SHOULD WE FEAR HIPAA UPON US?

Steven C. Laird
Law Offices of Steven C. Laird, P.C.
2400 Scott Avenue
Fort Worth, Texas 76103-2245
817-531-3000
1-800-448-2889

> Whatsoever, in connection with my professional service, or not in connection with it, I see or hear, in the life of men, which ought not to be spoken of abroad, I will not divulge, as reckoning that all such should be kept secret.
>
> Hippocratic Oath, circa 4th century B.C.

Confidentiality in connection with medical care is nothing new. What is new is the federal government's attempt to regulate health care providers' release, protection and security of confidential health information. The amount of written paperwork in medicine is staggering. Medical records are used by many different entities besides the health care providers giving treatment, including: insurance companies; billing services; marketers; medical information bureaus; employers who are self-insured; government agencies; and research facilities. Secondary users of health information include: drug marketers; public assistance programs; law enforcement agencies; courts and private database companies such as the Medical Information Bureau. [1] A sample of entities reviewing confidential patient information is included in Appendix "A".[2]

Privacy issues in health care are obvious. Because there was no national standard regarding patient privacy, the federal government believed that national privacy rules were needed. This need was heightened due to the rise in managed care, computer technology, increased demand for health information, commercial use of health data and concerns raised by the mapping of the human genome.[3]

The authors wish to acknowledge Bill Waites for his assistance in the initial preparation of this paper. Bill Waites, CompuPak Advanced Technology, 6336 Juneau Road, Fort Worth, Texas 76116. (817) 738-3729. Mr. Waites is a management consultant who provides services as an expert witness in technology and commercial transactions, business processes and HIPAA training, policies and procedures.

What is HIPAA?

[1] *Introduction to Health Privacy*, Health Privacy Project, July 2001, Institute for Health Care Research and Policy, Georgetown University, at http://www.healthprivacy.org.html. (last visited 8-18-03).
[2] Appendix "A", *Flow of Patient Health Information Inside and Outside the Healthcare Industry*, American Health Information Management Association (AHIMA), 2003, Accessed online at http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_018217.pdf is Reprinted with permission from the American Health Information Management Assocation.
[3] *Introduction to Health Privacy*, Health Privacy Project, July 2001, Institute for Health Care Research and Policy, Georgetown University, at http://www.healthprivacy.org.html (last visited 8-18-03).

HIPAA stands for the Health Insurance Portability and Accountability Act of 1996, Public Law 104-91. This law was created by the U.S. Department of Health and Human Services by permission of the United States Congress to address issues of medical privacy. Prior to the enactment of HIPAA, it was believed by Congress that the patchwork of laws in place were not adequate to protect ongoing privacy concerns in medical records, especially in light of the rapid rise of electronic formats for medical records. The HIPAA rules provide a new nationwide minimum standard for medical privacy and was enacted on August 21, 1996.

The deadline to comply with the new Privacy Rule was April 14, 2003 for the majority of covered entities, which includes health plans, health-care clearinghouses and healthcare providers who transmit health information in electronic form in connection with certain transactions.[4 & 5] In practical terms, almost all hospitals and physicians will be subject to the new HIPAA privacy requirements as just about all hospitals and physicians now use electronic methods for billing, enrollment and eligibility verification purposes. Additionally, the new privacy rules set up restrictions on covered entities (such as pharmacies) using patient information for marketing purposes without the patient's specific authorization.[6 & 7]

Tommy G. Thompson, the Secretary of the U.S. Department of Health and Human Services has stated, "The new protections give patients greater access to their own medical records and more control over how their personal information is used by their health plans and health care providers. Consumers will get a notice explaining how their health plans, doctors, pharmacies and other health care providers use, disclose and protect their personal information. In addition, consumers will have the ability to see and copy their health records and to request corrections of any errors included in their records. Consumers may file complaints about privacy issues with their health plans or providers or with our Office for Civil Rights." [8]

---

[4] *HIPAA Privacy Rule and Public Health—Guidance from CDC and the U.S. Dept. of Health and Human Services*, 52 MMWR Early Release – Apr. 11, 2003, at p.2.

[5] Certain small health plans have until April 14, 2004 to comply.

[6] *Fact Sheet*, U.S. Dept. of Health & Human Services, 2, Apr. 14, 2003 available at http://www.hhs.gov/news/facts/privacy.html. (last visited 8-1-03).

