

The Lawyer's Ethical and Legal Duties to protect Private Information



Claude E. Ducloux
Attorney At Law

Board Certified | Texas Board of Legal Specialization
Civil Trial Law | Civil Appellate Law

Director of Education – Law Pay

Austin Bar Video Series – Sponsored by Law Pay

Sources of Authority:

- **Ethical References:**

Rule 1.05, Texas Disciplinary Rules of Professional Conduct

Rule 503, Texas Rules of Evidence “Lawyer-Client Privilege”

How to Define it: What is:

“Privileged Information?” – everything your client tells you!

“Unprivileged Information?” – what client allows you to reveal, or law requires you reveal.

Exceptions to Confidentiality - Ethical Rules:

What is a lawyer's duty under Texas Family Code
§ 261.001 or § 261.401 (defining) for child abuse? .

TFC § 261.109 is the penalty for failure to report.

Texas Human Resources Code § 48.002 (elder abuse)?

THRC § 48.052 is penalty for failure to report.

TRDPC Rule 1.05(c) Exceptions to confidentiality. Crime,
likelihood of serious bodily harm or fraud?

Look at Exceptions to **Rule of Evidence 503 (d)**:

To prevent crime or fraud; claiming through same decedent;

Breach of duty between Client and Lawyer or vice-versa.

Rule 1.05 (c) also allows you to reveal confidences in two special situations:

(5) to defend yourself in a dispute between lawyer and the client;

(6) to establish a defense to a criminal charge, civil claim or disciplinary complaint against lawyer “or the lawyer’s associates” based upon conduct or claims by the client.

You may reveal UNPRIVILEGED (*huh?*) information to carry out representation effectively, or defend yourself, etc. Rule 1.05 (d)

Rule 21c, “Privacy Protection for Filed Documents”

Effective Jan. 1, 2014 under the Texas Rules of Civil Procedure

RULE 21c. PRIVACY PROTECTION FOR FILED

DOCUMENTS. (a) Sensitive Data Defined. Sensitive data consists of: (1) a driver's license number, passport number, social security number, tax identification number, or similar government-issued personal identification number; (2) a bank account number, credit card number, or other financial account number; and (3) a birth date, a home address, and the name of any person who was a minor when the underlying suit was filed.

(b) Filing of Documents Containing Sensitive Data Prohibited.

Unless the inclusion of sensitive data is specifically required by a statute, court rule, or administrative regulation, an electronic or paper document, except for wills and documents filed under seal, containing sensitive data may not be filed with a court unless the sensitive data is redacted.

(c) Redaction of Sensitive Data; Retention Requirement. Sensitive data must be redacted by using the letter "X" in place of each omitted digit or character or by removing the sensitive data in a manner indicating that the data has been redacted. The filing party must retain an unredacted version of the filed document during the pendency of the case and any related appellate proceeding.

(d) Notice to Clerk. If a document must contain sensitive data, the filing party must notify the clerk by:

(1) designating the document as containing sensitive data when the document is electronically filed; or

(2) if the document is not electronically filed, by including, on the upper left-hand side of the first page, the phrase: "NOTICE: THIS DOCUMENT CONTAINS SENSITIVE DATA."

(e) Non-Conforming Documents. [The clerk may not refuse to file a document that containing sensitive data, but give you a deadline to correct.]

§ 501.001 of the Texas Business and Commerce Code: CERTAIN USES OF SOCIAL SECURITY NUMBER PROHIBITED.

(a) A person, other than a government or a governmental subdivision or agency, may not:

(1) intentionally communicate or otherwise make available to the public an individual's social security number;

(2) display an individual's social security number on a card or other device required to access a product or service provided by the person;

(3) require an individual to transmit the individual's social security number over the Internet unless:

(1) the Internet connection is secure; or

(2) the social security number is encrypted;

Bus & Comm Code Section 501 (cont'd)

(4) require an individual's social security number for access to an Internet website unless a password or unique personal identification number or other authentication device is also required for access; or

(5) except as provided by Subsection (f), print an individual's social security number on any material sent by mail, unless state or federal law requires that social security number to be included in the material.

Added Sections provide penalties of up to \$500 per offense.

Chapter 181 of Texas Health and Safety Code “Medical Records Privacy

Primary Statutes:

- HIPAA: Health Information Privacy and Accessibility
- HITECH: stands for Health Information Technology for Economic and Clinical Health (2009)
- “Omnibus Rule” (2013) protecting patients’ health data

Chapter 181 Tx H. & S. Code, cont'd

“Covered Entity:” the new conundrum;

Are Lawyers “Covered Entities” subject to the Act?

You may be if:

- a. You collect or store PHI;
- b. You come into possession of PHI;
- c. Obtain or store PHI, or your are an employee of somebody who does any of the above.

NOW WHAT DO YOU NEED TO DO?

(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.

(2-a) "Disclose" means to release, transfer, provide access to, or otherwise divulge information outside the entity holding the information.

- What training is required?
- What can happen if you do it wrong?
- Injunctive relief and civil penalties, see
§ 181.201(a)
- Can you be subject to disciplinary action? See
§ 181.201(b)

Sec. 181.003. SOVEREIGN IMMUNITY. This chapter does not waive sovereign immunity to suit or liability.

