HIPAA Administrative Simplification

PRICEWATERHOUSECOOPERS

Applicability to Pharma

William R. Braithwaite, MD, PhD
"Doctor HIPAA"

Pharmaceutical Regulatory and Compliance Congress and Best Practices Forum

Philadelphia, PA
November 15, 2002

HHS Required to Adopt Standards:

- Electronic transmission of specific administrative and financial transactions (including data elements and code sets)
  - ✓ List includes claim, remittance advice, claim status, referral certification, enrollment, claim attachment, etc.
  - ✓ Others as adopted by HHS.
- Unique identifiers (including allowed uses)
  - ✓ Health care providers, plans, employers, & individuals.
  - ✓ For use in the health care system.
- Security and electronic signatures
  - ✓ Safeguards to protect health information.
- Privacy
  - ✓ For individually identifiable health information.

Applicability

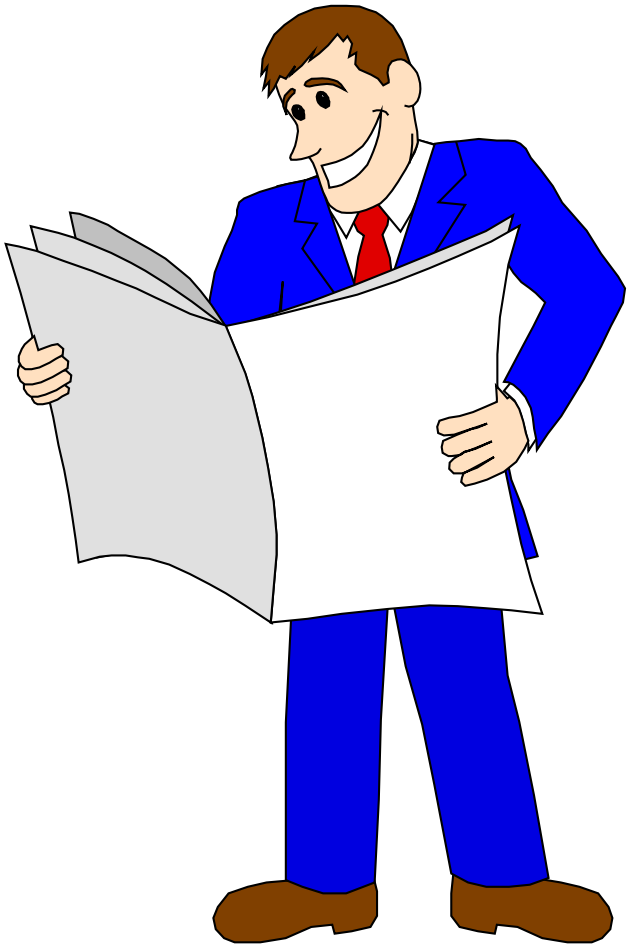
- Applies directly only to Covered Entities:
  1. Health Plans.
     - Including ERISA plans.
  2. Health Care Clearinghouses.
     - Including most PBMs.
  3. Health Care Providers who elect to conduct administrative transactions electronically.
     - Including all providers > 10 FTE who bill Medicare.
     - Includes pharmacies (both local and mail order).
- Applies indirectly to Business Associates:
  - ✓ Agent who handles Protected Health Information (PHI) on behalf of a Covered Entity.

HIPAA Standards Philosophy

- To save money:
  - every payer must conduct standard transactions.
  - no difference based on where transaction is sent.
- Standards must be
  - industry consensus based (whenever possible).
  - national, scalable, flexible, and technology neutral.
- Implementation costs must be less than savings.
  - Savings may depend on integrated implementation of requirements; compliance effort alone may not be enough.
- Continuous process of rule refinement:
  - Annual update maximum (for each standard) to save on maintenance and transitions.

HIPAA Timeline

- ✓ Transactions Final Rule - 8/17/00
  - Compliance plan by 10/16/02
  - Modifications final rule expected 12/27/02
  - Testing by 4/16/03
  - Compliance by 10/16/03
- ✓ Privacy Final Rule - 12/28/00
  - Modifications Final Rule 8/14/02
  - Compliance by 4/14/03
- ✓ Employer ID NPRM - 6/16/98
  - Final Rule - 5/31/02
  - Compliance by 7/30/04
- ✓ National Provider ID NPRM - 5/7/98
- ✓ Security NPRM - 8/12/98



New Final Rules and NPRMs

- Expected by Q1 2003 (some as early as 12/27/02):
  - ✓ Security Final Rule
  - ✓ National Provider ID Final Rule
  - ✓ Health Plan ID NPRM
  - ✓ Claim Attachment NPRM

