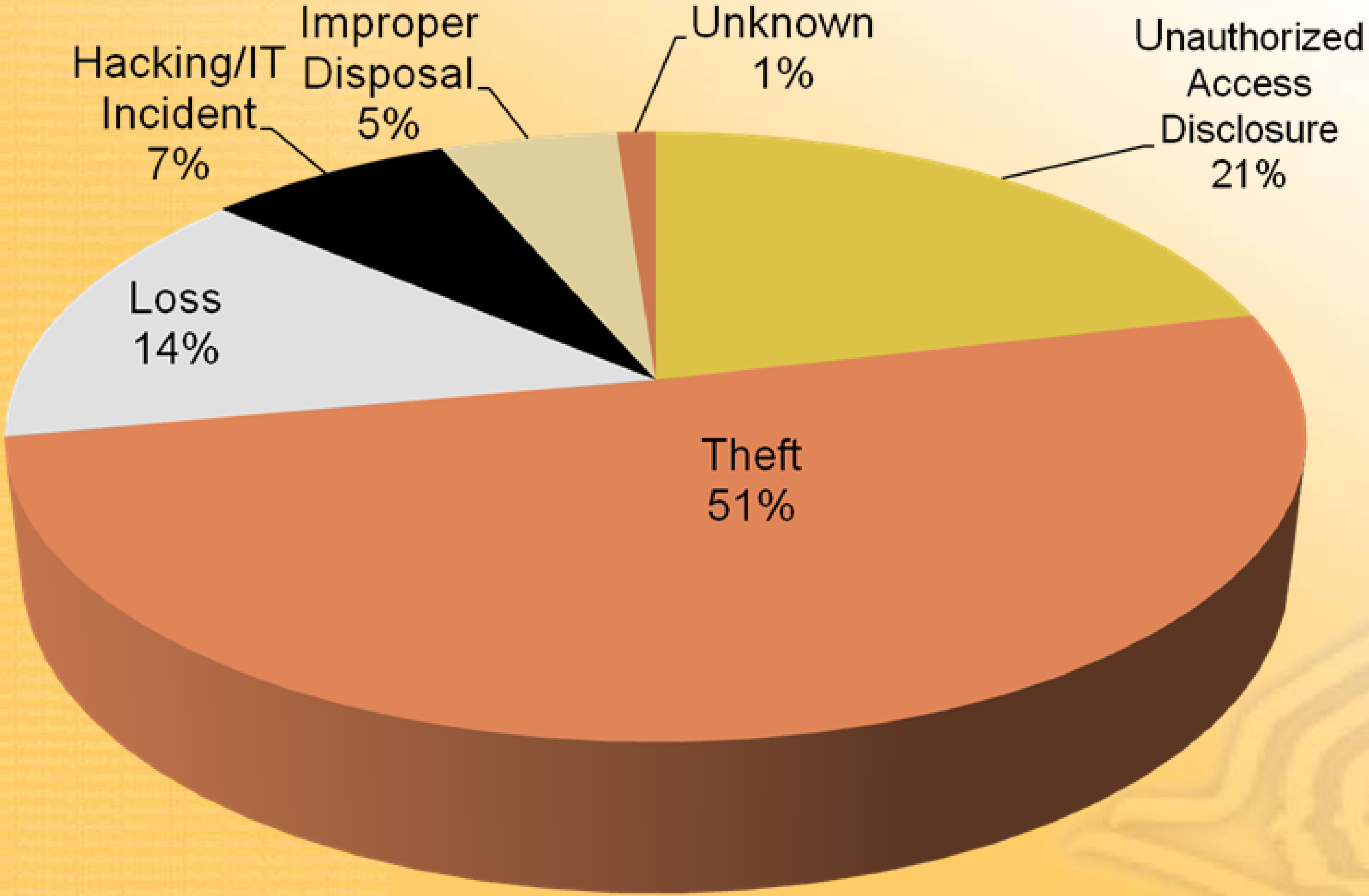
Breach Notification Highlights

September 2009 through March 2012

- 409 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 37% of large breaches
  - Paper records are 24% of large breaches
- 50,000+ reports of breaches of under 500 individuals

