

THE CONSUMER WORKGROUP

LEGAL ANALYSIS

ON

MEDICAL PRIVACY ISSUES

PREPARED FOR THE

HEALTH INFORMATION TECHNOLOGY ADVISORY COMMITTEE,
(HITAC)

PREPARED BY:

PETER MACKOUL, ESQ.

HIPAA SOLUTIONS, LC
130 INDUSTRIAL BOULEVARD, SUITE 130
SUGAR LAND, TEXAS, 77478

DRAFT VERSION 1.2 JUNE 30, 2006

TABLE OF CONTENTS

1	EXECUTIVE SUMMARY	4
2	BACKGROUND INFORMATION.....	6
3	THE UNITED STATES CONSTITUTION & THE RIGHT TO PRIVACY.....	6
3.1	THE 5 TH CIRCUIT FEDERAL COURT OF APPEALS & THE RIGHT TO PRIVACY.....	6
3.1.1	<i>Background Information</i>	7
3.1.1.1	Federal Case Law, Documenting & Defining Legal Barriers & Challenges to HIE	8
3.1.1.2	The Connection Between The Right to Privacy & Medical Records	10
3.1.1.2.1	The Federal Constitutional Standard of Review	11
3.1.1.2.1.1	Additional Information on the Westinghouse Case.....	12
3.1.1.2.1.1.1	The 5 th Circuit & The Standard of Review in Texas	14
3.2	ANALYSIS	15
3.3	RECOMMENDATIONS	17
3.4	HIPAA AND THE CONSTITUTIONAL RIGHT TO PRIVACY IN MEDICAL RECORDS.....	19
3.4.1	<i>The Federal Application of the Sunderland case in Louisiana</i>	23
3.4.1.1	Other Federal cases within the 5 th Circuit that Merit Attention	25
3.5	ANALYSIS	29
3.6	RECOMMENDATIONS	29
4	THE STATE OF TEXAS & THE CONSTITUTIONAL RIGHT TO PRIVACY.....	33
4.1	ANALYSIS:	34
4.2	RECOMMENDATIONS:	34
4.3	HIPAA & THE APPELLATE COURTS IN TEXAS	35
4.3.1	<i>Analysis of the Abbott v. the Texas Department of Mental Health and Mental Retardation, case, 2006 WL 1649003, no other citation currently available.</i>	36
4.3.1.1	Analysis of the Abbott Case including Recommendations.....	36
4.3.1.2	The Specific Holding as it Relates to Medical Information in the Abbott case.	41
4.3.2	<i>Summary of Recommendations</i>	44
4.4	ANALYSIS	46
4.5	RECOMMENDATIONS	46
5	THE CONSUMER WORKGROUP METHODOLOGY DEFINED	47
5.1	INFORMATION GATHERING	47
5.1.1	<i>The first requirement or "charge" states:</i>	47
5.2	RESULTS	48
5.3	METHODOLOGY EMPLOYED ON FIRST DELIVERABLE.....	48
5.4	RECOMMENDATIONS:	49
5.4.1	<i>The second charge or requirement states:</i>	49
5.5	METHODOLOGY EMPLOYED ON THE SECOND DELIVERABLE	49
5.6	RECOMMENDATIONS	50
5.6.1	<i>The Third Charge or Requirement States:</i>	50
5.7	METHODOLOGY EMPLOYED ON THE THIRD DELIVERABLE.....	50
5.8	RECOMMENDATIONS	50
6	APPLICATION OF THE METHODOLOGY TO THE INFORMATION GATHERED.....	50
6.1	INTRODUCTION.....	50
6.2	APPLICATION OF "METHODOLOGY" TO THE FIRST DELIVERABLE:	51
6.2.1	<i>Question Presented:</i>	51
6.2.1.1	Response:	51
6.2.1.2	Categorization: (Real or Perceived Barrier)	51
6.2.1.3	Legal Justification	52
6.2.1.4	Recommendation.....	54

6.2.2	Question Presented.....	58
6.2.2.1	Response.....	58
6.2.2.2	Categorization, (Real or Perceived Barriers).....	58
6.2.2.3	Legal Justification.....	59
6.2.2.4	Recommendation.....	60

1 EXECUTIVE SUMMARY

The purpose of this document is to provide the reader with a clear understanding of the *“real and perceived legal, regulatory and business barriers that could hinder participation in health information exchange.”* A methodology was developed to assist the reader in understanding these barriers. This methodology produced recommendations based on input from stakeholders.

The law impacting *“Health Information Technology”* (HIT), and *“Health Information Exchange,”* (HIE), ranges from the need to comply with complex regulatory compliance schemes to individual constitutional rights. For example, the 5th Circuit Court of Appeals has ruled that individuals have a “constitutional right to privacy” in their medical records. The Supreme Court of the State of Texas also recognizes this same individual right for citizens in the State of Texas. There are a myriad of laws on the State and Federal levels affecting HIT and HIE.

A specific methodology was developed to fulfill the responsibilities of the Consumer Work Group. That work flow is outlined and applied in this document to produce specific recommendations based on information gathered from stakeholders. Stakeholders consist of public and private entities, including healthcare providers, schools and universities.

This document provides recommendations based on federal and state statutory, regulatory, and constitutional law. These findings indicate the complexity associated with the legal barriers impacting HIE and HIT.

Finally this document is a work in progress; additional information will be provided in the final version.

A Note to the Reader

The information contained in this document is meant for informational purposes only and not intended to act as a substitute for the advice of an attorney.

Please contact appropriate legal counsel before acting on any of the information contained in this document.

Finally case law in this area is constantly changing; this document represents current holdings.

2 BACKGROUND INFORMATION

The Consumer workgroup is responsible for *“documenting real and perceived legal, regulatory and business barriers that could hinder participation in health information exchange.”* The workgroup is also responsible for *“defining legal challenges that all states encounter with respect to federal regulations;”* and *“documenting specific Texas regulations and policies that might impact the adoption of Health Information Technology, (HIT), and Health Information Exchange, (HIE).”*

In order to fulfill these responsibilities a “methodology” was developed to produce credible recommendations based on specific legal requirements utilizing information gathered from responsible stakeholders.

All three of these responsibilities involve both the United States Constitution and the Constitution of the State of Texas. For example, the U.S. constitution presents some *“real legal barriers that could hinder participation in health information exchange.”* These federal constitutional barriers will be *“defined as challenges that affect the State of Texas;”* also, specific *“Texas constitutional barriers will be defined that may impact the adoption of HIT and HIE.”*

These constitutional barriers will be documented and defined before presenting the methodology approved by the Health Information Technology Advisory Committee, or HITAC. Practical recommendations will be offered to assist the HITAC and State Legislature in handling these complex issues. There are hundreds of federal and state laws that impact HIT and HIE; however the most significant are constitutional in nature; thus must be dealt with first and should be considered significant.

3 THE UNITED STATES CONSTITUTION & THE RIGHT TO PRIVACY

The privacy of medical information involves “constitutional issues” on both the federal and state levels affecting all citizens and organizations in the State of Texas. After defining these challenges, analysis will follow explaining how they could hinder participation in HIE.

Although there are numerous specific state and federal laws that regulate medical privacy, the 5th Circuit Court of Appeals, (affecting the State of Texas), has placed the idea of medical privacy in a category deserving constitutional protection through its ruling in the legal process.

3.1 THE 5TH CIRCUIT FEDERAL COURT OF APPEALS & THE RIGHT TO PRIVACY

3.1.1 BACKGROUND INFORMATION

Seventy eight years ago, Mr. Justice Brandies wrote in a dissenting opinion that *“the makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the government, the right to be let alone-the most comprehensive of rights and the right most valued by civilized men. To protect, that right, every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.”*¹

The phrase the *“the right to be let alone the most comprehensive of rights and the right most valued by civilized men”* appeared in Plante v. Gonzalez,² a Fifth Circuit Federal Court of Appeals decision, (hereinafter referred to as the 5th Circuit). That case provided precedent³ for the application of the U.S. Supreme Court decision in Whalen v. Roe⁴ that provided the *“strand of privacy”* defined as protecting medical information.

Defining *“barriers and challenges”* requires a determination of whether the ‘privacy’ of

¹ Olmstead v. United States, 1928, 277 U.S. 438, 478, 48 S.Ct. 564, 572, 72 L.Ed. 944

² Plante v. Gonzalez, 575 F.2d 1119, (5th Cir. 1978) at page 1127 (see footnote 13).

³ **Precedent:** a prior reported opinion of an appeals court which establishes the legal rule (authority) in the future on the same legal question decided in the prior judgment. See also **Stare decisis:** (stah-ree duh-sigh-sis) n. Latin for "to stand by a decision," the doctrine that a trial court is bound by appellate court decisions (precedents) on a legal question which is raised in the lower court. Reliance on such precedents is required of trial courts until such time as an appellate court changes the rule, for the trial court cannot ignore the precedent (even when the trial judge believes it is "bad law"). For example see: or LA Chem v. Bingham, or 550 F.Supp. 1136, wherein the District Court applied Whalen to their decision.

⁴ Whalen v. Roe, 429 U.S. 589, (U.S. Sct. 1977)

medical information involves rights that may be classified as fundamental or “*implicit in the concept of ordered liberty.*” For example as the Federal 3rd Circuit Court of Appeals stated in Doe v. Southeastern Pennsylvania Transportation Authority, (SEPTA), 72 F.3rd 1133, (3rd Cir. 1995), (certiorari denied by Doe v. Southeastern Pennsylvania Transp. Authority, 519 U.S. 808), at 1134, “*This appeal requires that we probe the depth and breadth of an employee's conditional right to privacy in his prescription drug records.*” Also, “*As a preliminary matter, this court must decide if a person's medical prescription record is within the ambit of information protected by the Constitution.*” Id at 1137.

