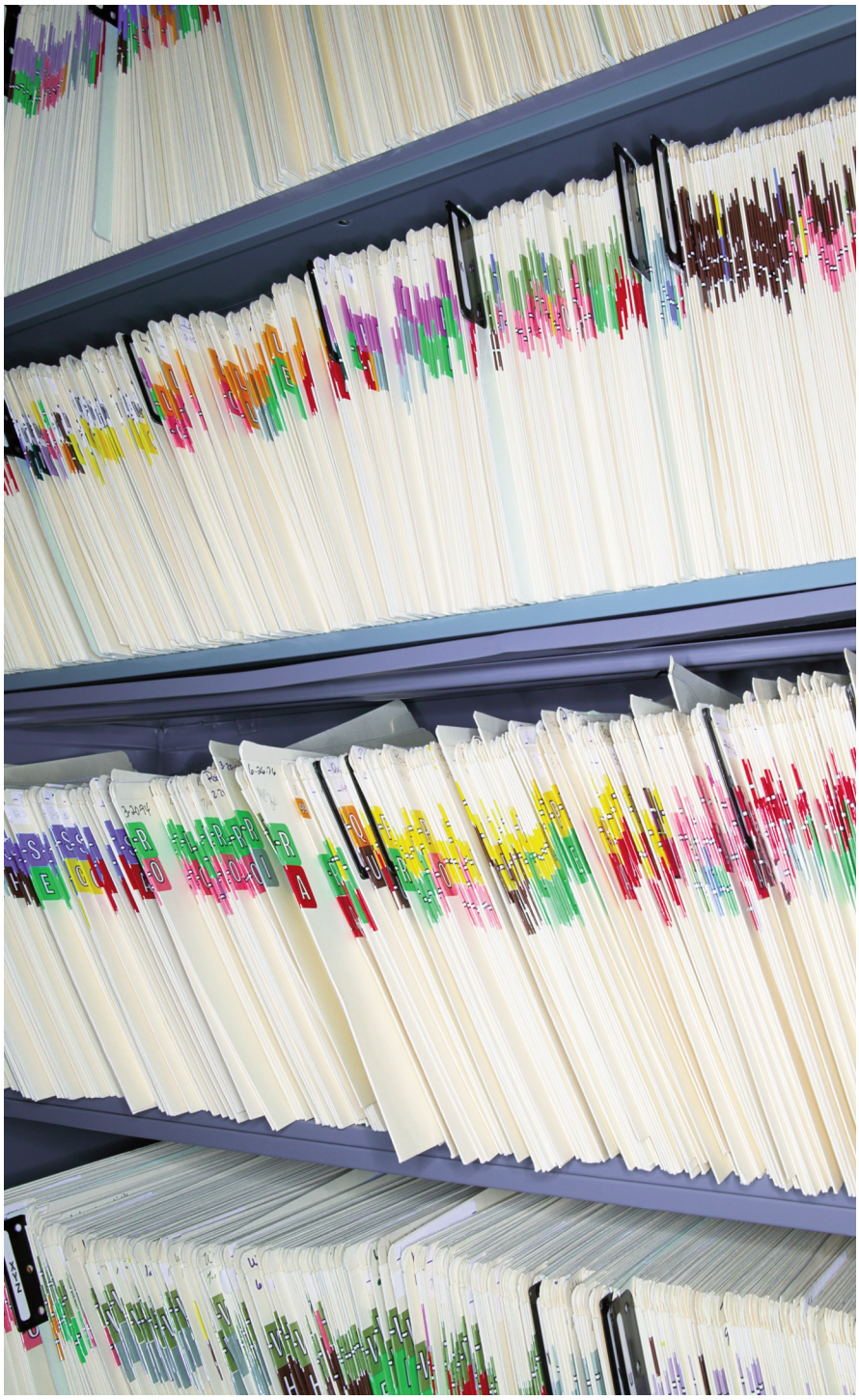
HIPAA AND MEDICAL RECORDS PRIVACY

A survival guide for Texas attorneys.

