

Update on the Omnibus Final Rule and Policy Guidance

Susan McAndrew

Deputy Director, Health Information Privacy
Office for Civil Rights/HHS

21st Annual HIPAA Summit
February 19, 2013

Omnibus Final Rule – What's New for Consumers

- Right to Electronic Copy of Electronic Health Record
 - Right to direct copy to designated 3d party
- Prohibition on Sale of PHI without Authorization
- Marketing Communications Paid for by 3d Party Require Authorization
 - Limited exceptions for refill reminders and current prescriptions
- Easy Way to Stop Fundraising Communications
- Right to Restrict Disclosures to Health Plans of Treatment/Services Paid for in Cash

GINA Provisions

- Requires “Genetic Information” to be treated as PHI
- Prohibits Health Plans from using/disclosing genetic information for underwriting purposes
- Terms and definitions track regulations prohibiting discrimination in provision of health insurance based on genetic information

Omnibus Final Rule – Non-statutory Provisions

- Student Immunization
 - Makes it easier for parents to permit providers to release student immunization records to schools
- Research
 - Allows researchers to use single authorization for more than one research purpose
 - Relaxes policy on authorizations for future research
- Notice of Privacy Practices
 - Updates required to Notices of Privacy Practices
 - Relaxes distribution requirements for Health Plans
- Decedent Information
 - Protections limited to 50 years after death
 - Eases access to friends and families

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

Omnibus Final Rule – What’s New for Breach

- Breach Notification Provisions
 - Replaces “harm to individual” with more objective measure of compromise to the data as threshold for breach notification
 - Other provisions of 2009 IFR adopted without major change

Omnibus Final Rule – What’s New for Enforcement

- Enforcement Provisions
 - Adopts increased CMP amounts and tiered levels of culpability from 2009 IFR
 - Clarifies “Reasonable Cause” Tier
 - Willful Neglect Penalties do not require informal resolution
 - Intentional wrongful disclosures may be subject to civil, rather than criminal, penalties

Policy Guidance -- Compliance Tools

- De-identification Guidance

<http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveridentities/De-identification/guidance.html>

- Sample Business Associate Contract Language

<http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveridentities/contractprov.html>

- Risk Analysis Guidance

<http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidance.html>

- Security for Mobile Devices (video/web)

<http://www.healthit.gov/mobiledevices>

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!



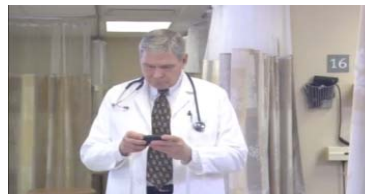
Dr. Anderson's Office Identifies a Risk



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

- Fact sheets
- Posters
- Brochures



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**
- 6 Install **security software** and keep it up to date
- 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



Managing Mobile Devices in Your Health Care Organization

Health care providers and professionals are using mobile devices in their work. Covered entities comply with HIPAA Privacy and Security rules to protect and secure health information, when using mobile devices. As a leader within your organization, you are responsible for developing and implementing mobile device procedures and policies that will protect the health information patients entrust to you.

Five steps your organization can take to help manage mobile devices in your health care setting:

1. **Conduct a risk analysis** to identify threats to your organization's internal network or systems, if used as an electronic health record system. Understand the risks to your organization and decide to allow the use of mobile devices.
2. **Consider the risks** when using mobile devices to transmit the health information your organization holds.
3. **Conduct a risk analysis** to identify threats to your organization's internal network or systems, if you are a solo provider, or may conduct the risk analysis yourself. If you work for a large provider, the organization may conduct it.
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




Mobile Devices: Know the RISKS. 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.



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.



Mobile Device Program: 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.

Policy Guidance -- Compliance Tools

What's in the Works

- Fact Sheets/Q&A on new provisions
- Breach Risk Assessment Tool
- Minimum Necessary Guidance
- Better Compliance Tools for Small Entities
- Adaptation of SAG Training for Covered Entities
- Expanded Consumer Materials/Videos

Questions?

OCR website

HHS.gov/ocr/privacy