About HIPAA

Christopher Adams

HIPAA – the Health Insurance Portability & Accountability Act of 1996 – is the dominant regulation concerning medical privacy in the United States. To most consumers of healthcare in the United States, "HIPAA" is a reference on a permission form that a healthcare provider asks a patient to complete before the patient can receive care. Actually, HIPAA is an initiative to reduce healthcare costs by standardizing the data exchanges between providers and insurers. Before HIPAA, a clinic that deals with a dozen different insurers might need a dozen different employees to handle the different forms and procedures. After HIPAA, a single person can support the information needs of multiple insurers as well as those of patients. The permission forms address privacy concerns posed by easier access to data via electronic storage and transmission.

The HIPAA regulations address:

- Electronic transactions and code sets
- National identifiers
- Privacy
- Security

Keep in mind that HIPAA is mainly about healthcare insurance and the privacy of medical data that accompanies insurance claims. This affects who is covered by the act and who is not.

Electronic Transaction Standards

Health care data is typically exchanged via one of several electronic media:

- Electronic data interchange (EDI) – sometimes referred as business-to-business (B2B)
- The Internet and web-based applications
- Direct data entry (DDE) via dial-up modem
- Sending a diskette or tape
- Using a credit card swipe machine at a point of service (POS)
- Using "faxback" telephone voice response

HIPAA regulates a fixed set of transactions:

- Claims or equivalent encounter information
- Payment and remittance advice
- Claim status inquiry and response
- Eligibility inquiry and response
- Referral certification and authorization inquiry and response
- Enrollment and disenrollment in a health plan
- Health plan premium payments
- Coordination of benefits (between health plans)
- Claims attachment
- First report of injury

Any transmission of a HIPAA transaction, by any of the media listed above, is covered by the HIPAA standards.

HIPAA standardizes code sets used within the transactions:

- Physician services (with code set CPT-4, a large coding system for services)
- Non-physician health services (HPCTS, another large coding system)
- Medical supplies, orthotics, and durable medical equipment (HPCTS)
- Diagnosis codes (ICD-9-CM, a large coding system for disease)
- In-patient hospital procedures (ICD-9)
- Dental services
- Drugs and biologics (NDC)
- Type of facility (small set defined by X12)

National Identifiers

As of 2006, HIPAA requires that health providers, health plans, and employers have standard national numbers that identify them on standard transactions. A providers and health plans obtain their identifiers from CMS. An employer identifies itself with the Employer Identification Number (EIN) that was issued by the Internal Revenue Service.

The original act also called for a national patient identifier. The creation of such an identifier was indefinitely postponed in response to political opposition due to privacy concerns.

The Privacy Rule

The privacy rule says that individually identifiable health information (IIHI) must be protected. IIHI includes any record containing data that identifies an individual or is a reasonable basis for identifying an individual.

Protected health information (PHI) does not apply to de-identified data. HIPAA allows three techniques for de-identifying data:

- Safe harbor
- Statistically sound technique
- Limited data set

Safe Harbor Rule

HIPAA provides for a safe harbor – a precise list of attributes without which a record cannot be ascribed to an individual.

The data is safe if all of the following are removed:

- Name
- Street address
- Telephone number
- FAX number
- Email address
- URL
- IP address
- License number
- Vehicle ID
- Health plan number
- Account number
- Device identifier
- Social Security Number
- Medical record number
- Biometric identifiers
- Full face photos
- Any other uniquely identifying number, characteristic, or code

Furthermore, certain attributes must be modified to encompass sufficiently large populations:

- Extreme ages of 90 and over must be aggregated to a category of 90+ to avoid identification of very old individuals
- Any location must be broadened to encompass at least 20,000 people – a ZIP code must be abbreviated to its first three digits

Statistically-Sound De-Identification

Algorithmic de-identification typically involves some combination of:

- Removal of certain safe-harbor identifiers
- Substitution of other identifiers with randomly calculated values that assure the distinction of individuals without actually identifying them

Limited Data Set

The HIPAA rules allow for a limited data set when the safe harbor too restrictive. In a limited data set, most safe-harbor identifiers are disallowed. Allowed data included:

- Admission, discharge, and service dates
- Date of death
- Age
- 5-digit ZIP code

For the collection and use of a limited data set, a data use agreement from each subject is required.

The Security Rule

The security rule covers the same information as that covered by the privacy rule, but only when that information is in electronic form. Whereas the privacy rule addresses what must be protected, the security rule deals with how to do so.

The security rule dictates:

- An information security officer
- Risk analysis
- Quality assurance
- Training

The Security Rule says that responsibility for security should be assigned to a specific individual to provide an organizational focus and importance to security. The security officer may be anyone in the organization, and may perform the role part-time only.

The Security Rule requires risk analysis: the identification of potential threats and vulnerabilities, estimating potential losses from those threats, and the identification of safeguards and the extent to which they reduce exposure to the threats.

The Security Rules requires security policies and procedures be developed and maintained in written form.

The Security Rule requires training of the workforce as reasonable and appropriate to perform their functions in the facility.

Covered Entities

Who is covered by the regulation?

- Healthcare providers
  - Individuals – physicians, nurses, pharmacists, …
  - Organizations – hospitals, laboratories, HMOs, pharmacies, …
- Health plans (payers)
- Healthcare clearinghouses (data handlers)

Any of these entities that transmits **any** health information in electronic form with a HIPAA transaction, or on its behalf pays another entity to do so, is covered by HIPAA. Note the emphasis. Regardless of the extent to which an entity employs electronic transactions, the privacy and security rules apply to the entity's entire operation.

Covered health plans include public as well as private insurers. HIPAA covers Medicare, Medicaid, and federal employee insurance.
Entities such as billing agents and information technology providers do not qualify as clearinghouses and are not, therefore, covered by HIPAA. However, their business operations can be affected by their dealings with covered entities.

Who is not covered by HIPAA?

- Workers compensation programs
- Property and casualty insurers
- Small self-administered health plans (with fewer than 50 members)
- Providers who conduct **all** standard transactions by paper, telephone or FAX (from a dedicated fax machine and not from a computer)

A provider's operation is either entirely covered by HIPAA or is not at all covered. The exclusion pertains not only to the transaction requirements but also to the privacy and security rules.

References

Center for Medicare and Medicaid Services. “HIPAA 101 For Health Care Providers’ Offices.” HIPAA Information Series, Volume 1, Paper 1, May 2003.

Center for Medicare and Medicaid Services. “Are You a Covered Entity?” HIPAA Information Series, Volume 1, Paper 2, May 2003.

Rada, Roy. HIPAA@IT Essentials: Health Information Transactions, Privacy, and Security. 2nd ed. HIPSS-IT LLC, 2003.