BY MARTIN MERRITT AND PAT SOUTER



A MEDICAL RECORD CONTAINS NOT ONE, BUT THREE KINDS OF SENSITIVE INFORMATION. First is sensitive, private information about a patient's health. This is what many people likely think of when they hear or read about physician-patient confidentiality. A second kind of sensitive information is basic financial data, such as Social Security numbers, credit card numbers, and date of birth, all of which could be valuable to ordinary identity thieves. The final type is a chart that contains diagnosis codes, health insurance plan identification numbers, and perhaps Medicare numbers, which is extremely valuable to highly sophisticated thieves who can steal hundreds of thousands of dollars using a single identity. Collectively, these categories of information are known in health law circles as "protected health information" or PHI.[1] The risk of theft is also why the government is so serious about enforcing the Health Insurance Portability and Accountability Act and the Texas Medical Records Privacy Act.

According to a report in the *Journal of the America Medical Association*, 29 million patient records were jeopardized in just three years through nearly 1,000 data breaches.[2] Reuters ominously reports, "As attackers discover new methods to make money, the health care industry is becoming a much riper target because of the ability to sell large batches of personal data for profit.[3]"

It is this nationwide financial threat, more so than the concern that state privacy laws were inadequate, that seems to have directly led to the enactment of a number of federal laws, including HIPAA, the Health Information Technology for Economic and Clinical Health Act, and the omnibus rules.[4] These are complemented by the Texas Medical Records Privacy Act, Health and Safety Code §181.001, *et. seq.*, which provides even greater regulation than federal law. The Texas law applies to all attorneys who come into possession of patient records and requires the exercise of much more care—and certainly a great deal more care than Texas litigators historically exercised under the Texas Rules of Evidence and Texas Rules of Civil Procedure. This article discusses the impact that these new medical privacy rules may have on the practice of law in Texas.

FEDERAL HIPAA AND THE TEXAS MEDICAL PRIVACY ACT

At the risk of over-simplifying 225 years of constitutional law, protecting a patient's privacy expectations relating to his or her medical records generally falls under the police powers reserved to the states by the 10th Amendment.[5] The result is 50 different sets of rules, one for each state. Adding to this complexity, in Texas it seems every health care profession secured from the Legislature its own confidentiality statute.[6] Consequently, patient privacy expectations were codified in nearly a dozen ill-fitting and frequently conflicting Texas statutes. Any federal attempt to fashion a single medical privacy rule to reduce cyber crime must necessarily satisfy the 10th Amendment and the needs of a diverse number of factions, including a state's need to carry on the business of its courts.

The Texas Rules of Evidence historically solved this problem, largely by obliterating any protection afforded by these dozen or so patient confidentiality statutes.[7] Commonly, medical records were filed into the public record with little or no redaction. Sensitive information was freely passed between lawyers, expert witnesses, economists, accountants, consultants, and other witnesses. Records were blown up into huge exhibits, which often stayed posted during an entire trial. Many were simply left on tables in open court. Laptops containing health care information might be left unattended in unlocked courtrooms for hours each day. Certainly, no one kept track of copies of medical records or tried to secure the records' destruction or return at the conclusion of the case.

The need to carry on the business of the courts does not require us to do so recklessly. Congress felt that more could be done to protect the public against the risk of health care financial crime, even in the courtroom setting. In 2009, Congress set out to add teeth to the pre-Internet HIPAA patient privacy and security rules of 1996. Although Congress had the power under the commerce clause to take on the task, the constitutional scheme for how a bill becomes a law makes Congress poorly equipped to do so. Even the slightest tweaking after trial and error would require approval of both houses and the president's signature. Congress wisely gave itself a limited amount of time to get it right, and, then by default, the job fell precisely where it belongs—to the Office for Civil Rights of the U.S. Department of Health and Human Services. The resulting omnibus final rules became effective in February 2013.[8]

Because the HIPAA final omnibus rule is a regulation, not a federal statute, it must specifically identify the rule's enabling statute. This includes the subject and the party to be regulated. Because there likely is no enabling statute allowing the OCR to regulate attorneys, accountants, and anyone else coming into possession of health care data, the states must enact laws under the powers reserved to them. Hence, we have the Texas Medical Records Privacy Act, which became effective September 1, 2012.