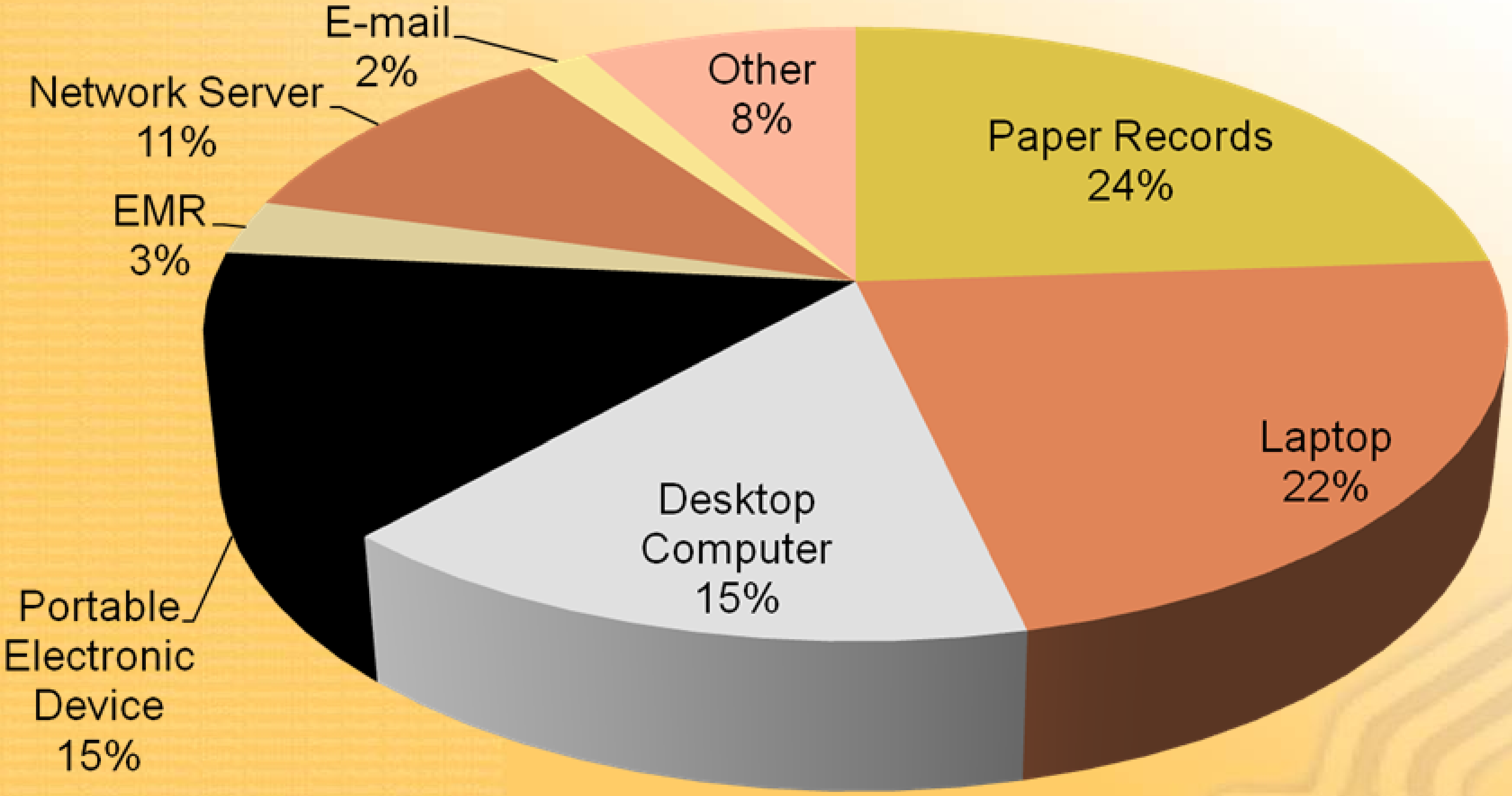
Breach Notification:

