

OCR Updates

Susan McAndrew, J.D.
Deputy Director for Health Information Privacy
Office for Civil Rights

HIT Policy Committee
December 4, 2013

Overview of OCR

- Policy
- Compliance and Enforcement
- Public Awareness/Outreach

CLIA

- September 14, 2013 delay in enforcement of HIPAA requirement for Certain CLIA and CLIA-exempt laboratories to revise their Notices of Privacy Practices (NPP)
- Final rulemaking for CLIA rules opening labs to access requirements for test results is at OMB for clearance
- Joint rulemaking with CMS

HIPAA and NICS NPRM

- April 19, 2013 issued ANPRM on whether HIPAA prevents some states from reporting individuals disqualified from having a gun for mental health reasons to the National Instant Criminal Background Check System (NICS)
- Over 2000 comments received
- NPRM is at OMB
- 60 day comment period when NPRM is published

HIPAA and Mental Health Disclosures

- Guidance requested at Congressional testimony April 16, 2013
- Disclosures to friends and family
- “Duty to Warn”

HIPAA/HITECH

Accounting of Disclosures

- NPRM issued 2011
- Public comment raised issues with proposed access reporting
- Updating information received and exploring options

Enforcement Highlights

- Continued focus on Security Rule compliance
 - Affinity Health Plan – over \$1.2 million
 - ePHI left on photocopier drives
 - Wellpoint - \$1.7 million
 - Faulty testing of programming updates left information accessible on web portal
 - Idaho State University -- \$400,000
 - Disabled firewall exposed ePHI to breach
- Privacy
 - Shasta Regional Medical Center -- \$275,000
 - Patient medical records shared with media

Multi-year Audit Plan

Description	Vendor	Status/Timeframe
Audit program development study	Booz Allen Hamilton	Closed 2010
Covered entity identification and cataloguing	Booz Allen Hamilton	Closed 2011
Develop audit protocol and conduct audits	KPMG, Inc.	Closed 2011-2012
Evaluation of audit program	PWC, LLP	Open Conclude in 2013

Overall Findings & 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

Security Results

58 of 59 providers
had at least one
Security finding or
observation

**No complete &
accurate risk
assessment in
two thirds of
entities**

- 47 of 59 providers,
- 20 out of 35 health plans
and
- 2 out of 7 clearinghouses

Security addressable
implementation
specifications:
Almost every entity
without a finding or
observation met by
fully implementing
the addressable
specification.

Overall Cause Analysis

- For every finding and observation cited in the audit reports, audit identified a “Cause.”
- Most common across all entities: **entity unaware of the requirement.**
 - in 30% (289 of 980 findings and observations)
 - **39% (115 of 293) of Privacy**
 - **27% (163 of 593) of Security**
 - **12% (11) of Breach Notification**
 - Most of these related to elements of the Rules that explicitly state what a covered entity must do to comply.
- Other causes noted included but not limited to:
 - Lack of application of sufficient resources
 - Incomplete implementation
 - Complete disregard

Cause Analysis – Top Elements

Unaware of the Requirement

Privacy

- Notice of Privacy Practices;
- Access of Individuals;
- Minimum Necessary; and,
- Authorizations.

Security


- Risk Analysis;
- Media Movement and Disposal; and,
- Audit Controls and Monitoring.

