SERVING FAMILIES IN GEORGIA AND TENNESSEE
ELDER LAW
PRACTICE OF DAVID L. MCGUFFEY
Connecting Health, Wealth and Peace of Mind

David L. McGuffey, CELA*
Elder Law | Special Needs Law | Estate Planning
**Certified Elder Law Attorney by the National Elder Law Foundation*

HIPAA 2014

What You Need to Know

P.O. Box 2023, Dalton, Georgia 30722
Telephone (706) 428-0888 ▫ Toll Free (800) 241-8755 ▫ Fax (706) 395-4008
www.mcguffey.net

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA").[1]

HIPAA was adopted to ensure health insurance coverage after leaving an employer (Part I of the Act). HIPAA also provides standards for facilitating healthcare related electronic transactions (Part II of the Act). To improve the efficiency and effectiveness of the health-care system, HIPAA includes administrative simplification provisions requiring the Department of Health & Human Services ("HHS") to adopt national standards for electronic health-care transactions. When enacting these changes, Congress recognized that advances in electronic technology could erode the privacy of health information. Consequently, Congress mandated adoption of federal privacy protections for certain individually identifiable health information.[2] This paper focuses on the health privacy regulations.

The federal statute is enabling legislation; it is not the privacy rule. *See* 42 U.S.C. § 1320d et seq.[3] The HIPAA regulations are found in Title 45 of the Code of Federal Regulations, Parts 160, 162 and 164. Specifically, the privacy rule (also called the security rule) is found at 45 C.F.R. Part 164, Subpart E (§ 164.500 through 164.534). Security standards are at 164.302 through 164.318. Requirements relating to a covered entity's duty following improper use or disclosure of protected health information are at 45 C.F.R. 164.400 through 164.414.

HHS published a final Privacy Rule in December 2000, which was later modified in August 2002. This Rule set national standards for the protection of individually identifiable health information by three types of covered entities: health plans, health care clearinghouses, and health care providers who conduct the standard health care transactions electronically. Compliance with the Privacy Rule was required as of April 14, 2003 (April 14, 2004, for small health plans).

HHS published a final Security Rule in February 2003. This Rule sets national standards for protecting the confidentiality, integrity, and availability of electronic protected health information. Compliance with the Security Rule was required as of April 20, 2005 (April 20, 2006 for small health plans).[4]

General Privacy Rule.

A covered entity or business associate may not use or disclose protected health

---

1 Public Law 104-191.

2 The Privacy Rule establishes a Federal floor of safeguards to protect the confidentiality of medical information. http://www.hhs.gov/ocr/privacy/hipaa/faq/privacy_rule_general_topics/188.html.

3 Section 1320d-1 provides "The Secretary shall establish specifications for implementing each of the standards adopted under this part."

4 http://www.hhs.gov/ocr/privacy/hipaa/administrative/index.html.

information, except as permitted or required by Subpart E of the regulations (§ 164.500 through § 164.534) or by subpart C of part 160.[5] *See* 45 C.F.R. § 164.502(a).

The Privacy Rule:

- gives patients more control over their health information;
- sets boundaries on the use and release of health records;
- establishes appropriate safeguards that the majority of health-care providers and others must achieve to protect the privacy of health information;
- holds violators accountable with civil and criminal penalties that can be imposed if they violate patients' privacy rights;
- strikes a balance when public health responsibilities support disclosure of certain forms of data;
- enables patients to make informed choices based on how individual health information may be used;
- enables patients to find out how their information may be used and what disclosures of their information have been made;
- generally limits release of information to the minimum reasonably needed for the purpose of the disclosure;
- generally gives patients the right to obtain a copy of their own health records and request corrections; and
- empowers individuals to control certain uses and disclosures of their health information.

[5] Subpart C of Part 160 relates to compliance and enforcement by the Secretary.

The privacy rule applies uniformly to most protected health information. Psychotherapy notes are the primary exception.[6] If information relates to an individual's past, present or future physical or mental health condition or payment for treatment of the condition, and if it contains information that identifies or provides a reasonable basis for believing the individual could be identified, then the rule probably applies.

Definitions.