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

OCR HITECH Audit Program

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

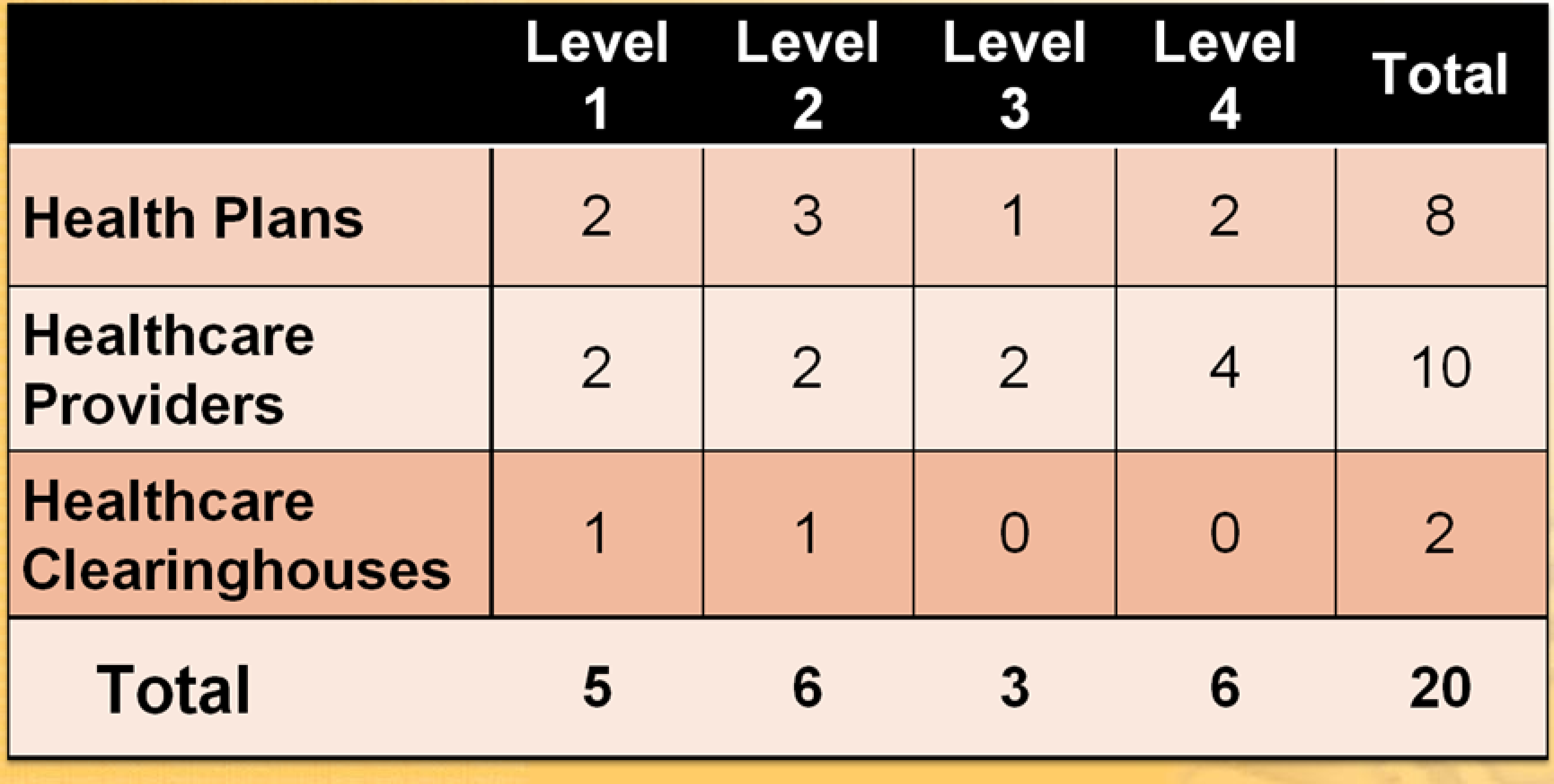
Who Will be Audited?

- 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

Overview of the Pilot Audit Program

- Develop the audit protocol
- Test--Initial use of protocol in 20 audits & protocol refinement
- Implement--remainder of the audits conducted (up to 95 audits) using the revised protocol
- Ongoing, periodic feedback and refinement of Protocol
- Reporting—program and entity specific

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

HITECH/HIPAA NPRM

- HITECH Provisions:
  - **Business associates**
  - **Marketing and fundraising**
  - **Sale of protected health information**
  - **Electronic access**
  - **Right to request restrictions**
  - **Enforcement**
- Other HIPAA Provisions:
  - **Notice of privacy practices**
  - **Research authorizations**
  - **Student immunization records**
  - **Decedent information**