[7] SB 1136 states what is a covered entity under Texas law and mirrors the HIPAA language so that anyone who is a covered entity under HIPAA is also a covered entity under Texas law. *See*, S.B. 1136, 2003 Leg., 78th Sess. (Tex. 2003), which amends Tex. Health & Safety Code, §181.001, subsection (b)(2) regarding who is a "covered entity" for Access to Certain Private Health Information, as follows:

(2)"Covered entity" means any person who:

(A) for commercial, financial, or professional gain, monetary fees, or dues, or on a cooperative, nonprofit, or pro bono basis, engages, in whole or in part, and with real or constructive knowledge, in the practice of assembling, collecting, analyzing, using, evaluating, storing, or transmitting protected health information. The term includes a business associate, health care payer, governmental unit, information or computer management entity, school, health researcher, health care facility, clinic, health care provider, or person who maintains an Internet site;

(B) comes into possession of protected health information;

(C) obtains or stores protected health information under this chapter; or

(D) is an employee, agent, or contractor of a person described by Paragraph (A), (B), or (C) insofar as the employee, agent, or contractor creates, receives, obtains, maintains, uses, or transmits protected health information.

[8] News Release, Statement by Tommy G. Thompson, U.S. Dept. of Health & Human Services on Fri. Apr. 11, 2003, at www.hhs.gov/news/press/2003pres/20030411/html. (last visited 8-1-03).

Who is Covered by the Privacy Rule:

1. Health Plans
    a. Includes health, dental, vision, prescription drug insurers, HMOs, Medicare, Medicaid, Medicare+Choice, Medicare supplement insurers, long-term care insurers
2. Health Care Providers
    a. Every health care provider, regardless of size, who electronically transfers health information in connection with certain transactions is covered under this Act.[9]
3. Health Care Clearinghouses
    a. Ex: billing services, community health information systems

What is Covered by the Privacy Rule:

"The Privacy Rule protects all *"individually identifiable health information"* held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper or oral. The Privacy Rule calls this information "*protected health information (PHI).*" [10]

"Individually identifiable health information" is information, including demographic data that relates to:

a. the patient's past, present, or future physical or mental health or condition,
b. the provision of health care to the individual or
c. the past, present or future payment for the provision of health care to the individual,[11]

and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual (i.e. name, address, birth date, Social Security Number). See 45 C.F.R. §160.103 (Exhibit G).

De-identified Health Information can be used without restrictions.[12]

---

[9] For all intents and purposes, most health care providers are covered by HIPAA. If a provider and/or its billing agent only operates on a paper basis and does not submit insurance claims electronically, then that provider would not be subject to HIPAA.

[10] *Summary of The HIPAA Privacy Rule*, *OCR Privacy Brief*, U.S. Dept. of HHS, 3, (Last revised 05/03) available at http://www.hhs.gov/ocr/privacysummary.pdf.html. (last visited 8-20-03) at 3, & 45 C.F.R. §160.103 (Exhibit G).

[11] *Summary of The HIPAA Privacy Rule*, *OCR Privacy Brief*, U.S. Dept. of HHS, (Last revised 05/03) available at http://www.hhs.gov/ocr/privacysummary.pdf.html. (last visited 8-20-03) at 4.

[12] 45 C.F.R. §164.514(b). De-identified information can be accomplished by removing certain identifying information of the patient, the patient's relatives/employers/household members. Included in the categories to de-identify include removing: all geographic subdivisions smaller than a State, all dates except for years directly related to the individual (including birth date, admission/discharge date & date of death). Fax numbers, e-mail addresses, medical record numbers, telephone numbers, health plan beneficiary numbers, account numbers, social security numbers, vehicle identifiers and serial numbers, license plate numbers, Internet Protocol (IP) numbers, Biometric identifiers including finger and voice prints, full face photographic images, and any other unique identifying number, characteristic or code. The covered entity

What is NOT Covered Under the Privacy Rule:

An individual's authorization is NOT required to:

1. Disclose protected health information to the patient
2. To treat a patient
3. For payment for services given to the patient
4. For health care operations (ex: quality assessment, medical reviews, legal services, underwriting risk)
5. If information is provided to a non-covered entity. Ex: a health assessment survey for the Red Cross filled out by the patient, as part of donating blood would not be protected as the Red Cross is not a covered entity.[13]

Treatment of a patient has been defined as "..the provision, coordination, or management of health care related services for an individual by one or more health care providers, including consultation between providers regarding a patient and referral of a patient by one provider to another."[14]

Under the Act there is no particular form for obtaining consent for disclosure of information for treatment, payment and health care operations. [15] However, the act does have certain implementation criteria that must be included.

Physicians do not need a patient's written authorization to send a copy of the patient's medical records to another provider who is treating the patient.[16]

General Principles for Use and Disclosure under Privacy Rule:

1. The individual who is the subject of the information or the individual's personal representative may permit the release of the information and must do so in writing
2. As the Privacy Rule permits or requires 45 C.F.R §164.502(a)

What Do The Covered Entities Now Have to Do Under HIPAA?[17]

---

may not have actual knowledge that the remaining information could be used alone or in combination with any other information to identify an individual who is subject of the information.

[13] *Summary of HIPAA Privacy Rule*, at p. 6, Health Privacy Project, Sept. 13, 2002, Institute for Health Care Research and Policy, Georgetown University, available at http://www.healthprivacy.org./usr_doc/RegSummary02.pdf.html. (last visited 8-18-03).

[14] 45 C.F.R. §164.501.

