HIPAA Traps for Unwary Practitioners

State Bar of Texas
2004 Advanced Medical Malpractice Course

Tim Riley

RILEY LAW FIRM
1225 N. Loop W., Ste. 810
Houston, TX 77008-1757
(713) 868-1717
Fax (713) 868-9393
E-Mail TDR@TxTrial.com
Web www.TxTrial.com

HIPAA Traps for Unwary Practitioners

Table of Contents

Index of Authorities

Cases

Statutes

Rules

Secondary

HIPAA Traps for Unwary Practitioners

I. INTRODUCTION

HIPAA is a federal statute designed to protect the confidential health information of patients. The statute in general only applies to health care providers and health insurers. More indirectly, though, lawyers representing health care providers are probably deemed the statutory "business associates" of the providers, subject to certain conditions to receive confidential patient information. Moreover, the general ethical provisions applicable to all counsel, regardless of who they may represent in a particular proceeding, dictate that lawyers closely safeguard confidential medical and health information of all persons that may come into the lawyer's possession from any source.

A. Background of the Act and The Privacy Rule

The Health Insurance Portability and Accountability Act of 1996, or "HIPAA," was enacted during the Clinton Administration to improve the portability and continuity of health insurance coverage. *See* Pub.L. No. 104-191, 110 Stat. 1936 (1996). In light of the anticipated increase in the transmission of health information as a result of HIPAA, Sections 261 through 264 of the act required the Secretary of Health and Human Services to propose and pass standards for the privacy and security of such health information.

On November 3, 1999, the Secretary issued proposed rules in compliance with the congressional mandate. After receiving over 52,000 public comments, the initial version of the Privacy Rule was published on December 28, 2000. 65 FR 82462. Final modifications to the Privacy Rule were published in final form on August 14, 2002. 67 FR 53182. The entire text of the Privacy Rule is too lengthy to be duplicated as an appendix to this article. However, the entire text can be found at www.hhs.gov/ocr/regtext.html.

According to Tommy G. Thompson, Secretary of the U.S. Department of Health and Human Services, "[T]he 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." In short, the Privacy Rule was intended to limit the use or disclosure of PHI to the minimum amount necessary to accomplish a permitted and intended purpose. 45 CFR §§ 164.502(b, 164.514(d).

The federal government makes available two very helpful brochures which explain the requirements of the HIPAA Privacy Rule. The first is a four page "Fact Sheet," a copy of which is attached to this article as Appendix A. The second is a 23 page "Summary of the HIPAA Privacy Rule," attached as Appendix B.

B. Persons and Entities Covered Under HIPAA

The provisions of the Privacy Rule are directed toward compliance by "covered entities." Included within that definition are individual and group health care plans, including health, dental, vision, and prescription drug insurers, as well as HMOs, Medicare, Medicaid, and long-term care insurers. Covered as well are all "providers of services," which includes institutional providers such as hospitals, and all "providers of medical or health services," meaning all physicians, dentists, and other practitioners. 45 CFR Part 162.

C. Business Associates

When a person or entity covered by HIPAA uses a contractor to perform services or activities, the burden is on the health care provider to ensure that the privacy provisions are enforced by the "business associate" of the health care provider. The term "business associate" is defined to include any person or organization, other than a member of a covered entity's workforce, who performs certain functions or activities on behalf of, or provides certain services to, a covered entity which involve the use or disclosure of protected information. Business associate services to a covered entity are limited to *legal*, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services

D. What is Protected

The Privacy Rule protects any individually identifiable health information in any form, written, verbal, or electronic. This is referred to as "protected health information," or "PHI." 45 CFR § 160.103.

PHI includes information relating to the patient's past, present, or future physical or mental health or condition, the provision of health care to the patient, or payment or non-payment for health care. To be covered, though, the PHI must be specifically identifiable with respect to a particular patient. In other words, if the information contains names, addresses, social security numbers, or other identifying data that might be linked with a particular patient, the information is PHI.

The scope of information included in PHI is therefore extremely broad. Items as simple as immunization records would appear to be protected PHI. The names of a patient's regular treating physicians also appear to fall within the scope, as would "bounced check" information, if the payment was made for health care.

However, information that is not specifically referable to a particular patient is defined as "de-identified health information." De-identified health information does not disclose any identities, nor does it provide any reasonable basis by which an individual patient might be identified. Information can be de-identified by a formal determination by a qualified statistician, or by the removal of any specified identifiers of the individual and of the individual's relatives, household members, and employers. Demographic data which makes no direct or implied identification of any individual patient ordinarily would not be considered PHI.