Under this state act, Texas attorneys are now subject to greater regulation. The law applies nearly any time you come into possession of patient medical records in your professional capacity. Federal law also indirectly applies to you if you acquire protected health care records because you have been retained to work for a health care client who is directly regulated. In such a case, you are likely considered a "business associate"[9] under federal law, requiring you to sign a business associate's agreement. The health care client is directly regulated, and you, as a non-regulated private attorney, must agree to become federally regulated by contract. If you do not wish to sign a BAA, the client is not allowed under federal law to provide you with any records.

It is important to note that neither HIPAA privacy and security rules nor the Texas statute create any private cause of action in favor of the patient. Only the government can impose sanctions, which include injunctions, fines, disciplinary actions, and potentially the exclusion of evidence obtained in violation of privacy laws.

THE LITIGATION PROBLEM

A litigator's daily routine embodies the antithesis of privacy. Generally, no person may refuse to testify,[10] or refuse to produce documents, as long as the matter is relevant to an issue to be decided in court. All relevant evidence is potentially admissible in the public court system and, once admitted, is likely reportable in the local newspaper or other media.[11]

Under Texas Rule of Evidence 509, the burden is upon the party asserting privilege to claim it, or the privileged can be considered waived.[12] Further, under Rule 509

(unlike many of the medical privilege statutes), it does not matter whether the patient is a party or a stranger to the case.[13] In such a case, a *properly obtained* medical record normally can be used in court, over objections, even if the disclosure is not expressly authorized by a licensing board rule or health care statute.

The federal update to HIPAA privacy and security rules was not designed to interfere with the manner in which courts conduct business. The 7th U.S. Circuit Court of Appeals has observed that when Congress enacted HIPAA, the government did not have in mind the creation of any new privileges or interference with court proceedings.[14] This conclusion is supported by comments to HIPAA regulations at 45 C.F.R. §164.512(e).[15]

Regardless of intent, HIPAA and the Texas Medical Records Privacy Act do have the effect of forcing Texas attorneys to think about protecting and securing sensitive medical data at all stages of litigation. Not only could you encounter evidentiary objections for noncompliance with HIPAA or other medical privacy laws but Texas Health and Safety Code §181.202 now authorizes disciplinary action—particularly if there is evidence that the violations of the law are egregious and constitute a pattern or practice.

10 TIPS FOR TEXAS ATTORNEYS DEALING WITH MEDICAL RECORDS

Federal HIPAA and the recent Texas patient privacy statute are derived from principles of medical ethics,[16] which frequently place parties and their attorneys in a type of Catch-22.[17] This is why Congress historically steered clear of attempting to interfere with state rules of court. The Texas Legislature took a big step forward with the Texas Medical Records Privacy Act, but the statute is difficult to comprehend. Until we receive better guidance from the courts, this list of 10 tips is meant to assist Texas attorneys in dealing with medical records.

1. **Always obtain records through a valid authorization or court order.** Simply because records are relevant does not mean that they were legally obtained under HIPAA and Texas law. Improperly obtained records may be subject to a motion to exclude and possible sanctions. The Texas Attorney General's Office has created a patient authorization designed to meet HIPAA and Texas law, available at texasattorneygeneral.gov.[18] If you cannot obtain a signed authorization order, you must follow the Rules of Civil Procedure for obtaining records. Where the patient is not a party, this can be problematic for the attorneys and the health care custodian of records. Complicating matters, the Department of Health and Human Services advises on its website that a subpoena issued by a court reporter or attorney is not a court order.