[15] *Summary of The HIPAA Privacy Rule*, *OCR Privacy Brief*, U.S. Dept. of HHS, (Last revised 05/03) available at http://www.hhs.gov/ocr/privacysummary.pdf.html. (Last visited 8-20-03) at p. 5.

[16] *Your Frequently Asked Questions On Privacy*, U.S. Dept. of Health & Human Services, Answer ID 271, Updated 7-18-2003, available at http://www.hhs.gov/ocr/hipaa/html. (last visited 8-18-03). *See also*, 45 C.F.R. § 164.506 and definition of "treatment" at 45 C.F.R. §164.501.

[17] F*act Sheet*, U.S. Dept. of Health & Human Services, Apr. 14, 2003 at p.3 available at http://www.hhs.gov/news/facts/privacy.html (last visited 8-1-03).

1. The covered entities must have written policies and procedures to protect the confidentiality of their patients' protected health information.
2. There must be a written description of the staff that has access to the protected information, on how it will be used and when it may be disclosed. There must be documentation that describes what data can be accessed by each staff member, how it will be used and how it may be disclosed.
3. Business Associates of the covered entities must agree to the same limitations on the use and disclosure of the information.[18]
4. Covered entities must train their employees in their privacy procedures and designate an individual to be a Privacy Officer to ensure the procedures are followed. If covered entities learn an employee failed to follow these procedures, then they must take appropriate disciplinary action.
5. Private sector and government facilities/entities must comply with these requirements.

Some of the New Policies that Covered Health Care Organizations May Adopt

[18] Arguably, attorneys and their experts may be considered business associates when they receive protected health information in performance of legal services in medical malpractice cases. Under the Privacy Rule, §160.103, (Exhibit G) 164.502(e) (Exhibit H), 164.504(e)(Exhibit I) , and 164.532 (d) & (e) (Exhibit J), deal with a "business associate."

A "business associate" is a person who:

a. On behalf of a covered entity performs or assists in the performance of a function or activity involving the use or disclosure of individually identifiable health information, such as claims processing or administration, data analysis, utilization review, quality assurance, billing practice management; or

b. Provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for a covered entity.

Written contracts which require the business associate not to use or disclose the information other than what is permitted or required by the contract is the usual safeguard utilized with business associates to protect protected health information. The contract must also provide that the business associate will:

1. Report to the covered entity any known inappropriate use or disclosure;
2. Ensure that any agents (such as a subcontractor) agrees to the same restrictions on the covered information;
3. Make available protected health information in its possession for inspection, copying, and amendment;
4. Incorporate any amendments forwarded by the covered entity;
5. Make available information required to provide an accounting of disclosures;
6. Make its relevant books relating to the uses and disclosures of protected health information available to the Secretary for compliance oversight; and
7. Return or destroy all protected health information received from, or created or received on behalf of the covered entity at the termination of the contract, if feasible.

The new Privacy Rules do not set out specific administrative, technical and physical safeguards that a health care provider must adopt.[19] Some of the policies organizations may adopt include[20]:

- Use of a cover sheet with a confidentiality statement when faxing
- Process for verification of fax numbers before faxing
- Leaving no patient messages on answering machines or with family members
- Leaving messages asking for patients to return phone calls
- Restricting the posting of patient information on white boards/other boards that may be seen by visitors
- Restrictions for overhead pages
- Limiting vendor access and requiring vendors to sign confidentiality agreements
- Shredding of all papers with identifiable information
- Developing a secure method of transporting documents
- Securing computer identification
- Enabling automatic logouts on computers

Information that May Be Disclosed Without Patient Consent for Public Health Activities to a Public Health Authority[21 & 22]:

- Reporting of disease, injury, and vital events (e.g. birth, or death)
- Conducting public health surveillance, investigations and interventions.
- Report child abuse or neglect to a public health or other government authority legally authorized to receive such reports
- A person subject to jurisdiction of the Food and Drug Administration (FDA) concerning the quality, safety, or effectiveness of an FDA-related product or activity for which that person has responsibility
- A person who may have been exposed to a communicable disease or may be at risk for contracting or spreading a disease or condition, when legally authorized to notify the person as necessary to conduct a public health intervention or investigation

An individual's employer, under certain circumstances and conditions, as needed for the employer to meet the requirements of the Occupational Safety and Health Administration, Mine Safety and Health Administration, or a similar state law.

HOW TO GET THE MEDICAL INFORMATION

[19] Candace Grey, *Understanding and Complying With* HIPAA, 18 J. of PeriAnesthesia Nursing 3, 182-185, June 2003, at 183.
[20] *Id.*
[21] Or to an entity working under a grant of authority from a public health authority, or when directed by a public health authority, to a foreign government agency that is acting in collaboration with a public health authority.
[22] Adapted from 45 C.F.R. §164.512(b).