Defined terms appear throughout the privacy rule. The most important are:

Covered entity means (1) a health plan; (2) a health care clearinghouse; or (3) a health care provider who transmits any health information in electronic form in connection with a transaction covered by the HIPAA regulations. 45 C.F.R. § 160.102 and § 160.103. The HIPAA privacy rule applies to covered entities. 45 C.F.R. § 164.104(a); § 164.500(a). Compliance with the security standards has been required for covered entities since April 20, 2005. § 164.318(c).

[6] Psychotherapy notes, defined at 45 C.F.R. § 164.501, means notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. Psychotherapy notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: Diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

Business associates are those who use protect health information while providing services to covered entities. 45 C.F.R. § 160.103. A "business associate" is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. A member of the covered entity's workforce is not a business associate. A covered health care provider, health plan, or health care clearinghouse can be a business associate of another covered entity. The types of functions or activities that may make a person or entity a business associate include payment or health care operations activities, as well as other functions or activities regulated by the Administrative Simplification Rules.[7]

Protected health information means individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. The exceptions are education records covered by the Family Education Rights and Privacy Act, records regarding adult students and employment records held by the covered entity as employer. 45 C.F.R. 160.103. See also 45 C.F.R. § 164.105(a)(2)(i)(C).

Individually identifiable health information means information that (1) includes demographic information collected from an individual, (2) were created or received by a health care provider, health plan, employer or health care clearinghouse, and relate to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (3) identifies the individual or if there is a reasonable basis to believe the information can be used to identify the individual. 45 C.F.R. 160.103.

Designated record set means a group of records maintained by or for a covered entity that is: (i) The medical records and billing records about individuals maintained by or for a covered health care provider; (ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
(iii) Used, in whole or in part, by or for the covered entity to make decisions about individuals. Further, it includes any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity. 45 C.F.R. § 164.501.

Disclosure means the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information. 45 C.F.R. § 160.103.

Use means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information. 45 C.F.R. § 160.103.

---

[7] http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html.

Breach means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part [Sections 164.500 through 164.534] which compromises the security or privacy of the protected health information. 45 C.F.R. § 164.402.

Other defined terms include: ANSI, Compliance date, Electronic media, Electronic protected health information, Group health plan, Health care, Health care clearinghouse, Health care provider, Health information, Health insurance issuer, Health maintenance organization, Health plan, implementation specification, Organized health care arrangement, Person, Small health plan, Standard, Standard setting organization, State, Trading partner agreement, Transaction, and Workforce. *See* 45 C.F.R. § 160.103. Additional definitions are found at 45 C.F.R. § 164.103, § 164.304, 164.402 and § 164.501.

Relationship to State Law.

The federal rule pre-empts any State law relating to the privacy of individually identifiable health informations unless the State law is more stringent than a standard, requirement, or implementation specification adopted under the HIPAA regulations. 45 C.F.R. § 160.203(b).[8] The HIPAA regulations pre-empt any other contrary provision of State law unless HHS determines the provision of State law is necessary (1) to prevent fraud and abuse relating to the provision of or payment for health care; (2) to ensure appropriate State regulation of insurance and health plans; (3) for State reporting on health care delivery or costs; or (4) for purposes of serving a compelling need relating to public health, safety or welfare. Certain rules relating to controlled substances are also exempt. The process for requesting an exemption is found in 45 C.F.R. § 160.204.

Duties of Covered Entities.

Covered entities must: (1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits; (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information; (3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part; and (4) Ensure compliance with this subpart by its workforce. 45 C.F.R. § 164.306(a). They must implement policies and procedures to prevent, detect, contain and correct security violations. 45 C.F.R. § 164.308(a)(1)(i). This includes securing electronic information, password management, and sanctioning workforce members who violate the security standards.[9]

---

[8] Georgia law provides that no licensed physician is required to release medical information, except to public health authorities, unless required by law, statute or lawful regulation, or unless it is pursuant to a written authorization from the patient or the patient's health agent. O.C.G.A. § 24-12-1.