- More standards to come in future:
  - ✓ First Report of Injury
  - ✓ Electronic Prescriptions
  - ✓ Patient Medical Record Information (PMRI)
  - ✓ Public Health Reporting

5 Principles of Fair Info Practices

- Openness [Notice]
  - ✓ Existence and purpose of record-keeping systems must be publicly known.
- Individual Participation [Access]
  - ✓ Individual right to see records and assure quality of information.
    - – accurate, complete, and timely.
- Security [Safeguards]
  - ✓ Reasonable safeguards for confidentiality, integrity, and availability of information.
- Accountability [Enforcement]
  - ✓ Violations result in reasonable penalties and mitigation.
- Limits on Collection, Use, and Disclosure [Choice]
  - ✓ Collected only with knowledge and permission of subject.
  - ✓ Used only in ways relevant to the purpose for which the data was collected.
  - ✓ Disclosed only with permission or overriding legal authority.

Privacy Scope: What is Covered?

- Protected health information (PHI) is:
  - ✓ Individually identifiable health information,
  - ✓ Transmitted or maintained in any form or medium,
  - ✓ Held by covered entities or their business associates.

- De-identified information is not covered.
  - ✓ Specific rules determine de-identification.

Individual's Rights

- Individuals have the right to:
  - ✓ A written notice of information practices from health plans and providers.
  - ✓ Inspect and obtain a copy of their Designated Record Set (DRS).
  - ✓ Obtain an accounting of disclosures.
  - ✓ Amend their records.
  - ✓ Request restrictions on uses and disclosures.
  - ✓ Accommodation of reasonable communication requests.
  - ✓ Complain to the covered entity and to HHS.

Key Points

- Covered entities can provide greater protections if they want.
- Required disclosures are limited to:
  - ✓ Disclosures to the individual who is the subject of information.
  - ✓ Disclosures to OCR to determine compliance.
- All other uses and disclosures in the Rule are permissive.

Uses and Disclosures

- Must be limited to what is permitted under 4 mechanisms in the Rule:
  - ✓ Treatment, payment, and health care operations (TPO).
  - ✓ Uses and disclosures involving the individual's care or directory assistance,
    - Requiring an opportunity to agree or object.
  - ✓ For specific public policy exceptions.
  - ✓ All others as specifically authorized by individual.
- Requirements vary based on type of use or disclosure.

Health Care Operations examples

- ✓ outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies.
- ✓ population-based activities relating to:
  - improving health or reducing health care costs,
  - protocol development,
  - case management and care coordination,
  - contacting of health care providers and patients with information about treatment alternatives.
- ✓ evaluating performance of providers and plans.
- ✓ training programs.
- ✓ accreditation, certification, licensing, or credentialing.

Policy Exceptions

- Covered entities may use or disclose PHI without a consent or authorization only if the use or disclosure comes within one of the listed exceptions & certain conditions are met;

  - ✓ As required by law.
  - ✓ For public health.
  - ✓ For law enforcement.
  - ✓ Coroners, medical examiners, funeral directors.
  - ✓ …
  - ✓ Health care oversight.
  - ✓ For research.
  - ✓ Organ transplants.

Using PHI for Research Purposes

- 6+ ways PHI can be used for research:

1. De-identified PHI
2. Limited Data Set with Data Use Agreement
3. PHI with IRB/Privacy Board waiver
4. PHI for research protocol preparation
5. PHI of deceased
6. PHI with authorization of subject

- plus, Healthcare Operations, Public Health, and as otherwise required by law (registry, reportable).

How does HIPAA affect research?

- ✓ New burdens for IRBs.
- ✓ Voluntary registries must now get patient authorization.
- ✓ Liability fears may dissuade CEs from sharing data with researchers.
- ✓ New forms for research subjects.
- ✓ Health Plans and Providers must track and account for research disclosures made without authorizations.

Marketing under 8/14/02 Final Rule

- Marketing may not be done without specific authorization of the individual …
- Marketing definition INCLUDES:
  - ✓ communications about a product or service that encourage recipients to purchase or use the product or service.
  - ✓ arrangements whereby the CE discloses PHI to the another entity, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product or service.
- BUT …
- Individual ability to opt-out removed.
- AND …

Marketing Exclusions

- Marketing definition EXCLUDES communications by CE:

(i) To describe a health-related product or service, including:

- ✓ entities participating in a health care provider network or health plan network;
- ✓ replacement of, or enhancements to, a health plan; and
- ✓ health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits.

(ii) For treatment of the individual; or

(iii) For case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual.