Obtaining Medical Records Under HIPAA:

a. Patients Obtaining Their Own Records – §164.524 (Exhibit M)

- Covered entities should provide copies of the requested records within 30 days. (The covered entity has 60 days to comply if the records are off-site. In addition, the covered entity may also have 30 day extension if they provide a written statement of the reasons for the delay and the date by which they will provide the requested records.)
- Charges may be made to the patient for reasonable copying and sending of the records.
- A health care provider should provide each patient with a Notice on their first visit after April 14, 2003 and the patient may restrict the use or disclosure of their information beyond that in the notice, but the covered entities do NOT have to agree to those changes.[23]
- A patient may have grounds to file a complaint with OCR when the covered entity does not provide complete access to the patient's medical records, refuses to make requested corrections to the medical chart or there was marketing information using the patient's health information without first obtaining the patient's consent.[24]
- Patients may inspect and/or copy their records.
- A patient may have their right to inspect or copy denied if:
    - A patient requests his or her own psychotherapy notes
    - When information has been compiled in reasonable anticipation of a legal proceeding (civil, criminal or administrative)
    - When certain information is in the possession of a clinical laboratory and is exempt from disclosure
    - When information pertains to an inmate
    - When information is obtained during research and the patient has agreed to the denial of access or
    - When information was obtained under a promise of confidentiality from someone other than a provider and access would likely reveal its source.[25]

A patient may have their denial to inspect or copy his/her records reviewed when:

- When a health care professional determines that inspection and copying requested is "reasonably likely" to endanger the safety of the patient or another;
- If the patient wants information about another person and a health care professional determines that inspection and copying is reasonably likely to cause substantial harm to the other person; or

[23] *Fact Sheet*, U.S. Dept. of Health & Human Services, 2, Apr. 14, 2003 available at http://www.hhs.gov/news/facts/privacy.html. (last visited 8-1-03).
[24] *Your Frequently Asked Questions On Privacy*, U.S. Dept. of Health & Human Services, Answer ID 348, Updated 7-18-2003, available at http://www.hhs.gov/ocr/hipaa/html. (last visited 8-18-03).
[25] Hugh Barton, *Health Information and Patient Rights Under HIPAA*, 65 Tex. B.J. 824, 826 (Oct. 2002).

- The patient's personal representative requests information and the provider determines that inspection and copying requested is "reasonably likely" to endanger the safety of the patient or another."[26]

Medical Information Board

A patient has the right to obtain a copy of any Medical Information Board (MIB) record compilation. MIB is an organization of over 500 insurance companies that may have medical information on an individual, including information concerning serious health conditions or other factors that could affect longevity, i.e. an affinity for a dangerous sport. If MIB has a file on a person, that person has a right to see and correct the file. To obtain a copy of a file, contact MIB Inc., P.O. Box 105, Essex Station, Boston, MA. 02112, Telephone: (617) 426-3660, http://www.mib.com. See Appendix "B" for the MIB Request for Record Search & Disclosure of MIB Record Information for Residents of the United States of America.

b. Attorneys Obtaining Copies of Patient Records

- An attorney must present an authorization that complies with HIPAA in order to obtain medical records.

c. Subpoena or Discovery Request

- HIPAA requires that the covered provider receive "satisfactory assurance" from the requesting party (i.e. attorney) that they have complied with HIPAA . This would entail notifying the patient (or the patient's attorney if the patient is represented by counsel) that the records have been requested or securing a qualified protective order. In a qualified protective order the order must set out the following:
    a. The parties will not use or disclose the medical records for any purpose other than litigation or the proceeding for which the information was requested.
    b. The parties will destroy or return to the health care provider the medical records and all copies made at the end of the litigation or proceeding.[27]

d. Court Order

- Medical records may be disclosed pursuant to a signed court order. The court order should expressly set out what information may be released.[28]

Amendment of Records – 45 C.F.R. §164.526 (Exhibit K)

[26] Hugh Barton, *Health Information and Patient Rights Under HIPAA*, 65 Tex. B.J. 824, 826 (Oct. 2002). 45 C.F.R. §164.524.
[27] Maxine Harrington, *Obtaining Medical Records Under HIPAA In Judicial or Administrative Proceedings*, TCBA Bulletin (August 2003) at 8.
[28] *Id.*

Under HIPAA, a patient has the right to supplement or amend their own protected health information. Once a covered health care entity receives a patient's request to amend the medical record, the covered entity has 60 days to act on the request. The deadline may be extended 30 days if the health care provider provides a written statement to the patient with the reasons for the delay and the date by which the covered entity will fulfill the request. [For example, a patient can request that a second opinion report be placed in his/her record.]

If the covered entity agrees to amend the records then:

1. The covered entity must make the amendment;
2. Inform the patient in a timely fashion that the amendment was accepted and
3. Provide the amendment to entities identified by the patient and other entities known by the provider to have received the erroneous information.

When can a covered entity DENY the request to amend the records?