E. Not Protected under the Privacy Rule

Significant to both legal and medical practitioners, the Privacy Rule has no applicability to the disclosure of PHI to the patient. Similarly, no authorization for release of PHI is required to treat a patient. Physicians also do not need a patient's written authorization to send the patient's medical records to another provider *who is treating the patient.* (Contrast this with the provision of PHI to experts not involved in patient care, though, discussed *supra.*

F. Means of compliance

Beyond simply not giving out medical records without proper authorization, there are a number of examples as to how a health care provider must comply organizationally with HIPAA's requirements. Organizational polices that may be adopted, for example, may include:

- Using a cover sheet with a confidentiality statement when faxing anything containing PHI.
- Verifying fax numbers before faxing.
- Verifying that someone will be present to receive sensitive faxes.
- Leaving no patient messages containing PHI on answering machines or with family members.
- Leaving messages which identify a physician, asking for patients to return phone calls.
- Restricting the posting of patient information on boards that may be seen by visitors.
- Limiting vendor access and requiring vendors to sign confidentiality agreements.
- Shredding all papers with PHI.
- Developing a secure method of transporting documents.
- Securing computer identification.
- Enabling automatic logouts on computers.

Grey, Catherine, *Understanding and Complying with HIPAA,* 18 J. of PeriAnesthesia Nursing 3, 182, 183, June 2003.

II. PENALTIES FOR NON-COMPLIANCE

A. Civil Penalties

HHS may impose civil monetary penalties of $100 per violation against a covered person or entity for failing to comply with Privacy Rule requirements. The aggregate penalty may not exceed $25,000 per year.

B. Criminal Penalties

Any person who knowingly obtains or discloses

individually identifiable health information in violation of the Privacy Rule can be fined up to $50,000 and imprisoned for up to one year. The criminal penalties can be increased to $100,000, and the incarceration can be increased to five years, if the wrongful conduct involved false pretenses. If the offending party intended to sell, transfer, or use individually identifiable health information for commercial advantage, financial gain, or to inflict malicious harm, he can be fined up to $250,000 and imprisoned for up to ten years.

C. Enforcement

The provisions of the Privacy Rule are enforced by the Department of Justice. Aggrieved persons must file written complaints with HHS to initiate an investigation.

III. CLIENT OBTAINING RECORDS

The patient is always entitled to obtain copies of his or her own medical records from health care providers. A covered entity has 30 days from the date of request to produce the records, 60 days if the records are offsite. 45 CFR § 164.524. However, the health care provider can decline to let the patient inspect or copy the records if:

- A patient requests his or her own psychotherapy notes;
- The information requested has been compiled solely in reasonable anticipation of litigation;
- The information requested is laboratory information to which the Clinical Laboratory Improvement ACT (CLIA), prohibits access;
- The information relates to an inmate;
- The information has been obtained during research and the patient has agreed to the restriction on access to the information; or
- The information was obtained under a promise of confidentiality from someone other than a provider and access would likely reveal its source.

IV. OBTAINING MINOR'S RECORDS

Generally, a parent is considered the personal representative of a minor, authorized to consent to the disclosure of the minor's PHI. However, the health care provider can refuse to recognize the parent as the authorized representative if the provider reasonably believes that the child has been or may be subjected to domestic violence, abuse, or neglect, or that treating the parent as a personal representative could endanger the child.

V. ESTATE REPRESENTATIVE OBTAINING RECORDS

An individual has the right to appoint a personal representative, who has the same rights to obtain the patient's medical records as that enjoyed by the patient. Generally, state law determines whether a person is qualified as a personal representative.

For adults, holders of a health care power of attorney, legal guardians appointed by a court, and holders of a general power of attorney, are all authorized personal representatives. However, the power of attorney must give the holder the right to make health care decisions for the patient to be effective. In other words, the standard power of attorney involved in representing a client in a lawsuit is not sufficient to make counsel the patient's personal representative so that the attorney can request records without a signed authorization from the patient.

As to decedents, an executor, administrator, or other personal representative of the estate qualifies as a personal representative of the patient under the Privacy Rule. 45 CFR § 164.502(g)(4).

VI. PATIENT'S COUNSEL OBTAINING CLIENT INFORMATION

An attorney for a patient may obtain the patient's medical records. However, the attorney must present a HIPAA-compliant authorization to the health care provider. Unfortunately, there is no standard form of a HIPAA-compliant authorization. Accordingly, many health care providers reject authorizations submitted, requiring the submission of their uniquely-designed HIPAA-compliant authorization. In light of the penalties involved for improper disclosures, perhaps that is not surprising.

In any event, according to HHS:

> An authorization is a detailed document that gives covered entities permission to use protected health information for specified purposes, which are generally other than treatment, payment, or health care operations, or to disclose protected health information to a third party specified by the individual. An authorization must specify a number of elements, including a description of the protected health information to be used and disclosed, the person authorized to make the use or disclosure, the person to whom the covered entity may make the disclosure, an expiration date, and, in some cases, the purpose for which the information may be used or disclosed.

