HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA)
PUB. L. 104-191, 45 C.F.R. PARTS 160, 162, AND 164
(HIPAA SECURITY AND PRIVACY RULES)

SUMMARY OF KEY PROVISIONS

- Protects individuals' health information while allowing the flow of health information to provide/promote high quality health care and to protect the public's health and well-being.

- National minimum set of privacy protections – not a set of "best practices".

STATE PREEMPTION

- Preempts "contrary" provision of state law.

  (1) Impossibility – impossible to comply with state and federal laws.

  (2) Obstacle – state law provision is an obstacle to accomplishing full purposes/objectives of HIPAA.

- Exceptions to preemption:

  (1) Secretary of Health and Human Services (HHS) – determination that state law provision:

  (a) Necessary to prevent fraud and abuse re: provision of or payment for health care;
  (b) Necessary to ensure appropriate state regulation of insurance and health plans;
  (c) Necessary for state reporting on health care delivery or costs;
  (d) Necessary for serving a compelling need related to public health, safety, or welfare and intrusion into privacy is warranted; or
  (e) Has a principal purpose of regulation of manufacture, registration, distribution, dispensing or other control of any controlled substance.

  (2) State counsel – determination that state law provision:

  (a) Provides for reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance, investigation, or intervention; or
  (b) Relates to privacy of individually identifiable health information and is more stringent than HIPAA Privacy Rule; or
  (c) Requires health plan to report, or provide access to, information for management and financial audits, program monitoring and evaluation, or the licensure or certification of facilities or individuals.

  (3) Only few requests for exception submitted to Secretary of HHS. None granted because state laws were not contrary to HIPAA.

PRIVACY RULE (§§ 164.500 – 164. 534)

General Provisions - Applicability

- Applies to "Covered entity" or "Business associate" (§ 164.502).

- May only use or disclose "Protected health information" (§ 164.502):

  (1) As permitted by Privacy Rule; or
  (2) As required by Privacy Rule; or
  (3) As individual who is subject of the health information, or individual's personal representative, authorizes in writing.

- " Protected health information" (PHI) (§ 160.103).

  (1) Individually identifiable health information that is transmitted or maintained in any form or media – electronic, paper, or oral.
  (2) Exclusions:

    (a) Employment records of covered entity in role as employer.
    (b) Education and certain records covered by Family Educational Rights and Privacy Act (20 U.S.C. § 1232g).

- "Covered entity" (§ 160.103).

(1) "Health plan" (§ 160.103).
(2) "Health care clearinghouse" (§ 160.103).

(a) Public or private entity that processes/facilitates processing of information in nonstandard format or containing nonstandard data content into standard data elements or standard transaction, or vice versa.
(b) Examples: billing service, repricing company, community health management information system, value added networks and switches who performs processing.
(c) "Format" and "data content" - data elements related to a "transaction" (§ 162.103).
(d) "Transaction" (§ 160.103).

(i) Transmission of information between two parties to perform financial or administrative activities related to health care.
(ii) Covered information transmission: health care claims/equivalent, health care payment and remittance advice, coordination of benefits, health care claim status, enrollment/disenrollment in health plan, eligibility for health plan, health plan premium payments, referral certification and authorization, first report of injury, health claims attachments, health care electronic funds transfers (EFT), other transactions Secretary of HHS may prescribe.

(e) "Standard transaction" – transaction complies with standard for that transaction adopted by Secretary of HHS (45 C.F.R Part 162 HIPAA Transactions Rule) (§ 162.103).

(3) "Health care provider" (§ 160.103).

(a) Institutional providers of services – e.g., hospital,
(b) Non-institutional providers of medical or health services – e.g., physicians, dentists, pharmacists; and
(c) Other person or organization who furnishes, bills or is paid for health care in normal course of business.
(d) Provider transmits health information electronically in connection with a transaction (financial or administrative activity related to health care governed by HIPAA).

- "Business associate" (§ 160.103).

(1) Person or organization who:

(a) On behalf of a covered entity, creates, receives, maintains PHI for function or activity regulated by HIPAA.
(b) Examples: claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, certain patient safety activities, billing, benefit management, practice management, repricing.