1. When the information was not created by the covered entity, unless the originator of the protected health information is no longer available to make the amendment; or
2. It is not part of the designated record; or
3. It would not be available for inspection; or
4. The record is accurate and complete.

What happens when the covered entity refuses to amend the records?

1. The covered entity must give the patient a timely written denial with the basis for the denial; the patient's right to submit a written statement disagreeing with the denial and how to exercise that right; a statement that the patient can request the covered entity to include the patient's request and denial in future disclosures of the patient's records (if the patient does not file a statement of disagreement); and a description of how the patient can file a complaint with the covered entity or the Secretary of Health and Human Services.
2. If the patient files a statement of disagreement, the covered entity may file a rebuttal and must provide a copy of the rebuttal to the patient.
3. The request for amendment, the denial, the statement of disagreement by the patient (if submitted) and any rebuttal, or a summary or such information must be provided with any subsequent disclosures of the protected health information.

Answers from the United States Department of Health and Human Services to Medical Records Questions:

- **May a health care provider disclose parts of a medical record that were created by another provider?**

"Answer:

Yes, the Privacy Rule permits a provider who is a covered entity to disclose a complete medical record including portions that were created by another provider, assuming that the disclosure is for a purpose permitted by the Privacy Rule, such as treatment."[29]

- **Can a patient obtain a copy of their entire medical record?**

Answer:

Yes[30] A case-by-case justification is not needed for disclosing the medical record to the individual who is the subject of the protected health information.

- **Does the HIPAA Privacy Rule allow parents the right to see their children's medical records?**

"Answer:

Yes, the Privacy Rule generally allows a parent to have access to the medical records about his or her child, as his or her minor child's personal representative when such access is not inconsistent with State of other law.

There are three situations when the parent would not be the minor's personal representative under the Privacy Rule. These exceptions are when the minor is the one who consents to care and the consent of the parent is not required under State or other applicable law; (2) then the minor obtains care at the direction of a court or a person appointed by a court; and (3) when, and to the extent that, the parent agrees that the minor and the health care provider may have a confidential relationship. However, even in these exceptional situations, the parent may have access to the medical records of the minor related to this treatment when State or other applicable law requires or permits such parental access. Parental access would be denied when State or other law prohibits such access. If State or other applicable law is silent on a parent's right of access in these cases the licensed health care provider may exercise his or her professional judgment to the extent allowed by law to grant or deny parental access to the minor's medical information.

Finally, as is the case with respect to all personal representatives under the Privacy Rule, a provider may choose not to treat a parent as a personal representative when the provider reasonably believes, in his or her professional

[29] *Your Frequently Asked Questions On Privacy*, U.S. Dept. of Health & Human Services, Answer ID 214, Updated 7-18-2003, available at http://www.hhs.gov/ocr/hipaa/html. (last visited 8-18-03)
[30] *Your Frequently Asked Questions On Privacy*, U.S. Dept. of Health & Human Services, Answer ID 213, Updated 7-18-2003, available at http://www.hhs.gov/ocr/hipaa/html. (last visited 8-18-03).

judgment, that the child has been or may be subjected to domestic violence, abuse or neglect, or that treating the parent as the child's personal representative could endanger the child."[31]

- **Can a person access someone's medical record if they have that person's health care power of attorney?**

Answer:

"Yes, an individual that has been given a health care power of attorney have the right to access the medical records of the individual related to such representation to the extent permitted by the HIPAA Privacy Rule 45 CFR 164.524. However, when a physician or other covered entity reasonably believes that an individual, including an unemancipated minor has been or may be subjected to domestic violence, abuse or neglect by the personal representative, or that treating a person as an individual's personal representative could endanger the individual, the covered entity may choose not to treat that person as the individual's personal representative, if in the exercise of professional judgment, doing so would not be in the best interests of the individual."[32]

- **Under HIPAA what costs can the patient be charged for getting a copy of their records?**

Answer:

The Privacy Rule allows a patient to pay a reasonable cost for obtaining a copy of their records. This fee may include only the copying cost (including supplies and labor) and postage if the records are mailed. The fee may not include costs associated with searching for and retrieving the requested information.[33]

- **Can an adult or emancipated minor's personal representative access that person's medical record?**

Answer:

"The HIPAA Privacy Rule treats an adult or emancipated minor's personal representative as the individual of purposes of the Rule regarding the health care matters that relate to the representation, including the right access under 45 C.F.R. 164.524. The scope of the access will depend on the authority granted to the personal representative by other law. If the personal representative is authorized to make health care decisions, generally, then the personal representative may have access to the individual's protected health information regarding health care in general. On the other hand, if the authority is limited, the personal representative may have access only to protected health information that may be

---

[31] *Your Frequently Asked Questions On Privacy*, U.S. Dept. of Health & Human Services, Answer ID 227, Updated 7-18-2003, available at http://www.hhs.gov/ocr/hipaa/html. (last visited 8-18-03).