Next Steps for OCR

Formal Program Evaluation 2013



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
- 

Revise Protocol to reflect Omnibus Rule



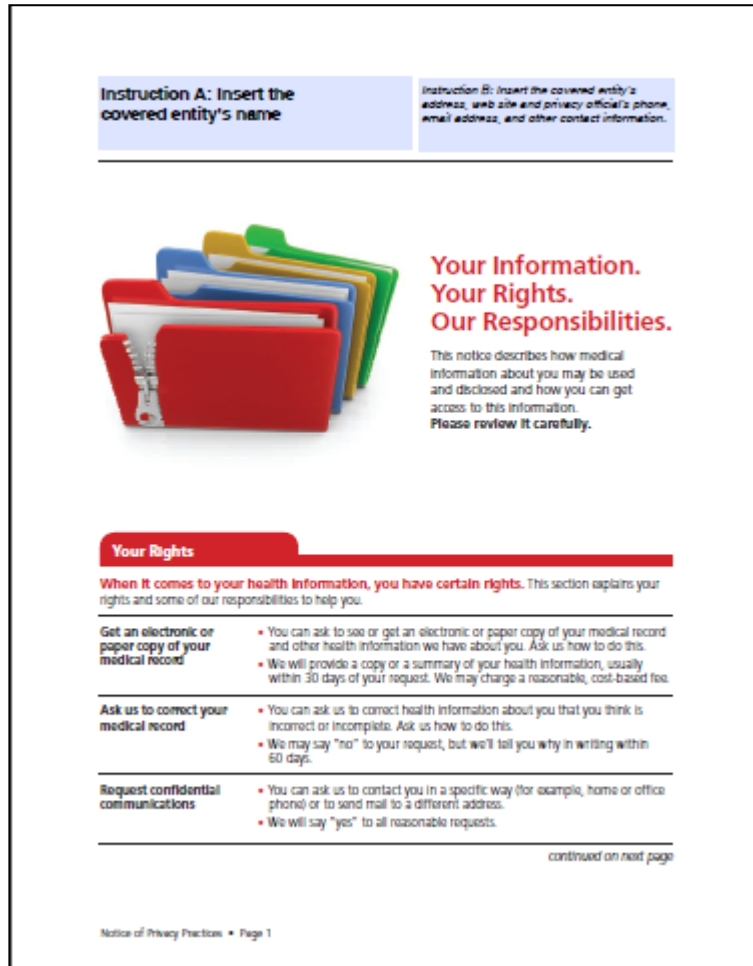
Ongoing program design and focus

- Business Associates
- Accreditation /Certification correlations?

Health Information Privacy Education and Outreach Efforts

December 2013 Metrics

Model Notices of Privacy Practices



- Notice in the form of a booklet;
- A layered notice that presents a summary of the information on the first page, followed by the full content on the following pages;
- A notice with the design elements found in the booklet, but formatted for full page presentation.
- A text only version of the notice.

<http://www.hhs.gov/ocr/privacy/hipaa/modelnotices.html>

Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule: A Guide for Law Enforcement


What is the HIPAA Privacy Rule?
 The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule provides Federal privacy protections for individually identifiable health information, called protected health information or PHI, held by most health care providers and health plans and their business associates. The HIPAA Privacy Rule sets out how and with whom PHI may be shared. The Privacy Rule also gives individuals certain rights regarding their health information, such as the rights to access or request corrections to their information.

Who must comply with the HIPAA Privacy Rule?
 HIPAA applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically (e.g., billing a health plan). These are known as covered entities. Hospitals, and most clinics, physicians and other health care practitioners are HIPAA covered entities. In addition, HIPAA protects PHI held by business associates, such as billing services and others, hired by covered entities to perform services or functions that involve access to PHI.

Who is not required to comply with the HIPAA Privacy Rule?
 Many entities that may have health information are not subject to the HIPAA Privacy Rule, including:

- employers,
- most state and local police or other law enforcement agencies,
- many state agencies like child protective services, and
- most schools and school districts.

While schools and school districts maintain student health records, these records are in most cases protected by the Family Educational Rights and Privacy Act (FERPA) and not HIPAA. HIPAA may apply however to patient records at a university hospital or to the health records of non-students at a university health clinic.



Under what circumstances may a HIPAA covered entity disclose PHI to law enforcement?

A HIPAA covered entity may disclose PHI to law enforcement with the individual's signed HIPAA authorization.

A HIPAA covered entity also may disclose PHI to law

- To comply with a court order or court-ordered warrant, a subpoena or summons issued by a judicial officer, or an administrative request from a law enforcement official (the administrative request must include a written statement that the information requested is relevant and material, specific and limited in scope, and de-identified information cannot be used).

