U.S. DEPARTMENT OF
HEALTH AND HUMAN SERVICES

**OFFICE FOR
CIVIL RIGHTS**

OCR UPDATE and OUTREACH
Stepping Up Compliance in 2014

Susan McAndrew, J.D.

Deputy Director, Health Information Privacy Division

U.S. Department of Health and Human Services

Office for Civil Rights

22nd National HIPAA Summit

February 5, 2014

Overview

- What's Done

- What's to Come

- In HIPAA Privacy, Security and Breach Notification
  - Policy
  - Enforcement
  - Outreach

HIPAA Privacy, Security, Breach Policy -- Rulemaking

- ## What's Done:
  - Omnibus Final Rule
    - HITECH provisions, including final rulemaking on IFR enforcement penalties & breach notification
    - GINA provisions
    - Other rule changes
  - NICS NPRM
  - CLIA Final Rules on access rights to test results direct from labs

- ## What's to Come:
  - From HITECH
    - Accounting of Disclosures
    - Methods for sharing penalty amounts with harmed individuals
  - NICS Final Rule

HIPAA/NICS NPRM

- January 2013 – one of 23 executive actions to reduce gun violence
- April 2013 – ANPRM on need for HIPAA rule change for NICS reporting – over 2000 comments
- January 2014 – NPRM
  - Express permission for designated NICS reporters or entities making commitment or adjudication decisions
  - Limited to identity, demographics; not clinical data or medical records
- Comments due by March 10, 2014

CLIA Final Rule

- Final Rule on display at FR – February 3
- CMS – Amends CLIA regulations to allow labs to give patient access to completed test results
- OCR – Amends HIPAA right to access to remove exemption for CLIA labs
  - Individual has right to access and get copy of PHI in DRS of labs, including right to electronic copy
  - Access obligations on labs same as for other covered entities
  - Individual can still go through physician to obtain test results
- Dates
  - Publish in FR -- February 6
  - Effective Date -- April 7
  - HIPAA Compliance Date -- October 8

HIPAA Privacy, Security, Breach Policy -- Guidance

What's Done:

Omnibus Final Rule

- De-identification
- Combined Regulation Text
- Sample BA provisions
- Refill Reminder
- Factsheets on Student immunizations and Decedents

Model Notice of Privacy Practices*

Guide to Law Enforcement*

Letters from Leon

- Dear Provider – duty to warn, serious and imminent threats
- Right to access – updated for e-access requirements

What's to Come:

Omnibus Final Rule

- Breach Safe Harbor Update
- Breach Risk Assessment Tool
- Minimum Necessary
- More on Marketing
- More Factsheets on other provisions

Model Notice

- Spanish version
- Web based version

Other Guidance

- Permitted mental health disclosures
- Security Rule guidance updates

Model Notices of Privacy Practices
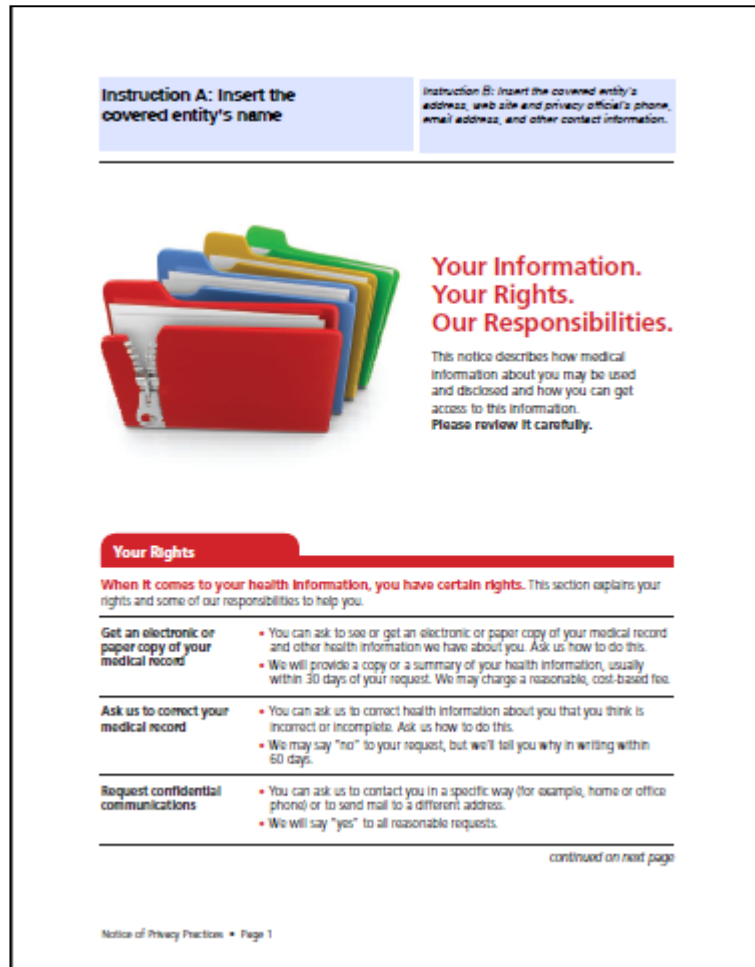
- Notice in the form of a booklet;

