U.S. DEPARTMENT OF
HEALTH AND HUMAN SERVICES

OFFICE FOR
CIVIL RIGHTS

OCR UPDATE and OUTREACH

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

21st Annual HIPAA Summit
February 19, 2013

Omnibus Final Rule – Important Dates

- Public Display at Federal Register – January 17, 2013
- Published in Federal Register – January 25, 2013
- Effective Date – March 26, 2013
- Compliance Date – September 23, 2013
- Conform BA contracts – September 22, 2014

Omnibus Final Rule HITECH/GINA/HIPAA

- HITECH Provisions:
  - Business associates
  - Marketing and fundraising
  - Sale of protected health information
  - Electronic access
  - Right to request restrictions
  - Enforcement
- GINA Provisions:
  - Genetic information as PHI
  - No use for underwriting
- Other HIPAA Provisions:
  - Notice of privacy practices
  - Research authorizations
  - Student immunization records
  - Decedent information

Omnibus Final Rule – What's New for Business Associates

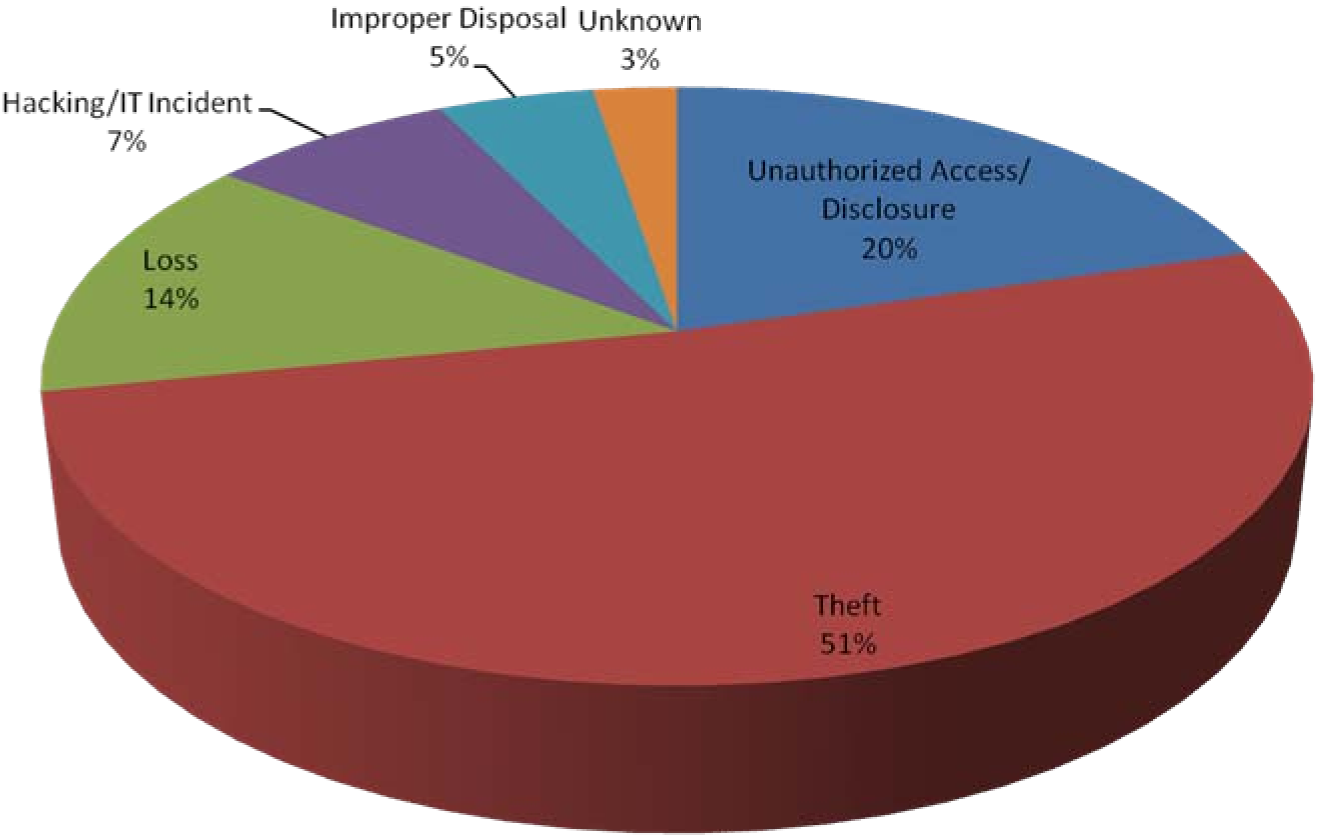
- BAs must comply with the technical, administrative, and physical safeguard requirements under the Security Rule
  - Liable for Security Rule violations
- BA must comply with use or disclosure limitations expressed in its contract and those in the Privacy Rule
  - Criminal and civil liabilities for violations
- BA definition expressly includes Health Information Organizations, E-prescribing Gateways, and PHR vendors that provide services to covered entities
- Subcontractors of a BA are now defined as a BA
  - BA liability flows to all subcontractors