[9] A covered entity is not considered to have violated the privacy rule if a workforce member is a whistleblower, meaning there was a good faith basis for believing the covered entity engaged in unlawful conduct, violated a professional or clinical standard, or that care or treatment poses a danger if the disclosure is to a health oversight agency or to an attorney retained for the benefit of the workforce member. 45 C.F.R. § 502(j)(1). A similar exemption exists if a workforce member who is a

Workstations must be secure and users must have unique user names or numbers so users may be tracked. Electronic data must be encrypted. Document disposal and the disposal of electronic media must be secure. Procedures must be in place to authenticate electronic media to ensure it has not been altered or destroyed in an unauthorized manner. A covered entity that uses business associates must have a contract requiring that the business associate comply with HIPAA. § 164.314(a)(2)(i).

If security is breached, a covered entity must notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach. 45 C.F.R. § 164.404(a)(1). The notice must be in writing and must comply with § 164.404(c). If the breach involves more than 500 residents, then prominent media outlets serving the area must be notified. § 164.406(a). HHS must be notified of breaches, although breaches involving less than 500 residents are entered in a log and reported not less than 60 days after the end of each calendar year. § 164.408.

Right to File a Complaint.

A person who believes a covered entity is not complying with HIPAA may file a complaint with HHS. 45 C.F.R. § 160.306(a). Complaints must be in writing, must name the person who is the subject of the complaint, must and describe the acts or omissions believed to violate HIPAA, and be filed within 180 days of when the complainant knew or should have known the act or omission occurred. 45 C.F.R. § 160.306(b). Retaliation is prohibited. *See* 45 C.F.R. § 160.316. HHS maintains a website instructing individuals regarding how to file complaints.[10]

Security Risk Assessment.

Covered entities are required to conduct a risk assessment of their healthcare organization. 45 C.F.R. § 164.308. A risk assessment tool, released on March 28, 2014, is available at http://www.healthit.gov/providers-professionals/security-risk-assessment.

Civil Money Penalty.

HIPAA provides for a civil money penalty if HHS determines that a covered entity violated the regulations. 45 C.F.R. § 160.402. Violations include those committed by workforce member acting with the scope of their employment. Exceptions apply when a business associate violates the rule if the covered entity complies with regulations relating to business associates, the covered entity did not know about the activity and the covered entity did not fail to take required protective steps to prevent a violation. The minimum penalty ranges from $100 to $50,000 depending on whether the covered entity knew of the violation, whether there was willful neglect, or for a continuing violation after the entity knew or should have known to take corrective action. The maximum civil money penalty for identical violations is $1,500,000 per calendar year. 45 C.F.R. § 160.404. One of the factors considered

crime victim makes a report to law enforcement. 45 C.F.R. § 502(j)(2).

[10] http://www.hhs.gov/ocr/privacy/hipaa/complaints/.

in determining the penalty amount is how the covered entity responds to complaints. 45 C.F.R. § 160.408. HHS cannot impose a civil money penalty if the covered entity establishes an affirmative defense, which includes a showing that the violation was not due to willful neglect, and that the violation was corrected during the 30 day period beginning on the first date the covered entity knew or should have known. 45 C.F.R. § 160.410(b)(2)(ii).

Private Litigation.

There is no private cause of action under HIPAA. *Bradley v. Pfizer, Inc.*, 440 Fed. Appx. 805 (11th Cir. 2011); *Crawford v. City of Tampa*, 397 Fed. Appx. 621 (11th Cir. 2010); *Sneed v. Pan Am Hosp.*, 370 Fed. Appx. 47 (11th Cir. 2010) *Smith v. Daniels*, 2010 U.S. Dist. LEXIS 124736 (N.D. Ga 2010). *See also Dean v. New Orleans*, 544 Fed. Appx. 353 (5th Cir. 2013); *Regan v. United States Dep't of Veterans Affairs*, 518 Fed. Appx. 160 (4th Cir. 2013); *Stankovic v. Smith*, 2012 U.S. Dist. LEXIS 117339 (E.D.N.Y. 2012).

Depending on the circumstances, there may or may not be a cause of action under State law for violating a patient's right to privacy.

However, State law provides that any provider who in good faith releases copies of medical records in accordance with O.C.G.A. § 31-33-2 shall not have been found to have violated any criminal law or be civilly liable to a patient, the patient's estate or any other person. Further, even if there is a right to privacy, that right may be waived. *Canziani v. Visting Nurse Health Sys.*, 271 Ga. App. 677 (2005).[11]

Required Disclosures.[12]

A covered entity is required to disclose protected health information:

- To an individual, when requested under, and required by § 164.524 or § 164.528; and
- When required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the covered entity's compliance with this subchapter.