- 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;

- Different versions for plans and health care providers.

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

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

New HIPAA Privacy Rule Blue Card for Law Enforcement
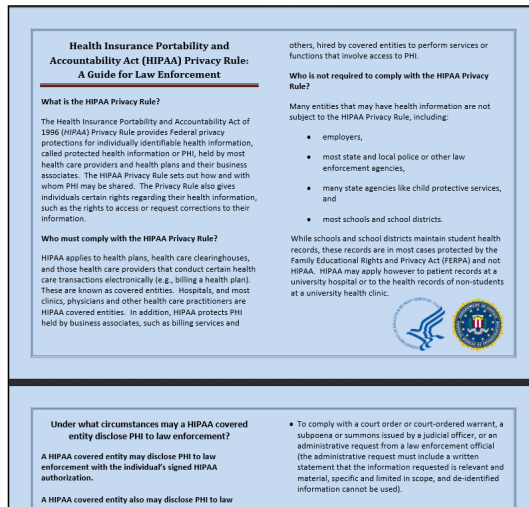
- Developed in cooperation with the HHS Office of Assistant Secretary for Preparedness and Response and the Federal Bureau of Investigation

- 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

http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/emergency/final_hipaa_guide_law_enforcement.pdf

HIPAA Privacy, Security, Breach Compliance and Enforcement

- ## What's Done
  - ### Resolution Agreements/Corrective Action Plans
    - 5 RA/CAPs in CY13
    - Total Resolution Amounts of $3,740,780
  - ### Investigated Complaints/Compliance Reviews
    - 4,459 investigative closures in CY13
    - 3,467 closed with corrective action
  - ### Breach Reports
    - 800 Breaches involving 500 or more individuals
    - 92,000 Breaches involving fewer than 500 individuals

Enforcement Highlights for CY13

- ## 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
  - Adult & Pediatric Dermatology -- $150,000
    - Stolen unencrypted thumb drive; lacked risk analysis, and policies/procedures for breach notification

- ## Privacy
  - Shasta Regional Medical Center -- $275,000
    - Patient medical records shared with media

HIPAA Compliance/Enforcement
(As of December 31, 2013)

	TOTAL (since 2003)
Complaints Filed	90,000
Cases Investigated	31,925
Cases with Corrective Action	22,026
Civil Monetary Penalties & Resolution Agreements (since 2008)	$18.6 million