New HIPAA Privacy Rule Blue Card for Law Enforcement

- Developed in cooperation with the HHS Office of Assistant Secretary for Preparedness and Response and the Federal Bureau of Investigation
- Provides a basic description of the HIPAA Privacy Rule and identifies entities that are and are not required to comply.
- Outlines several disclosure permissions that allow the disclosure of health information to law enforcement in common law enforcement situations



AIDS.gov/privacy Highlights

- 27,435 unique visitors to AIDS.gov/privacy
 - May 20 – Sept 30
- September highlights:
 - 6,919 unique visitors
 - 49% traffic from digital ads, adam4adam 91% of referrals
 - 49% Mobile
 - 81% only visit aids.gov/privacy
 - Average view time 4 minutes, 43 seconds > Average for all AIDS.gov pages is 2:44

Outdoor & Transit



Outdoor impressions of 3,532,622

Online impressions of 19,362,659

Transit 8,514,168

Print 4,345,800 (readers)

Community Outreach Attendance at the Pride events

Oakland 50,000

Atlanta 40,000

Washington DC 20,000

Chicago 12,000

NYC 10,000

US Conference on AIDS - New Orleans 3,000

Total 135,000 estimated attendees



OCR's YouTube Videos



Your New Rights Under HIPAA
264,157 Views



The HIPAA Omnibus Rule
269,989 Views



Your Health Information, Your Rights
113,307 Views



**Su Informacion de Salud,
Sus Derechos**
503,831 Views



The Right to Access Your Health Information
84,421 Views



**Treatment, Payment and Health
Care Operations**
77,811 Views



EHRs: Privacy and Security
5,300 Views



**Communicating with Friends
And Family**
97,247 Views



Explaining the Notice of Privacy Practices
124,705 Views



HIPAA Security Rule
290,615 Views

TOTAL VIEWS FROM FEBRUARY 16 2012 - DECEMBER 3, 2013: 1,831,383

Visit us at <http://www.youtube.com/USGovHHSOCR>

New Tools for Consumers

Health Information Privacy

Office for Civil Rights

Civil Rights

Health Information Privacy

[OCR Home](#) > [Health Information Privacy](#) > [Understanding HIPAA Privacy](#) > [For Consumers](#)

Guidance Materials for Consumers

HHS OCR - Your Health Information, Your Rights



Playlist: HIPAA: Your Health Information, Your Rights. (7 videos)



Omnibus HIPAA Rulemaking

HHS announces a [final rule](#) that implements a number of provisions of the HITECH Act to strengthen the privacy and security protections for health information established under HIPAA.

Know Your Rights

Right to Access Your Health Information

- ▶ [Right to Access Memo](#)
- ▶ [Learn more with our Educational Videos](#)

Consumer Brochures in More Languages

[繁體中文](#) - [Traditional Chinese](#)

[简体中文](#) - [Simplified Chinese](#)

[한국어](#) - [Korean](#)

[Polski](#) - [Polish](#)

[Русский](#) - [Russian](#)

[Español](#) - [Spanish](#)

[Tagalog](#) - [Tagalog](#)

[Tiếng Việt](#) - [Vietnamese](#)

HIPAA

- Understanding HIPAA Privacy
 - For Consumers
 - For Covered Entities
 - Special Topics
 - Related Links
 - Summary of the HIPAA Privacy Rule
 - Summary of the HIPAA Security Rule
 - Training Materials
- HIPAA Administrative Simplification Statute and Rules
- Enforcement Activities & Results
- How to File a Complaint
- News Archive
- Frequently Asked Questions

PSQIA

- Understanding PSQIA Confidentiality
- PSQIA Statute & Rule
- Enforcement Activities & Results
- How to File a Complaint

Printer Friendly Brochures

- [Your Health Information Privacy Rights](#)
- [Privacy, Security, and Electronic Health Records](#)
- [Understanding the HIPAA Notice](#)
- [Sharing Health Information with Family Members and Friends](#)

More Information

- [Your Medical Records](#)
- [Employers and Health Information in the Workplace](#)
- [Personal Representatives](#)
- [Family Members and Friends](#)
- [Court Orders and Subpoenas](#)
- [Notice of Privacy Practices](#)
- [Right to Access Memo](#)

Protecting Patients Rights: New OCR Resource Center at Medscape.org

Video Programs
module imbedded into
page for dynamic
interest

OCR Educational Links,
Including Mobile Device
Content

Protecting Patients' Rights

INTRODUCTION

The Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services administers and enforces the Health Information Privacy, Security, and Breach Notification Rules, issued under the Health Insurance Portability and Accountability Act of 1996, otherwise known as HIPAA, and the Health Information Technology for Economic and Clinical Health (HITECH) Act. In doing so, we play an important role in ensuring that individuals' health information remains private and secure, and that individuals have rights to their health information.

