United States Department of Health & Human Services

Office of the Secretary
Office for Civil Rights (OCR)

Personal Health Records & HIPAA: HIPAA Privacy Rule Helps Now, and into the Future

Susan McAndrew, J.D.
Deputy Director for Health Information Privacy
April 24, 2008

HIPAA Privacy Rule Helps: Overview

- HIPAA Privacy Rule as Foundation for NHIN
  - Privacy and Security Are Integral to NHIN
    - Necessary for Public Trust
    - Public Participation Is Engine for Adoption
  - HIPAA Levels Playing Field
    - Nationally Accepted Standards for Privacy and Security Already in Place
    - Uniform National Baseline of Protection – More Is Still Good

HIPAA Helps: Overview

- HIPAA Privacy Rule as Facilitator – Not Obstacle to HIT/HIE Adoption
  - Standards Reflect Many Hard Choices Balancing Privacy and Access in Healthcare Setting
  - Narrows Privacy Debate to New Areas of Risk and Opportunity for Consumers
  - Flexibility Allows Rules to Adapt to HIE Needs without Lowering Baseline for All
- PHR Good Illustration for Assessing New Risks and Opportunities

HIPAA Privacy Rule Helps

Before We Contemplate the Future,

We Should Understand the Present…

What Is a PHR?

Sample Functionality	Content Examples
From Clip Board to Longitudinal Record	Medications, Doctors, Allergies, Health Care Encounters, Insurance Coverage
Clinical Communication Patient and Provider	Specific Information Exchange or Messaging
Routine Reminders Rx Refills	Prescriptions, Appointments, Yearly Reminders
"Search Engine"	Medical Education, Wellness Coaching

PHR and HIPAA Privacy

- Who Offers?
  - Provider
  - Health Plan
  - Employer (or Group of Employers)
  - Direct-to-Consumer Marketer

- What Information Flows Are Involved in the Functionality of the PHR?

PHR and HIPAA Privacy (cont'd)

- Provider or Plan (Covered Entity) offers PHR directly or engages Business Associate to do so
  - Offer and Management of PHR to Enrollees/Patients Permitted as Healthcare Operation
  - Information in PHR = PHI
  - CE/BA Obligations to Protect PHI Attach
  - Privacy Rule Allows CE/BA to Offer Individual More Control of PHI (e.g., access) in PHR

PHR and HIPAA Privacy Rule

- Employer or Vendor Offers PHR
  - Typically Will Not be Covered Entities
  - Management of PHR and Data in PHR Not Protected by the Privacy Rule
    - Consumer Must Rely on and Consider Carefully Privacy Promises from Employer or Vendor
  - Privacy Rule Controls Movement of PHI from CE into these PHRs
    - PHI Provided to Individual or with Authorization
    - Includes PHI from Employee's Health Plan

HIPAA Helps into the Future

HIPAA Privacy Rule and the Future:

PHRs and the NHIN…

Gaps for Future PHR & NHIN

- Accountability
  - New Players Typically Not Covered by HIPAA
    - Certain Health Care Providers
    - Providers of Network Services
    - Providers of Data Management Services
    - Providers of PHR Services
  - Can Business Associate Contracts Work and Provide Adequate Accountability in the NHIN?

Gaps for Future of PHR & NHIN

- Uniformity – How Much Is Really Needed
  - Preemption
    - Harmonizing Federal and State Laws
    - Ex: Consents
  - "Flexible and Scalable" Standards
    - Harmonizing Business Practices
    - Ex: Minimum Necessary
  - Privacy and Security Solutions for Interoperable Health Information Exchange
    - Looking for Answers

Opportunities for Future PHR & NHIN

- PHR = Opportunities for the Consumer to Engage in NHIN and Take Advantage of HIT
  - 24/7 Access to Their Health Information
  - Ability to Migrate Information into PHR to Create a Longitudinal Health Record
  - Ability to Consolidate Health Information from Multiple Providers to Better Manage Their Own Care
  - Capability to Control Access by Others
- Requires Interoperable, Portable, Secure PHR

United States Department of Health & Human Services

Office of the Secretary
Office for Civil Rights (OCR)

Questions?

http://www.hhs.gov/ocr/hipaa/

Susan McAndrew, J.D.
Deputy Director for Health Information Privacy
April 24, 2008