Permitted Uses and Disclosures.[13]

A covered entity is permitted to use or disclose protected health information as follows:

- To the individual;[14]

---

[11] In *Canziani*, a ptient claimed her right to privacy was violated by a visiting nurse's communication with a health insurance company. However, Canziani signed a patient agreement authorizing the nurse or any other nurse to care for her in her home and to communicate with her insurance company if necessary in order to receive proper payment. The Court found she could not maintain an action for invasion of privacy based on the very actions she authorized pursuant to her signed agreement.

[12] 45 C.F.R. § 164.502(a)(2).

[13] 45 C.F.R. § 164.502(a)(1).

[14] 45 C.F.R. § 164.502(a)(1)(i). Section 164.524(a) makes it clear that the individual has a right of access to inspect and obtain a copy of protected health information, except for psychotherapy notes, information developed for litigation and records subject to the Clinical Laboratory Improvements Act. *See also* O.C.G.A. § 31-33-2(a)(2) which requires release of a "complete and current copy" of the patient's record upon written request from the patient or the person authorized to have access to the patient's record under an advance directive for health care. Psychotherapy notes are treated

- For treatment, payment, or health care operations, as permitted by and in compliance with § 164.506;[15]
- Incident to a use or disclosure otherwise permitted or required by this subpart, provided that the covered entity has complied with the applicable requirements of §§ 164.502(b), 164.514(d), and 164.530(c) with respect to such otherwise permitted or required use or disclosure;
- Except for uses and disclosures prohibited under § 164.502(a)(5)(i),[16] pursuant to and in compliance with a valid authorization under § 164.508;
- Pursuant to an agreement under, or as otherwise permitted by, § 164.510; and
- As permitted by and in compliance with this section, § 164.512, § 164.514(e), (f), or (g).
- PHI may be used to create information that is not individually identifying information, or may share PHI with a business associate for the purpose of creating such information. § 164.502(d). If de-identified information meets the requirements of § 164.514, then the security rules does not apply.

Disclosures to Personal Representatives.[17]

A covered entity must, except as provided in paragraphs (g)(3)[18] and (g)(5)[19] of this section, treat a personal representative as the individual for purposes of this subchapter.[20]

- Implementation specification: adults and emancipated minors. If under applicable law a person has authority to act on behalf of an individual who is an adult or an emancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation.

---

differently from other mental health information both because they contain particularly sensitive information and because they are both the personal notes of the therapist that typically are not required or useful for treatment, payment or health care operations purposes other than by the mental health professional who created the notes. http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/mhguidancepdf.pdf.

[15] The terms treatment, payment and health care operations are defined in Section 164.501. Any consent given for treatment, payment or health care operations is not effective to permit use or disclosure that would require a different authorization under § 164.508. See 45 C.F.R. § 164.506(b)(2). The implantation specification for use in connection with treatment, payment or health care operations is found at 45 C.F.R. § 506(c).

[16] Prohibits use or disclosure of genetic information for underwriting purposes.

[17] 45 C.F.R. § 164.502(g).

[18] Subsection (g)(3) relates to unemancipated minors.

[19] Subsection (g)(5) provides that a covered entity may elect to not treat a person as a personal representative if there is a reasonable belief the person abused the patient or that doing so would endanger the patient.

[20] O.C.G.A. § 31-32-1, et.seq., the Georgia Advance Directive for Health Care Act, establishes a means for appointing a health agent who would be authorized to receive PHI. The statutory form is found at O.C.G.A. § 31-32-4, but variations are permitted. Other forms, such as Five Wishes and Critical Conditions, are acceptable so long as they include the required statutory elements. See also O.C.G.A. § 31-33-2(a)(2).