Sample forms that are intended to be HIPAA compliant can be found at a number of internet sites, including:

www.cdhs.state.co.us/HIPAA/hipaa_forms.htm
http://www.mc.vanderbilt.edu/HIPAA/MC3916.pdf
http://www.state.me.us/bds/HIPAA/PDF/AUTHORIZATION%20TO%20RELEASE%20INFORMATION.pdf
http://www.hr.ucdavis.edu/Forms/All/HIPAAFORMS/001.

Several samples are attached to this paper as Appendix C.

VII. COUNSEL OBTAINING RECORDS FROM CLIENT PHYSICIAN

Under HIPAA, attorneys representing health care providers in medical liability lawsuits arguably are the "business associates" of the health care provider. A covered health care provider is required to undertake efforts to ensure that the patient's right of privacy is protected by its business associates. Accordingly, before passing PHI to business associates, the health care provider must secure a "Business Associate Agreement." 45 CFR §§ 164.502(g)(3)(ii), 164.524.

In general, the Business Associate Agreement must require the Business Associate:

- Not to use or disclose Protected Health Information other than as permitted or required by the Agreement or as Required By Law.
- To use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement.
- To mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information.
- To report to the Covered Entity any use or disclosure of the Protected Health Information not provided for by the Agreement.
- To ensure that any agent, including a subcontractor, to whom the Business Associate provides Protected Health Information received from, or created or received by the Business Associate on behalf of Covered Entity, agrees to the same restrictions and conditions that apply through the agreement to the Business Associate with respect to such information.
- To provide access, at the request of the Covered Entity, to an Individual in order to meet the requirements under 45 CFR § 164.524.
- To make internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the use and disclosure of Protected Health Information to the Secretary (of HHS) or the Covered Entity.
- To document all disclosures of Protected Health Information and information related to such disclosures as would be required for the Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR § 164.528.
- To provide to the Covered Entity information gathered to permit the Covered Entity to respond to a request by an Individual for an accounting of

disclosures of Protected Health Information in accordance with 45 CFR § 164.528.

An article reflecting the requirements for sample Business Associate contract provisions is attached hereto as Appendix D.

With regard to the use of the PHI by the Business Associate, the rules provide that, except as otherwise limited in the Agreement, the Business Associate may use Protected Health Information to carry out the legal responsibilities of the Business Associate. In addition, the Business Associate may disclose Protected Health Information provided that: (a) disclosures are required by law, or (b) the Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the agreement of the receiving party to notify the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

VIII. SHARING RECORDS WITH EXPERTS/CO-COUNSEL, ETC.

The Business Associate Agreement must require the Business Associate to use the PHI in the same manner as the restrictions on the use of same applied to the health care provider. Additionally, the Business Associate must be required by the agreement to obtain similar agreements from any person or entity with whom the PHI is shared. There is no requirement, however, that those agreements be in writing.

IX. OBTAINING RECORDS VIA SUBPOENA

HIPAA allows health care providers to produce records in response to a lawful subpoena, if: (1) a qualified protective order has been sought, or (2) reasonable notice of the subpoena has been given to the patient with any objections resolved. It would appear, therefore, that the notice of intent to take a deposition on written questions, without objection, would authorize health care providers to produce records without further authorization. However, many health care providers are so concerned about HIPAA liability that they are refusing to produce records in response to a subpoena. In that instance, counsel will have little choice but to either obtain a HIPAA-compliant authorization or a court order.

X. INTERPLAY BETWEEN HIPAA AND CHAPTER 74, TEXAS CIVIL PRACTICES AND REMEDIES CODE

There are several interesting interplays between the requirements of HIPAA and the provisions of Chapter 74, Texas Civil Practices and Remedies Code. They are worthy of examination. However, federal law is clear that, in the case of conflict, federal law trumps the conflicting state statute. 45 CFR § 160.203. To be in conflict, it must be the case that the health care provider cannot comply both with state law and the federal requirements. *Id.* at § 160.202.

A. Failure to supply statutory authorization with notice of suit

The Texas statute could not be clearer. If a patient fails to provide the statutory authorization form with the notice of claim, *or* revokes it or modifies it in any regard, the health care provider can have the court immediately abate all aspects of the proceeding for 60 days. The 60 days do not begin running until a statutory-compliant authorization has been furnished. Tex. Civ. Prac. & Rem. Code § 74.052(a)(b).