Breach Notification Highlights

September 2009 through January 7, 2013

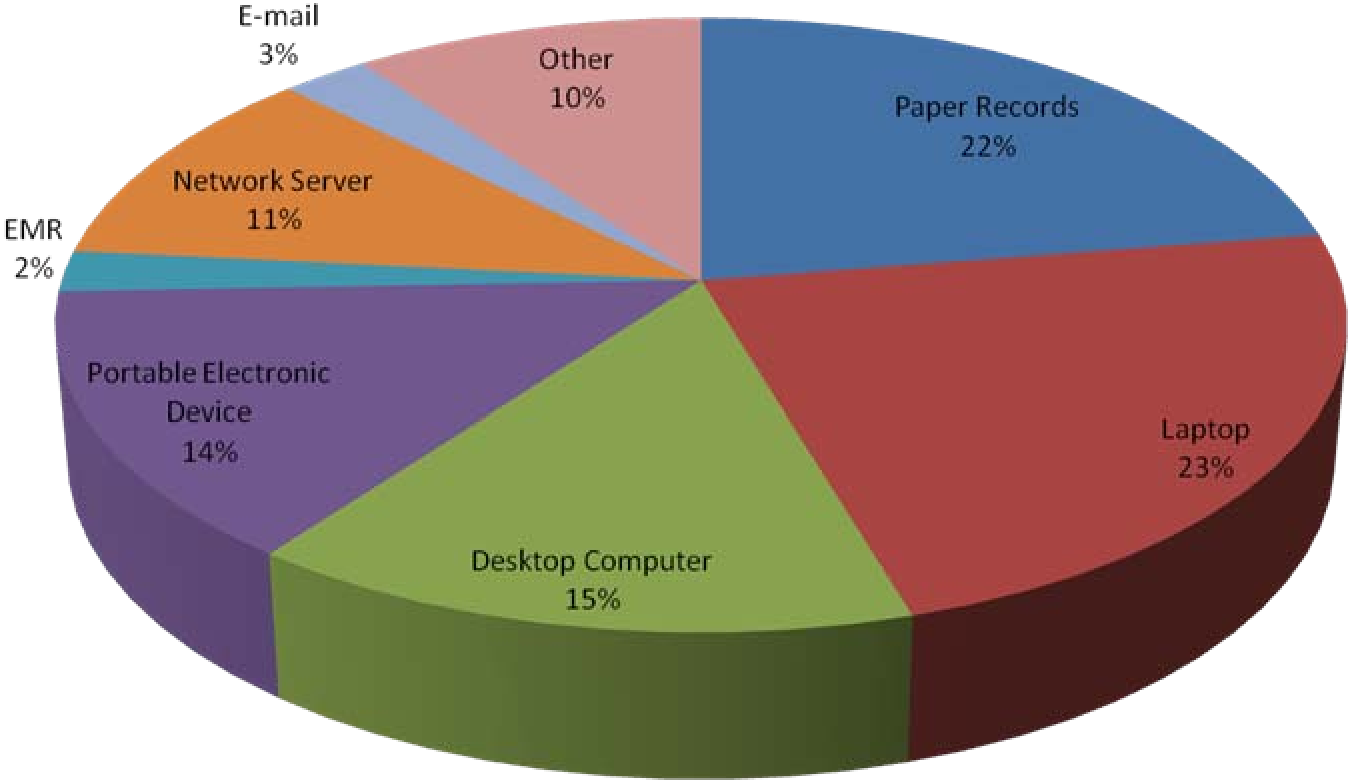
- 525 reports involving over 500 individuals
- Over 64,000 reports involving under 500 individuals
- Top types of large breaches
  - Theft
  - Unauthorized Access/Disclosure
  - Loss
- Top locations for large breaches
  - Laptops
  - Paper records
  - Desktop Computers
  - Portable Electronic Device