A note to the reader, the 5th Circuit has relied upon certain 3rd Circuit Court of Appeals decisions in this area of the law, thus justifying the use of the Doe case. The U.S. Supreme Court denied a “*writ of certiorari*”⁵ in Doe thus stating that the lower court's ruling, or the 3rd Circuit Court's ruling shall stand. Case law or decisions from the 5th Circuit represent the law that all individuals and organizations in Texas, Louisiana, and Mississippi must follow. Consequently, special attention will be given to the decisions of that court and all associated district courts that affect the States of Texas, Louisiana and Mississippi. Specific legal justification will be presented for considering other federal circuit and district court rulings.

3.1.1.1 FEDERAL CASE LAW, DOCUMENTING & DEFINING LEGAL BARRIERS & CHALLENGES TO HIE

⁵ **Certiorari** n. (sersh-oh-rare-ee) a writ (order) of a higher court to a lower court to send all the documents in a case to it so the higher court can review the lower court's decision. Certiorari is most commonly used by the U.S. Supreme Court, which is selective about which cases it will hear on appeal. To appeal to the Supreme Court one applies to the Supreme Court for a writ of **certiorari**, which it grants at its discretion and only when at least three members believe that the case involves a sufficiently significant federal question in the public interest. By denying such a writ the Supreme Court says it will let the lower court decision stand, particularly if it conforms to accepted precedents (previously decided cases).

The 5th Circuit has addressed the issue of whether or not a “right to privacy” exists in relation to medical information in the National Treasury Employees Union v. U.S. Department of Treasury case, or 25 F. 3rd 237, (5th Cir. 1994).

For example, that court stated, referring to U.S. Supreme Court and the 3rd Circuit Court of Appeals cases, as follows: *“Although the constitutional right to privacy remains largely undefined, there are at least two clear strands of privacy interests that have been addressed by the courts. Whalen v. Roe, 429 U.S. 589, 598-99, 97 S.Ct. 869, 876, 51 L.Ed.2d 64 (1977). The particular right asserted here is the “individual interest in avoiding disclosure of personal matters,” id., which is properly called the right to confidentiality. Plante v. Gonzalez, 575 F.2d 1119, 1132 (5th Cir.1978). In addressing the merits of an individual’s right to confidentiality claim, a court must weigh the government’s interest in disclosure against the individual’s privacy interest. Woodland v. City of Houston, 940 F.2d 134, 138 (5th Cir.1991); Fraternal Order of Police, Lodge 5 v. City of Phila., 812 F.2d 105, 110 (3d Cir.1987); see Plante, 575 F.2d at 1134.” National Treasury Employees Union v. U.S. Department of Treasury 25 F. 3rd 237at 242.*

The court cited several significant cases including a Supreme Court case or Whalen v. Roe. Whalen was analyzed by the 5th Circuit in Plante v. Gonzales, 527 F 2nd 1119, (5th Cir. 1978). In the Plante case the court made a very clear statement that the 5th Circuit recognizes the “right to privacy.” The court stated: *“Americans have a constitutional right to privacy. The right springs from several of the Bill of Rights amendments, and is incorporated in the due process protected by the fourteenth amendment. Griswold v. Connecticut, 1965, 381 U.S. 479, 85 S.Ct. 1678, 14 L.Ed.2d 510. Academic discussion of a right to privacy dates at least to the common law arguments of Louis Brandeis and Samuel Warren in 1890. Brandeis and Warren, The Right to Privacy, 4 Harv.L.Rev. 193 (1890).” Plante at 1127.*

Justice Brandies characterized the “Right to Privacy” as the *“the right to be let alone the most comprehensive of rights and the right most valued by civilized men,” Plante at 1127.* See also, Olmstead v. United States, 1928, 277 U.S. 438, 478, 48 S.Ct. 564, 572, 72 L.Ed. 944.” In the Plante decision, the 5th Circuit described the right to privacy *“involving at least two different kinds of interests.” Id. at 1128.* The court stated, *“The cases sometimes characterized as protecting ‘privacy’ have in fact involved at least two different kinds of interests. One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions.” Id. at 1128.* The court went onto restate the first “strand” of the right to privacy citing Whalen v. Roe. The court stated, *“there is another strand to the right to privacy properly called the right to confidentiality. See Gerety, Redefining Privacy, 12 Har.Civ.R.Civ.L.Rev. 233 (1977). The Supreme Court has defined this branch as “the individual interest in avoiding disclosure of personal matters”. Whalen v. Roe, 429 U.S. at 599, 97 S.Ct. at 876.” Id. at 1132.* As stated above, this is significant because it is the first strand or interest that involves medical privacy.

3.1.1.2 THE CONNECTION BETWEEN THE RIGHT TO PRIVACY & MEDICAL RECORDS

In the Treasury case, the 5th Circuit made the connection between the right to privacy and medical information, essentially applying the right to an individual's, (in this case a public employee's), medical information. The court stated, "we begin this inquiry by noting that whether a public employee's expectation of privacy with regard to a certain zone of personal information is reasonable depends, in part, upon society's established values and its expectations of its public servants, as reflected in our representative government. See, e.g., *Fraternal Order of Police*, 812 F.2d at 113 (**expectation of privacy with respect to medical information is reasonable because various rules and statutes recognize its confidential character**); see also *Trop v. Dulles*, 356 U.S. 86, 101, 78 S.Ct. 590, 598, 2 L.Ed.2d 630 (1958) (discussing the "evolving standards of decency" reflected in constitutional rights). Treasury at 243.

The 5th Circuit cited the Fraternal Order of Police or FOP case, decided by the 3rd Circuit Court of Appeals. That court made a very clear statement that medical information was included in the constitutional right to privacy, for example, they stated: "In determining whether information is entitled to privacy protection, we have looked at whether it is within an individual's reasonable expectations of confidentiality. The more intimate or personal the information, the more justified is the expectation that it will not be subject to public scrutiny. See *Westinghouse*, 638 F.2d at 577 & n. 5. **Applying this approach, we have repeatedly held that medical information such as that sought by questions 18, 19 and 20 is entitled to privacy protection against disclosure.** *Id.*; *In Re: Search Warrant (Sealed)*, 810 F.2d 67 (3d Cir.1987); *Shoemaker v. Handel*, 795 F.2d 1136, 1144 (3d Cir.), cert. denied, --- U.S. ----, 107 S.Ct. 577, 93 L.Ed.2d 580 (1986); *Trade Waste*, 780 F.2d at 234; see also *Whalen*, 429 U.S. at 599-600, 97 S.Ct. at 876-77. **In fact, medical information may be accorded special treatment under**

various rules and statutes in recognition of its confidential character. See, e.g., [Fed.R.Civ.P. 35](#) (higher burden for discovery of medical information than for discovery generally); Freedom of Information Act, [5 U.S.C. § 552\(b\) \(6\)](#) (exemption of medical files).” [Fraternal Order of Police Lodge 5, v. Philadelphia](#), 812 F.2nd 105, (3rd Cir. 1987), at 112 – 113. See also [Doe v. SEPTA](#) wherein the 3rd Circuit made the very clear statement that the constitutional right to privacy applies to prescription records.⁶

3.1.1.2.1 THE FEDERAL CONSTITUTIONAL STANDARD OF REVIEW

In the [Treasury](#) case the 5th Circuit provided the “*standard of review*” applicable to this constitutional right. They stated: “*in conducting this balance, the Fifth Circuit applies what has been aptly described as an intermediate standard of review rather than a strict-scrutiny analysis.* See [Woodland](#), 940 F.2d at 138; [DuPlantier v. United States](#), 606 F.2d 654 (5th Cir.1979); [Plante](#), 575 F.2d at 1134; see also [Barry v. City of New York](#), 712 F.2d 1554, 1559 (2d Cir.), cert. denied, 464 U.S. 1017, 104 S.Ct. 548, 78 L.Ed.2d 723 (1983).” [Treasury](#) at 243, (see footnote number two).

Also, in the [Treasury](#) case, the 5th Circuit Court cited the FOP case twice, which used

⁶ [Doe v. SEPTA](#), 72 F. 3rd. 1133, (3rd Cir. 1995) at 1138. The Appellate Court stated: “It is now possible from looking at an individual's prescription records to determine that person's illnesses, or even to ascertain such private facts as whether a woman is attempting to conceive a child through the use of fertility drugs. This information is precisely the sort intended to be protected by penumbras of privacy. See [Eisenstadt v. Baird](#), 405 U.S. 438, 450, 92 S.Ct. 1029, 1036, 31 L.Ed.2d 349 (1972) (“If the right of privacy means anything, it is the right of the individual ... to be free from unwanted governmental intrusions into matters so fundamentally affecting a person as the decision whether to bear or beget a child.”). An individual using prescription drugs has a right to expect that such information will customarily remain private. The district court, therefore, committed no error in its holding that there is a constitutional right to privacy in one's prescription records.

the law in the Westinghouse⁷ case, another 3rd Circuit Court decision. As well, a Federal District Court in Dallas recognized the validity of the Westinghouse case in U.S. v. Lasco, 531 F.Supp. 256, (ND Texas, 1980) at 263. That court stated, “for the reasons set forth in Westinghouse, supra at 574, I conclude that Respondent has standing to assert its employees privacy rights with respect to the subpoenaed materials in question here.” After the District Court concluded that “the personnel files in question do fall within a protected zone of privacy... the next step in the analysis is to weigh the societal interest in disclosure of the records against the asserted privacy interest on the particular facts of the case. Westinghouse, supra at 578.” Id. at 263.

The court then outlined the “seven pronged test” as follows: “The appropriate factors for consideration are (1) the type of record requested, (2) the information that it does or might contain, (3) the potential for harm in any subsequent nonconsensual disclosure, (4) the injury from disclosure to the relationship in which the record was generated, (5) the adequacy of safeguards to prevent unauthorized disclosure, (6) the degree of need for access, and (7) whether there is an express statutory mandate, articulated public policy, or other recognizable public interest militating toward access.” Id. at 263 See also Doe v. SEPTA, which used the same seven prong test, in relation to prescription records, (*certiorari denied*, 519 U.S. 808). In the Lasco case the court concluded, that “because of the inclusion of factors one and two, above, that I have assumed without deciding that the personnel files fall within constitutionally protected zone of privacy.” Lasco at 263 – 264.