- Implementation specification: unemancipated minors. If under applicable law a parent, guardian, or other person acting in loco parentis has authority to act on behalf of an individual who is an unemancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation, except that such person may not be a personal representative of an unemancipated minor, and the minor has the authority to act as an individual, with respect to protected health information pertaining to a health care service, if:
    - The minor consents to such health care service; no other consent to such health care service is required by law, regardless of whether the consent of another person has also been obtained; and the minor has not requested that such person be treated as the personal representative; (B) The minor may lawfully obtain such health care service without the consent of a parent, guardian, or other person acting in loco parentis, and the minor, a court, or another person authorized by law consents to such health care service; or
    - A parent, guardian, or other person acting in loco parentis assents to an agreement of confidentiality
    - between a covered health care provider and the minor with respect to such health care service.
- Implementation specification: Deceased individuals. If under applicable law an executor, administrator, or other person has authority to act on behalf of a deceased individual or of the individual's estate, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation.[21]

Other Permitted Uses and Disclosures.

The HIPAA privacy rule is not absolute. It recognizes that certain disclosures are beneficial, such as those where information must be shared to ensure that a patient receives the best treatment.

Section 164.510 provides that a covered entity may use or disclose protected

[21] See 45 C.F.R. § 164.502(g)(4). 45 C.F.R. § 164.502(f) requires compliance with the privacy rule for 50 years following the death of an individual. The Georgia statute governing who has access to a deceased patient's records is found at O.C.G.A. § 31-33-3(a)(2)(A) through (D). In *Alvista Healthcare Ctr., Inc. v. Miller*, 296 Ga. App. 133 (2009), the Court held that a nursing home was obligated to release a decedent's medical records to a surviving spouse who was pursuing a wrongful death action because access to the records was authorized under O.C.G.A. § 31-33-2 and § 51-4-2.

health information, provided that the individual is informed in advance of the use or disclosure and has the opportunity to agree to or prohibit or restrict the use or disclosure, in accordance with the applicable requirements of this section. The covered entity may orally inform the individual of and obtain the individual's oral agreement or objection to a use or disclosure permitted by this section.

Directories.
Unless the individual objects, a covered entity may include limited information in a directory. Permitted information includes the individual's name, the individual's location in the provider's facility, the individual's condition described in general terms that do not communicate specific medical information; and the individual's religious affiliation. The information may be communicated to members of the clergy and to other persons who ask for the individual by name. Section 164.510(a)(1).

Persons involved in care.
A covered entity may disclose limited information to a person involved in the individual's care. The information disclosed must be directly related to that person's involvement with the individual's care or payment for care. A covered entity may also disclose information necessary to identify or notify a personal representative or other person responsible for the individual's care. If the patient is present and has capacity, the covered entity must obtain consent, provide the individual with an opportunity to object, or reasonably infer under the circumstances that the individual does not object. Section 164.510(b).[22] In situations where the patient is not present, lacks capacity, or if there is an emergency, the covered entity may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual and, if so, disclose only the protected health information that is directly relevant to the person's involvement with the individual's health care. 45 C.F.R. § 164.510(b)(3).

Errands for the Patient.
A covered entity may use professional judgment and its experience with common practice to make reasonable inferences of the individual's best interest in allowing a person to act on behalf of the individual to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of protected health information. Section 164.510(b)(3).

Abuse or Neglect.
A covered entity may disclose protected health information about an individual whom the covered entity reasonably believes to be a victim of abuse, neglect, or domestic violence to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect, or domestic violence. Section 154.512(c).

---

[22] The provider may ask the patient's permission to share relevant information with family members or others, may tell the patient he or she plans to discuss the information and give them an opportunity to agree or object, or may infer from the circumstances, using professional judgment, that the patient does not object. A common example of the latter would be situations in which a family member or friend is invited by the patient and present in the treatment room with the patient and the provider when a disclosure is made. http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/mhguidancepdf.pdf.

Judicial and administrative proceedings.
A covered entity may disclose protected health information in response to an order of a court or administrative tribunal, provided that it discloses only the protected health information expressly authorized by the order.[23] It may disclose protected health information in response to a subpoena, discovery request or other lawful process if the individual had notice and there was no objection, or if a qualified protective order has been entered. Section 164.512(e).[24]

Disclosure Pursuant to Authorization.

General rule. Except as otherwise permitted or required by Subpart E, a covered entity may not use or disclose protected health information without an authorization that is valid under section 164.508. When a covered entity obtains or receives a valid authorization for its use or disclosure of protected health information, its use or disclosure must be consistent with the authorization.[25]

Valid Authorizations – Core Elements. A valid authorization under section 164.508 must include the following elements:

- A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion.
- The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure.
- The name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure.
- A description of each purpose of the requested use or disclosure. The statement "at the request of the individual" is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose.
- An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. The statement "end of the research study," "none," or similar language is sufficient if the authorization is for a use or disclosure of protected health information for research, including for the creation and maintenance of a research database or research repository.
- Signature of the individual and date. If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must also be provided.