GINA

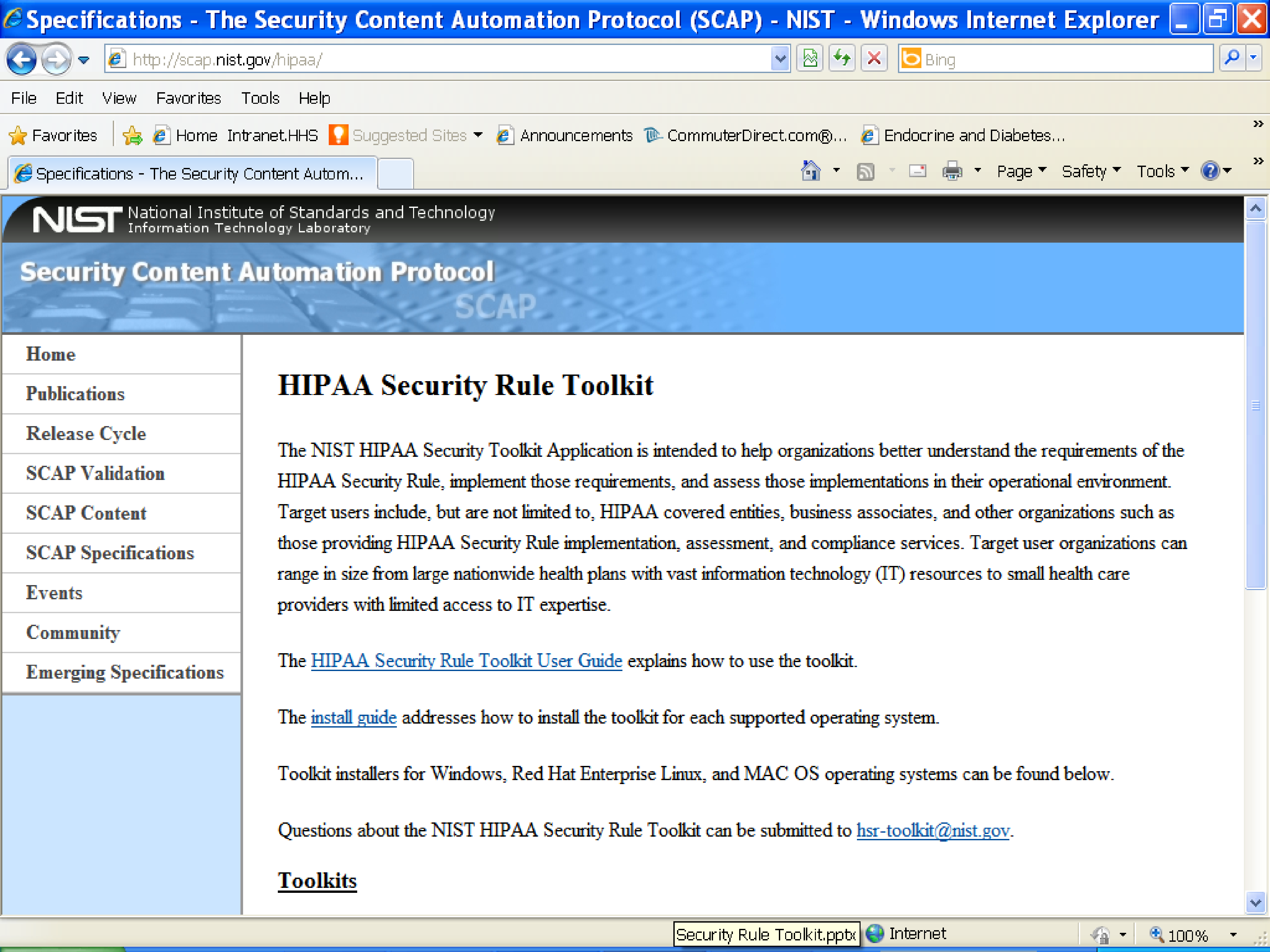
- Genetic Information Non-discrimination Act
  - Requires "genetic information" be treated as protected health information under HIPAA
  - Prohibits the use or disclosure of genetic information for underwriting purposes by health plans
  - Terms and definitions track regulations prohibiting discrimination 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 – more to come
- De-identification Guidance
  - – Target date – April 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**


Specifications - The Security Content Automation Protocol (SCAP) - NIST - Windows Internet Explorer
http://scap.nist.gov/hipaa/
Bing
File
Edit
View
Favorites
Tools
Help
Favorites
Home
Intranet.HHS
Suggested Sites
Announcements
CommuterDirect.com®...
Endocrine and Diabetes...
Specifications - The Security Content Autom...
Page
Safety
Tools
NIST National Institute of Standards and Technology
Information Technology Laboratory
Security Content Automation Protocol
SCAP
Home
Publications
Release Cycle
SCAP Validation
SCAP Content
SCAP Specifications
Events
Community
Emerging Specifications
Security Rule Toolkit.pptx
Internet
100%

HIPAA Security Rule Toolkit

The NIST HIPAA Security Toolkit Application is intended to help organizations better understand the requirements of the HIPAA Security Rule, implement those requirements, and assess those implementations in their operational environment. Target users include, but are not limited to, HIPAA covered entities, business associates, and other organizations such as those providing HIPAA Security Rule implementation, assessment, and compliance services. Target user organizations can range in size from large nationwide health plans with vast information technology (IT) resources to small health care providers with limited access to IT expertise.

The HIPAA Security Rule Toolkit User Guide explains how to use the toolkit.

The install guide addresses how to install the toolkit for each supported operating system.

Toolkit installers for Windows, Red Hat Enterprise Linux, and MAC OS operating systems can be found below.

Questions about the NIST HIPAA Security Rule Toolkit can be submitted to hsr-toolkit@nist.gov.

Toolkits

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.