[32] *Your Frequently Asked Questions On Privacy*, U.S. Dept. of Health & Human Services, Answer ID 220, Updated 7-18-2003, available at http://www.hhs.gov/ocr/hipaa/html. (last visited 8-18-03).

[33] *Your Frequently Asked Questions On Privacy*, U.S. Dept. of Health & Human Services, Answer ID 353, Updated 7-18-2003, available at http://www.hhs.gov/ocr/hipaa/html. (last visited 8-18-03). *See also*, 45 C.F.R. §164.524.

relevant to making decisions within the personal representative's authority. For example, if a personal representative's authority is limited to authorization for artificial life support, then the personal representative's access to protected health information is limited to that information which may be relevant to decisions about artificial life support.

There is an exception to the general rule that a covered entity must treat an adult or emancipated minor's personal representative as the individual. Specifically, the Privacy Rules does not require a covered entity to treat a personal representative as the individual, if, in the exercise of professional judgment, it believes doing so would not be in the best interest of the individual because of a reasonable belief that the individual has been or may be subject to domestic violence, abuse or neglect by the personal representative, or that doing so would otherwise endanger the individual. This exception applies to adults both emancipated and unemancipated minors who may be subject to abuse or neglect by their personal representative."[34]

- **Does the HIPAA Privacy Rule require that covered entities document all oral communication?**

Answer:

No. The Privacy Rule does not require covered entities to document oral information that is disclosed or used for treatment, payment or health care operations. However, if the communication (whether oral or written) requires a documentation in the Rules then the communication must be documented. For example, if a public health authority is called about a case of tuberculosis by a treating physician, then the physician must maintain a record that he or she made the disclosure of tuberculosis to the public health authority.[35]

- **Does HIPAA apply to janitorial services?**

Answer:

In general, a janitor emptying a wastebasket with protected health information is incidental disclosure and is permitted by HIPAA without the necessity of the janitor signing a business associate contract. However, if the protected health information is routinely handled by the person or they shred the documents then it is likely that person would be considered a business associate by HIPAA and a business associate contract ensuring privacy would be needed.[36]

---

[34] *Your Frequently Asked Questions On Privacy*, U.S. Dept. of Health & Human Services, Answer ID 221, Updated 7-18-2003, available at http://www.hhs.gov/ocr/hipaa/html. (last visited 8-18-03).
[35] *Your Frequently Asked Questions On Privacy*, U.S. Dept. of Health & Human Services, Answer ID 370, Updated 7-18-2003, available at http://www.hhs.gov/ocr/hipaa/html. (last visited 8-18-03).
[36] *Your Frequently Asked Questions On Privacy*, U.S. Dept. of Health & Human Services, Answer ID 243, Updated 7-18-2003, available at http://www.hhs.gov/ocr/hipaa/html. (last visited 8-18-03).

- **Does HIPAA change how a person grants a health care power of attorney?**

Answer:

No. [37]

- **May personal representatives access health information based on a non-health care power of attorney?**

Answer:

"No. Except with respect to decedents, a covered entity must treat a personal representative as the individual only when that person has authority under other law to act on the individual's behalf on matters related to health care. A power of attorney that does not include decisions related to health care in its scope would not authorize the holder to exercise the individual's rights under the HIPAA Privacy Rule. Further, a covered entity does not have to treat a personal representative as the individual if, in exercise of professional judgment, it believes doing so would not be in the best interest of the individual because of a reasonable belief that the individual has been or may be subject to domestic violence, abuse or neglect by the personal representative, or that doing so would otherwise endanger the individual.

With respect to personal representatives of deceased individuals, the Privacy Rule requires a covered entity to treat the personal representative as the individual as long as the person has the authority under law to act for the decedent or the estate. The power of attorney would have to be valid after the individual's death to qualify the holder as the personal representative of the decedent."[38]

LIABILITY FOR RELEASE OF INFORMATION

Filing A Complaint with the Office of Civil Rights (OCR) for HIPAA Violation:

Complaints must be:

1. Filed in writing (may be done by mail, fax or e-mail) and should be made our to the attention of the OCR Regional Manager
2. Name the entity that is the subject of the complaint
3. Describe the acts and omissions believed to be violated
4. Be filed within 180 days of when you knew that the act or omission complained of occurred. (OCR may extend the 180-day period if you can show "good cause.")
5. The violation has to have occurred on or after April 14, 2003 (or on or after April 14, 2004 for small health plans) for OCR to have the authority to investigate.
6. You may call 1-800-368-1019 if you have a question about filing a complaint.
7. A copy of the recommended OCR Health Information Privacy Complaint form is attached as Appendix "C".

---

[37] *Your Frequently Asked Questions On Privacy*, U.S. Dept. of Health & Human Services, Answer ID 219, Updated 7-18-2003, available at http://www.hhs.gov/ocr/hipaa/html. (last visited 8-18-03).

[38] *Your Frequently Asked Questions On Privacy*, U.S. Dept. of Health & Human Services, Answer ID 224, Updated 7-18-2003, available at http://www.hhs.gov/ocr/hipaa/html. (last visited 8-18-03).