---

[23] In some instances judicial authorizations are sought by the parties. *See, e.g., Baker v. Wellstar Health Sys.*, 288 Ga. 336 (2010). In others, the law requires execution of an authorization under § 164.508. For example, in Georgia, a plaintiff in a medical malpractice case is required to give an authorization releasing medical information to the defense attorney. *See* O.C.G.A. § 9-11-9.2.

[24] A qualified protective order is one meeting the requirements of 45 C.F.R. § 164.512(e)(1)(v).

[25] 45 C.F.R. § 164.508(a)(1).

Required Statements. In addition to the core elements, an authorization must contain statements adequate to place the individual on notice of all of the following:

- The individual's right to revoke the authorization in writing, and either:
    - The exceptions to the right to revoke and a description of how the individual may revoke the authorization; or
    - To the extent that the information in paragraph (c)(2)(i)(A) of this section is included in the notice required by § 164.520, a reference to the covered entity's notice.
- The ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization, by stating either:
    - The covered entity may not condition treatment, payment, enrollment or eligibility for benefits on whether the individual signs the authorization when the prohibition on conditioning of authorizations in paragraph (b)(4) of this section applies; or
    - The consequences to the individual of a refusal to sign the authorization when, in accordance with paragraph (b)(4) of this section, the covered entity can condition treatment, enrollment in the health plan, or eligibility for benefits on failure to obtain such authorization.
- The potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient and no longer be protected by this subpart.

Plain Language. An authorization must be written in plain language.

Copy to the individual. If a covered entity seeks an authorization from an individual for a use or disclosure of protected health information, the covered entity must provide the individual with a copy of the signed authorization.

Certain Prohibited Uses and Disclosures.

A health plan shall not use genetic information for underwriting purposes. Covered entities and business associates may not sell protect health information. 45 C.F.R. § 164.502(a)(5).

If a covered entity is required to have a notice regarding its use and disclosure of PHI, then it may not use or disclosure PHI in a manner that is inconsistent with its notice. 45 § 164.502(i); § 164.520.

Minimum Necessary:

Where disclosure is made or requested, a covered entity or business associate must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. 45 C.F.R. § 164.502(b)(1).

Limits on Minimum Necessary Rule:

The minimum necessary rule does not apply to:

- Disclosures to or requests by a health care provider for treatment;
- Uses or disclosures made to the individual, as permitted under paragraph (a)(1)(i) of this section or as required by paragraph (a)(2)(i) of this section;
- Uses or disclosures made pursuant to an authorization under § 164.508;
- Disclosures made to the Secretary in accordance with subpart C of part 160 of this subchapter;
- Uses or disclosures that are required by law, as described by § 164.512(a); and
- Uses or disclosures that are required for compliance with applicable requirements of this subchapter.

Restrictions and Confidential Communications.

Individuals may request that use or disclosure of his or her PHI be restricted. 45 C.F.R. § 164.522(a)(1)(i). A covered entity is not required to agree to a restriction, but if it agrees, then use or disclosure that violates the restriction is not permitted unless disclosure is required in connection with emergency treatment. Any agreed upon restriction must be documented in accordance with § 164.530(j).

Covered entities must accommodate reasonable requests to receive PHI by alternative means or at alternative locations. Health plans must make similar accommodations if disclosure would endanger the individual. 45 C.F.R. § 164.22(b)(1); § 164.502(h). A covered entity may require that the request be in writing, that payment be made, specification of the alternative address or other method of contact. The covered entity may not require an explanation regarding the basis for providing communications on a confidential basis.

Correcting Medical Records.

General Rule. Section 164.526(a)(1) provides that an individual has the right to have a covered entity amend protected health information or a record about the individual in a designated record set for as long as the protected health information is maintained in the designated record set.