2. **Properly authorized access to records is just the beginning.** It is the attorney's job to protect records *after lawfully obtaining them*. HIPAA and Texas Heath and Safety Code §181.001, for example, mandate a system-wide security analysis and training of staff, among other things.

3. **It is best to secure a court order permitting your intended use of medical records.** Even if you have a release and the records are relevant, you can never really be sure what the rules allow you to do with the records during litigation. A qualified protective order solves that problem by stating what you may and may not do with records during litigation, who may be permitted to obtain copies of records, and how to dispose of the records when they are no longer needed. Get together with opposing counsel and attempt to agree on a protective order, as you would do with any sensitive information under TRCP 21(c). Reduce the agreement to a signed court order. You may need a hearing in camera if an agreed order cannot be negotiated.

4. **Hire a professional to perform a security analysis and train your staff.** The government does not have the resources to examine your law firm's compliance with HIPAA and the Texas statute—until something bad happens, like a breach of security. Don't wait to take steps to keep the bad guys out of your firm's computers.

5. **Never send unencrypted medical information via email.** Law firms must begin to recognize that health records are just as valuable to thieves as financial records. One way to announce to clients and opposing counsel that you lack proper training and sophistication is to email unencrypted or un-redacted medical records. Which leads us to the next tip.

6. **De-identify or redact health information.** One of the best ways to protect health information is to de-identify or redact as much protected health information as you can—as soon as you can. If you don't need the name of the patient, for example, don't let that information leave the client. If your client can't redact the information before sending it to you, you can redact it before the information goes into your system. You can privately code the documents for identification and store the original hard copy under separate lock and key. This way, the information is useless to Internet thieves.

7. **Protect your employees' laptops, smartphones, tablets, and notebooks.** A big issue in the world of HIPAA enforcement involves employees' usage of their own personal portable devices to perform company business. If a device contains information affecting more than

500 individuals and your employee loses it, the HIPAA Breach Notification Rule[19] may require you to report the incident to the leading newspaper in your area. Many of the larger fines handed out by the OCR are in cases where a laptop or other device was lost—not stolen.

8. **Be responsible litigators.** You won't be able to obtain a court order before you file your pleadings. You can still be smart. Do not file medical records or reveal PHI in pleadings. Just because you have a right to plead medical details does not mean you should. If you must file medical records, do so in a sealed envelope as sensitive information under TRCP Rule 21(c).

9. **Keep track of medical records.** Once you become an attorney lawfully in possession of someone else's medical records, you are then supposed to keep up with them and get them back or destroy them when the case is over. To do so, you need to make a log or record of where any copies go.

10. **Destroy or return records to the client when the case is over.** This is both common sense and required by law. **TBJ**

