Electronic Discovery (and Privacy Issues)

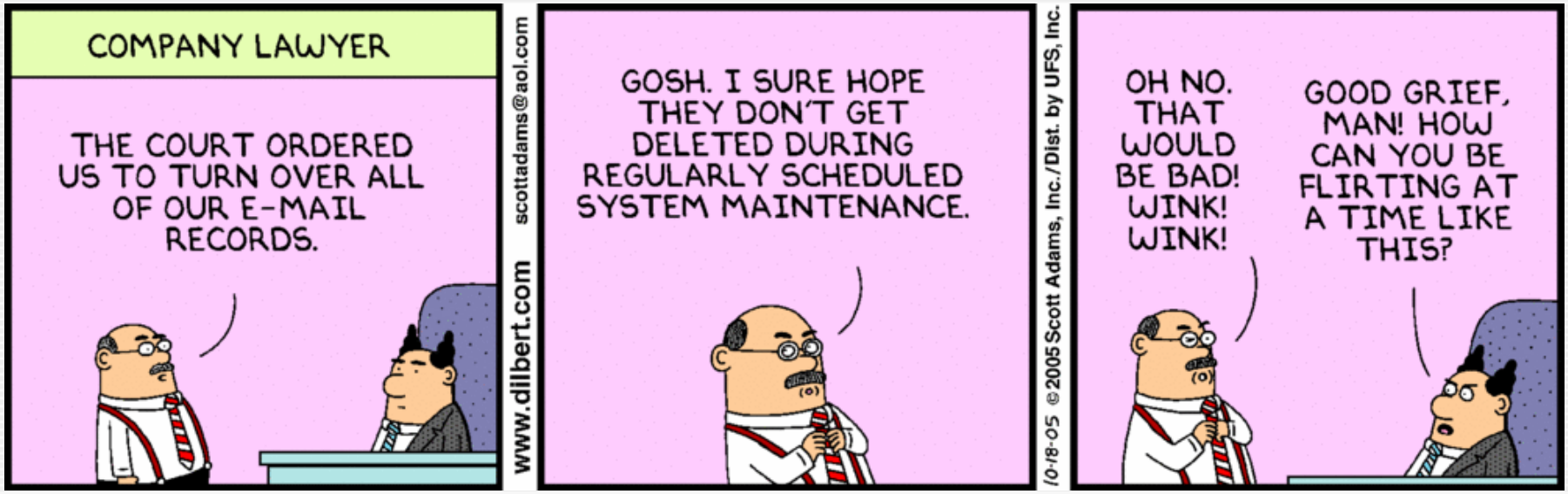
AMY DASHIELL

SCOTT DOUGLASS & MCCONNICO LLP

ROBERT SCHMIDT

CREWS LAW FIRM, P.C.

ELECTRONIC DISCOVERY



E- Discovery under the Texas Rules

TEX. R. C. P. 196.4

- To obtain discovery of data or information that exists in electronic or magnetic form, the requesting party **must** specifically request production of electronic or magnetic data **and** specify the form in which the requesting party wants it produced.
- The responding party **must** produce the electronic or magnetic data that is responsive to the request and is reasonably available to the responding party in its ordinary course of business.
- If the responding party cannot--through reasonable efforts--retrieve the data or information requested, the responding party **must** state an objection complying with these rules.

In re Weekley Homes, 295 S.W.3d 309 (Tex. 2009): Setting the standard for e-discovery

- "Texas Rule of Civil Procedure 192.3(b) provides for discovery of documents, defined to include electronic information that is relevant to the subject matter of the litigation." (Information may be inadmissible at trial as long as the information is reasonably calculated to lead to the discovery of admissible evidence.)

- "Rule 196 governs requests for production of documents, and Rule 196.4 applies specifically to requests for production of 'data or information that exists in electronic or magnetic form.'"

- "Emails and deleted emails storing in electronic or magnetic form . . . [a]re clearly 'electronic information.' . . . Accordingly, we look to Rule 196.4 in analyzing [plaintiff's] requests."