Breach Notification:
500+ Breaches by Type of Breach
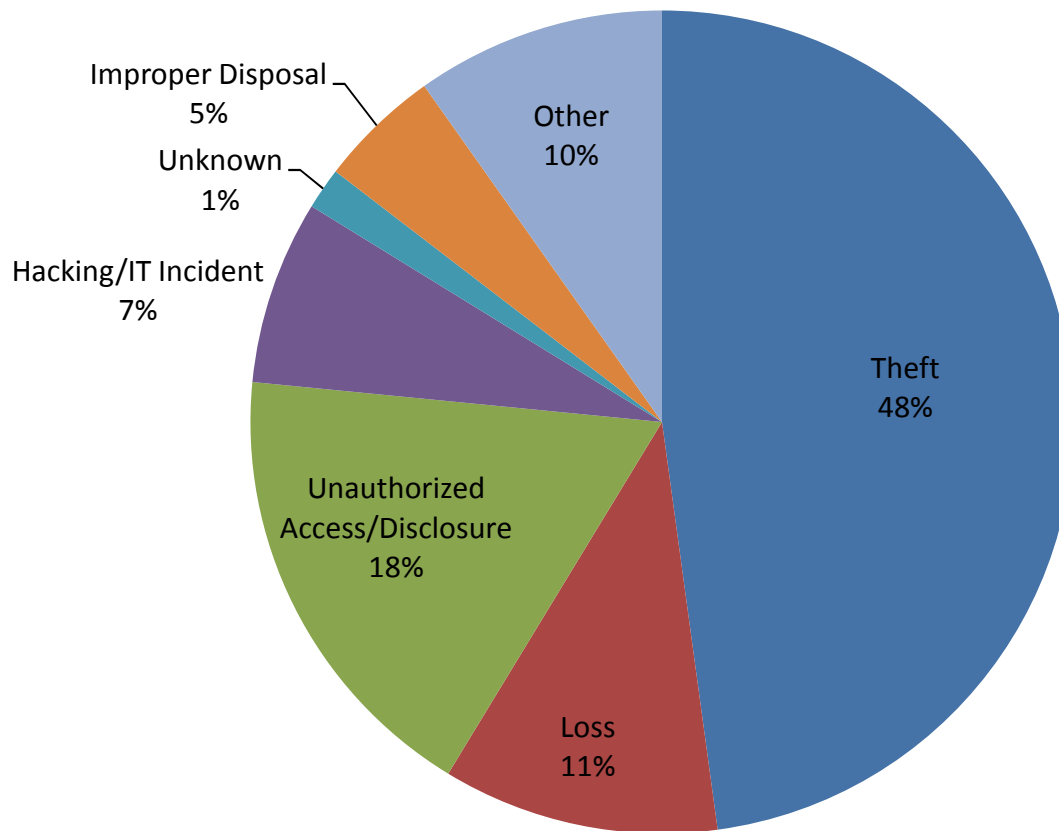
Data as of February 2014.

Breach Notification:
500+ Breaches by Location of Breach

Data as of February 2014.

U.S. Department of Health and Human Services, Office for Civil Rights
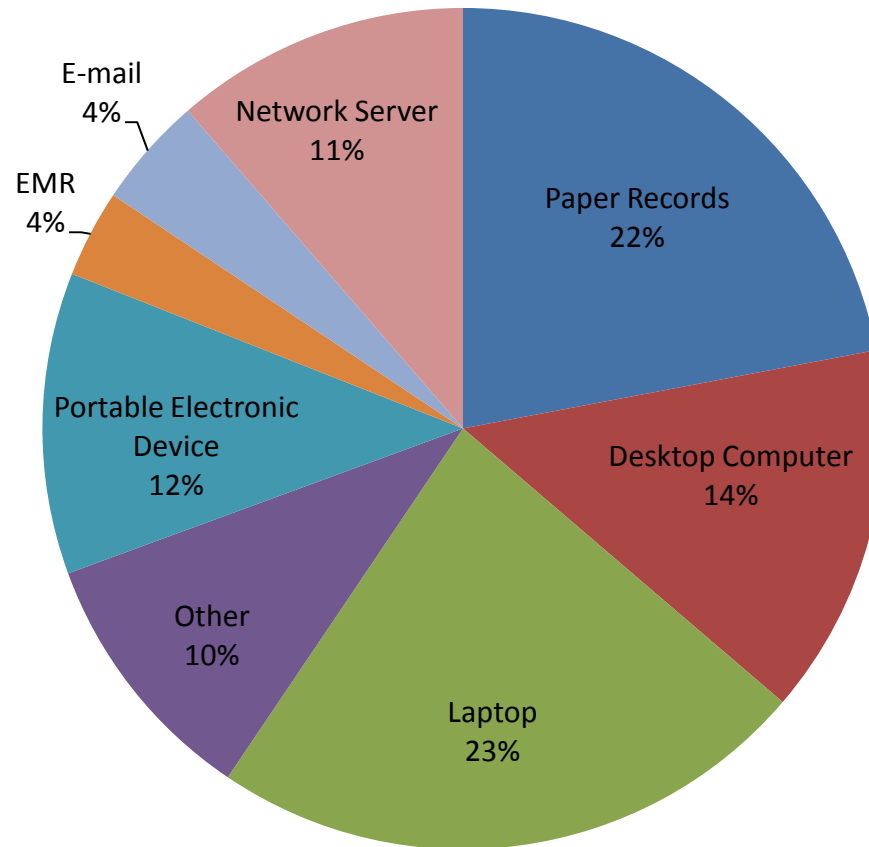
HIPAA Privacy, Security, Breach Compliance and Enforcement