Enforcement and Penalties under HIPAA:
It is to be enforced by the HHS Office for Civil Rights (known as "OCR") and the government has stated that it will be primarily complaint-driven for enforcement.[39] Since it will be a "voluntary compliance" with the new Privacy regulations, it is likely that if a violation is discovered that the offender will be asked to submit to a corrective plan of action rather than pay fines.[40] If it is an egregious offense, then the government is likely to pursue it.[41] There are criminal and monetary penalties[42] for violation of HIPAA. Currently, there are only 23 people assigned to handle grievances at the HHS Office for Civil Rights.[43]

Criminal Penalties:

The U.S. Department of Justice will enforce the criminal penalties. A person who knowingly obtains or discloses individually identifiable health information in violation of HIPAA faces a fine of $50,000 and up to one-year imprisonment.[44] The criminal penalties can be increased to $100,000 and up to 5 years imprisonment if the wrongful conduct involves false pretenses and the fine can increase to $250,000 and up to 10 years imprisonment if the wrongful conduct involves the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain or malicious harm.[45] Your complaint must be filed within 180 days of the incident. (You can also send a copy of the complaint to the Health Privacy Project to that they can monitor complaints and follow-up.)[46]

Civil Monetary Penalties:

In general, the penalty is $100 for each violation with the maximum of $25,000 per year for all violations of an identical requirement of prohibition.[47] The Health and Human Services department will enforce the monetary penalties.

INTERPLAY BETWEEN HIPAA AND STATE STATUTES

How Does State Law Effect HIPAA?

In general, HIPAA preempts state laws that are contrary to the Privacy Rule. "Contrary" means that it would be impossible for a covered entity to comply with both State and federal requirements, or that the provision of State law is an obstacle to accomplishing

---

[39] *Fact Sheet*, U.S. Dept. of Health & Human Services, Apr. 14, 2003 at p.3 available at http://www.hhs.gov/news/facts/privacy.html (last visited 8-1-03).
[40] Lee Spangler, *What's Happening With HIPAA*, Tex. Med., Apr. 2003, at 24.
[41] *Id.*
[42] 42 U.S.C. 1320d-5, 42 U.S.C. 1320d-6.
[43] Dana Hawkins, *A Healthy Dose of Privacy – A New Law Tries to Protect Patients' Medical Records – But Has Glaring Gaps*, U.S. News World Report, Apr. 28, 2003 at 53.
[44] Pub. L. 104-191; 42 U.S.C. §1320d-6.
[45] *Summary of The HIPAA Privacy Rule, OCR Privacy Brief*, U.S. Dept. of HHS, (Last revised 05/03) available at http://www.hhs.gov/ocr/privacysummary.pdf.html. (Last visited 8-20-03) at p. 18.
[46] The Health Privacy Project is part of the Institute for Health Care Research and Policy at Georgetown University, 1120 19th St. NW, 8th Floor, Washington, D.C. 20036, Telephone (202) 721-5614, facsimile: (202) 530-0128, www.healthprivacy.org
[47] http://www.hhs.gov/ocr/moneypenalties.html. (last visited 8-1-2003).

the full purposes and objectives of the Administrative Simplification provisions of HIPAA."[48] State laws which provide stronger privacy protection will continue to apply over and above the new Federal privacy standard.[49]

Exceptions to federal preemption[50] are:

1. If the State's law(s) provide greater privacy protections or privacy rights with respect to the privacy of an individual's identifiable health information
2. If the State's law(s) provide for the reporting of disease or injury, child abuse, birth, or death, or for public health surveillance, investigation, or intervention,
3. If the State's law(s) provide for certain health plan reporting, such as for management or financial audits.

When the more stringent State law and Privacy Rule are not contrary, then covered entities must comply with both laws.[51] See 45 C.F.R. Part 160, Subpart B for specific requirements related to preemption of State law.

Your client does not have the right to sue a health care provider in federal court for a violation of HIPAA but a documented violation of HIPAA's privacy provisions may strengthen a privacy care you bring in state court.[52]

Helpful Websites

(These websites are provided to assist you and the authors do not take responsibility for the content of these sites):

http://www.hhs.gov/ocr/hipaa/

(Comprehensive DHHS information on HIPAA. This site contains the entire Privacy Rule, as well as additional guidance materials.)

http://www.cms.hhs.gov/hipaa2

(Provides helpful information for Medicare and Medicaid Services)

http://www.ahima.org

(The American Health Information Management Association website)

http://www.gemedicalsystems.com/gecommunity/hippa/final_priv_exec_brief.pdf

(Summary of Final Rules Modification August 14, 2002)

---

[48] 45 C.F.R. §160.202.

[49] *Your Frequently Asked Questions On Privacy*, U.S. Dept. of Health & Human Services, Answer ID 188, Updated 3-3-2003, available at http://www.hhs.gov/ocr/hipaa/html. (last visited 8-18-03).