3.1.1.2.1.1 ADDITIONAL INFORMATION ON THE WESTINGHOUSE CASE

The Westinghouse case requires examination since it has been used and recognized by

⁷ U.S. v. Westinghouse, 638 F.2d 570

both the Circuit Court of Appeals and the District Court in Texas. In today's technological society and in the context of this HITAC project, the federal government and the states along with the vast majority of American citizens are aware of the need for privacy and security in relation to their personal medical records.⁸

However twenty six years ago the Appellate Court in the Westinghouse case provided a remarkable bit of insight into the issue of the privacy of medical information, well before the idea of a "National Health Information Network," or a vast regulatory scheme like the Health Information Portability and Accountability Act, (HIPAA).

That court stated there was a threat to "*one of the most fundamental and cherished rights of American citizenship,*" i.e., the right to privacy that the governmental use of computers represents. The court stated, "*there can be no question that an employee's medical records, which may contain intimate facts of a personal nature, are well within the ambit of materials entitled to privacy protection.*" Westinghouse at 577. Also that the "*proliferation in the collection, recording and dissemination of individualized information has made the public, Congress and the judiciary increasingly alert to the threat such activity can pose to one of the most fundamental and cherished rights of American citizenship, falling within the right characterized by Justice Brandeis as "the right to be let alone."* See *Olmstead v. United States*, 277 U.S. 438, 478, 48 S.Ct. 564, 572, 72 L.Ed. 944 (1928) (dissenting). *Much of the concern has been with governmental accumulation of data and the ability of government officials to put **information technology** to uses detrimental to individual privacy, which have been facilitated by the spread of data banks and by the increasing storage in computers of sensitive information relating to the personal lives and activities of private citizens.*" Id at 576. This remarkable bit of insight occurred at a time when technology was developing and not nearly as advanced as today.

⁸ For example see the latest breach, The Veteran's Administration violation wherein 26 million records some containing PHI were stolen. <http://www.fcw.com/article94794-06-06-06-Web> Also see <http://www.privacyrights.org/ar/ChronDataBreaches.htm> for a chronology of privacy breaches.

This same court made the following statement, “*privacy, thus, is control over knowledge about oneself. But it is not simply control over the quantity of information abroad; there are modulations in the quality of the knowledge as well. We may not mind that a person knows a general fact about us, and yet feel our privacy invaded if he knows the details. For instance, a casual acquaintance may comfortably know that I am sick, but it would violate my privacy if he knew the nature of the illness. Or a good friend may know what particular illness I am suffering from, but it would violate my privacy if he were actually to witness my suffering from some symptom which he must know is associated with the disease. Fried, Privacy, 77 Yale L. J. 475, 483 (1968)*” Id at 577, (see footnote number five).

3.1.1.2.1.1.1 THE 5TH CIRCUIT & THE STANDARD OF REVIEW IN TEXAS

In the Woodland v. City of Houston case, 940 F 2nd 134, the 5th Circuit talked about the level of review the State Supreme Court in Texas utilizes. They stated: “*The Supreme Court of Texas has only recently recognized a right of privacy in the Texas constitution. In State Emp. Union v. Dept. of Mental Health, 746 S.W.2d 203 (Tex.1987), the court first declared that the Texas constitution implicitly recognizes a right of privacy and then, without distinguishing confidentiality and autonomy cases, adopted a strict scrutiny test in the context of a confidentiality claim. “The right to privacy should yield only when the government can demonstrate that an intrusion is reasonably warranted for the achievement of a compelling governmental objective that can be achieved by no less intrusive, more reasonable means.” Id. at 205. **We believe that Texas would also view the application of its strict scrutiny test as a question of law.***” Woodland at 138.

3.2 ANALYSIS

It is very clear from the cases cited and the language of the 5th Circuit court that on the federal level the “**right to privacy**” extends to medical records and is protected by the United States Constitution as a fundamental right. This protection represents a real legal barrier that the HITAC should be aware of.

The cases cited are well established precedents including many Supreme Court rulings. This is an individual right, thus may be asserted by one person, and is not restricted to a class of litigants. With the heightened scrutiny surrounding “protected health information” through the passage of laws like HIPAA,⁹ the possibility of even more litigation further

⁹ http://www.washingtonpost.com/wp-dyn/content/article/2006/06/04/AR2006060400672_pf.html

Medical Privacy Law Nets No Fines: Lax Enforcement Puts Patients' Files At Risk, Critics Say
By Rob Stein, Washington Post Staff Writer, Monday, June 5, 2006; A01

WASHINGTON - In the three years since Americans gained federal protection for their private medical information, the federal government has received thousands of complaints alleging violations yet has not imposed a single civil fine and has prosecuted just two criminal cases.

Of the 19,420 grievances lodged so far, the most common allegations have been that personal medical details were wrongly revealed, information was poorly protected, more details were disclosed than necessary, proper authorization was not obtained or patients were frustrated getting their records.

The government has "closed" more than 73 percent of the cases — more than 14,000 — either ruling there was no violation or allowing health plans, hospitals, doctors' office or other entities simply to promise to fix whatever they had done wrong, escaping any penalty.

defining this constitutional right is very likely. In today's technological society with advent of computers and high speed transfers of information, the privacy and security of this type of information is imperative. The federal Courts were aware of this issue 26 years ago long before HIPAA and the nation wide State participation in "Regional Health

"Our first approach to dealing with any complaint is to work for voluntary compliance. So far it's worked out pretty well," said Winston Wilkinson, who heads the Department of Health and Human Services Office of Civil Rights, which is in charge of enforcing the law.

Though praised by hospitals, insurance plans and doctors, the approach has drawn strong criticism from privacy advocates and some health industry analysts. They say the administration's decision not to enforce the law more aggressively has failed to safeguard sensitive medical records and made providers and insurers complacent about complying.

"The law was put in place to give people some confidence that when they talk to their doctor or file a claim with their insurance company, that information isn't going to be used against them," said Janlori Goldman, a health care privacy expert at Columbia University.

"They have done almost nothing to enforce the law or make sure people are taking it seriously. I think we're dangerously close to having a law that is essentially meaningless," Goldman said.

The debate has intensified amid a government push to computerize medical records in order to improve the efficiency and quality of health care. Advocates say large centralized electronic databases will be especially vulnerable to invasions, making it even more crucial that existing safeguards be enforced.

The Health Insurance Portability and Accountability Act — commonly known as HIPAA — gave the job of enforcement to HHS, including the authority to impose fines of \$100 for each civil violation, up to a maximum of \$25,000.

HHS can also refer possible criminal violations to the Justice Department, which could seek up to \$250,000 in fines and 10 years in jail.

Wilkinson said his office has "been able to work out the problems by going in and doing technical assistance and education to resolve the situation."

Information Organizations.”

A simple reading of the cases should indicate to any reader, (no matter how well versed that reader may be in constitutional law), that the federal courts view privacy favorable, including the 5th Circuit. This is crucial in understanding the need to be sensitive to these issues as they relate to clearly delineated individual rights protected by the United States Constitution.

Finally, the next section will outline exactly how the Federal Courts, including a district Court falling under the 5th Circuit have included HIPAA in this “constitutional right to privacy in medical records.” Given the overwhelmingly favorable HIPAA rulings that have appeared to date,¹⁰ it is clear that this area of the law, or the privacy of medical records regulating technology, represents a developing area of the law.

3.3 RECOMMENDATIONS

The recommendations offered in this document relate to the “Health Information Technology” plan found in the Texas Health and Safety Code, chapter 104, section 104.0156.

That specific section states: “The advisory committee, [HITAC], shall develop a long-range plan for health care information technology, including the use of electronic medical records, computerized clinical support systems, computerized physician order entry, regional data sharing interchanges for health care information, and other methods of incorporating information technology in pursuit of greater cost-effectiveness and better patient outcomes in health care.”

¹⁰ A note of the Reader, this could change with further litigation, however right now, across the country there are over 180 Federal HIPAA cases interpreting this regulation and these cases are quite favorable to that body of law.

Any *“long range plan”* relating to the *“use of electronic medial records”* or the *“sharing”* of health care information **MUST** take into consideration all federal and state laws regulating these activities. This includes all state and federal constitutional issues associated with these activities. Obviously any recommendation the HITAC makes to the State legislature in relation to their statutory responsibilities must also take into consideration these legal issues. The recommendations offered in this document relate to the HITAC’s statutory responsibility to *“develop a long term plan,”* involving the use and sharing of health information.

1. HITAC Awareness:

The HITAC needs to incorporate, or include the fact that medical records are protected by the United States Constitution into any recommendations involving the HITAC’s work that they submit to the State Legislature. Medical privacy is considered as fundamental a right as free speech, according to the cases cited above.

2. State Legislator Awareness:

The HITAC needs to ensure that the State Legislature is aware of this information. This may be accomplished through further research and customized education geared towards State legislators.

3. Future Texas Legislation:

The HITAC should ensure that any legislation that may result from the HITAC’s work, takes into consideration the constitutional protections that surround medical information on the Federal level. In other words, the HITAC should ensure that the State Legislature understands what is involved on the federal level regarding the privacy of medical records in relation to future legislation. This would prevent litigation and the redrafting of legislation.

Although more information will be offered on the Supreme Court for the State of Texas, it must be noted that any specific legislation impacting health information exchange and disclosures would need to consider the Federal holdings outlined above, and the fact that medical information is the type of information entitled to privacy protections against disclosures on the federal level affecting the State of Texas.

4. Continued Education:

The HITAC should recommend the ongoing education of State Legislators in this complex area given their responsibilities and the level of public awareness and heightened scrutiny in this area of the law. This area of the law will change thus on-going education is necessary.

