Overview of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and CMS' Implementation

Mike Pagels, Director, Privacy Rights
and Protection Staff,
Center for Beneficiary Choices

March 2005

Contents of This Resource

- Overview of the HIPAA Privacy Rule provisions
- CMS implementation

2

HIPAA Privacy Rule and Privacy Act of 1974

- The Privacy Rule and Privacy Act of 1974 are based on the same fair information principles
- The Privacy Act protects records with individually identifiable information held by federal agencies
- The Privacy Rule applies to a covered entity's protected health information (defined by the Rule) and extends privacy requirements to the private sector

3

Purpose of HIPAA Provisions

- Improve efficiency and effectiveness of health care system by standardizing the electronic exchange of administrative and financial data
- Protect security and privacy of transmitted information

4

HIPAA Privacy Rule Chronology

➢ August 21, 1996:	HIPAA enacted
➢ December 28, 2000:	Final Privacy Rule published on Standards for Privacy of Individually Identifiable Health Information (Privacy Rule)
➢ April 14, 2001:	Final Privacy Rule became effective after additional comment period
➢ August 14, 2002:	Final Privacy Modifications
➢ April 14, 2003:	Compliance date for most covered entities (April 2004 for small health plans)

5

Who's Covered

Covered Entities

- All health **plans**
- All health care **clearinghouses**
- Health care **providers** who transmit health information electronically in connection with standard transactions

6

Business Associates (BA)

- BA uses protected health information (PHI) to perform activities on behalf of covered entity or provide services to covered entity
- Satisfactory assurance (usually in contract) that BA will safeguard PHI
  - If both govt. agencies, may use a memorandum of understanding (MOU)
- Covered entity:
  - Responsible for known violation of business associate agreement
  - Does not have to monitor the BA

7

What is Covered

- Protected health information (PHI) is:
  - Individually identifiable health information
  - Transmitted or maintained in any form or medium
- Held by covered entity or its business associate
- **Note**: PHI does not include: Education records covered by Family Educational Rights & Privacy Act, and employment records held by covered entity as an employer

8

Individual Rights

- Receive a written privacy notice of information practices from providers and health plans
- Inspect and obtain a copy of PHI
- Amend PHI
- Request an accounting of disclosures of PHI
- Have reasonable requests for confidential communications accommodated
- Request restrictions on uses and disclosures for payment, treatment and health care operations
- File a complaint with the covered entity and the HHS Office for Civil Rights (OCR)

9

Uses and Disclosures of PHI

- Required
  - To the individual
  - To the HHS Secretary for compliance
- Permitted
  - For treatment, payment, and health care operations
  - Opportunity to agree or object (i.e., facility directory or family member)
  - For specific public priorities (e.g., public health or health oversight)
- Individual authorization needed for all other uses and disclosures of PHI (e.g., marketing)

10

Privacy Board

- Reviews and approves requests to use and disclose PHI for research purposes
- Data use agreements required to ensure privacy protection
- No Privacy Board review for Limited Data Sets that do not contain specified direct identifiers

11

Administrative Requirements

Flexible and Scalable

- Must have a Privacy Official
- Develop privacy policies regarding uses and disclosures of PHI
- Provide privacy training to workforce
- Develop a system of sanctions for employees who violate policies

12

Compliance and Enforcement HHS Office for Civil Rights (OCR)

12/28/2000—Secretary delegated the authority to OCR to enforce the HIPAA Privacy Rule

- Administer, interpret, implement, and enforce Privacy Rule
- Impose civil monetary penalties

www.hhs.gov/ocr/hipaa

13

CMS Implementation of the HIPAA Privacy Rule

CMS Programs that are Covered Health Plans:

- Medicare Fee-for-Service (Original Medicare Health Plan)
- Medicare Advantage (MA) Plans
- Medicare Advantage Prescription Drug Plans (MA PDPs) and Prescription Drug Plans (PDPs)
- Medicaid
- State Children's Health Insurance Program

14

Responsibility for Ensuring Compliance

- CMS is directly responsible for the Original Medicare Plan
- The appropriate State Agency is responsible for Medicaid and SCHIP programs
- MA, MA PDPs and PDPs are covered entities and responsible for their own compliance