Breach Notification: 500+ Breaches by Type of Breach



Data as of January 2013.

Breach Notification: 500+ Breaches by Location of Breach



Data as of January 2013.

HIPAA Compliance/Enforcement
(As of December 31, 2012)

	TOTAL (since 2003)
Complaints Filed	77,200
Cases Investigated	27,500
Cases with Corrective Action	18,600
Civil Monetary Penalties & Resolution Agreements (since 2008)	$14.9 million

Major Enforcement Actions of 2012

- BCBS Tennessee ($1.5 M)
  - E-PHI stored on servers stolen from deactivated data center after construction/relocation to new facility
  - Reevaluate threats/vulnerabilities to e-PHI caused by changing operational environment and manage risk
- Phoenix Cardiac Surgery ($100K)
  - E-PHI disclosed through Internet when provider used third party application hosted in the cloud
  - Business associate agreements required when sharing data with cloud computing service providers
- Alaska DHSS ($1.7M)
  - Portable storage device stolen from personal vehicle symptomatic of widespread failure to implement program-wide information security safeguards
  - Risk analysis to identify location and safeguards for PHI, training and controls for portal devices

Major Enforcement Actions of 2012

- Massachusetts Eye and Ear Institute ($1.5M)
  - Stolen personal laptop of physician using device as desktop substitute
  - Covered entity had not implemented a program to mitigate identified risks to e-PHI
  - Encrypt data stored on end-user devices
- Hospice of Northern Idaho ($50K)
  - Breach affecting 400 individuals when laptop stolen
  - Provider had not conducted a risk assessment or taken other measures to safeguard e-PHI as required by Security Rule

