Privacy, Confidentiality and Security Subcommittee

Update to NCVHS on its HIPAA Section 1179 public meeting

May 6-7, 2015

Objectives for the Public Meeting

1. Understand the current and anticipated financial services practices involving personal health data
2. Review how HIPAA Section 1179 is being interpreted and applied in light of these practices, and
3. Identify what NCVHS might recommend, if anything, that might be helpful (outreach, education, technical assistance, guidance or something else)

What is Section 1179?

Section 1179 of the Health Insurance Portability and Accountability Act (HIPAA) creates an exemption from compliance with HIPAA and accompanying rules when a financial institution is

> "engaged in authorizing, processing, clearing, settling, billing, transferring, or collecting payments."

Why this provision?

- Exempt from HIPAA "core" financial activities involving payments
  - Example – patient pays provider by check or credit card; both patient's and provider's bank get PHI.
- Distinguish clearinghouse under HIPAA from banking system's automated clearing house (ACH).
- N.B.: Business Associates were created by subsequent privacy regulations.

NCVHS 2004 Letter to the Secretary on § 1179

HHS should

1. Clarify the nature of § 1179 exemption, to whom it applies;
2. Recommend to providers and payers use of BAAs with financial institutions
3. Consider whether encryption should be required for PHI moving through ACH network

HITECH Changes

- Business associates now subject to HIPAA rules directly, even without a business associate agreement

- Allocation of responsibility becomes more important because of breach notification

Examples of financial services for healthcare

- Cash management (lock box, cash disbursement)
- ACH Networks
- EDI payments processing (remittance consolidation)
- Lockbox processing
- Healthcare credit practices
- Online/mobile payments
- Revenue cycle consultation
- Credit care operations
- HSA/HRA/MSA/FSA support
- Data analytics

How should we interpret § 1179 today?

- What are the "treasury" functions that are clearly within §1179?
- When is a bank doing clearinghouse functions?
- When should a bank be a legal business associate?

How do financial institutions think their functions fit into HIPAA?

- Legal structure of HIPAA v. Banking statutes
- Conflicts and gaps amomg legal regimes
- Opportunities for clarity in interpretation?
- Opportunities for harmonization?

Gaps in financial industry understanding of HIPAA

- "We're exempt, so we don't have to worry"

  BUT: Just because there is no BAA, does not relieve them of liability

- Understanding of actual requirements of HIPAA
  - Minimum necessary v. meaningful use
  - Amendments and corrections

Gaps in health sector management of relationships with financial institutions

- Inconsistencies in when, how BAs are executed
- Competencies in vendor assurance
  - Risk assessment
  - Security risk assessment
  - Privacy impact assessments

Opportunities for learning from financial industry

- Health care can learn about security from banking
  - Strong audit functions (with some exceptions)
  - Compliance functions
  - Investment in security
  - Vendor assurance

Opportunities for financial services to learn from health sector

- Privacy as a value promoting trust
- Limitation on data sharing functions
- Consumer orientation

Related issues in a changing environment

- Wearables
- Mobile apps for health, banking, other services
- Alternative payment services
- Non-covered entities, no BAs
- Expansion of Big Data analytics
- DWG could generate more examples?

Possible recommendations to HHS for 2015

- Convene health-financial cross-industry work group
  - policy and best practices for advancing privacy
  - evolving role of consumers
- Issue guidance on BAAs, other provisions of the Rules
  - for provider, health plans and financial services organizations
- Conduct gap analysis of HIPAA v. banking regs on privacy
- Outreach to financial services sector by OCR
- Further study on use of big data analytics

Next steps on financial services and HIPAA?

- Hear from DWG
- Predictive analytics
- Hear from non-traditional financial services:
  - Paypal, Apple, others that do not collect health info
  - Amazon – collects customer purchase data

Potential topics for PCS Subcommittee, NCVHS?

- Data as an asset
- Non-HIPAA covered entities
- Wearables
- Mobile technology
- Wellness programs – recent issued guidance from OCR
- Predictive analytics