GETTING HIP TO HIPAA
Thomas R. Hoffman, JD, CAE
ACR Associate General Counsel
AAPM 48th Annual Meeting
August 2, 2006

LYRICS (aka HIPAA LANDSCAPE)
• Message
• Terminology
• HIPAA Framework: Administrative Simplification?!
  • Privacy Standards
  • Security Standards
  • Transactions and Code Sets Standards
  • Unique Identifiers
• Helpful Government & ACR Guidance

HIPAA Lives On...
Message
• HIPAA is law of the land
• It’s here to stay BUT...
• You can manage its requirements
HIPAA Privacy Rule

- HIPAA enacted 1996
- First “final” rule 2000
- Amended rules published 2002
- Effective April 14, 2003

**Terminology Lesson**

- PHI (Protected health information): Individually identifiable health information
  - Name
  - SS Number
  - Medical Record Number
  - Account Number
  - Driver License Number

**Use**

With respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information [45 CFR §160.103]

Clear as mud, maybe disclosure is easier!

**Disclosure**

The release, transfer, provision of access to or divulging in any other manner of information outside the entity holding the information [45 CFR §164.103].

Maybe only dirty water now – the key word is “outside”
HIPAA Privacy Rule

- Required uses and disclosures
  - To patients (or personal representatives) on request
  - To HHS for compliance or enforcement action

- Incidental use and disclosure?
  - Yes if permitted use (discussing PHI with dosimetrist)

HIPAA Privacy Rule

- PTO - (Not Paid Time Off)
  - Payment
  - Treatment
  - Operations (Quality Assurance; credentialing)

- Can disclose PHI for these reasons without consent

HIPAA Privacy Rule

- Business Associate Contract
  - Merely providing software to a health care organization does not create a business associate (BA) relationship
  - However, if the vendor provides services that require it to access PHI to assist with data processing or to perform other functions for the health care organization, the vendor would be a business associate

More HIPAA Notes to Sing...

Security Standards

- Effective April 2003, enforceable April 2005
- Apply only to electronic transmissions
- Incorporate broad PHI safeguards
  - Administrative (managing security process)
  - Physical (facility access controls)
  - Technical (data encryption)
HIPAA Security Standards

- Conduct thorough risk analysis
- "Technology-neutral": one size does not fit all
- Adopt reasonable controls on PHI
- Communicate early and often with IT vendor(s)

What does this mean to a physicist?!

Role: covered entity or business associate?
- Physicist as employee = agent and part of CE
  - Could serve as BA to other hospital or facility
- **Physicist as independent contractor = BA to health care provider CE (would execute BA agreement)**
  - and as CE if handling PHI for diagnosis or treatment (no BA contract needed)

Service contract tips:
- Conform BA contracts to privacy rule
- Hold BA to security safeguards
- Ask for “HIPAA compliance certificate”

More HIPAA Notes

Transactions Rule
- Effective October 2003 → “interoperability”
- Apply to 10 EDI transactions
  - Claims and encounter information
  - Payment and remittance advice
- Official code sets → ICD-9, CPT®
- CMS only accepts compliant claims
And More Works...

Unique Identifier Standards
• Employer Identification Number: effective July 2002
• National Provider Identifier (NPI)
  – Standard, portable unique ID for providers
  – Final rule adopted January 2004
  – Must use starting May 2007 for HIPAA transactions

Keeping in Tune with HIPAA
Government is here to help!
• HHS Office for Civil Rights has ample privacy toolkit
  • www.hhs.gov/ocr/hipaa
• CMS offers security, transactions links
  • http://www.cms.hhs.gov/hipageninfo/01_overview.asp?

ACR has model policies and procedures
• www.acr.org