Audit Program

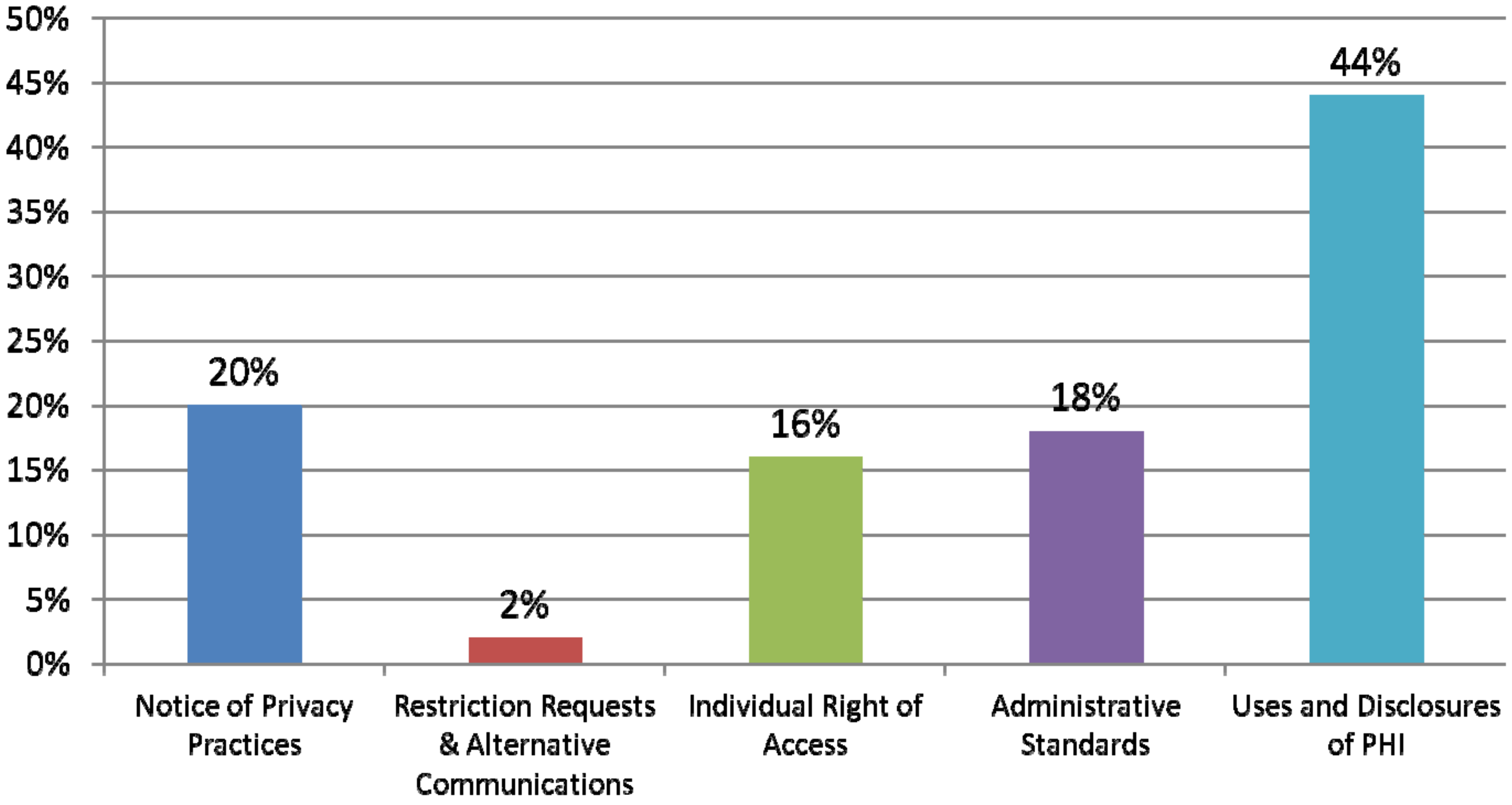
- HITECH Act – Sec. 13411
  - Periodic audits to ensure covered entities and business associates comply with requirements of HIPAA and HITECH

- Audit Objectives
  - Examine mechanisms for compliance
  - Identify best practices
  - Discover risks and vulnerabilities that may not have come to light through complaint investigations and compliance reviews
  - Renew attention of covered entities to health information privacy and security compliance activities