In re Weekley: Proper Rule 196.4 procedure

- Party seeking to discover electronic information must make a **specific request** for that information and **specify the form of production**. TEX. R. CIV. P. 196.4.
- The responding party must then produce any electronic information that is "responsive to the request and . . . **reasonably available** to the responding party in its ordinary course of business." *Id.*
- If "the responding party cannot-through **reasonable efforts**-retrieve the data or information requested or produce it in the form requested," the responding party **must object** on those grounds. *Id.*

In re Weekley procedure, part 2

- The parties should make reasonable efforts to resolve the dispute without court intervention. TEX. R. CIV. P. 191.2.
- If the parties are unable to resolve the dispute, either party may request a hearing on the objection, TEX. R. CIV. P. 193.4(a), at which **the responding party must demonstrate that the requested information is not reasonably available** because of undue burden or cost, TEX. R. CIV. P. 192.4(b).
- If the trial court determines the requested information is not reasonably available, the court may nevertheless order production upon a showing by the requesting party that **the benefits of production outweigh the burdens imposed**, again subject to Rule 192.4's discovery limitations.

In re Weekley procedure, part 3

- If the benefits are shown to outweigh the burdens of production and the trial court orders production of information that is not reasonably available, sensitive information should be protected and the **least intrusive means** should be employed. TEX.R. CIV. P. 192.6(b).
- The **requesting party must also pay the reasonable expenses** of any **extraordinary** steps required to retrieve and produce the information. TEX.R. CIV. P. 196.4.
- Finally, when determining the means by which the sources should be searched and information produced, **direct access to another party's electronic storage devices is discouraged**, and courts should be extremely cautious to guard against undue intrusion.

In re Weekley Homes: Guidance re: requesting deleted emails

Deleted Emails:

- "Rule 196.4 requires specificity, and [plaintiff] did not specifically request deleted emails."
- "To ensure compliance with the rules and avoid confusion . . . parties seeking production of deleted emails should expressly request them."
- "Because [plaintiff] did not initially specifically request deleted emails as Rule 196.4 requires, [defendant] had no obligation to object in its response that deleted emails were not 'reasonably available' . . . in its ordinary course of business."

In re Weekley:
Practice tips

- "[P]rior to promulgating requests for electronic information, parties and their attorneys should share relevant information concerning **electronic systems and storage methodologies** so that agreements regarding protocols may be reached or, if not, trial courts have the information necessary to craft discovery orders that are not unduly intrusive or overly burdensome."
- "The critical importance of learning about relevant systems early in the litigation process is heavily emphasized in the federal rules. Due to the 'volume and dynamic nature of electronically stored information,' **failure to become familiar with relevant systems early on can greatly complicate preservation issues, increase uncertainty in the discovery process, and raise the risk of disputes**."

In re Weekley: Direct access to devices is discouraged

- "Providing access to information by ordering examination of a party's electronic storage device is particularly intrusive and should be generally discouraged, just as permitting open access to a party's file cabinets for general perusal would be."

- "HFG's conclusory statements that the deleted emails it seeks 'must exist' and that deleted emails are in some cases recoverable is not enough to justify the highly intrusive method of discovery the trial court ordered, which afforded the forensic experts 'complete access to all data stored on [the Employees'] computers.'"

- "Direct access to a responding party's electronic storage devices is more likely to be appropriate 'when there is some direct relationship between the electronic storage device and the claim itself.'"

MRT, Inc. v Vounckx, 299 S.W.3d 500 (Tex. App.—Dallas 2009, no pet.): A cautionary tale

- "[A]ppellants requested certain 'documents,' which was defined to include 'any computer-generated, computer-stored, or electronically-stored matter ...."

- "[T]he parties here did not exchange information about their electronic systems and, not surprisingly, had different expectations of what the various requests for electronic discovery entailed, resulting in much confusion and multiple discovery motions before the trial court.

Oops

- "Appellants did not request the production of or refer specifically to backup tapes in their requests for production" and "the parties did not exchange information about their electronic systems or storage methodologies."
- "At depositions…appellants' counsel learned of IMEC's computer backup tapes."
- "IMEC…indicated that all backup tapes existing before 2000 had been destroyed."
- Plaintiff "filed a motion seeking a spoliation instruction based on the destruction of pre-2000 backup tapes."

BUT no abuse of discretion in denying continuance and refusing to submit spoliation instruction

- "**Because [plaintiff] did not initially specifically request production of the backup tapes or documents that resided only on [defendant's] backup tapes, we conclude [defendant] had no duty to object in its responses that the backup tapes or the documents contained on them were not reasonably available**."

- "Because appellants did not meet their burden of demonstrating [defendant] knew or should have known the pre-2000 backup tapes contained material and relevant evidence with respect to their claims, they **failed to establish that [defendant] had a duty to preserve the backup tapes in question**."