[50] *Summary of The HIPAA Privacy Rule, OCR Privacy Brief*, U.S. Dept. of HHS, (Last revised 05/03) available at http://www.hhs.gov/ocr/privacysummary.pdf.html. (Last visited 8-20-03) at p. 17.

[51] *Your Frequently Asked Questions On Privacy*, U.S. Dept. of Health & Human Services, Answer ID 403, Updated 3-13-2003, available at http://www.hhs.gov/ocr/hipaa/html. (last visited 8-18-03).

[52] *Health Privacy: Know Your Rights*, Health Privacy Project, available at http://www.healthprivacy.org/usr_doc/Rights_flyer.pdf, (last visited 8-18-03).

http://www.hhs.gov/ocr/combinedregtext.pdf
(OCR/HIPAA Privacy Regulation Text October, 2002)

http://www.aapsonline.org/
(Association of American Physicians and Surgeons' website)

http://www.hhsc.state.tx.us/NDIS/NDISTaskForce.html
(Texas Health and Human Services Commission website)

http://www.healthprivacy.org
(Health Privacy Project of the Institute for Health Care Research and Policy Georgetown University)

CRITICISM OF HIPAA:
Some physicians are concerned that HIPAA will intrude upon patient care if the physicians/health care providers are overzealous or misunderstand the application of the new HIPAA rules in relaying patient information during patient treatment.[53] Other physicians are concerned that the new Rules require unnecessary paperwork.[54]

> "Unlike the creator of Frankenstein, the creator of HIPAA, a hero to armies of useless paper generators and the members of Congress who voted for it, appears to be ignorant of, or at least unconcerned by, the unintended consequences…. HIPAA, however, has dropped a 2,000-pound bunker-busting bomb on a flea."[55]

Some critics believe that HIPAA has not gone far enough to protect patient's privacy rights. Loopholes that have been identified include drug companies paying providers to send marketing pitches or samples to their patients without the patients knowing the source of the payment for the information.[56] In addition, most Web sites are not covered so that people sharing health information online may not be protected.[57] Other loopholes include health information gathered by pre/post employment physicals, drug tests, worker's compensation, employee assistance programs, and nosy healthcare workers who may look at your records.[58]

Since *ex parte* communication is not a part of HIPAA, we have created letters for attorneys and clients to sign that does not permit *ex parte* communication. Sample letters to health care providers limiting *ex parte* communication are attached as Exhibit "D.

---

[53] Deeb Salem & Stephen Pauker, *The Adverse Effects of HIPAA on Patient Care*, N. Engl. J. Med.349(3), July 2003 at 309.
[54] Daniel Duke, *HIPPA: ineptitude run amok"* Tex. Medicine, June 2003 at 9.
[55] *Id.*
[56] Dana Hawkins, *A Healthy Dose of Privacy – A New Law Tries to Protect Patients' Medical Records – But Has Glaring Gaps*, U.S. News World Report, Apr. 28, 2003 at 53.
[57] *Id.*
[58] *Id.*

OPPOSITION TO HIPAA:

There are some that have voiced their opposition to HIPAA, including the Association of American Physicians and Surgeons and Consumer Alert.[59] The Association of American Physicians & Surgeons, Inc. has sued in the U.S. District Court in the Southern District of Texas, Houston Division, Civil Action No. H-01-2963, styled *The Association of American Physicians & Surgeons, Inc., et al v. United States Department of Health and Human Services, et al*. This case was dismissed on June 14, 2002 by Judge Sim Lake for failure to show that the Plaintiffs had suffered any actual or imminent injury due to enforcement of the Privacy Rule, failure to have ripe claims for judicial review and lack of standing.

Form from The Association of American Physicians and Surgeons (AAPS) – In Opposition to HIPAA

The APPS is opposed to HIPAA as violating patient's right to privacy and allowing medical records to be given to third parties that include marketers, the government and insurance companies. The APPS has stated that "The only guaranteed way to protect your privacy is to ask your doctor to become a "non-covered" entity under HIPAA."[60]

APPS has provided a form that a patient may utilize to ensure that a patient gives their consent prior to a patient's records being turned over to a third party. It is attached as Appendix "E" to this paper.

BOTTOM LINE: HOW WILL HIPAA CHANGE OBTAINING MEDICAL RECORDS IN A MEDICAL MALPRACTICE CASE

Time will tell how HIPAA changes the landscape of privacy for patients and obtaining medical records by attorneys/patients. At this time it would appear that except for HIPAA language changes in authorizations that there will be no significant changes we will see in accessing and obtaining our patient's records. A copy of our HIPAA compliant authorization is attached as Exhibit "F."

[59] See http://aapsonline.org/ and www.consumeralert.org - James Plummer, policy analyst, June 1, 2003, Consumers' Research Magazine.

[60] AAPS website http://www.aapsonline.org.html, HIPAA Information for Patients - 12/20/2002 (last visited 8-4-03).