B. Ex parte communications with patient's health care providers

The statutory authorization form required by Chapter 74 of the Texas Civil Practices and Remedies Code specifically references verbal information as well as written. Tex. Civ. Prac. &

Rem. Code § 74.052. Clearly, the Texas Legislature had in mind that, coincident with receipt of a notice of a potential health care liability claim, the patient must provide the health care provider with a HIPAA-compliant authorization,. The authorization would allow the potential defendant not only to obtain all medical records for the past five years, but also to obtain "verbal information" regarding the patient from other health care providers.

Arguments have been raised that the state law does not allow a health care provider, however, to discuss any aspects of the patient's care or condition beyond what is contained in the medical records produced. Some attorneys write to physicians to advise them that the patient is not waiving the privacy protections of HIPAA by signing a statutorily-required authorization form. Whether the recipient agrees to honor that attempted limitation, and what action if any can be taken for his failing to honor it, remain open questions.

Another open question is whether an "end run" attempt to prevent what the Texas statute clearly allows would give rise to a right to abate the case pursuant to § 74.052. Accordingly, the better course may be simply to write to the physicians and request that the claimant's attorney be notified to be present when any discussions occur, so that the patient's right of privacy can be protected.

C. Authorization by family members of decedents

As noted above, HIPAA requires that authorization for release of PHI from someone other than the patient be from a duly qualified "personal representative" of the patient. 45 CFR § 164.502(g)(4). However, the Texas statute provides that an authorization for release of a decedent's records may be signed by a parent, spouse, or adult child of the deceased. Tex. Civ. Prac. & Rem. Code § 74.051(e).

A number of health care institutions are refusing to recognize authorizations signed by such persons unless they have also been qualified as personal representatives of the estate of the decedent by court order. Their concern in that regard may well be legitimate. Accordingly, it may be necessary to have an estate opened and a representative appointed in some instances to obtain a decedent's records. Alternatively, a court order compelling production of the records would be sufficient under both HIPAA and Texas law.

XI. CONCLUSION: COUNSEL REQUIREMENTS UNDER HIPAA AND RELATED DUTIES REGARDING CONFIDENTIALITY OF PROTECTED HEALTH INFORMATION

Since HIPAA does not apply to anyone other than health care providers, insurers, HMOs, and the like, legal counsel is under no threat of direct sanctions, civil or criminal, for failing to comply with HIPAA's requirements. Even when counsel is subject to a Business Associate Agreement, precluding the unauthorized release of PHI, the sanctions of HIPAA for violations run against the health care provider, not the business associate.

Consider, however, the situation where the health care provider has secured a Business Associate Agreement from counsel, prohibiting the lawyer from the unauthorized disclosure of patient PHI, but the lawyer nonetheless is careless and the information is disclosed. A complaint is made to the Office of Civil Rights, resulting in monetary and other sanctions against the health care provider. Would the health care provider in that instance have a cause of action against his lawyer for consequential damages arising from the lawyer's breach of contract or breach of fiduciary duty?

Moreover, when a lawyer receives information confidential to a patient, the lawyer is charged under state law with a duty to disclose the information no further than the extent consistent with the authorized

purpose for which the information was obtained. Tex. Occ. Code § 159.005. Moreover, a person who is "aggrieved" by a violation of this provision can prove a cause of action for damages against the offending party. *Id.* at § 159.009. However, the one court that has addressed this statute held that it was inapplicable to anyone other than a physician with a physician-patient relationship with the patient. *Warnke v. Boone,* 4 S.W.3d 266 (Tex.App.-Houston [14th Dist.] 1998, no pet.).

Lawyers have a duty to their clients to protect a clients' "confidential information." Tex. Disc. R. of Prof. Conduct § 1.05. Clearly, that would include a client's PHI. Accordingly, lawyers have an ethical duty to their clients to protect the clients' PHI from any disclosure beyond that required by the representation. (Query, though, whether a patient's PHI can be the "confidential information" of a client-physician. In other words, if a lawyer improperly discloses a patient's PHI provided by the physician-client of the lawyer, might the lawyer be subject to a grievance for failing to protect the "confidential information" of the doctor, even though it was not the doctor's health information that was disclosed?)

In general, lawyers have no duty to non-clients. However, the bottom line is that both the Texas Legislature and the United States Congress have expressed their common sense belief that patient information is worthy of high levels of protection. Accordingly, the spirit of the Texas Disciplinary Rules of Conduct, the Texas Occupations Code, and HIPAA clearly dictate that lawyers, as officers of the court, act in a manner to protect the PHI of even non-clients. While the *Warnke v. Boone* case appears to absolve lawyers from liability to non-clients for the unauthorized disclosure of confidential health information, the ethical implications of our public duties lead to a conclusion that procedures similar to those required of health care providers under HIPAA be adopted by all Texas lawyers.