In re Master Flo Valve, Inc., 2016 WL 316491 (Tex. App. – Houston [14th Dist.], n.p.h.) Keyword searches

- "An order that a party conduct certain keyword searches of its electronic files intrudes on a party's right to develop its own means of searching for responsive documents without court involvement or interference by the opposing party."
- "Absent evidence that a party has previously failed to adequately search for responsive documents, generally, a trial court should not be involved in managing how a party performs searches of its electronic data for responsive documents."

Chevron Phillips Chem. Co. LP v. Kingwood Crossroads, L.P., 346 S.W.3d 37 ((Tex. App. – Houston [14th Dist.], 2011, writ denied)

- [Defendant] shall conduct a further search of its e-mails, under the supervision of an independent third-party experienced in the discovery of electronic information, including all e-mails that may be stored on servers, back-up tapes, or otherwise. . . The expense of such search shall be borne by [Defendant]"
- Search included key word searches.
- Sanction upheld of $637,612.50 in attorneys fees.
- See ***In re Waste Mgmt. of Tex., Inc.***, 392 S.W.3d 861, 876 (Tex. App.—Texarkana 2013, n.p.h.) Fact that large amount of electronic discovery had been ordered, by itself, does not amount to an overly broad discovery order.

In Re State Farm Lloyds

(Tex. App. – 13th Dist. Corpus Christi-Edinburg, October 28, 2015) (writ pending) 2015 WL 6510647, 2015 Tex. App. LEXIS 11038

- January 8, 2016, Texas Supreme Court granted insurer's motion to stay discovery of electronically stored information pending resolution of its petition for writ of mandamus in a bad faith lawsuit.
- Questions involve production of electronic information in format requested (native or near native) or "reasonably usable format" and removal of metadata.
- Stay tuned…

E-Discovery under the Federal Rules

"Although we have not amended our rules to mirror the federal language, our rules as written are not inconsistent with the federal rules or the case law interpreting them"

- *In re Weekley*, 295 S.W.2d at 316.

Federal Meet and Confer Requirements

- F.R.C.P. 26(f) – Conference of Parties; Planning for Discovery.
  - (2) ***Conference Content; Parties' Responsibilities.*** In conferring, the parties must . . . [d]iscuss any issues about preserving discoverable information; and develop a proposed discovery plan.
  - (3) ***Discovery Plan.*** A discovery plan must state the parties' views and proposals on:
    - (C) any issues about disclosure or discovery or preservation of electronically stored information, including the form or forms in which it should be produced.
- F.R.C.P. 37(f) Failure to Participate in Framing a Discovery Plan
  - If a party or its attorney fails to participate in good faith in developing and submitting a discovery plan as required by Rule 26(f), the court may . . . require that party or attorney to pay to any other party the reasonable expenses, including attorney's fees, caused by the failure.

Electronic Document Production

- F.R.C.P. 26(b)(2)(B) – *Specific Limitations on Electronically Stored Information*.
  - A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost.
  - On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost.
  - If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C).

FRCP 26(b)(1): Scope

The 2015 Amendments place the "proportionality" language back front and center in the "Scope" definition:

(b)(1) Unless otherwise limited by court order…Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, ans whether the burden or expense of the proposed discovery outweighs its likely benefit…."

Notes to FRCP 26 Changes

- **Note 13**: "What seemed an explosion in 1993 has been exacerbated by the advent of e-discovery. The present amendment again reflects the need for continuing and close judicial involvement in the cases that do not yield readily to the ideal of effective party management."
- **Note 16**: "The burden or expense of proposed discovery should be determined in a realistic way. This includes the burden or expense of producing electronically stored information."

Attorney obligations: in 2004, Judge Scheindlin Raised the Bar for Lawyers

Zubulake v. UBS Warburg, LLC
229 FRD 422 (S.D.N.Y. 2004)

Zubulake

- 5 opinions in a case Judge Scheindlin described as "a relatively routine employment discrimination dispute in which discovery has now lasted over two years."
- "Early in the litigation, UBS's counsel – both in-house and outside – instructed UBS personnel to retain relevant electronic information. Notwithstanding these instructions, certain UBS employees deleted relevant emails. Other employees never produced relevant information to counsel."

Obligations Outlined in *Zubulake*

- Addresses "**counsel's obligation** to ensure that relevant information is preserved by giving clear instructions . . . and, perhaps more importantly, a client's obligation to heed those instructions."
- "When communication between counsel and client breaks down, conversation becomes 'just crossfire,' and there are usually casualties."
- "Once a party reasonably anticipates litigation, it **must suspend** its routine document retention/destruction policy and put in place a 'litigation hold' to ensure the preservation of relevant documents."

