The Office of the National Coordinator for Health Information Technology

HIPAA 101 for Entrepreneurs

ONC Innovation Exchange

December 13th, 2013

Joy Pritts, JD
Chief Privacy Officer
Office of the National Coordinator
Health Information Technology

Office of the Chief Privacy Officer
The Office of the National Coordinator for Health Information Technology

Who is Covered Under HIPAA Privacy Rule?

- **Covered Entities (CEs)**
  - Health plans
  - Health care providers that conduct certain transactions (generally claims-related) in electronic form
  - Health care clearinghouses
- **Business Associates (Bas)**

Perform certain functions or activities *on behalf of a covered entity* that involve the use or disclosure of PHI including:

  - Data analysis
  - Data aggregation
  - Claims processing
  - Quality assurance
  - Legal services
  - Accounting
  - Others specified

Who is NOT Covered Under HIPAA Privacy Rule?

- **Does not cover**
  - Providers who don't accept health insurance (generally)
    - Many dentists
    - Boutique practices
    - Internet health services that only accept credit cards (e.g., mental health consultants)
  - Many recipients of PHI from covered entities
  - Recipients of health information directly from consumers (e.g., health web sites where consumers fill out surveys)

Patient Focus

- Right of access
  - HITECH—electronic access
  - Blue Button Initiative
- Patient control
  - More granular control
    - Data Segmentation
  - Meaningful Consent

Marketing & Fundraising

- **Marketing**
  - Communications about health-related products and services by covered entity to individuals now marketing and require authorization if paid for by third party
  - Limited exception for refill reminders (and similar communications)
    - Payment must be reasonably related to cost of communication
  - Face to face marketing communications and promotional gifts of nominal value still permitted without authorization
- **Fundraising**
  - Covered entity (CE) may use additional information to target fundraising communications but must provide easy way for individuals to stop receiving solicitations

Sale of PHI

- Even where disclosure is permitted, CE is prohibited from disclosing protected health information (PHI) (without individual authorization) in exchange for remuneration
  - Includes remuneration received directly or indirectly from recipient
  - Not limited to financial remuneration
- If authorization obtained, authorization must state that disclosure will result in remuneration
- Note: Does not apply to de-identified information

Sale of PHI

- Exceptions:
  - Treatment & payment
  - Sale of business
  - Remuneration to BA for services rendered
  - Disclosure required by law
  - Public health
  - Research, if remuneration limited to cost to prepare and transmit PHI
  - Providing access or accounting to individual
  - Any other permitted disclosure where only receive reasonable, cost-based fee to prepare and transmit PHI

Federal Trade Commission

- Section 5 of the FTC Act jurisdiction to prevent "unfair or deceptive acts or practices in or affecting commerce"
- Deceptive acts: a representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances and is material to the consumer
  - Consumer would potentially not buy product or use serviced offered absent the deception
  - Intent not required
  - Actual harm not required

Federal Trade Commission

- Unfair acts: cause or are likely to cause substantial injury consumers that is not reasonably avoidable by consumers themselves and not outweighed by benefits to consumer


Office of the Chief Privacy Officer
The Office of the National Coordinator for
Health Information Technology


HealthIT.gov