- ## What's to Come
  - ### Resolution Agreements/Corrective Action Plans
    - Continue to increase activity and resources
    - Maintain focus on fundamentals of compliance programs
    - Address emerging issues
  - ### Investigated Complaints/Compliance Reviews
    - New web portal for complaints/centralized intake
      - https://ocrportal.hhs.gov/ocr/cp/complaint_frontpage.jsf
    - Strategic approach to increase efficiencies, identify cases for investigation
  - ### Breach Reports
    - Redesigned website for 500+ postings
    - http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html

Compliance and Enforcement
Audit – What's Done

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	Closed 2013

Compliance and Enforcement
Audit – What's Done
Lessons Learned

Privacy	Security
• Notice of Privacy Practices; • Access of Individuals; • Minimum Necessary; and, • Authorizations.	• Risk Analysis; • Media Movement and Disposal; and, • Audit Controls and Monitoring.

Compliance and Enforcement Audit – What's to Come

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?

Public Awareness/Compliance Tools

What's Done

- Emphasis on Access
  - **Information Is Powerful Medicine Campaign**
- Privacy and Security on YouTube
  - **http://www.youtube.com/user/ USGovHHSOCR**
- Medscape: free CME and CE Training
  - **Resource Center**
  - **5 Training Modules**
- ONC collaborations on Security
  - **Mobile Devices**
  - **Security Rule Games**
- Fact Sheets/Translations into 7 languages

What's to Come

- **Find new partners to extend IIPM campaign**

- **Find new content and more translations**

- **6th Module coming soon**

- **Risk analysis tool for small providers**

- **New content and always improving "usability" of website**

AIDS.gov/privacy Highlights

- 27,435 unique visitors to AIDS.gov/privacy
  - May 20 – Sept 30

- Total Impressions/Views:
  - Outdoor impressions of 3,532,622
  - Online impressions of 19,362,659
  - Transit impressions 8,514,168
  - Print impressions 4,345,800 (readers)