15

Quality Improvement Organizations (QIOs) and Survey and Certification

- Information sought by QIOs is required by statute or regulation; therefore, PHI may be disclosed to QIOs without an individual's authorization.
  - QIOs are not business associates of providers
- PHI may be disclosed for survey and certification work as required by law and for health oversight activities
  - State Survey Agencies are not business associates of the surveyed entities
- PHI may be disclosed without the subject individual's authorization to the extent a law mandates such disclosure or for health oversight activities

16

CMS Communication Strategy & Outreach

- Notice of Privacy Practices for the Original Medicare Plan
- 1-800-MEDICARE
- FI/Carrier instructions and other CMS privacy guidance
- Centralized process to respond to individuals who exercise their privacy rights or file a complaint
- RO contacts for complaints about contractor privacy violations
- **NOTE**: ROs continue to respond to inquiries (as they did before HIPAA) using existing customer service procedures

17

Notice of Privacy Practices for the Original Medicare Plan

- Published in *Medicare & You* handbook and posted on www.medicare.gov
- Plain language notice explains
  - how Original Medicare uses and discloses personal medical information
  - individual rights and how to exercise them
  - Medicare's legal duties
  - where to go for more information on privacy.

18

1-800-MEDICARE Scripts

- Scripts address the individual rights listed in the Notice of Privacy Practices for the Original Medicare Plan
- Scripts accessed by the Customer Service Representatives since October 2002:
  - Notice of Privacy Practices for the Original Medicare Plan
  - How to file a complaint
  - How to request an accounting of disclosures
- Call center staff refer callers to appropriate staff in CMS. If the referral is to central office, callers are told to write to Privacy Complaints, or Accounting of Disclosures, or HIPAA Privacy Record Access at U.S. Department of Heath and Human Services, Centers for Medicare & Medicaid Services.

19

FI & Carrier Instructions

- Disclosure Desk Reference for Call Centers (Call Center Chart)
- FFS Contractor Guidance
- FFS Contractor Guidance on the Business Associate Provisions
- Core Elements and Required Statements for a Valid Authorization
- Joint Letter Regarding Disclosures to Facilitate Proper Billing

20

Websites (Internet)

- **www.medicare.gov**
  - Notice of Privacy Practices for the Original Medicare Plan
  - FAQs
  - Beneficiary Chart on Requesting Personal Information by Phone
- **cms.hhs.gov/hipaa/privacy**
  - Notice of Privacy Practices for the Original Medicare Plan
  - CMS Implementation Documents
  - Link to HHS Office for Civil Rights
- **www.hhs.gov/ocr/hipaa**

21

Websites (Intranet)

- Beneficiary Confidentiality Board papers and minutes
- HIPAA Privacy Rule (link to OCR web site)
- HHS OCR Privacy Guidance
- Designation of HHS Health Care Components
- Notice of Privacy Practices for the Original Medicare Plan
- CMS Privacy Rule Implementation Plan
- The HIPAA Privacy Rule and Research (NIH)
- The HIPAA Privacy Rule and Public Health (CDC)
- Link to CMS's Privacy Act home page
  - Systems of Records Notices
  - CMS Computer Matching Agreements
  - Link to Privacy Act

22

Websites (Intranet)

(continued)

- CMS Information Security and Privacy Training
- CMS Privacy Policies and Implementation Documents
  - Policy Papers
    - Minimum Necessary
    - Limited Data Set
  - Program Memoranda
  - Frequently Asked Questions
  - Process for Responding to Requests to Exercise Privacy Rights
  - SHIP Standard Operating Procedure
  - Medicare Advantage, QIO, Survey & Cert Information

23

Privacy Rights and Protection Staff/CBC

- Mike Pagels, Director, 410-786-5759
- Marla Aron, 410-786-3260
- Amy Chapper, 410-786-0367
- Robin Getzendanner, 410-786-9621
- Jennifer Kordonski, 410-786-1840

BCB @ cms.hhs.gov

24