LEARN ABOUT COMPLYING WITH THE HIPAA PRIVACY AND SECURITY RULES

- Patient Privacy: A Guide for Providers **CME**
HIPAA gives patients much control over how their data are used. Do your practice's policies protect their rights?
April 26, 2012
- HIPAA and You: Building a Culture of Compliance **CME**
Health care privacy is everyone's responsibility. Learn steps to safeguard patient information throughout the care environment.
June 26, 2012
- Examining Compliance With the HIPAA Privacy Rule **CME**
An unsecured laptop or outdated privacy policies could lead to hefty fines. Is your practice HIPAA-compliant?
June 27, 2012

RESOURCES FOR MEDICAL PROFESSIONALS AND BUSINESS ASSOCIATES

- Are You a Covered Entity?
- For Small Providers, Small Health Plans, and Other Small Businesses
- Summary/Guidance on Significant Aspects of the Privacy and Security Rules
- Fast Facts for Covered Entities
- Business Associates FAQs
- Simple Business Associate Agreement
- Security Rule Guidance (Materials)
- Guidance on Risk Analysis
- Mobile Device Security
- Communicating with a Patient's Family, Friends, or Others Involved in the Patient's Care
- FAQs About the Dispose of Protected Health Information
- Training Materials on the HIPAA Privacy Rule

RESOURCES FOR YOUR PATIENTS

- Your Health Information Privacy Rights
- Privacy, Security, and Electronic Health Records
- Understanding the HIPAA Notice
- Sharing Health Information with Family Members and Friends
- HIPAA Videos for Consumers

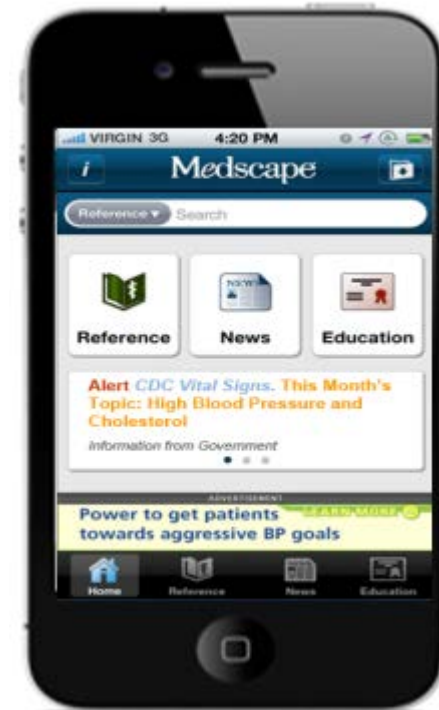
Supported by the U.S. Department of Health and Human Services, Office for Civil Rights

POLLING QUESTION

Who in your practice is responsible for updating privacy and security policies?

- Office manager
- Chief privacy officer
- Chief information officer
- Quality assurance manager
- Other