Continuing Obligations

- **"A party's discovery obligation does not end with the implementation of a 'litigation hold'-to the contrary, that's only the beginning."**
  - "Counsel must become fully familiar with her client's document retention policies, as well as the client's data retention architecture."
  - "This will invariably involve speaking with [IT] personnel . . . [and] communicating with 'key players' in the litigation, in order to understand how they store information."

Obligation to Monitor Compliance

- **"[I]t is *not* sufficient to notify all employees of a litigation hold and expect that the party will then retain and produce all relevant information."**
  - "Counsel must oversee compliance with the litigation hold monitoring the party's efforts to retain and produce the relevant documents."
  - "Counsel must take affirmative steps to monitor compliance so that all sources of discoverable information are identified and searched."

Attorney Responsibilities

- "**First**, counsel must issue a 'litigation hold' at the outset of the litigation . . . ."
- "**Second**, counsel should communicate directly with the 'key players' in the litigation . . . ."
- "**Finally**, counsel should instruct all employees to produce electronic copies of their relevant active files . . . [and] must also make sure that all backup media . . . is identified and stored in a safe place."
- "Once counsel takes these steps (or once a court order is in place), a party is fully on notice of its discovery obligations. **If a party acts contrary to counsel's instructions or to a court's order, it acts at its own peril."**

Reasonable Conduct Redefined

- UBS Took Several Steps to Preserve Documents:
  - "UBS's in-house attorneys gave oral instructions . . . **immediately** after Zubulake filed her EEOC charge . . . instructing employees not to destroy or delete material potentially relevant to Zubulake's claims, and in fact to segregate such material into separate files for the lawyers' eventual review."
- But those actions were not enough:
  - **First**, neither in-house or outside counsel communicated the litigation hold instructions to a key employee.
  - **Second**, even though litigation hold instructions were communicated to another key employee, no one ever asked her to produce her files.
  - **Third**, counsel failed to protect relevant backup tapes.

Sanctions under F.R.C.P. 37(e)

- ***Former*** F.R.C.P. 37(e) – Failure to Provide Electronically Stored Information.
  - Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information that is lost as a result of good-faith operation of an electronic information system.

- *2015 Advisory Notes:*
  - "This limited rule has not adequately addressed the serious problems resulting from the continued exponential growth in the volume of such [electronically stored] information. Federal circuits have established significantly different standards for imposing sanctions or curative measures on parties who fail to preserve electronically stored information. These developments have caused litigants to expend excessive effort and money on preservation in order to avoid the risk of severe sanctions if a court finds they did not do enough."

New F.R.C.P. 37(e)

- *New* F.R.C.P. 37(e) – Failure to Preserve Electronically Stored Information
  - If electronically stored information that should have been preserved…is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery, the court:

    (1)upon finding prejudice to another party…may order measures **no greater than necessary** to cure the prejudice; or

    (2)only upon finding that the party acted with **the intent to deprive another party of the information's use in litigation** may:

    (A) presume the lost information was unfavorable to the party;

    (B) instruct the jury that it may or must presume the information was unfavorable to the party; or

    (C) dismiss the action or enter a default judgment.

HM Electronics, Inc. v. R.F. Technologies, Inc., 2015 WL 4714908 (S.D.Cal)

- Recommended adverse inference and monetary sanctions and stated that under new subsection (e) "the Court would reach the same result"
- Found that Defendants intentionally deleted electronic information
- **Recommended monetary sanctions against the client, the defense firm and the lawyer "personally," and an adverse inference instruction to the jury**

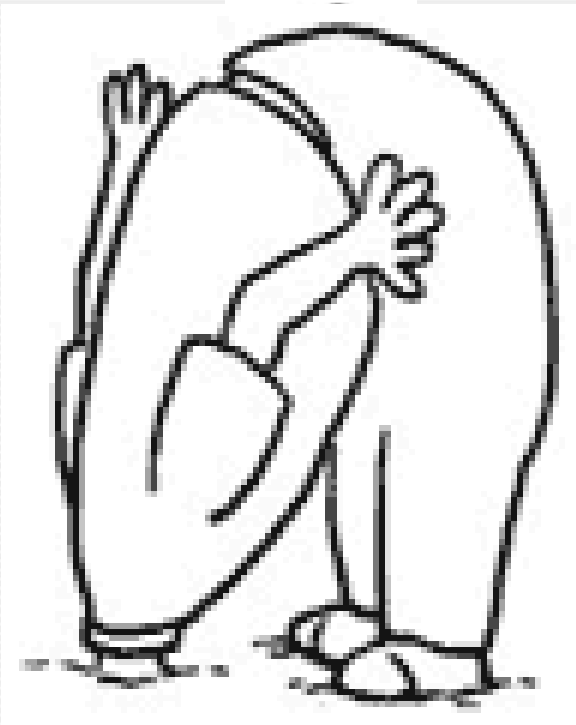
HM Electronics, cont.