(2) Person or organization who:

(a) Provides certain services involving use or disclosure of PHI.
(b) Services limited to: legal, actuarial, accounting, consulting, data aggregation per § 164.501, management, administrative, accreditation, financial.

(3) Excludes member of covered entity's workforce.
(4) Covered entity may be business associate of another covered entity.

Permitted Disclosures of PHI

- Disclosures are discretionary, not mandatory.

- Disclosures to individuals who are subject of PHI other than when required for access or accounting of disclosures (§ 164.502).

- Disclosures for treatment, payment or health care operations (§§ 164.502, 164.506).

    (1) Covered entity's own treatment, payment or health care operations; or
    (2) Treatment activities of a health care provider; or
    (3) Payment activities of another covered entity or health care provider; or
    (4) Health care operations of another covered entity if:

        (a) Each covered entity has or had relationship to individual subject of PHI;
        (b) PHI pertains to the relationship; and
        (c) Disclosure is for competency or assurance activities, or for health care fraud and abuse detection or compliance.

    (5) Covered entity may obtain consent of individual unless authorization required under § 164.508 or another condition must be met.

- Disclosures incident to use or disclosure otherwise permitted or required (§§ 164.502, 164.514, 164.530).

- Disclosures pursuant to and in compliance with valid authorization (§§ 164.502, 164.508).

- Disclosures pursuant to individual's opportunity to agree or object (§§ 164.502, 164.510).

- Disclosures pursuant to public interest and benefit activities (§§ 164.502, 164.512).

  (1) Disclosures required by law (§§ 164.512 (a), 164.103).

      (a) Mandate contained in law compels use or disclosure of PHI and is enforceable in a court of law, e.g., statutes, regulations, court orders.
      (b) Disclosure complies with and limited to relevant requirements of law.

  (2) Disclosures to public health authority for public health activities (§§ 164.512 (b), 164.501).

      (a) Public health authority – authority/agency responsible for public health matters as part of official mandate and authorized by law:

          (i) To collect or receive PHI to prevent or control disease, injury, or disability, including conduct of public health surveillance, investigations and interventions; or
          (ii) To receive reports of child abuse or neglect.

      (b) Person subject to FDA re: FDA regulated products or activities for quality, safety

and effectiveness purposes, such as adverse event report, tracking of products, product recalls and post-marketing surveillance.

(c) Person who may have contracted or been exposed to a communicable disease when notification is authorized by law as part of a public health intervention or investigation.

(d) An employer, re: employee, requested by employer:

(i) For information concerning a work-related illness or injury or workplace related medical surveillance; and

(ii) Information needed by employer to comply with OSHA, Mine Safety Health Administration, or similar state law.

(3) Disclosures to health oversight agency for health oversight activities (§§ 164.512(d); 164.501).

(a) Health oversight agency/authority - authorized by law:

(i) To oversee public or private health care system, or

(ii) To oversee government programs in which health information is necessary to determine eligibility or compliance, or

(iii) To enforce civil rights laws for which health information is relevant.

(b) Legally authorized health oversight activities includes: audits; civil, administrative, or criminal investigations, proceedings or actions; inspections; licensure or disciplinary actions; other activities necessary for oversight of health care system, government benefit programs, or programs or entities for which health information necessary to determine compliance with civil rights laws.

(c) Excludes investigation /activity of individual that doesn't arise out of or directly related to:

(i) Receipt of health care; or
(ii) Claim for public benefits related to health care; or
(ii) Qualifications for, or receipt of, public benefits or services when individual's health integral to claim for public benefits or services.

(d) Joint activities or investigations are included if health oversight activity/investigation in conjunction with oversight activity or investigation related to claim for public benefits not related to health care.

(4) Disclosures in judicial and administrative proceedings (§ 164.512 (e)).

(a) In response to order of court or administrative tribunal and disclose only PHI expressly authorized by such order; or
(b) In response to subpoena, discovery request or other law process if:

(i) Receives satisfactory assurance that reasonable efforts are made to notify subject of PHI of request, or
(ii) Receives satisfactory assurance that reasonable efforts are made to secure a protective order.