HIPAA/OCR Poll Question
Updated Quarterly

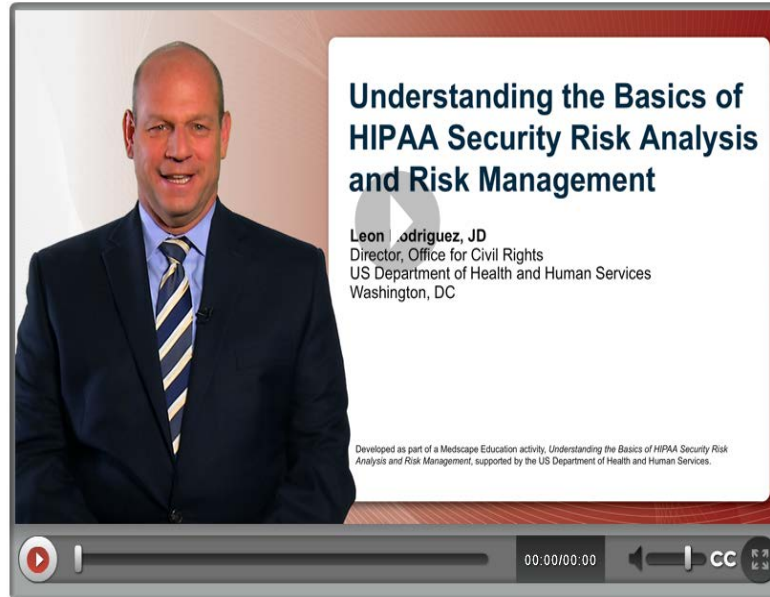


<http://www.medscape.org/sites/advances/patients-rights>

Understanding the Basics of Risk Analysis and Risk Management

Posting Date: 9/13/13

- 7,951 Total Learners
- 17,730 Total Page view
- 4,746 MD Learners
- 1,541 Nurse Learners
- 124 Pharmacist Learners
- 227 Phys Assistants
- 1,313 (Other HCP's)
- 1,957 MD Test Takers
- 971.50 Credits



Supported by the U.S. Department of Health and Human Services, Office for Civil Rights

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/810563>

Your Mobile Device and Health Information Privacy and Security

Posting Date: 9/13/13

- 8,285 Total Learners
- 16,980 Total Page Views
- 4,700 MD Learners
- 1,945 Nurse Learners
- 174 Pharmacist Learners
- 276 Phys Assistants
- 1,190 (Other HCP's)
- 1,934 MD Test Takers
- 477.75 Credits



Your Mobile Device and Health Information Privacy and Security

Leon Rodriguez, JD
Director, Office for Civil Rights
US Department of Health and Human Services
Washington, DC

Farzad Mostashari, MD, ScM
National Coordinator for Health Information Technology
US Department of Health and Human Services
Washington, DC

Developed as part of a Medscape Education activity, *Your Mobile Device and Health Information Privacy and Security*, supported by the US Department of Health and Human Services.

Supported by the U.S. Department of Health and Human Services, Office for Civil Rights

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

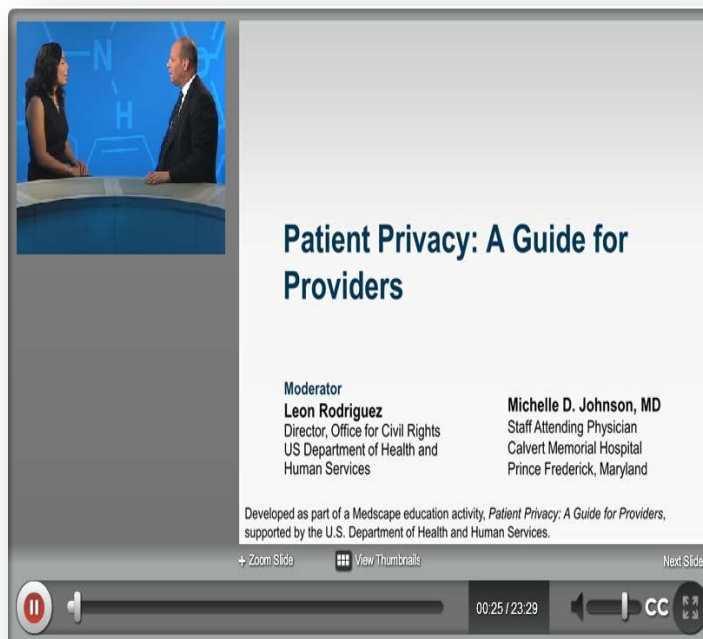
Medscape, LLC is accredited by the Accreditation Council for Continuing Medical Education (ACCME) to provide continuing medical education for physicians.