Audit Pilot Observations

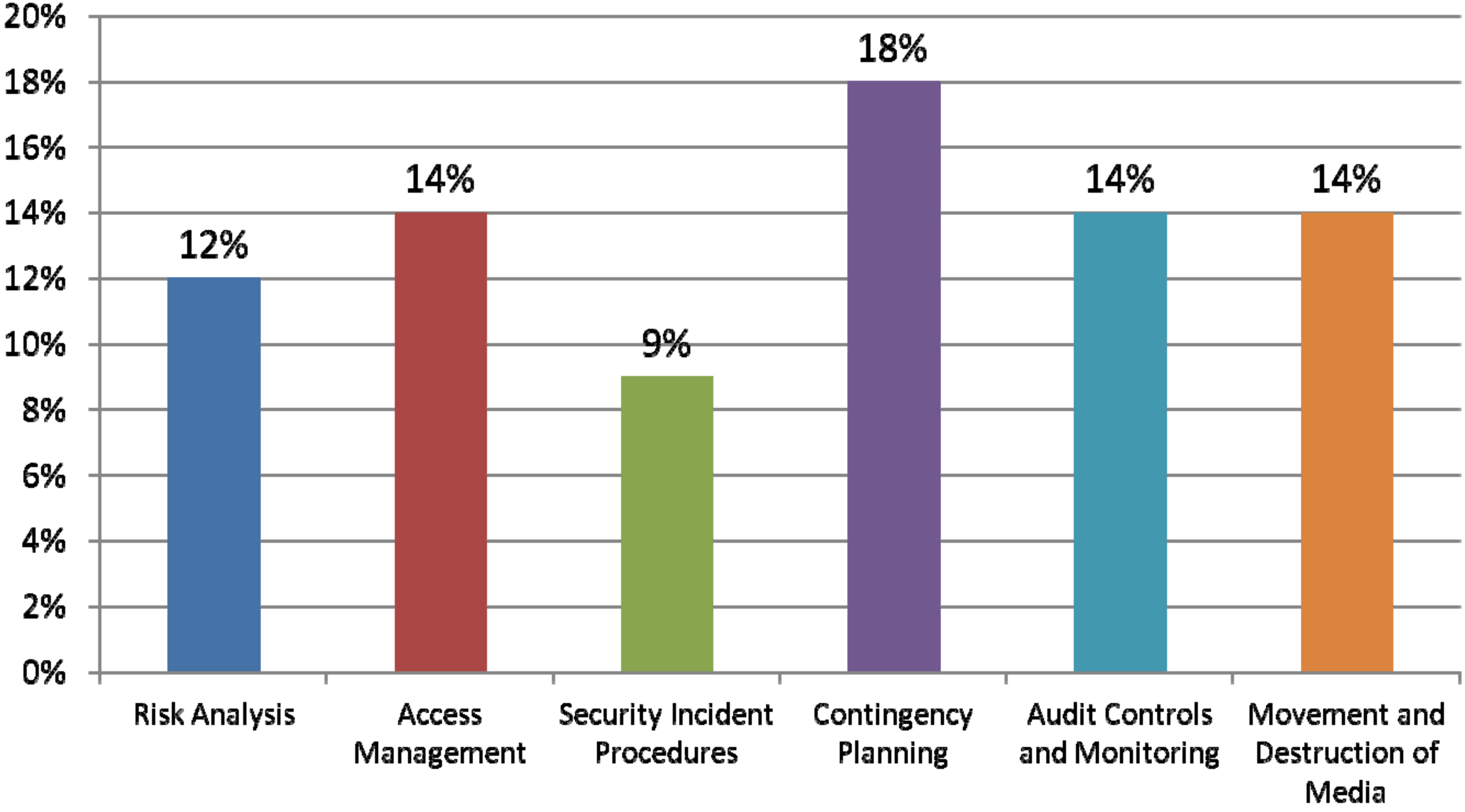
- Completed Audits of 115 entities
  - 61 Providers, 47 Health Plans, 7 Clearinghouses
- No findings or observations for 13 entities (11%)
  - 2 Providers, 9 Health Plans, 2 Clearinghouses
- Total 979 audit findings and observations
  - 293 Privacy
  - 592 Security
  - 94 Breach Notification
- Percentage of Security Rule findings and observations was double what would have been expected based on protocol
- Smaller entities (*Level 4)* struggle with all three areas

Types of Privacy Rule Audit Findings



Data as of December 2012.

Types of Security Rule Audit Findings



Data as of December 2012.