5. Oversight Activities:

The HITAC should recommend the creation of a group that analyzes current and future legislation to ensure that it does not violate these fundamental rights, especially in today's environment given the level of public awareness of these issues.

3.4 HIPAA AND THE CONSTITUTIONAL RIGHT TO PRIVACY IN MEDICAL RECORDS

HIPAA has been applied by two federal district courts along with the constitutional right to privacy in medical information in two cases. One of these federal trial courts was within the 5th Circuit thus may be applicable to the State of Texas. The "precedential" value of these two decisions in relation to the 5th Circuit Court of Appeals will be outlined in footnote number eleven.¹¹ Finally, footnote number twelve¹² provides the reader

¹¹ One of the most cited cases relating to Federal District Court cases being used as precedent is Colby v. J.C. Penny Company, 811 F.2d 1119, (7th Cir. 1987). The Appellate Court stated: "...and even in that situation, district judges in this circuit must not treat decisions by other district judges, in this and a fortiori in other circuits, as controlling, unless of course the doctrine of res judicata or of collateral estoppel applies. Such decisions will normally be entitled to no more weight than their intrinsic persuasiveness merits. The reasons we gave for giving some though not controlling weight to decisions of other federal courts of appeals do not apply to decisions of other district courts, because the responsibility for maintaining the law's uniformity is a responsibility of appellate rather than trial judges and because the Supreme Court does not assume the burden of resolving conflicts between district judges whether in the

with an understanding of “precedential” value between 5th Circuit decisions.

In U.S. v. Sunderland, 143 F. Supp. 2nd 609, (2001), the District Court in Virginia, (like the 5th Circuit), also cited the 3rd Circuit Court of Appeals. In Sunderland the Court referred to the Doe case, mentioned directly above. That court stated, citing the Whalen v. Roe as follows: *“federal courts have acknowledged the importance of protecting patient privacy in medical records. In Doe v. Southeastern Pennsylvania Transportation Authority, 72 F.3d 1133, 1138 (3rd Cir.1995), the Third Circuit recognized a constitutional right to privacy in a patient's prescription records. This*

same or different circuits. Federal district judges in Detroit do not make law that is binding on federal district judges in Chicago.” Essentially this means that Federal District Court opinions do not carry precedential value from one Circuit to another, or for that matter even within the Circuit itself. This statement also indicates that other Circuit Courts of Appeals decisions do carry some weight, although not controlling weight. Finally, it must be noted that this statement does indicate some exceptions that do apply to “other Federal District Courts.”

¹² In Bonner v. city of Pritchard, 661 F.2d 1206, (11th Cir. 1981), wherein the fifth circuit was split into two parts, the Appellate Court decided to utilize “old fifth” circuit rulings for the choice of governing law applicable to the new 11th Circuit. That statement illustrates how the old fifth and the new 11th use their own decisions and other circuit court decisions as precedent. The Circuit Court stated:

“II. The choice of governing law

Under the established federal legal system the decisions of one circuit are not binding on other circuits. “(I) t is common knowledge that the decisions of the court of appeals for one circuit are not binding upon the courts of appeals for other circuits.” 1B J. Moore, Federal Practice P 04.02(1) (1980). The various circuits differ somewhat in the extent to which they treat their own decisions as binding on themselves. Some appear at times to treat their own decisions as merely persuasive; others by rule or practice permit one panel to overrule another after prior notice to all judges of what is proposed, followed by no objection. The old Fifth followed the absolute rule that a prior decision of the circuit (panel or en banc) could not be overruled by a panel but only by the court sitting en banc. The Eleventh Circuit decides in this case that it chooses, and will follow, this rule.”

right, however, is not absolute, and must be balanced against the government's interests in obtaining the information. See *id.*; see also *Whalen v. Roe*, 429 U.S. 589, 602, 97 S.Ct. 869, 51 L.Ed.2d 64 (1977) (applying balancing test); *Patients of Dr. Barbara Solomon v. Bd. of Physician Quality Assurance*, 85 F.Supp.2d 545, 548 (D.Md.1999) (predicting Fourth Circuit would apply balancing test to medical record disclosure).” *Sunderland* at 611 – 612.

Also that “not only have the courts recognized the importance of the privacy of medical records, but Congress has addressed the issue as well. As part of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), [Pub.L. No. 104-191, §§ 261-264](#), 110 Stat.1936 (1996), Congress directed the Secretary of Health and Human Services to promulgate final regulations setting privacy standards for medical records. Pursuant to this directive, the Secretary has recently issued Standards [for Privacy of Individually Identifiable Health Information \(“Standards”\), 65 Fed.Reg. 82,462 \(Dec. 28, 2000\)](#) (to be codified at 45 C.F.R. pts. 160 & 164). The rules restrict and define the ability of health plans, health care clearinghouses, and most health care providers to divulge patient medical records.” *Id* at 612.

Essentially, in the same case, this district court included HIPAA in their analysis of this constitutional right to privacy in medical records. Also, and as significantly, this court actually applied HIPAA to the facts in this case before the law became effective. The court stated: “Although the Standards were effective April 14, 2001, compliance is not required until April 14, 2003. See [66 Fed.Reg. 12,434 \(Feb. 26, 2001\)](#) (to be codified at 45 C.F.R. pts. 160 & 164). Nevertheless, the Standards indicate a strong federal policy to protect the privacy of patient medical records, and they provide guidance to the present case.” *Id* at 612.

In the same paragraph, this court made the following statement in reference to the HIPAA regulations: “Although not presently binding on the Hospital or this court, I find

these regulations [HIPAA], to be persuasive in that they demonstrate a strong federal policy of protection for patient medical records. Likewise, courts have recognized that disclosure of medical records touches on constitutional concerns.” Id at 612

Finally, this court applied both the “balancing” test from the 3rd Circuit court in SEPTA and HIPAA **in conjunction** to determine the outcome of this case. The court stated: “*applying a balancing test,*¹³ *I find the government’s interests in obtaining the prescription records in this case to be compelling. In its prosecution of a medical doctor accused of criminally acting without a legitimate medical purpose and beyond the bounds of medical practice, evidence concerning the prescription drugs received by the doctor’s patients is highly relevant. However, in light of the strong federal policy*¹⁴ *in favor of protecting the privacy of medical records, I find that it would be “unreasonable or oppressive” to permit disclosure of these records at trial without opportunity for the affected patient to object.* [Fed.R.Crim.P. 17\(c\).](#)’ Id at 613.

Along with the constitutional balancing test recognized by the 5th Circuit Court of Appeals¹⁵ noted in footnote number thirteen, this court made its decision “*in accord with the Standards issued by the Secretary of Health and Human Services... [HIPAA].*”

¹³ *Doe v. SEPTA* 72 F. 3rd. 1133 (1995): “*Westinghouse* mandates a consideration of seven different factors. They are: (1) the type of record requested; (2) the information it does or might contain; (3) the potential for harm in any subsequent nonconsensual disclosure; (4) the injury from disclosure to the relationship in which the record was generated; (5) the adequacy of safeguards to prevent unauthorized disclosure; (6) the degree of need for access; and (7) whether there is an express statutory mandate, articulated public policy, or other recognizable public interest favoring access. [Westinghouse, 638 F.2d at 578](#). Although some of these factors may be in Doe’s favor, overall, we believe the balance weighs on the side of permitting the disclosures present here.”

¹⁴ The Court is referring to the HIPAA Regulations before they actually came into affect in 2003.

¹⁵ In the Treasury case cited above, the 5th Circuit recognizes the validity of the FOP case, also cited above, which in turn recognizes the validity of the *Westinghouse* case and the seven prong balancing test outlined in footnote thirteen directly above.

Sunderland at 613.

Again, the federal district court stated applying section 164.512 (e) of HIPAA as follows: *“I condition my denial of the Hospital's motions to quash on the requirement that the government provide written notice prior to production of the subpoenaed records to the last known address of each individual whose records are sought under the subpoena. The notice must inform the individual that he or she may object to disclosure within five business days of the date the notice was mailed. If the government objects to giving notice, it must show cause before this court as to why notice would be unduly burdensome or prejudicial in a particular instance. I will resolve all objections by the government or by affected individuals before the start of trial.”* Id at 613.

3.4.1 THE FEDERAL APPLICATION OF THE SUNDERLAND CASE IN LOUISIANA

Similarly, the Federal District Court in an unpublished opinion in United States of America ex rel Mary Jane Stewart et al. v. Louisiana Clinic 2002 WL 31819130 (E.D.La. 2002), (falling under the 5th Circuit Court of Appeals thus having potential significance to the State of Texas), agreed with the Sunderland decision.

In fact that trial court acted in the same manner as the Sunderland court by applying HIPAA before it actually became effective. Essentially this district court placed the content of the Sunderland decision under the umbrella of the 5th circuit involving HIPAA and the constitutional right to privacy in medical records. Again as stated in the Colby decision, these trial courts within the 5th Circuit must *“give considerable weight to those decisions unless and until they have been overruled or undermined by the decisions of a higher court, or other supervening developments, such as a statutory overruling.”* ¹⁶

¹⁶ In the Colby case the Circuit Court stated in relation to district courts: *“The most complex relationship is between a court and its own previous decisions. A court must give considerable weight to those*

Colby v J.C. Penny 811 F.2d 1119, at 1123.

The District Court in Louisiana selected specific language from the Sunderland case that inculcates one prong of the seven prong balancing test outlined in the Westinghouse case. Simply stated, the balancing test requires the analysis of whether or not there is “*an express statutory mandate, articulated public policy, or other recognizable public interest favoring access.*” [Westinghouse, 638 F.2d at 578.](#) Ultimately this court found the legal mandate relating to “disclosure” or “favoring access.”

For example, the court held: “*I find that both relators and defendants have complied with the HIPAA regulations at issue by seeking an appropriate protective order and that the court has the authority to order disclosure of nonparty patient information, subject to such a protective order, without conducting a contradictory hearing or having the parties obtain the patients' consent.*” See 2002 WL 31819130 (E.D.La. 2002), (note no other citation is available). Although the holding of this case is significant, the entire case requires careful examination since the trial judge used a part of the holding in the Sunderland case from the Northern District of Virginia.