Expected Security Final Rule

- Definitions and applicability harmonized with privacy.
- Requirements clarified and redundancies removed.
- Same philosophy as NPRM.
  - ✓ Organization specific risk analysis and documentation of decisions.
  - ✓ Only applies to electronically maintained and transmitted health information.
  - ✓ Continues to be technology neutral.
- No electronic signature standard.
- Rule expected 12/27/02.
  - ✓ Compliance expected in February 2005.

Administrative Requirements

- Apply to both privacy and security.
- Flexible & scalable (i.e., requires thought!).
- Covered entities required to:
  - ✓ Designate a responsible official (privacy/security).
  - ✓ Develop policies and procedures (P&P),
    - including on receiving complaints.
  - ✓ Train workforce on HIPAA **&** entity's P&P.
  - ✓ Develop a system of sanctions for employees who violate the entity's policies.
  - ✓ Meet documentation requirements.
    - you didn't do it if it's not documented.

Enforcement Philosophy

- Enforcement by investigating complaints.
  - ✓ No HIPAA police force -- OCR not OIG for privacy.
- Fines by HHS are unlikely (and small).
  - ✓ Required by HIPAA to help people comply!
- Fines and jail time possible from DOJ.
  - ✓ Where intent can be proven (difficult to do).
- BUT, real risk comes from
  - ✓ Civil liability from private lawsuits.
- Dictates Risk Management Approach

Other Privacy Drivers

- E.U Data Directive
- E.U – U.S. Safe Harbor
- New federal privacy law being proposed
- State Privacy Laws (new state laws)
- Consumer Protection Law (State)
- Federal Trade Commission (Eli Lilly).
- Internet Privacy (e.g., COPPA)
- Reputation Assurance
- Business Disruption prevention

Pharma Privacy – 6 Areas of Impact

- Drug Discovery
- Research
- Marketing
- Sales
- HR
- Customer Support/Service

Drug Discovery

- Genetic Studies
  - ✓ Taking genetic samples and using related health information requires research IRB approval and individual authorization.
- Tissue Samples
  - ✓ Not PHI per se, but usually accompanied by PHI.
  - ✓ May become PHI in future, since genetic information in sample could be used to identify an individual.

Research

- Clinical Trails – phases 1 thru 4
  - ✓ New language required in patient authorizations
- Use of CROs
  - ✓ Identifiable information on patients may not be disclosed to pharmaceutical firm without specific authorization
- Pharmacovigilence
  - ✓ Adverse event reporting allowed under public health/FDA
- Patient Registries
  - ✓ Authorization required unless under public health law
  - ✓ Special case: expiration date = “None”
- Financial interests
  - ✓ Personal financial info on investigators

Marketing

- Data Warehouses
  - Multiple sources of data; under authorizations?
- Web Sites
  - Privacy statements must be adhered to (FTC)
- Direct Mail
  - Covered entity must obtain an authorization for any use or disclosure of protected health information for marketing
- Patient Support Programs
  - Patient authorization required if covered entity
- Disease Management or Wellness Programs
  - Treatment by provider, operations by plan, else BA
- Drug Compliance; Preceptorships
  - Require patient authorization

Sales

- Detail Reps – calling on physicians
  - ✓ Physicians may be using HIPAA privacy to ward off calls
  - ✓ Not excluded by HIPAA, but may require education
- Patient Care Coordinators
  - ✓ Clinicians looking at records may fall under treatment
- Sales Info (NDC or IMS)
  - ✓ Data available may change to meet new definition of de-identified
- Switch Programs
  - ✓ Allowed under HIPAA rules but not advisable without individual permission (CVS/Giant public reaction)

Human Resources

- Health Benefits
  - ERISA Health Benefit Plan for employees is covered
- Clinics
  - Not usually covered unless conducting electronic transactions
- EAPs
  - Not usually covered unless providers of ‘health care’
- Flexible Spending Accounts
  - May be covered as Health Plan
- Background Checks prerequisite to employment
  - Employment requirements for health information require HIPAA compliant individual authorization

Customer Services/Support

- Reimbursement Programs
  - ✓ Not addressed directly in HIPAA rules, but most likely will require patient authorizations.
- Indigent Care
  - ✓ May require HIPAA authorization.
- Adverse Event Reporting
  - ✓ Permitted without authorization (but must be accounted for)

- Bottom Line Recommendation:
  - ✓ Each activity must be looked at closely in terms of what is done with what and whom, not at what it is called.
  - ✓ Evaluate on basis of fair information principles first, then rules and regulations.

Questions?

Bill.Braithwaite@us.PwCglobal.com

http://www.pwchealth.com/hipaa.html

http://aspe.hhs.gov/admnsimp

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

www.cms.hhs.gov/hipaa/

ncvhs.hhs.gov

www.wedi.org

snip.wedi.org

Only 150 days left!

PRICEWATERHOUSECOOPERS