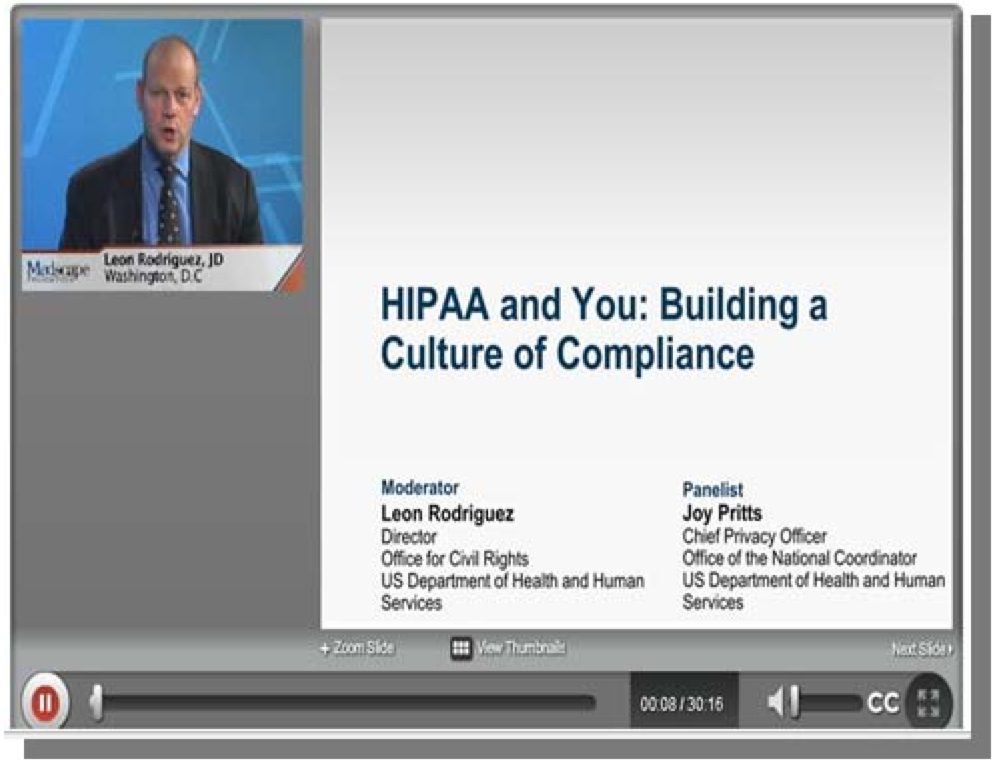
Public Awareness

- Emphasis on Access
- Privacy and Security on YouTube

  http://www.youtube.com/user/USGovHHSOCR
- Fact Sheets/Translations into 7 languages

Medscape: Free CME and CE Training

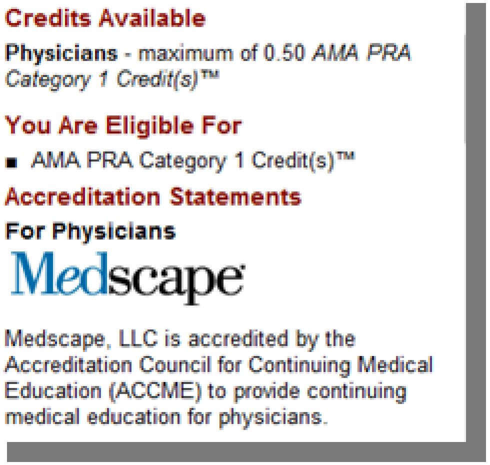
HIPAA: Creating Awareness and Educating Providers on the Importance of Compliance



HIPAA and You: Building a Culture of Compliance

Moderator
Leon Rodriguez
Director
Office for Civil Rights
US Department of Health and Human Services

Panelist
Joy Pritts
Chief Privacy Officer
Office of the National Coordinator
US Department of Health and Human Services