For example, the court stated, “*In the instant case, relators and the United States argue that the HIPAA Standards do not apply because the final compliance date for health care providers is April 14, 2003. In this regard, I agree with District Judge Jones of the Northern District of Virginia, who stated:*

decisions unless and until they have been overruled or undermined by the decisions of a higher court, or other supervening developments, such as a statutory overruling. But it is not absolutely bound by them, and must give fair consideration to any substantial argument that a litigant makes for overruling a previous decision.”

Nevertheless, the Standards indicate a strong federal policy **to protect the privacy of patient medical records**, and they provide guidance to the present case. In [45 C.F.R.] § 164.512(e), the regulations define when and how disclosures are permitted for judicial and administrative proceedings. Although not presently binding on the Hospital or this court, I find these regulations to be persuasive in that they demonstrate a strong federal policy of protection for patient medical records. *Sutherland*, 143 F.Supp.2d at 612. Moreover, the Standards will require full compliance in a mere four months, at a time when this lawsuit will still be ongoing (trial is set for October 2003) and the patient records at issue will be in full use by the parties.

Thus, the court will analyze the HIPAA regulatory scheme. [45 C.F.R. § 164.512](#) allows a health care provider to disclose protected health information during judicial proceedings under certain circumstances without the written authorization of the patient or an opportunity for the patient to agree or object to the disclosure.” See 2002 WL 31819130 (E.D.La. 2002), (note no other citation is available)

This federal court also strongly agreed with the application of HIPAA given the constitutional nature of the issue as clearly outlined in the *Sunderland* case, which this federal district court utilized. The court stated: “All parties agree (and I strongly agree) that there is good cause for entry of a protective order concerning the medical records of nonparty patients in this case, Fed.R.Civ.P. 26(c), and that the order should at the very least comply with 45 C.F.R. § 164.512(e) (v)” See 2002 WL 31819130 (E.D.La. 2002), (note no other citation is available)

Again, the Consumer Workgroup is responsible for “documenting real and perceived legal, regulatory and business barriers that could hinder participation in health information exchange,” also for “defining legal challenges that all states encounter with respect to federal regulations.” Clearly this type of a legal development qualifies as a real barrier or challenge to the adoption of HIE with in the State of Texas. Finally with further litigation it will be another challenge to many other States as well.

At this time, it may be stated that HIPAA is connected with and involves the constitutional right to privacy in medical information as utilized by the 5th Circuit to adjudicate this fundamental privacy right.

3.4.1.1 OTHER FEDERAL CASES WITHIN THE 5TH CIRCUIT THAT MERIT ATTENTION

Although time constraints prevent the exhaustive delineation of case law, certain holdings involving HIPAA affecting the State of Texas will be reviewed to provide the reader with an understanding of the state of the law.

This section of the document will focus on two significant cases that may assist the reader in understanding the significance of the federal HIPAA regulations in the State of Texas.

The first case is United States v. Diana Zamora, 408 F.Supp.2d 295 (S.D.Tex. 2006). The case is significant in that it addressed the issue of whether or not HIPAA was preempted by laws in the State of Texas involving medical privacy. Although the district court in the Louisiana case already addressed the preemption issue by actually applying HIPAA before it became effective in 2002, this case makes the very clear statement that HIPAA pre-empts Texas law. In fact the specific Texas law that was pre-empted involved the sensitive issue of HIV disclosures or 81.103 of the Texas Health and Safety Code.

In the Zamora case, the issue was whether or not Bay Area Healthcare Limited, doing business as Corpus Christi Medical Center, could release the medical records of Diana Zamora in relation to a blood alcohol test and other medical information in those records. Again, the preemption issue arose involving the Texas Health and Safety Code specifically section 81.103.

For example, in the Attorney General's "*Preemption Analysis of Texas Laws Relating to the Privacy of Health Information and the HPA Privacy Rules*," dated November 2004, the AG reported that section 81.103 of the Texas Health and Safety Code was not preempted by HIPAA. The question was presented in relation to section 81.103 as follows: "*Is State Law Preempted?*" the response offered by the AG's report was "No."¹⁷ The federal district court dealt with this issue specifically, in a separate section entitled "**B. Preemption of Texas Health and Safety Code Section 81.103,**"¹⁸ in the Zamora case.

The Zamora court reviewed the arguments of both sides before concluding that Bay

¹⁷ See the "Preemption Analysis of the Texas Laws Relating to the Privacy of Health Information and the Health Insurance Portability and Accountability Act and Privacy Rules, (HIPAA)", page 161.

¹⁸ See US v. Zamora, 408 F. Supp 2nd. 295, at 299.

Area's arguments "*must fail*,"¹⁹ in that Bay Area contended that they could not release this medical information due to section 81.103 of the Texas Health and Safety Code. (Also it must be noted that this court applied the HIPAA privacy rule in their analysis to the facts of this case before addressing this preemption analysis; consequently actually applied the HIPAA privacy rule in this Texas case).²⁰

For example the court stated: "*Bay Area contends that the requested records cannot be released solely upon subpoena due to Section 81.103 of the Texas Health and Safety Code. This provision provides that the results of HIV tests are confidential, and may not be released except as provided. Tex. Health & Safety Code § 81.103 (a). An individual that has been tested may voluntarily consent, in writing, to the disclose test results to a third party. Tex. Health & Safety Code § 81.103 (d). Bay Area argues that the requested records cannot be disclosed without a specific written authorization by defendant.*"²¹

The District Court summarized the government's argument before ruling on this issue as follows: "*The government, however, argues that this State law is preempted by HIPAA. As a general rule, State law that is contrary to any provision of HIPAA is preempted. 45 C.F.R. § 160.203. There are exceptions to this general rule including where [“the provision of State law relating to the privacy of individually identifiable health information and is more stringent than a standard requirement ...”] 45 C.F.R. § 160.203(b). [“More stringent”] for purposes of this case is where the state law [“provides greater privacy protection for the individual who is the subject of the individually identifiable health information.”] 45 C.F.R. § 160.202.*"²²

¹⁹ Id at 299.

²⁰ See generally *United States of America v. Diana Zamora*, 408 F. Supp 2nd. 295, 2006 U.S. Dist. LEXIS 1894, and decided January 10, 2006, filed January 10, 2006.

²¹ *Zamora*, at 299.

²² Id. at 299.

Even though the district court questioned the applicability of section 81.103, they compared that code to HIPAA and concluded; *“even assuming that defendant did undergo HIV testing as part of her hospital visit, any results would not be relevant to the medical records that the government seeks. As such, the appropriate remedy would be to redact any references to HIV testing. Consequently, Bay Area’s arguments regarding the applicability of § 81.103 in this case must fail.”*²³

Again, although the court did not have to make this comparison as the actual applicability was in question, they did so anyway making the clear statement that HIPAA preempts the Texas Health and Safety Code, specifically section 81.103.

To summarize, many federal level courts, including the District Court in the Southern District of Texas, have applied the HIPAA privacy rule preempting state laws in the process of dealing with federal issues.

The second case that requires examination involves the application of the HIPAA rules to prisoners. Generally, prisoners do not receive the same “individual rights” as non-incarcerated individuals.

However in Smith v. Zungia,²⁴ the Federal District Court documented their “finding of facts” to rule on the issues of the case. That court stated: *“Based on a preponderance of the evidence and applicable law, I make the following finds of fact and conclusions of law.”* The court then offered a conclusion of law involving HIPAA and the rights of prisoners. They stated, *“An inmate’s right to **privacy** during his **medical** examination emanates from the Health Insurance Portability and Accountability Act of 1996, [Pub.L. No. 104-191, 110 Stat.1936](#) (“HIPPA”), which has served to implement new precautionary regulations for **medical** providers.”*

²³ Id at 299.

²⁴ 2006 WL 1207685 (W.D.Tex.), no other citation is available.

This is significant because, on the federal level, prisoners have the rights and protections afforded by the HIPAA regulations. HIPAA also regulates the rights of emancipated and un-emancipated minors providing them with specific rights and exceptions.²⁵

3.5 ANALYSIS

The impact of these rulings are significant because they highlight potential barriers and challenges to the adoption of HIE and HIT that must be considered and addressed in an effective fashion. The interpretation of the HIPAA regulations by federal circuit and district court means that real compliance is required by all stakeholders.

Connecting the HIPAA regulations with a federal constitutional issue signifies the importance the federal judiciary places on these regulations. Again, the HIPAA regulations were used before they became applicable and actually combined in the court's analysis, with a fundamental individual constitutional right, (i.e., the right to privacy in medical records), to decide a case.

Finally, the manner in which the HIPAA regulations have been enforced by the federal courts is definitive. HIPAA regulations have been applied across the country by federal courts, pre-empting the laws in many states even if those laws appeared to more "more stringent" and the laws of the State of Texas are not exceptions to the HIPAA regulations.

3.6 RECOMMENDATIONS

²⁵ 45 CFR § 164.502 (g) (2) - (3).

6. Clarity on the Need to Comply with HIPAA:

The HITAC should recommend to the Governor’s Office or the State Legislature that an official statement be issued by the appropriate authority(s) reaching all appropriate stakeholders, or organizations and individuals subject to the HIPAA rules, that HIPAA applies to the State of Texas and that compliance with the regulations is mandated.

This statement or series of announcements should be targeted towards all stakeholders, including but not limited to health care providers, i.e., physicians and hospitals or insurance companies. All appropriate hybrid entities should be unequivocally informed of the need to comply with HIPAA. This includes all appropriate State agencies, counties, cities and all appropriate local governmental units. This also includes independent school districts and universities as appropriate.

Clear and unequivocal terms need to be developed and communicated to all stakeholders impacted by HIPAA, to ensure that all appropriate private and public entities understand exactly how the HIPAA regulations apply to them and why they need to comply with these regulations beyond simply “stating they are in compliance.”