Information Is Powerful Medicine
AIDS.gov/privacy
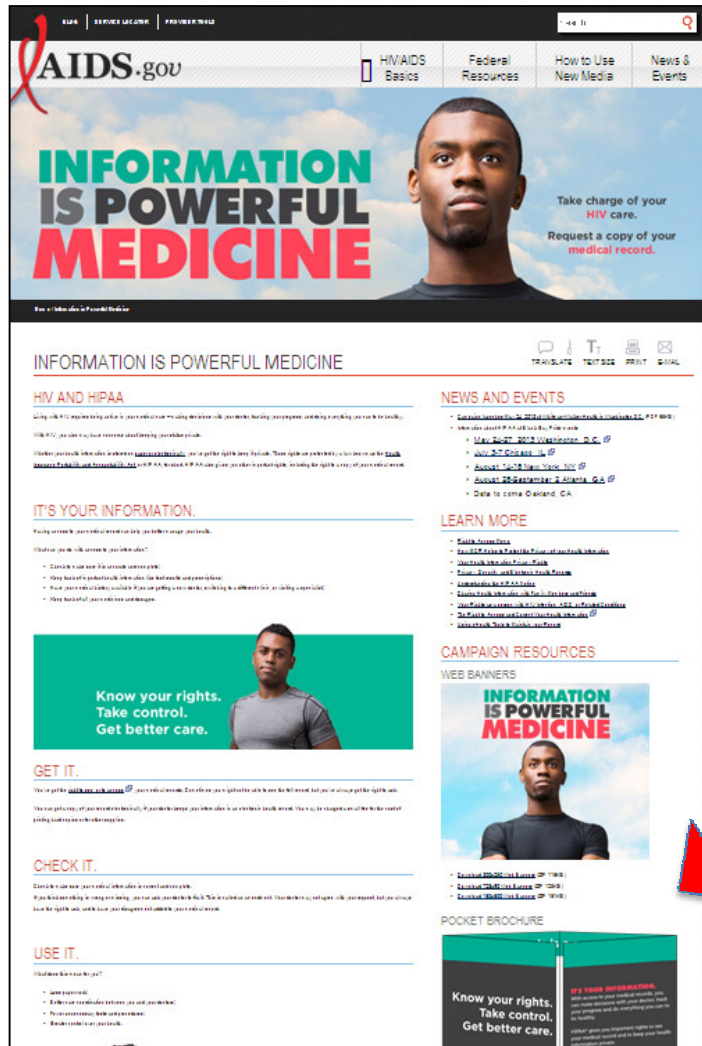
Clear and concise

- Fact Sheets
- Posters
- Brochure
- FAQs
- Video
- Mobile Platform

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

Pocket Brochures and Posters
Distributed nationally with 58 community partners.

Outdoor & Transit

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

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
264,781 Views

The HIPAA Omnibus Rule
273,927 Views

Your Health Information, Your Rights
116,291 Views

Su Informacion de Salud, Sus Derechos
503,898 Views

The Right to Access Your Health Information
84,909 Views

Treatment, Payment and Health Care Operations
77,967 Views
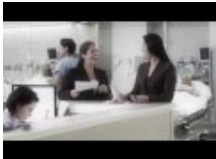
EHRs: Privacy and Security
5,645 Views

