U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

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/coveredentities/De-identification/guidance.html
- Sample Business Associate Contract Language

  http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/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

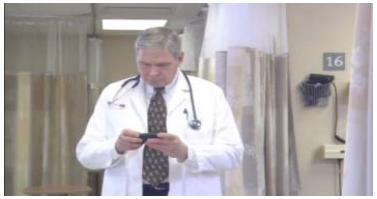
The videos explore mobile device risks and discuss privacy and security safeguards providers and professionals can put into place to mitigate risks.

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 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 applications (apps) before downloading.

Maintain physical control of your mobile device.

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

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