7. Audits & Reviews of State and Local Governmental Organizations:

The HITAC should recommend that the State Legislature create an independent State controlled audit group responsible for auditing all affected governmental organizations as to their “real level” of HIPAA compliance.²⁶ The HITAC

²⁶ <http://www.davickservices.com/Courthouse%20for%20Sale%20-%20Cheap.htm> “Court House for Sale Cheap”

committee should recommend that this independent audit group conduct substantive, unannounced and random audits of specific public entities that are impacted by HIPAA, to determine their level of HIPAA compliance.

Again as stated above, any long range plan involving the disclosure, use and request of the content of “electronic medical records” must consider all appropriate state and federal laws and regulations governing individual’s medical information, (or PHI).

Further, recommendation number 7 relates to HIPAA in that many of these local and state level entities provide medical services, or health insurance services as either covered entities or hybrid entities. For example, many Texas Counties have EMS, Fire, and Police Departments that perform medical services, or operate Indigent Health Care departments, or offer group health plans benefits to their employees which would subject them to the HIPAA rules.

Also, since these governmental entities have the potential for huge and potentially improper disclosures of PHI, (please see footnote 26 directly below that discusses an improper disclosure of 20 million county records containing the medical and personal information of citizens in Fort Bend County), it is crucial that these entities comply with all State and Federal rules and regulations pertaining to medical information, (or PHI).

8. HITAC Recommendations & Advice:

The HITAC needs to ensure that any advice or recommendations they submit to the State Legislature in relation to their statutory responsibilities, comply with all appropriate HIPAA regulations including all of the rules. This includes any products they recommended or actually select.

9. Future Legislation:

The HITAC should recommend to the State Legislators that any legislation they pass related to HIE and HIT as a result of the HITAC’s efforts, comply with all appropriate HIPAA regulations and requirements.

10. Legislative Oversight Committee:

The HITAC should recommend that the State Legislature create an independent oversight committee to ensure that any future legislation regarding the uniform use of software, networking and business practices takes into consideration all HIPAA requirements.

11. State Legislator Continuing Education on HIPAA:

The HITAC should recommend continuing education on the federal interpretation and use of the HIPAA regulations as that develops and impacts individuals and

organizations in the State of Texas for State Legislators. This program could be used to educate the public and stakeholders as well. This may include education on how to actually comply with this complex legislation, taught in layman's terms.

12. Audits and Reviews of Private Stakeholders:

The HITAC should recommend that the State Legislature create an independent State controlled audit group responsible for auditing all private organizations impacted by HIPAA as to their current status of HIPAA compliance. The HITAC committee should recommend that this independent audit group conduct substantive, unannounced and random audits of specific private organizations to determine their level of HIPAA compliance.

13. Guidelines and Resource for Stakeholders:

The HITAC should recommend that the State Legislature develop a set of coherent and practical guidelines and resources that can be implemented by stakeholders to meet the needs of compliance with HIPAA regulations and to reduce the cost and complexity of compliance which will reduce the resistance by stakeholders to comply with the mandates. Again this recommendation is based upon the HITAC's statutory responsibilities associated with their long range plan.

4 THE STATE OF TEXAS & THE CONSTITUTIONAL RIGHT TO PRIVACY

The Supreme Court of the State of Texas has specifically recognized the constitutional right to privacy. That court stated in the Texas State Employees Union, v. Texas Department of Mental Health and Retardation case, 746 S.W.2d 203, (1987) as follows: *“We do not doubt, therefore, that a right of individual privacy is implicit among those “general, great, and essential principles of liberty and free government” established by the Texas Bill of Rights. TEX.CONST., art. I, Introduction to the Bill of Rights. We hold that the Texas Constitution protects personal privacy from unreasonable intrusion. This right to privacy should yield only when the government can demonstrate that an intrusion is reasonably warranted for the achievement of a compelling governmental objective that can be achieved by no less intrusive, more reasonable means.”* Id at 205.

Although this court did not specifically state they recognize a right to privacy in medical records, they used a strict standard of review in relation to the right to privacy.

However in the In re Crestcare Nursing and Rehabilitation case, 2006 WL 408226, (February 2006), the Appeals Court of Texas cited Whalen v. Roe mentioning that *“an individual’s medical records are within the zone of privacy protected by the United States Constitution.”*²⁷

That court stated, *“The right to privacy is not expressly mentioned in either the federal constitution or our state constitution. However, the Supreme Court has held that a right of personal privacy, or a guarantee of certain areas or zones of privacy, exists under the United States Constitution. See, e.g., [Griswold v. Connecticut, 381 U.S. 479, 484, 85 S.Ct. 1678, 1681, 14 L.Ed.2d 510 \(1965\)](#). Similarly, the Texas Supreme Court has held that the Texas Constitution protects personal privacy from unreasonable intrusion. [Tex.](#)*

²⁷ 2006 WL 408226, no other citation is available.

[State Employees Union v. Tex. Dep't of Mental Health & Mental Retardation, 746 S.W.2d 203, 205 \(Tex.1987\).](#) The term "right to privacy" is a generic term encompassing various rights recognized in decisions of the United States Supreme Court as well as in other federal and state courts." ²⁸

The court also stated, "An individual's medical records are within a zone of privacy protected by the United States Constitution. [Whalen v. Roe, 429 U.S. 589, 601, 97 S.Ct. 869, 877, 51 L.Ed.2d 64 \(1977\).](#)" Finally, "The cases protecting privacy have involved at least two different kinds of interests. [Whalen, 429 U.S. at 599, 97 S.Ct. at 876.](#) One is the individual interest in independence when making certain kinds of important decisions and another is the interest in avoiding disclosure of personal matters. [Id.](#) It is the second aspect of the right to privacy that concerns us here. This "disclosural privacy" encompasses the ability of individuals to determine for themselves when, how, and to what extent information about them is communicated to others." ²⁹

4.1 ANALYSIS:

Although the Texas Supreme Court did not specifically mention a right to privacy in medical records, they have utilized the strict scrutiny standard of constitutional review to analyze privacy cases. This level of review may present a potential barrier to the adoption of HIE and HIT.

4.2 RECOMMENDATIONS:

²⁸ 2006 WL 408226

²⁹ 2006 WL 408226

14. Monitor the Development of the Right to Privacy in the State of Texas

The HITAC should recommend that the right to privacy recently ruled on by the State Supreme Court of Texas be monitored in relation to the development of that right as that case law development relates to medical records. Again in order to create a long range plan, these legal requirements must be taken into consideration.

4.3 HIPAA & THE APPELLATE COURTS IN TEXAS

In Harmon v. State, the Court of Appeals of Texas, in Houston, (1st District), applied HIPAA even though, as the Court stated, “we also note that compliance with **HIPAA** was not required when appellant’s medical records were sought because the **HIPAA** regulations did not become effective until April 14, 2003. [45 C.F.R. § 164.534\(a\) \(2001\)](#).”³⁰

Even though the Harmon court overruled the appellant’s HIPAA issue because compliance was not actually required when the appellants records were sought, they applied HIPAA in that case stating: “Even if **HIPAA** imposed a new statutory right of privacy that trumps the State’s power to issue grand-jury subpoenas in a criminal investigation, disclosure of medical records under **HIPAA** is permissible without an individual’s permission when the information is disclosed for law enforcement purposes and is obtained pursuant to a grand-jury subpoena. [45 C.F.R. § 164.512\(f\) \(1\) \(ii\) \(B\) \(2002\)](#).”³¹

³⁰ 2003 WL 21665488 (Tex.App.-Hous. (1dist)), Not Reported in S.W. 3d.

³¹ 2003 WL 21665488 (Tex.App.-Hous. (1dist)), Not Reported in S.W. 3d.

4.3.1 ANALYSIS OF THE ABBOTT V. THE TEXAS DEPARTMENT OF MENTAL HEALTH AND MENTAL RETARDATION, CASE, 2006 WL 1649003, NO OTHER CITATION CURRENTLY AVAILABLE.

A note to the reader, recommendations to the HITAC will be offered in two areas, first in the analysis of the case itself, and again in a separate section summarizing these recommendations. Recommendations will be bolded in the analysis section of this document, for easy access by the reader.

4.3.1.1 ANALYSIS OF THE ABBOTT CASE INCLUDING RECOMMENDATIONS

The Abbott case and the publicity it has received since being released provides the HITAC with an excellent example of the need for clarification on what law to follow and what rulings mean in this area of the law.

This analysis will show the level of misinterpretation and outright confusion associated with these types of decisions. As an example, only three days after the decision was released, KLTV 7 stated in a headline on the decision: *“State public information laws override federal health care privacy laws. That’s what a Texas appeals court ruled today in a case being eyed by public information advocates across the country.”*³² In another media release, the Austin American Statesman stated: *“Appeals court reverses previous ruling in release of personal health information.”*³³

Contrary to the headlines provided by the Austin American Statesman, this specific case did not actually involve the use of PHI, but only statistical information which was clearly stated by the Appellate Court in this ruling. The headlines in the referenced articles along with many other media sources picked up the theme released from the

³² <http://www.kltv.com/Global/story.asp?S=5042293&nav=1TjD>

³³ <http://www.statesman.com/news/content/news/stories/local/06/17opinion.html>

Associated Press that HIPAA was “trumped by the PIA.” This is an excellent example of the level of confusion that surrounds not only HIPAA, but State privacy laws as well.

Again, these headlines state the “Public Information Act trumps HIPAA,” thus inferring that the free and unfettered release of medical information is legally acceptable. The casual reader would conclude that this case allows organizations to freely release PHI or medical information under the guise of the Public information Act without concerns about violating any Federal or State laws. In fact as this analysis will demonstrate nothing could be further from the **reality** of the Appellate Court’s ruling in the Abbott case.