<http://www.medscape.org/viewarticle/810568>

Patient Privacy: A Guide for Providers

Posting Date: 4/26/13

- 20,560 Total Learners
- 37,469 Total Page Views
- 6,426 MD Learners
- 5,041 Nurse Learners
- 403 Pharmacist Learners
- 647 Phys Assistants
- 8,043 (Other HCP's)
- 3,518 MD Test Takers
- 1741.75 Credits



Patient Privacy: A Guide for Providers

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

Michelle D. Johnson, MD
Staff Attending Physician
Calvert Memorial Hospital
Prince Frederick, Maryland

Developed as part of a Medscape education activity, *Patient Privacy: A Guide for Providers*, supported by the U.S. Department of Health and Human Services.

+ Zoom Slide View Thumbnails Next Slide >

00:25 / 23:29

Supported by the U.S. Department of Health and Human Services, Office for Civil Rights

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.

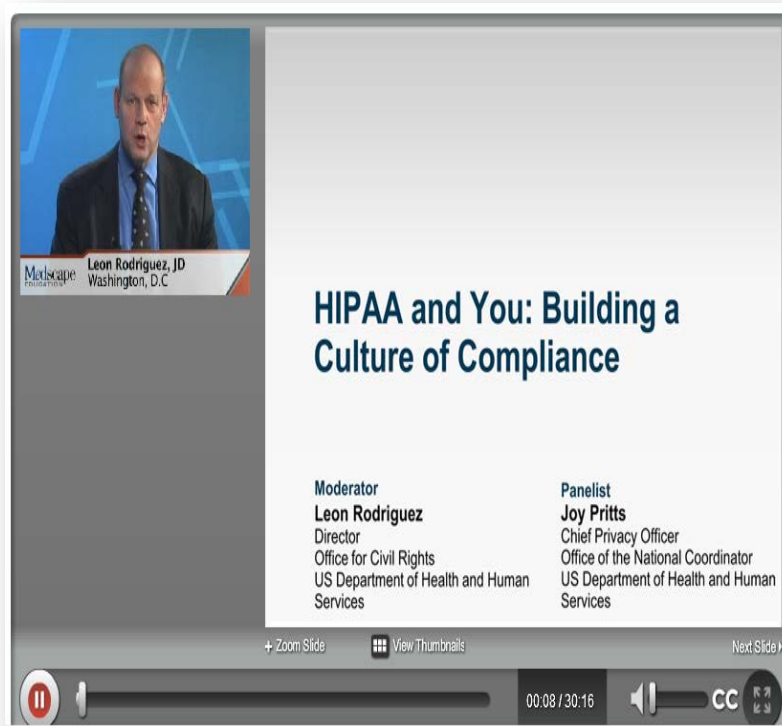
<http://www.medscape.org/viewarticle/781892?src=ocr>

HIPAA and You: Building a Culture of Compliance

CME Released: 06/29/2012;
Reviewed and Renewed:
06/28/2013; Valid for credit
through 06/28/2014

- 8,503 Total Learners
- 16,476 Total Page Views
- 1,193MD Learners
- 2,274 Nurse Learners
- 140 Pharmacist Learners
- 139 Phys Assistants
- 4,757 (Other HCP's)
- 598 MD Test Takers
- 295.50 Credits

* Report reflects 6/28/13 to
10/20/13



Leon Rodriguez, JD
Washington, D.C.

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
---	--

+ Zoom Slide View Thumbnails Next Slide ▶

00:08 / 30:16

Supported by the U.S. Department of Health
and Human Services, Office for Civil Rights

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>

Examining Compliance with the HIPAA Privacy Rule

CME Released:
06/27/2012; Reviewed
and Renewed:
06/27/2013; Valid for
credit through
06/27/2014

- **7,658 Total Learners**
- **20,182 Total Page Views**
- **1209 MD Learners**
- **1,888 Nurse Learners**
- **146 Pharmacist Learners**
- **118 Phys Assistants**
- **4,297 (Other HCP's)**
- **681 MD Test Takers**
- **336.75 Credits**

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

Supported by the U.S. Department of Health and Human Services, Office for Civil Rights

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.

* Report reflects
6/27/13 to 10/20/13

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