(5) Disclosures to a law enforcement official for 6 law enforcement purposes (§§ 164.512(f), 164.103).

(a) Disclosures required by law and pursuant to process (164.512(f)(1).

(i) Required by statute; or
(ii) Pursuant to court order or court-ordered warrant, or subpoena or summons issued by a judicial officer; or
(iii) Grand jury subpoena; or
(iv) Administrative request, including administrative subpoena or summons, civil or authorized investigative demand or similar process, if:

(A) Information sought is relevant and material to a legitimate law enforcement inquiry,
(B) Request is specific and limited in scope to extent reasonably practical in light of purposes for which information is sought, and
(C) De-identified information could not reasonably be used.

(b) Identification and location of suspect, fugitive, material witness or missing person (§ 164.512(f)(2).

(i) Can only disclose name and address, date and place of birth, SSN, ABO blood type and rh factor, type of injury, date and time of treatment, date and time of death, and description of distinguishing physical characteristics.

(c) Requests for information about victims of crime other than child abuse victims or adult victims of abuse, neglect or domestic violence (§ 164.512(f)(3)).

(i) Victim agrees, or

(ii) Victim unable to agree because of incapacity or emergency and law enforcement official represents that:

(A) PHI not intended to be used against victim,
(B) Is needed to determine whether another person broke the law, and
(C) Investigation materially and adversely affected by waiting until victim can agree.

(iii) Covered entity believes disclosure is in best interest of individual.

(d) Disclosures about decedents to alert law enforcement to the deaths if covered entity suspects deaths resulted from criminal conduct (§ 164.512(f)(4)).

(e) Disclosures for crimes on premises and covered entity believes in good faith PHI is evidence of the crimes (§ 164.512(f)(5)).

(f) Disclosures to report crimes in an emergency (§ 164.512(f)(6)).

(i) Covered health care provider providing emergency health care in medical emergency not on premises.
(ii) Provider may disclose PHI to alert law enforcement official to:

(A) Commission and nature of crime;
(B) Location of crime or of victims; and
(C) The identity, description, and location of perpetrator of crime.

(6) Disclosures to avert serious threat to health and safety (§ 164.512(j)).

(a) Consistent with applicable law and standards of ethical conduct.
(b) Covered entity believes in good faith the disclosure of PHI necessary:

(i) To prevent or lessen serious and imminent threat to health or safety of a person or public, and disclosure made to person/persons reasonably able to prevent or lessen threat, or
(ii) For law enforcement authorities to identify or apprehend individual who appears to have escaped from correctional institution or other lawful custody or who covered entity reasonably believes may have caused serious physical harm to victim of violent crime.

Required Disclosures of PHI

- Individual has a right of access to own PHI (§ 164.524).

(1) Can inspect and obtain copy of PHI in designated record set.
(2) Exceptions:

(a) Psychotherapy notes;
(b) Information compiled in reasonable anticipation of, or for use in, civil, criminal, or administrative action or proceeding;
(c) PHI subject to Clinical Laboratory Improvement Amendments if access prohibited; and
(d) PHI exempt from Clinical Laboratory Act pursuant to 42 C.F.R.§ 493(a)(2).

(3) Covered entity may deny access, without individual's right to review of denial:

(a) Disclosure to inmate would jeopardize health, safety, security, custody or rehabilitation of an inmate or employee of correctional institution or responsible for transport; or
(b) Temporarily suspend right of access during research that include treatment if certain conditions met; or
(c) PHI obtained from someone other than health care provider under promise of confidentiality and access reasonably likely to reveal source of information.

(4) Denial of access, with individual's right to review of denial, if licensed health care provider determines, in exercise of professional judgment:

(a) Access reasonably likely to endanger life or physical safety of individual or other person, or
(b) PHI references another person and access reasonably likely to cause substantial harm to other person, or
(c) Request for access by personal representative and access reasonably likely to cause substantial harm to individual or other person.