To begin with the Appellate court in the Abbott case stated *“before addressing the claims made by the parties in this case, we first note that the information requested in this case does not seem to fall into the definitions of “protected health information” given in either HIPAA or the Privacy Rule. The request asked for allegations and investigations of abuse at various governmental facilities. Statistical information regarding allegations of abuse and subsequent investigations does not seem to relate to issues regarding health or condition in general and certainly does not relate to the health or condition of an individual, “the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.” See 42 U.S.C.A. §1320d (6) (emphasis added); 45 C.F.R. § 160.103.”*³⁴

Consequently, this case did not involve the use of PHI; statistical information was litigated. Generally, the HIPAA Privacy rule allows the free use of all information that has been de-identified.³⁵

Adding to the confusion as the Appellate Court stated is, *“the whole thrust of the Attorney General’s original letter opinion, his motion for summary judgment, and his*

³⁴ 2006 WL 1649003 (Tex.App.-Austin) No other citation is currently available.

³⁵ 45 CFR § 164.514

*briefs seems to assume that the information is protected health information that is subject to disclosure via an exception in the Privacy Rule.”*³⁶ In other words the Appellate court indicated there was a reference to PHI in this case by the AG’s Office when the case did not actually involve PHI. Also, *“the letter further concluded that requests for information made under the Public Information Act fall under an exception to nondisclosure found in the Privacy Rule that allows disclosure of health information if it is required by law and if the disclosure complies with the requirements of the law in question.”*³⁷

Given the Appellate Court’s statement in the paragraph above, i.e., that this case did not involve the use PHI, it appears that the AG’s Office is unaware of exactly what the definition of “Protected Health Information” means.³⁸ Consequently since the AG’s Office was apparently unsure of this basic definition, it is understandable that the local media would also be unsure of exactly what was decided in this case.

A part of the responsibility of the HITAC is to make ‘practical’ recommendations on the implementation of medical privacy and security rules in the State of Texas thus, **it may be advisable that the HITAC recommend some basic education for all governmental and law enforcement entities within the State including the AG’s Office that may have to deal with PHI and questions related to medical privacy on what the HIPAA regulations actually mean, and the importance of medical privacy on both the State and Federal level.**

In another comment the Appellate Court referred to another point of “*confusion,*” relating to the AG’s statements to the court in this case. For example, the court stated: *“the Attorney General does not contest that HIPAA generally applies or the Department’s assertion that the Department is a “covered entity” subject to the requirements of HIPAA*

³⁶ 2006 WL 1649003 (Tex.App.-Austin) No other citation is currently available.

³⁷ 2006 WL 1649003 (Tex.App.-Austin) No other citation is currently available.

³⁸ Please see the Privacy rule for that specific definition.

*and the Privacy Rule.”*³⁹

While the AG’s statements to the court indicated that HIPAA applies generally, in a previous statement in 2004 the AG’s Office released its “*Preemption Analysis of Texas Laws Relating to the Privacy of Health Information & the Health Insurance Portability and Accountability Act.*” In that 468 page exhaustive legal research document, (that was disseminated to the public on a broad basis), the AG’s Office stated that organizations and individuals in the State of Texas don’t need to follow Federal HIPAA because State laws are in fact not “pre-empted” by the HIPAA Privacy rule.

However, as the Appellate Court’s statement revealed, the AG’s Office clearly now does “*not contest that HIPAA generally applies...*” Up to the statement in the appellate case, no other mention from the AG’s Office that HIPAA generally applies to the State of Texas, has been offered to the public as guidance as to what law to follow.

It is important to note that in the Zamora case previously referenced in this document, a Federal District Court disagreed with the 2004 AG opinion, (stating that stakeholders in Texas don’t need to follow Federal HIPAA) when that court concluded HIPAA preempted a part of the Texas Health and Safety Code, specifically a section relating to HIV / AIDS. Also, and of great significance, a nurse was prosecuted and plead guilty to a Federal HIPAA violation in Texas.⁴⁰

³⁹ 2006 WL 1649003 (Tex.App.-Austin) No other citation is currently available.

⁴⁰ March 16, 2006 Doctor's Office Employee Convicted of Selling FBI Agent's Medical Records A Texas woman has been convicted of selling the confidential medical record information of a Special Agent with the Federal Bureau of Investigation (FBI) to a person she believed to be working for a drug trafficker. US Attorney Chuck Rosenberg announced her conviction today, and noted that Ramirez faces a maximum punishment of ten (10) years in federal prison, without parole, and a \$250,000 fine at her sentencing set for June 8, 2006. At a hearing held on Monday, March 6, 2006, before US District Judge Randy Crane, Ramirez pleaded guilty to the federal felony offense of wrongfully using a unique health identifier with the intent to sell individually identifiable health information for personal

Finally, please see the analysis, directly above, in the Louisiana Clinic case, (decided in 2002 by a Federal District Court within the 5th Circuit,), wherein the Federal District Court actually applied the HIPAA Privacy rule one year before the rule was enforceable to make their decision in that case.

It light of the situation described above and understanding the responsibility of the HITAC group to make practical recommendations to the State Legislature, **it seems to be a priority for the HITAC to require that the AG's Office clarify their previous statements that indicate HIPAA does not apply to the State of Texas.**

Also, as the remainder of this analysis will demonstrate that **the AG's Office should clarify the exact holding in this case for the purpose of informing the media and the public and all relevant stakeholders about the Appellate Court's ruling in relation to the actual release of medical information in this specific case.** Given the level of inaccurate publicity this case is generating so far,⁴¹ this issue has the impact to affect whether stakeholders follow either Federal HIPAA privacy laws or State privacy laws in relation to the Public Information Act and medical information.

In the alternative, **if the HITAC deems necessary the AG's Office should be educated as to the relevance of this information, in that they appear to be unsure of how HIPAA and medical privacy laws apply to the State of Texas.**

gain. The US proved that during the spring of 2005, Ramirez, who was employed at a doctor's office under contract to provide physicals and medical treatment to FBI agents, offered to and agreed for a price to provide the personal and medical information of an FBI agent to a person she thought was working for a drug trafficker.

<http://www.hipaadvisory.com/news/NewsArchives/2006/mar06.htm>

⁴¹ In fact over 17 news outlets have reported the same thing, that the PIA trumps HIPAA in Texas.

4.3.1.2 THE SPECIFIC HOLDING AS IT RELATES TO MEDICAL INFORMATION IN THE ABBOTT CASE.

The Austin American Statesman stated quoting the AG's Office, "*This opinion gives important guidance to every Texas governmental body that is faced with a public information request for medical information where (the Health Insurance Portability and Accountability Act) applies.*"⁴²

Although this general statement appears to indicate that HIPAA appears to apply to the PIA in the release of medical information, it does not clarify the specific nature of the ruling by the Appellate Court. The analysis that follows will provide the Appellate Court's holding that may assist the reader in understanding how the court actually ruled in this case relating to medical information, HIPAA and the PIA.

To begin with before offering the Appellate Court's holding in this case, it must be stated that numerous media outlets across the country are reporting that the PIA has "Preempted HIPAA."

Again, this kind of misinterpretation could not be further from the **reality** of the Appellate Court's ruling in this case. In fact according to the Appellate Court it was the other way around. The court stated that *HIPAA did not Pre-empted the PIA*. For example the court stated: "*because the Department can comply with both the Privacy Rule and with the Public Information Act, the Public Information Act is not preempted by the Privacy Rule.*"⁴³

The misinformation emanating from the media is significant because it may cause individuals to release PHI under the assumption that it is not a violation of any law either on the **State or Federal level**. The media misinformation may be due to a series of

⁴² <http://www.statesman.com/news/content/news/stories/local/06/17opinion.html>

⁴³ 2006 WL 1649003 (Tex.App.-Austin) No other citation is currently available.

misinformed statements coming from the AG's Office involving this issue. Please see the AG's Opinion on the Preemption Analysis involving HIPAA.

The Appellate Court's conclusion in this case outlined the way that the PIA and HIPAA work together. The Court's conclusions attempt to offer guidance to "covered entities" when dealing with a request for disclosure of medical information.

For example the court stated: *"We conclude that covered entities faced with a request for disclosure involving potentially protected health information must examine the information in light of HIPAA and the Privacy Rule to determine if the information is protected health information that is generally not subject to disclosure. 42 U.S.C.A. § 1320d(6); 45 C.F.R. § 160.103. If the request does not involve protected health information, then HIPAA and the Privacy Rule do not prohibit disclosure of the information. If the request asks for information that is protected health information, then the agency must ascertain if any exception to non-disclosure in the Privacy Rule applies. If no exception applies, the agency may release the information if potential identifiers are redacted or if a statistician determines that release of the information cannot be used to identify any individual. 45 C.F.R. § 164.514."*⁴⁴

Again, in relation to the HIPAA Privacy rule and exceptions to "non-disclosures" the court stated: *"If an exception to non-disclosure does apply, the agency must release the information. For example, if the request is made under the authority of a statute that requires disclosure, then the exception found in section 164.512(a) applies, and the agency must disclose the information as long as the disclosure complies with all relevant requirements of the statute compelling disclosure. Id. § 164.512(a)(1)."*

Finally the Appellate Court qualified this last statement about the exceptions to non-disclosures using the Public Information Act and offered specific guidance to all

⁴⁴ 2006 WL 1649003 (Tex.App.-Austin) No other citation is currently available.

stakeholders explaining how they should handle “requests for protected health information” under the PIA.

The court stated clearly: *“If a request for protected health information is made under the Public Information Act, then the exception to non-disclosure found in section 164.512(a) of the Privacy Rule applies, and the agency must determine whether the Act compels the disclosure or whether the information is excepted from disclosure under the Act. For example, if the information is considered confidential by judicial decision, statute, or the constitution, then the information is not subject to disclosure under the “confidential” exception to disclosure found in the Public Information Act. See Tex. Gov’t Code Ann. § 552.101; see also Tex. Occ.Code Ann. § 159.002 (West 2004) (patient records and communications between patient and physician confidential).”*

The Appellate Court appears to be making the clear statement that medical information is considered confidential *“by judicial decision, statute, or the constitution,”* thus not actually disclose-able.