- "[Defense attorneys] should have been more transparent with Plaintiff's attorneys about the data collection process and the amount of data involved…Instead of familiarizing himself with his client's ESI and embracing transparency and collaboration in the discovery process, lead counsel chose to sign false discovery responses without making any effort to assure that the responses accurately reflected the Defendant's documents.
- "It was also not reasonable to sign discovery responses denying the existence of documents based solely on [the client's] word. Asking [the client rep] and accepting his response without asking other employees or collecting or sampling documents was not reasonable."

HM Electronics, cont.

- "[A]ttorneys withheld more than 150,000 non-privileged documents as privileged even though no privilege review was conducted…[they] delegated ESI discovery to another firm, which…used 59 exclusionary search terms to withhold documents as privileged."
- "[Defense counsel] could not answer simple questions about the ESI search methodology used. Worse, he disavowed any involvement or knowledge of the search methodology…The attorneys' total abdication of their obligation to communicate the duty to preserve evidence to their clients in an effective manner warrants severe sanctions."

Electronic Discovery Best Practices



Trust But Verify

Litigation Hold Memos

- Work *with* your client to craft a litigation hold memo as soon as you agree to representation
  - Work with IT staff and key players to understand the relevant systems and policies
  - Draft an initial list of custodians, and consider initial keyword searches
  - Speake with custodians directly to determine other sources of relevant documents
  - Consider whether personal devices need to be preserved (iPhones etc.)
- Confirm receipt of and compliance with the litigation hold memo with key players and custodians
- Periodically review and, if necessary, revise or update litigation hold
  - Consider whether expansion of custodians or areas of preservation are necessary after initial investigation

IRS/Lerner Emails – a lesson to us all

Timeline

- 2011 Lerner email crashes
  - Hard drive disposed, retrieved, disposed again
- May 22, 2013 Preservation Notice from Terrence Milholland:
  - "Given the current environment and ongoing investigations, until further notice, do not destroy/wipe/reuse any of the existing backup tapes for email…of any IRS employees….In other words, retain everything to do with email…"
- Yet in March 2014, 422 backup tapes were "degaussed"
- Milholland stated he was "blown away" when he learned of the destruction

Drafting Discovery

- Prior to sending any request, engage in communication with opposing counsel regarding the universe of documents and systems
- Be specific regarding both the request itself and the form requested
- Consider whether to use interrogatories or other discovery methods to gain information on sources of electronic information

Basic Interrogatories

INTERROGATORY NO. For ____ or any person who participated in the decision to terminate Plaintiff, identify:

(a) whether that person drafted, created, sent or received any electronic documents (including text messages, emails, word processing documents, instant messaging, chat, etc.) relating to the Plaintiff's termination of employment;

(b) each computer, device or email account/address on which the electronic documents were created;

(c) all actions taken to locate and preserve electronic documents of that person;

(d) any electronic documents drafted or received by that person have not been produced in response to Plaintiffs' requests for production of documents, and the reason the document was not produced.

INTERROGATORY NO. Identify and describe all actions taken to locate and preserve all documents (including electronic documents, emails, text messages) relating to Plaintiff's performance, termination of employment, and Plaintiff's requests for production of documents.

Corporate Representative Depositions

PLEASE TAKE NOTICE that on Tuesday, February 16, 2016, at 9:00 a.m. and continuing thereafter from day to day until completed, Plaintiff will take the oral deposition of the **designated representative(s) for Defendant** pursuant to Rule 199.2(b) of the Texas Rules of Civil Procedure/30(b)(6) of the Federal Rules of Civil Procedure in the law offices of _____.

The designated representative(s) for Defendant will be examined regarding:

(1) **Defendant's efforts/actions to locate and preserve documents relating to Plaintiff's termination, this lawsuit and/or that have been requested in Plaintiff's discovery requests**.