NOTES

1. PHI is any information about health status, provision of health care, or payment for health care that can be linked to a specific individual and includes photographs, names, addresses, dates of birth, fingerprints, automobile license plates, drivers licenses, health cards, and credit cards.
2. Vincent Liu, Mark A. Musen, and Timothy Chou, *Data Breaches of Protected Health Information in the United States*, 14 JAMA 1471, http://jama.jamanetwork.com/article.aspx?articleid=2247135.
3. Caroline Humer and Jim Finkle, *Your medical record is worth more to hackers than your credit card*, Reuters (Sept. 24, 2014), http://www.reuters.com/article/2014/09/24/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924.
4. Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat. 1936 (1996)., Health Information Technology for Economic and Clinical Health Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 226 (Feb. 17, 2009), codified at 42 U.S.C. §§ 300jj *et seq.*; §§17901 *et seq.*; Final Omnibus Rule 78 F.R. 5566 (January 25, 2013).
5. In U.S. constitutional law, police power is the capacity of the states to regulate behavior and enforce order within their territory for the betterment of the health, safety, morals, and general welfare of their inhabitants. Under the 10th Amendment to the U.S. Constitution, the powers not specifically delegated to the federal government are reserved to the states or to the people, which implies that the federal government does not possess all possible powers.
6. *See* Texas Medical Records Practice Act, Tex. Occ. Code 159.005-006; Dental Practice Act, Tex. Occ. Code 258.104; Podiatric Medical Records, Tex. Occ. Code 202.406; Texas Optometry Act, Tex. Occ. Code 351.352; Chiropractic Records, Tex. Occ. Code 201.405; Acupuncture Records, 22 TAC 183.10; Hospital Records, 241.152; Nursing Home Records, 40 TAC 19.1912; EMS Records, Tex. Health and Safety Code 773.093; Pharmacy Records, 22 TAC 291.28; Tex. Health and Safety Code 183.001, et seq.
7. *See* Tex. R. Civ. P. 509 or 510. This question was put to rest in favor of production in the seminal case, R.K., M.D., v. Ramirez, 887 S.W.2d 836 (Tex. 1994).
8. The OCD announced a final rule that implements a number of provisions of the HITECH Act to strengthen the privacy and security protections for health information established under HIPAA. Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the HITECH Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5566 (Jan. 25, 2013).
9. *See* 45 C.F.R. 164.502(e), 164.504(e), 164.532(d) and (e), http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html.
10. *See* Tex. R. Evid. 501(1): "... no person has a privilege to refuse to be a witness... ."
11. The Fundamentals of Health Law 76 (Barry D. Alexander, et al. eds., 6th ed. 2014).
12. Texas rules provide a mechanism for assertion of privilege and an in-camera inspection to determine relevance.
13. *See* Tex. R. Civ. P. 509 or 510., R.K. v. Ramirez, which analyzed Tex. R. Evid. 509(e)(4).
14. *See* Northwestern Memorial Hosp. v. Ashcroft, 362 F.3d 923 (7th Cir. 2004)(HIPAA creates no new privileges).
15. *See* 65 Fed. Reg. 82661-82710 (Dec. 28, 2000), http://aspe.hhs.gov/admnsimp/final/PvcFR05.txt. The final rule does not create any new duty or obligation to disclose protected health information but does permit covered entities to use or disclose protected health information when they are required by law to do so.
16. *See* American Medical Association Code of Medical Ethics, Opinion 5.05, http://www.ama-assn.org/ama/pub/physician-resources/medical-ethics/code-medical-ethics/opinion505.page.
17. *See* Thapar v. Zezulka, 994 S.W.2d 635 (1999). (Providers are often placed in a Catch-22 situation. If the provider discloses information, one party may be hurt. If the provider fails to disclose, another party may be hurt.)
18. Obtaining an agreed order, with notice and an opportunity for any non-party patient to object, and ordering the redaction or de-identification of any non-essential information before the records leave the custodian, would greatly simplify matters. http://www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/courtorders.html.
19. HITECH Breach Notification Interim Final Rule, Office for Civil Rights, U.S. Department of Health and Human Services, http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/breachnotificationifr.html.

MARTIN MERRITT

is a partner in Friedman & Feiger in Dallas, where he focuses on health law and health care litigation. He serves as the executive director of the Texas Health Lawyers Association.

PAT SOUTER

is a partner in Gray Reed & McGraw, where he focuses on transactional and administrative health care and securities and antitrust matters. He is a professor of health law at Baylor Law School. Souter serves as secretary of the Texas Health Lawyers Association.

STATE BAR OF TEXAS

Administrative and Public Law Section

The Administrative and Public Law Section of the State Bar of Texas sponsored the 17th Annual Mack Kidd Administrative Law Moot Court Competition in Austin on October 24th and 25th, 2014. The competition focuses on administrative law and enjoys active participation from numerous Texas law schools. Judges for the competition are recruited from the private sector, agency legal staff, and the judiciary. Justices from the Third Court of Appeals judge the final round. Pictured (L to R, back row) are Former Chief Justice J. Woodfin "Woodie" Jones, Justice Jeff Rose, Justice Melissa Goodwin and (L to R, front row) championship winners Stephen Bachran and Bianca Frisaura from St. Mary's University School of Law.