A covered entity may deny an individual's request for amendment, if it determines that the protected health information or record that is the subject of the request:

- Was not created by the covered entity, unless the individual provides a reasonable basis to believe that the originator of protected health information is no longer available to act on the requested amendment;
- Is not part of the designated record set;
- Would not be available for inspection under § 164.524;[26] or

[26] The general rule under 45 C.F.R. § 164.524 is that an individual has a right of access to inspect and copy protected health information about the individual in a designated record set for as long as it is maintained in the designated record set. Exceptions include (1) psychotherapy notes; (2) information compiled in reasonable anticipation of, or for use in, civil, criminal or administrative actions and proceedings; and (3) information subject to the Clinical Laboratory

- Is accurate and complete.

The covered entity must permit an individual to request that the covered entity amend the protected health information. The covered entity may require that the request for an amendment be in writing and provide a reason to support the requested amendment if it informs individuals in advance of the requirement.

The covered entity must take timely action, which means in most cases it must act within 60 days.

If the covered entity grants the request for an amendment, then it must take the following action:

- Making the amendment. The covered entity must make the appropriate amendment to the protected health information or record that is the subject of the request for amendment by, at a minimum, identifying the records in the designated record set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment.
- Informing the individual. In accordance with paragraph (b) of this section, the covered entity must timely inform the individual that the amendment is accepted and obtain the individual's identification of and agreement to have the covered entity notify the relevant persons with which the amendment needs to be shared in accordance with paragraph (c)(3) of this section.
- Informing others. The covered entity must make reasonable efforts to inform and provide the amendment within a reasonable time to:
    - Persons identified by the individual as having received protected health information about the individual and needing the amendment; and
    - Persons, including business associates, that the covered entity knows have the protected health information that is the subject of the amendment and that may have relied, or could foreseeably rely, on such information to the detriment of the individual.

If the covered entity denies the request, then it must provide the individual with a written denial in accordance with the following:

- Denial. The covered entity must provide the individual with a timely, written denial, in accordance with paragraph (b)(2) of this section. The denial must use plain language and contain:
    - The basis for the denial, in accordance with paragraph (a)(2) of this section;
    - The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement;
    - A statement that, if the individual does not submit

Improvements Act if that Act would prohibit disclosure.

a statement of disagreement, the individual may request that the covered entity provide the individual's request for amendment and the denial with any future disclosures of the protected health information that is the subject of the amendment; and

- A description of how the individual may complain to the covered entity pursuant to the complaint procedures established in § 164.530(d) or to the Secretary pursuant to the procedures established in § 160.306. The description must include the name, or title, and telephone number of the contact person or office designated in § 164.530(a)(1)(ii).

- Statement of disagreement. The covered entity must permit the individual to submit to the covered entity a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement. The covered entity may reasonably limit the length of a statement of disagreement.
- Rebuttal statement. The covered entity may prepare a written rebuttal to the individual's statement of disagreement. Whenever such a rebuttal is prepared, the covered entity must provide a copy to the individual who submitted the statement of disagreement.
- Recordkeeping. The covered entity must, as appropriate, identify the record or protected health information in the designated record set that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment, the covered entity's denial of the request, the individual's statement of disagreement, if any, and the covered entity's rebuttal, if any, to the designated record set.
- Future disclosures.
  - If a statement of disagreement has been submitted by the individual, the covered entity must include the material appended in accordance with paragraph (d)(4) of this section, or, at the election of the covered entity, an accurate summary of any such information, with any subsequent disclosure of the protected health information to which the disagreement relates.
  - If the individual has not submitted a written statement of disagreement, the covered entity must include the individual's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of the protected health information only if the individual has requested such action in accordance

with paragraph (d)(1)(iii) of this section.

- When a subsequent disclosure described in paragraph (d)(5)(i) or (ii) of this section is made using a standard transaction under part 162 of this subchapter that does not permit the additional material to be included with the disclosure, the covered entity may separately transmit the material required by paragraph (d)(5)(i) or (ii) of this section, as applicable, to the recipient of the standard transaction.

Conclusion

HIPAA creates a federal floor regarding the privacy of individually identifiable health information. It requires covered entities to safeguard PHI and limit access to PHI to uses and disclosures permitted under the HIPAA regulations. However, HIPAA's privacy rule is not absolute. When information is released, frequently decisions regarding its release are guided by the best interests of the patient.