Communicating with Friends And Family
97,428 Views

Explaining the Notice of Privacy Practices
124,888 Views

HIPAA Security Rule
291,263 Views

TOTAL VIEWS FROM FEBRUARY 16 2012 - JANUARY 30, 2013:   1,840,997

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

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

OCR's YouTube Videos

Your New Rights Under HIPAA
624 Views

Your Health Information, Your Rights
2,984 Views

The Right to Access Your Health Information
488 Views

EHRs: Privacy and Security
345 Views

Explaining the Notice of Privacy Practices
183 Views

The HIPAA Omnibus Rule
3,938 Views

Su Informacion de Salud, Sus Derechos
67 Views

Treatment, Payment and Health Care Operations
156 Views

Communicating with Friends And Family
181 Views

HIPAA Security Rule
648 Views

DECEMBER - JANUARY INCREASE: 9,614

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

HIPAA/OCR Poll Question Updated Quarterly

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

Understanding the Basics of Risk Analysis and Risk Management

- **11,964 Total Learners**
- **26,974 Total Page views**
- **6,640 MD Learners**
- **2,599 Nurse Learners**
- **184 Pharmacist Learners**
- **431 Physician Assistants**
- **2,110 (Other HCP's)**
- **3,168 MD Test Takers**
- **1574.75 Credits**
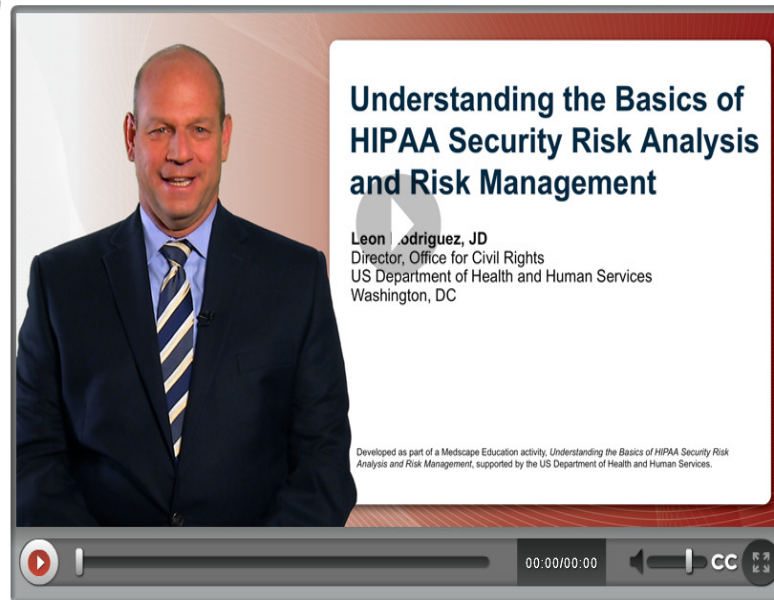
Supported by the U.S. Department of Health and Human Services, Office for Civil Rights

Understanding the Basics of HIPAA Security Risk Analysis and Risk Management

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

Developed as part of a Medscape Education activity, *Understanding the Basics of HIPAA Security Risk Analysis and Risk Management*, supported by the US Department of Health and Human Services.

00:00/00:00   CC

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.
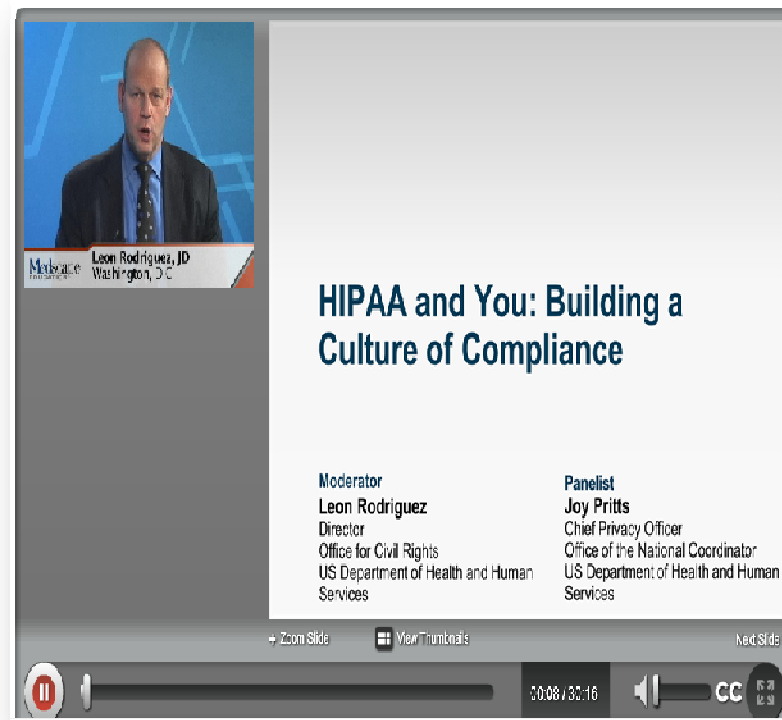
http://www.medscape.org/viewarticle/810563

Your Mobile Device and Health Information Privacy and Security

Posting Date: 9/13/13

- **13,969 Total Learners**
- **28,518 Total Page Views**
- **7,657 MD Learners**
- **3,627 Nurse Learners**
- **252 Pharmacist Learners**
- **586 Physician Assistants**
- **1,847 (Other HCP's)**
- **3,378 MD Test Takers**
- **836.50 Credits**

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

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.

