HIPAA Overview

Darren Skyles, Partner
McGinnis Lochridge

Darren S. Skyles
dskyles@mcginnislaw.com

HIPAA

- Health Insurance Portability and Accountability Act of 1996
  - Electronic transaction and code sets: Adopted standards for electronic transactions and standardized code sets to facilitate exchange of health information.
  - Unique Identifiers: Numbers that identify the various entities in any given healthcare transaction.
  - Privacy Standards: Rules for ensuring the privacy of protected health information (PHI).
  - Security Standards: Rules for ensuring the confidentiality, integrity and availability of PHI that is collected, maintained, used or transmitted electronically.

Darren S. Skyles
dskyles@mcginnislaw.com

Early Stages and Development of HIPAA (1992-1996)

- Over several decades, lurking and growing congressional and public concern over rising health care costs and breaches of patient privacy
  - (by 1992, health care costs 14.3% of gross domestic product).
- Workgroup for Electronic Interchange (WEDI).
- Continued push in early 1990's for administrative simplification provisions; standardization of data exchange in the health care process.

- Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, signed by Bill Clinton August 21, 1996.

Darren S. Skyles
dskyles@mcginnislaw.com

Early Stages and Development of HIPAA (2002-2009)

- Issuance of:
  - Security Rule
  - Standardization of health care transactions and administrative and coding formats (ICD-10)
- Executive Order, 2004 – To develop a nationwide interoperable health information technology infrastructure (goal by 2014).

- 2009 American Recovery and Reinvestment Act (HITECH Act) Amendments—additional safeguards and more focused enforcement of HIPAA rules as well as $20 billion in health IT funding + incentives.

Darren S. Skyles
dskyles@mcginnislaw.com

Covered Entity

- Covered Entity—Any of the following to the extent they transmit health information in an electronic format in connection with a HIPAA transaction:
  - Health Plan
  - Health Care Clearinghouse
  - Health Care Provider
- Business Associate—A person or organization that performs a function or activity on behalf of a covered entity, but is not a part of the covered entity's workforce.

Darren S. Skyles
dskyles@mcginnislaw.com

PHI

- Any information, whether oral or recorded, in any form or medium that:

- Is created or received by a health care provider, health plan; public health authority, employer; life insurer, school or university; or health care clearinghouse; and the information relates to the:
  - Past, present or future physical or mental health or condition of an individual;
  - Provision of health care to an individual; or past, present, or future payment for the provision of health care to an individual.

Darren S. Skyles
dskyles@mcginnislaw.com

Privacy Standards

- Protected Health Information (PHI)
  - Treatment, Payment & Health Care Operations (TPO)
    - Minimal Uses & Disclosures—Limiting PHI to minimum necessary to accomplish the intended purpose of the use, disclosure or request.
    - Opportunities for patient to agree or object.
  - Disclosures of PHI with patient Authorization
    - Psychotherapy Notes, Marketing, Fundraising, etc.
  - Disclosures where no patient Authorization required
    - Public Health Purposes, Judicial and Administrative Proceedings , Law Enforcement, etc.

Darren S. Skyles
dskyles@mcginnislaw.com

Security Standards

- Set minimal standards of security (i.e., not necessarily best practice standards).
- Covered Entities must Ensure + Protect:
  - confidentiality, integrity and availability of PHI;
  - against reasonably anticipated threats;
  - against reasonably anticipated impermissible uses or disclosures;
  - compliance by the Covered Entity's workforce.
  - Required and Addressable standards (Administrative, Physical and Technical)
  - compliance by the Covered Entity's workforce.
  - Required and Addressable standards (Administrative, Physical and Technical)

Darren S. Skyles
dskyles@mcginnislaw.com

HITECH ACT

- American Recovery and Reinvestment Act of 2009 a/k/a Health Information Technology for Economic and Clinical Health Act (HITECH)
- Expanded HIPAA:
  - Breach Notification
  - Ensured Business Associates are also subject to HIPAA
  - Increased penalties and authorized state attorneys general to enforce HIPAA in federal court

Darren S. Skyles
dskyles@mcginnislaw.com

Oversight of HIPAA

- HIPAA requires Secretary of the U.S. Department of Health and Human Services (DHHS) to adopt national uniform standards.
- Office for Civil Rights (OCR) implements and enforces the privacy and security rules.
- The Centers for Medicare and Medicaid Services (CMS) implements and enforces remainder (e.g., provisions pertaining to payment).
- State Attorneys General

Darren S. Skyles
dskyles@mcginnislaw.com

State Law Enforcement

- Texas Medical Records Privacy Act
- Any individual, business or organization (including any employee, agent or contractor of these) that possesses, obtains or stores PHI is required to protect the PHI in accordance with the Act.

  Requirements:

  - Providing timely job-specific training
  - Drafting and implementing policies and procedures
  - Considering what authorization from individuals is required when their PHI is subject to disclosure
  - Breach notification
- The Texas Attorney General enforces these privacy and security laws, and spot-checks and audits may be performed on businesses to ensure compliance. Penalties for a violation of the Act can range from $5,000 to $250,000 per violation, and for violations of identity theft protection laws, $2,000 to $50,000.

Darren S. Skyles
dskyles@mcginnislaw.com

Contact Information

Darren Skyles
McGinnis Lochridge
512-495-6109
dskyles@mcginnislaw.com

Health Law Practice Group
http://www.mcginnislaw.com/practices/health-law

Privacy and Data Security Practice Group
http://www.mcginnislaw.com/practices/privacy-and-data-security