Credits Available

Physicians - maximum of 0.50 *AMA PRA Category 1 Credit(s)™*

You Are Eligible For

- AMA PRA Category 1 Credit(s)™

Accreditation Statements

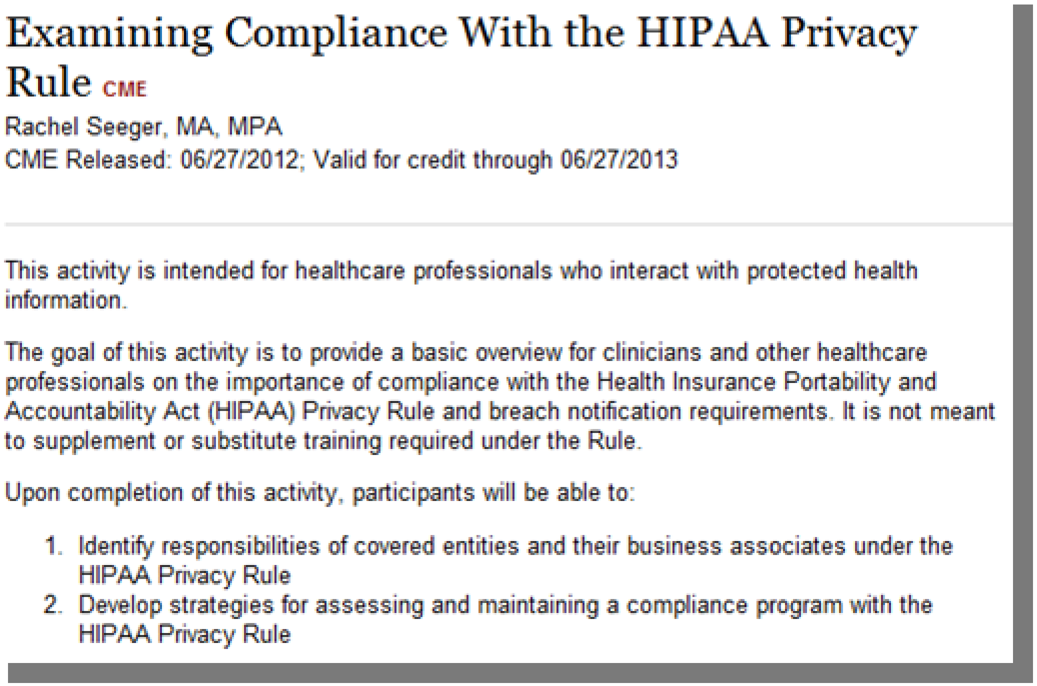
For Physicians

Medscape

Medscape, LLC is accredited by the Accreditation Council for Continuing Medical Education (ACCME) to provide continuing medical education for physicians.

http://www.medscape.org/viewarticle/762170?src=cmsocr

HIPAA: Creating Awareness and Educating Providers on the Importance of Compliance



Examining Compliance With the HIPAA Privacy Rule CME

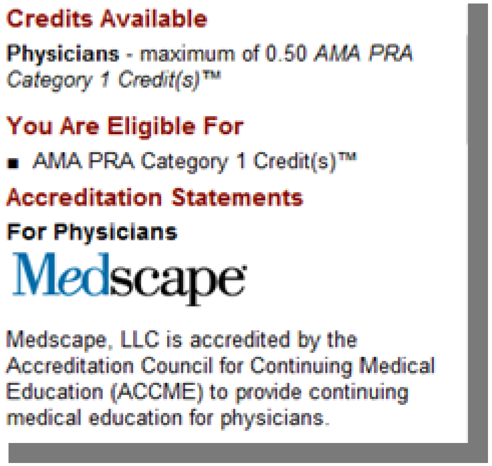
Rachel Seeger, MA, MPA
CME Released: 06/27/2012; Valid for credit through 06/27/2013

This activity is intended for healthcare professionals who interact with protected health information.

The goal of this activity is to provide a basic overview for clinicians and other healthcare professionals on the importance of compliance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and breach notification requirements. It is not meant to supplement or substitute training required under the Rule.

Upon completion of this activity, participants will be able to:

1. Identify responsibilities of covered entities and their business associates under the HIPAA Privacy Rule
2. Develop strategies for assessing and maintaining a compliance program with the HIPAA Privacy Rule



Credits Available

Physicians - maximum of 0.50 *AMA PRA Category 1 Credit(s)™*

You Are Eligible For

- AMA PRA Category 1 Credit(s)™

Accreditation Statements

For Physicians

Medscape

Medscape, LLC is accredited by the Accreditation Council for Continuing Medical Education (ACCME) to provide continuing medical education for physicians.

http://www.medscape.org/viewarticle/763251?src=cmsocr

Questions?

OCR website www.HHS.gov/OCR