Sec. 181.051. PARTIAL EXEMPTION. Except for Subchapter D, this chapter does not apply to:

- (1) [Insurance policies]
- (2) [entities created under Article 5.76-3, Insurance Code]; or
- (3) an employer.

Sec. 181.052. PROCESSING PAYMENT TRANSACTIONS BY FINANCIAL INSTITUTIONS.

[Entities who process payments, wages, benefit plans, financial institutions handling medical payments, reports TO credit reporting agencies; and complying with civil or criminal subpoena or a federal or state law]

- Sec. 181.056. AMERICAN RED CROSS. ...to provide biomedical services, disaster relief, disaster communication, or emergency leave verification services for military personnel.
- Sec. 181.057. INFORMATION RELATING TO OFFENDERS WITH MENTAL IMPAIRMENTS. This chapter does not apply to an agency described by Section [614.017](#) with respect to the disclosure, receipt, transfer, or exchange of medical and health information and records relating to individuals in the custody of an agency or in community supervision.

In family law cases, we normally “redact” by only listing the last four numbers of an account.

Social Security number xxx-xx-1234

Driver’s license number xxxxx1234

Bank account number x1234

Credit Card account x1234

QDROS: If an order is required to divide a retirement account, the order will not include sensitive information such as a social security number and the sensitive information will be sent to the plan administrator in a separate document.

- **Travis County: 512.854.9457**
- Do the clerks put e-filed documents online?
 - Yes, but **only attorneys** who have (free) subscription to Travis County Access can view them online;
 - However, **anyone who pays the fee** In-person may copy records/pay for records (even if “sensitive)

Bexar County, Nueces and Williamson are very similar:

- E-filed documents are generally NOT AVAILABLE except to case parties;
- If case is sealed, only case parties/attorneys (must see the supervisor).
- If not sealed, then anyone can search in-person or online by name, cause number, etc. **However**, you will only see a description/title - not the actual documents in Bexar County.
- **HOWEVER:** In Nueces & Williamson: CAN get documents if you come in person, even if “sensitive”

How to Keep PHI, and Other Sensitive Issues Private:

1. READ TRCP Rule 21C
2. Include in Client intake sheet and/or Client contract language regarding a lawyer's duty to report child abuse or elder abuse.
3. Have a Written Privacy Policy which Clients Acknowledge
4. Train Staff on Privacy Issues

PRIVACY POLICY AS TO SOCIAL SECURITY NUMBERS AND OTHER PRIVATE INFORMATION

- 1. SOCIAL SECURITY NUMBERS AND DRIVER'S LICENSE NUMBERS ARE ONLY USED AS NEEDED AND AS REQUIRED BY LAW.**
- 2. THESE PRIVATE NUMBERS ARE USED TO IDENTIFY PARTIES WHETHER FOR INITIAL SERVICE OF COURT DOCUMENTS, FOR CERTAIN COURT ORDERS, IN REQUIRED REPORTS FILED WITH THE STATE OF TEXAS, OR FOR OTHER REQUIRED PURPOSES.**
- 3. THESE PRIVATE NUMBERS RECEIVED FROM A CLIENT ARE CONFIDENTIAL, AND ARE NOT RELEASED FROM THE FIRM UNLESS AUTHORIZED BY THE CLIENT OR REQUIRED BY LAW**
- 4. THE EMPLOYEES OF THE FIRM HAVE ACCESS TO THIS PERSONAL INFORMATION.**
- 5. EVERY STEP IS TAKEN TO PROTECT YOUR PRIVACY. THIS INFORMATION IS KEPT SECURE WITHIN THE OFFICE OF THE FIRM IN FOLDERS, FILE DRAWERS AND COMPUTERS, UNTIL SUCH TIME THAT THE FILE INFORMATION IS RETIRED AND THE FILE REMOVED TO STORAGE IN COMPUTER FILES OR A LOCKED, OFF-SITE STORAGE FACILITY. THE CLIENT INFORMATION WILL EVENTUALLY BE SHREDDED OR OTHERWISE DELETED.**

I ACKNOWLEDGE THAT I HAVE READ THE ABOVE PRIVACY POLICY AND AGREE TO IT.

CLIENT SIGNATURE

DATE

Rule 1.05(b) is the general rule that a lawyer shall not reveal confidential information or use confidential information unless the client consents, nor use confidential information of a former client or use privileged information of a client for the advantage the lawyer or a third person, unless the client consents.

Rule 1.05(e) mandates disclosure: When a lawyer has “. . . information clearly establishing that a client is likely to commit a **criminal or fraudulent act that is likely to result in death or substantial bodily harm to a person**, the lawyer shall reveal confidential information to the extent revelation reasonably appears necessary to prevent the client from committing the criminal or fraudulent act.”

What do you need to do before you reveal confidential information?

Rule 1.02(d) requires the lawyer to make reasonable efforts to dissuade the client from committing the crime or fraud.

Same for corporate counsel. Must go “up the ladder” when you discover fraud

If Client refuses? “The Noisy Withdrawal”

What is our “Takeaway?”

- Be aware of the Rules and Statutes
- Institute Written policies for Sensitive Information
- Train your staff on those Policies
- Observe confidentiality
- Communicate policies to Clients