Responding to RFPs

- Pay attention to requests and follow the proper procedure for objections to *form* of production
  - What if no form specified?
- Keyword searches: work with opposing counsel to reach agreement on custodians and scope of search
  - If necessary, run test searches and refine as needed
  - Keep track of all searches and results
  - As with litigation hold, reevaluate after initial discovery to determine if additional searches are necessary

Miscellaneous

- Text Messages
  - A recent survey found that 79% of respondents used text messaging for business purposes
- Social Media
  - Discovery issues
  - Evidentiary issues
- Third Party vendors
  - Experience?
  - Increased use?

WHY IS COMPLYING WITH ELECTRONIC DISCOVERY RULES IMPORTANT?

- ETHICAL RULES – DUTY OF HONESTY… CASES TO BE DECIDED BY TRUTH
- SANCTIONS
- SPOLIATION (*See Brookshire Bros., Ltd. v. Aldridge*, 438 S.W.3d 9 (Tex. 2014))
- IMPACT ON JURY
- COST

HIPAA, TMRPA and ITEPA

HEALTH INSURANCE PORTABILITY
AND ACCOUNTABILITY ACT
PASSED IN 1996

TEXAS MEDICAL RECORDS PRIVACY ACT
EFFECTIVE 9-1-2012

IDENTITY THEFT ENFORCEMENT
AND PROTECTION ACT
EFFECTIVE 4-1-2009

HIPAA Facts

- U.S. Dept. of Health and Human Services is responsible for adopting rules to help patients and "other health care providers" keep personal information private.
- Goal is to protect from unauthorized disclosure "personally-identifiable health information" called "protected health information" or "PHI"
- HIPAA applies to "covered entities" and "business associates" of covered entities

How does HIPAA affect law firms?

- A Covered Entity may disclose PHI only pursuant to a HIPAA-compliant authorization.
  - Requirements set forth in 45 CFR 164.508(c)
  - Make sure your Authorization is HIPAA compliant
- *Ex parte* contact with treating physician, without authorization, may violate HIPAA.
- If your firm represents a "Covered Entity," you may have obligations as a "Business Associate."

How does HIPAA affect litigants?

- Where a covered entity is a party to a lawsuit, the covered entity may use/disclose protected health information for purposes of litigation.
- **45 CRF 164.501** exception for a covered entity's activities of conducting or arranging for legal services.
- "A covered entity that is a defendant in a malpractice action or a plaintiff in a suit to obtain payment may use or disclose protected health information for such litigation."
- Reasonable efforts to limit such uses and disclosures to the minimum necessary.

TMRPA Facts

- Broader in scope than HIPAA because it applies to any organization that obtains PHI, not just Covered Entities
  - Tex. Health & Safety Code 181.001(b) (2) defines "covered entity" to include "any person who…comes into possession of protected health information."
- Contains a training requirement:
  - Tex. Health & Safety Code 181.101 requires: "Each covered entity shall provide training to employees of the covered entity regarding the state and federal law concerning protected health information as necessary and appropriate for the employees to carry out the employees' duties for the covered entity."

ITEPA Facts

- Includes information related to “the physical or mental health or condition of the individual” as “sensitive personal information.” Tex. Bus. & Comm. Code 521.002
- Imposes on businesses a duty to protect such information
- Contains a disclosure requirement following a breach of security involving such information

ITEPA Duties

- Sec. 521.052. BUSINESS DUTY TO PROTECT SENSITIVE PERSONAL INFORMATION.

  (a) A business shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business.

  (b) A business shall destroy or arrange for the destruction of customer records containing sensitive personal information within the business's custody or control that are not to be retained by the business by:

  (1) shredding;

  (2) erasing; or

  (3) otherwise modifying the sensitive personal information in the records to make the information unreadable or indecipherable through any means.

ITEPA Notification Requirement

- Sec. 521.053(b)
  - "A person who conducts business in this state and owns or licenses computerized data that includes sensitive personal information shall disclose any breach of system security, after discovering or receiving notification of the breach, to any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made as quickly as possible, except as provided by Subsection (d) or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system."

Best Practices

- Obtain PHI through valid authorization or court order
- Address PHI in Protective Order
- Evaluate in-house security measures and train staff
  - Do not email documents containing PHI
  - De-identify or redact information if possible
  - Protect and limit access, including assess through phones etc.
- Be careful what you file
- Have destruction policies in place that safeguard PHI