(5) "Designated record set" (§ 164.501).

(a) Group of records maintained by or for a covered entity that is:

(i) Medical and billing records of covered health care provider; or
(ii) Enrollment, payment, claims adjudication, and case or medical management record systems of health plan; or
(iii) Used, in whole or in part, by or for covered entity to make decisions about individuals.

- Individual has right to accounting of disclosures of PHI (§ 164.528).

  (1) Right to accounting for 6 years prior to date on which request made.
  (2) Exceptions for disclosures:

    (a) To carry out treatment, payment, and health care operations (§ 164, 506); or
    (b) To individuals (§ 164.502); or
    (c) Incident to use or disclosure otherwise permitted or required (§ 164.502); or
    (d) Pursuant to authorization (§ 164.508); or
    (e) For facility's directory or persons involved in individual's care or other notification purposes (§ 164.510); or
    (f) National security or intelligence purposes (§ 164.512(k)); or
    (g) To correctional institutions or custodial law enforcement officials (§ 164.512(k)); or
    (h) As part of a limited data set (§ 164.514(e)); or
    (i) If occurred prior to HIPAA compliance date for covered entity.

  (3) Covered entity must temporarily suspend right to accounting for disclosures to health oversight agency or law enforcement official for time specified by agency or official.

    (a) Agency/official must provide written statement that accounting reasonably likely to impede agency's/official's activities and specify time for which suspension is required; or
    (b) If oral statement made, covered entity must:

      (i) Document statement, including identity of agency or official making the statement;

(ii) Temporarily suspend right to accounting; and
(iii) Limit temporary suspension to maximum of 30 days from date of oral statement unless written statement submitted during the 30 days.

- Disclosures to Secretary of HHS for HIPAA investigatory and compliance activities (§ 164.502, 45 C.F.R. Part 160, subpart C).

Minimum Necessary Rule

- When using, disclosing or requesting PHI, a covered entity must make reasonable efforts to limit PHI to minimum necessary to accomplish intended purpose, disclosure, or request (§ 164.502(b)).

- Does not apply to:

(1) Disclosures to or requests by a health care provider for treatment, or
(2) Uses or disclosures made to an individual, or
(3) Uses or disclosures made pursuant to an authorization (§ 164.508), or
(4) Disclosures made to Secretary of HHS for HIPAA investigatory and compliance activities, or
(5) Uses or disclosures that are required b law (§ 164.512 (a)), or
(6) Uses or disclosures required for covered entity to comply with HIPAA.

- Covered entity may reasonably rely on requested disclosure as minimum necessary when (§ 164.514(d)(3)):

(1) Making disclosures to public officials under § 164.512 if public official represents information requested is minimum necessary, or

(2) PHI is requested by another covered entity, or
(3) PHI requested by member of workforce or business associate of covered entity to provide professional services to covered entity if requestor represents that information requested is minimum necessary, or
(4) Documentation or representations that comply with applicable requirements of disclosure of PHI for research (§164.512(i)) provided by requestor of PHI.

- Covered entity may not use, disclose or request entire medical record except when entire medical record is specifically justified as amount reasonably necessary to accomplish purpose of use, disclosure, or request. (§ 164.514(d)(5)).

SHERRY L. GREEN
PRESIDENT
NATIONAL ALLIANCE FOR MODEL STATE DRUG LAWS (NAMSDL)

sgreen@namsdl.org
(505) 692-0457 (cell)

The successor to the President's Commission on Model State Drug Laws, NAMSDL is a 501(c)(3) non-profit corporation that was created in 1993. A non-partisan provider of legislative and policy services to local, state, and federal stakeholders, it is a resource for comprehensive and effective state drug and alcohol laws, policies, regulations, and programs and is funded by the United States Congress.

This project was supported by Grant No. G15599ONDCP03A, awarded by the Office of National Drug Control Policy to the National Alliance for Model State Drug Laws (NAMSDL). Points of view or opinions in this documents are those of the author and do not necessarily represent the official position or policies of the Office of National Drug Control Policy or the United States Government.