+ Zoom Slide   View Thumbnails   02:14 / 20:15   Next Slide ›   CC

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

- 25,184 Total Learners
- 45,835 Total Page Views
- 7,831 MD Learners
- 6,356 Nurse Learners
- 534 Pharmacist Learners
- 772 Physician Assistants
- 9,691 (Other HCP's)
- 4,497 MD Test Takers
- 2225.25 Credits
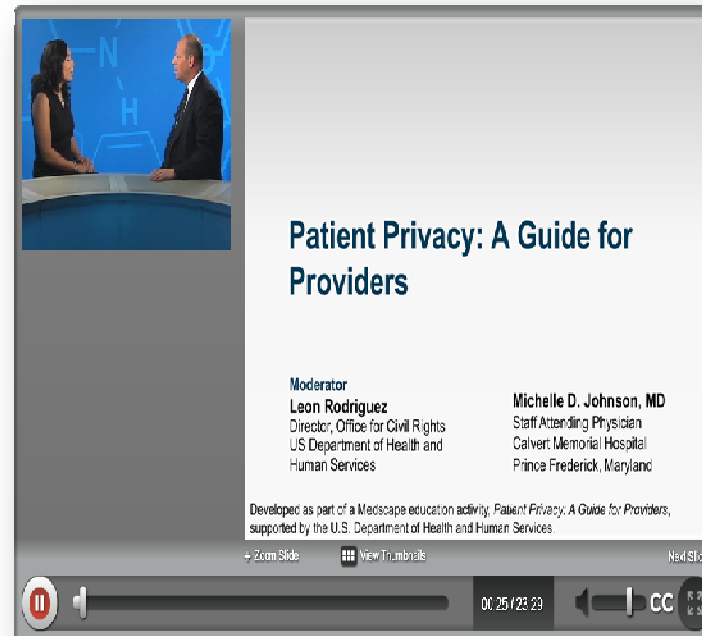
Supported by the U.S. Department of Health and Human Services, Office for Civil Rights

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/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

- **10,199 Total Learners**
- **26,222 Total Page Views**
- **1,832 MD Learners**
- **2,651 Nurse Learners**
- **223 Pharmacist Learners**
- **174 Physician Assistants**
- **5,319 (Other HCP's)**
- **1,165 MD Test Takers**
- **577 Credits**

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

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

- 10,199 Total Learners
- 26,222 Total Page Views
- 1,832 MD Learners
- 2,651 Nurse Learners
- 223 Pharmacist Learners
- 174 Physician Assistants
- 5,319 (Other HCP's)
- 1,165 MD Test Takers
- 577 Credits

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

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.

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

ONC/OCR Mobile Device Program Instructional Video Series

The videos explore mobile device risks and discuss privacy and security safeguards providers and professionals can put into place to mitigate risks.
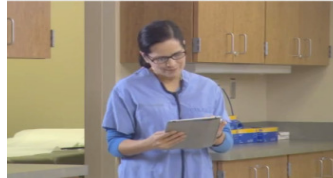
Securing Your Mobile Device is Important!
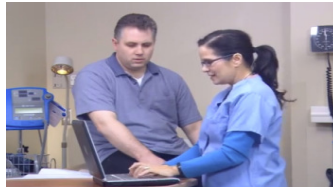
Dr. Anderson's Office Identifies a Risk

A Mobile Device is Stolen

Can You Protect Patients' Health Information When Using a Public Wi-Fi Network?
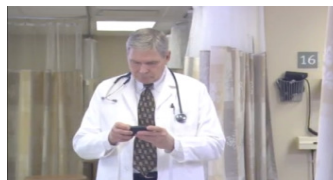
Worried About Using a Mobile Device for Work? Here's What To Do!

Downloadable Materials
www.healthit.gov/mobiledevices

- Fact sheets
- Posters
- Brochures

Mobile Device Program: Tips to Protect and Secure Health Information

Use a password or other user authentication.

Install and enable encryption.

Install and activate wiping and/or remote disabling.

Disable and do not install file- sharing applications.

Install and enable a firewall.

Install and enable security software.

Keep security software up to date.

Research mobile apps before downloading.

Maintain physical control of your mobile device.

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

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

Training Materials:
Security Video Game Released September 2012

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

New Tools for Consumers

Questions?

OCR website   www.HHS.gov/OCR