It appears that the clear legal message in the Appellate ruling is not getting through to the media and the AG’s Office may also need clarification since the message being disseminated is that the Public Information Act “trumps” HIPAA.

Once again since it is the responsibility of the HITAC to make practical recommendations, ***it is of the highest priority that a special medical privacy group be assembled consisting of State and Federal Privacy experts to assist in getting an accurate message out to the public at large and the stakeholders affected by both State and Federal privacy laws.***

Since a prosecution has occurred relating to HIPAA, and given the level of widespread misinformation emanating from a wide variety of sources, the inaccurate message that “The PIA trumps HIPAA,” without any further clarification, amounts to a disservice to stakeholders and the individual “constitutional rights” of American citizens, (as that right has been explained above in this document). ***The HITAC should reconsider their previous recommendations placing the responsibility of medical privacy and security compliance as the sole responsibility of the Attorney General’s Office since that Office has not projected a clear and consistent position on the applicability and importance of ensuring the implementation of medical privacy laws within the State of Texas on both the State and Federal levels***

Finally, the Appellate Court ruled as follows: *“No exception to disclosure in the Public Information Act applies to the release of statistical information regarding abuse at individual government facilities. See id. § § 552.101-.1425. The confidentiality exception listed in section 552.101 does not apply because no law renders the information confidential, and the Department has not referred us to any case, and we have found none, holding that aggregate statistical information of the type requested in this case is confidential.”* Also, *“therefore, we conclude that disclosure of the information requested will comply with all relevant requirements of the Public*

*Information Act, HIPAA, and the Privacy Rule.*⁴⁵

4.3.2 SUMMARY OF RECOMMENDATIONS

Given the all of the facts stated directly above these recommendations are offered as high priority recommendation for the HITAC to consider. **The dissemination of misleading or inaccurate information relating to a legal determination in a case, or statement from the Attorney General's Office would impact stakeholder's compliance with federal and state laws regulating the use and sharing of health information and the HITAC's "long range plan."**

15. Basic Education

It may be advisable that the HITAC recommend some basic education for all law enforcement individuals within the State including the AG's Office and other law enforcement officials on the HIPAA regulations and the importance of medical privacy on the State and Federal level.

16. Clarification of Past Statements

It appears necessary that the HITAC group require as a high priority, that the AG's Office clarify its previous statements that HIPAA does not apply to the State of Texas.

17. Clarification of Holding

⁴⁵ 2006 WL 1649003 (Tex.App.-Austin) No other citation is currently available.

In addition the AG's Office must clarify the exact holding in the Appellate case for the purpose of informing the public and all relevant stakeholders accurately about the ruling in relation to the actual release of medical information in this specific case.

18. AG Education

The AG's Office requires education as to the relevance of HIPAA and medical privacy laws, in that they appear to be unsure of how HIPAA and medical privacy laws apply to the State of Texas.

It is of the highest priority that a special medical privacy group be assembled consisting of State and Federal Privacy experts to assist in getting an accurate message out to the public at large and to the stakeholders affected by both State and Federal privacy laws.

Finally the HITAC should reconsider their previous recommendations placing the responsibility of medical privacy and security compliance as the sole responsibility of the Attorney General's Office since that Office has not projected a clear and consistent position on the applicability and importance of ensuring the implementation of medical privacy laws within the State of Texas on both the State and Federal levels.

Postscript: (A note to the reader):

Since the original draft of this document was submitted to the HITAC on June 30, 2006, the Court of Appeals in Austin has re-submitted their opinion in this case. Although all of the conclusions and statements of the Court cited in this document appear in the re-drafted opinion dated August 30, 2006, (please see 2006 WL 2504417 (Tex.App.-Austin), the Court added some additional language.

This language appears to be significant, the Appellate Court added information in footnote number four in the Conclusion section of the opinion relating to "statistical information."

In the body of the opinion the Court stated: *"Statistical information regarding allegations of abuse and subsequent investigations does not seem to relate to issues regarding health or condition in general and certainly does not relate to the health or condition of an individual, "the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual."*

In footnote number four the Court stated: *"In making this statement, we do not imply that statistical information can never constitute protected health information. Rather, we merely state that the information requested in this case does not seem to fall within the definitions of protected health information found in HIPAA or the Privacy Rule."*

The Appellate Court appears to be indicating that in some instances, statistical information can qualify as PHI.

Finally as stated case law in this area is constantly changing; this document represents current holdings.

4.4 ANALYSIS

Although the cases analyzed in this section are significant, at the present time there does not appear to be a great number of State Appellate court cases interpreting HIPAA, thus it may be a future challenge or barrier to the adoption of HIE and HIT.

4.5 RECOMMENDATIONS

19. Monitor the Development of the use of HIPAA

The HITAC should recommend that the development of the application of HIPAA be monitored with in the State of Texas.

The Consumer Workgroup utilizes a specific “methodology” to produce recommendations to the HITAC in relation to interview information gathered from stakeholders. That work flow will be outlined in detail before it is applied to the interview information to produce recommendations to the HITAC.

This section of the document provides the details of the methodology on how the Consumer Workgroup produced the recommendations based on interview information associated with the three responsibilities of “*documenting real and perceived legal, regulatory and business barriers that could hinder participation in health information exchange;*” and “*defining legal challenges that all states encounter with respect to federal regulations;*” finally, “*documenting specific Texas regulations and policies that might impact the adoption of Health Information Technology, (HIT), and Health Information Exchange, (HIE).*”

5 THE CONSUMER WORKGROUP METHODOLOGY DEFINED

5.1 INFORMATION GATHERING

The Consumer Work Group was tasked with three specific responsibilities involving state and federal medical privacy and security laws.

5.1.1 THE FIRST REQUIREMENT OR “CHARGE” STATES:

“Document real and perceived legal / regulatory / business barriers that could hinder participation in health information exchange.”

The second and third charges or deliverables state:

“Define legal challenges that all states encounter with respect to Federal regulations;

Document specific Texas regulations and policies that might impact the adoption of HIT and HIE.”

In order to fulfill this responsibility, health care provider organizations and practitioners in the field were interviewed. Thus, interviews of responsible individuals had to be completed.

The Consumer Work Group determined that the best way to interview practitioners about their problems with complying with federal and state privacy laws was to ask a series of general, non-leading questions that allowed the interviewees (or “stakeholders” the ability to candidly respond, yet remain anonymous as desired.

A series of questions were prepared and submitted to stakeholders for review and responses. For example, the following questions were asked, “What privacy rules give your organization the biggest headaches,” and “Can you offer 10 privacy rules that you believe are important.” The responses to these questions provided data for the first deliverable or charge of the Consumer Work Group stated directly above.

5.2 RESULTS

Stakeholders offered candid responses about their real and perceived problems, the level of awareness and attention their organization spent on complying with medical privacy laws. Again, that data was used to fulfill the requirements of the first charge or deliverable, specifically information gathering.

The Consumer Work Group employed a specific methodology in fulfilling the responsibility of completing the first deliverable to ultimately provide recommendations to the HITAC. That methodology will be outlined directly below.

5.3 METHODOLOGY EMPLOYED ON FIRST DELIVERABLE

Initially all responses were recorded and the interviewee allowed the ability to edit and ensure their responses were recorded accurately. In the alternative interviewees were simply given the questions to fill out on their own.

The information was gathered and sorted into two categories according to the responses tendered. The first category was “REAL” barriers and the second was “PERCIEVED” barriers. These categories were not determined subjectively but objectively according to legal analysis and specific case law and regulatory mandates.

For example, if stakeholders stated that their organization was unsure about what law to follow in Texas, that specific response, although quite real to the stakeholder and the organization, would be classified as a perceived barrier, or problem. The reasoning behind this classification is case law and court holdings applying the federal HIPAA privacy rules to the State of Texas, this includes a widely publicized prosecution for a violation of HIPAA as well.

Also, even if the interviewee was unaware of this information and truly did not believe their organization had to follow federal rules, the response would be classified as perceived because of the specific federal court ruling on this matter.

A “Real Barrier” would be a response such as ‘our organization follows Title 7 Chapter 611 Subtitle E entitled “Special Provisions Relating to Mental Illness and Mental Retardation, Mental Health Records of the Texas Health and Safety Code.’

The purposes of this categorization is simple, it will offer readers a clear picture of the barriers or problems associated with following medical privacy and security laws, (by real practitioners), while informing the readers of the law.

Immediately following the categorization of every response will be the legal justification for that specific categorization and whether that response shows an awareness of current law, (or is unaware of current law). This is critical to understanding since the legal landscape with medical privacy laws are constantly changing in today's environment.

Also, the purpose of offering legal information is to inform the reader of the laws and set the stage for offering recommendations. Recommendations will be provided through discerning problems that practitioners are having with actually following the laws.

Again, the purpose of the Consumer Work Group in fulfilling the first deliverable is to offer "real and perceived legal / regulatory / business barriers that could hinder participation in a health information exchange." These barriers or problems can only be discerned from actual people and organizations attempting to apply and follow the myriad of medical privacy laws on both the state and federal levels.

5.4 RECOMMENDATIONS:

As stated recommendations were a response to real and perceived problems the interviewees were having from actually complying with the laws. These recommendations are supported by legal analysis. Before a recommendation was offered by the Consumer Work Group, the problem the recommendation was derived from and meant to solve, was legally "vetted" or justified according to case law, statutory or regulatory requirements. In other words it was determined whether or not the problem the interviewee stated had a real document-able legal solution that could be solved by a recommendation based in legal precedent.

5.4.1 THE SECOND CHARGE OR REQUIREMENT STATES:

"Define legal challenges that all states encounter with respect to Federal regulations."

5.5 METHODOLOGY EMPLOYED ON THE SECOND DELIVERABLE

This deliverable can be satisfied by conducting case law research on HIPAA enforcement to date. Federal level cases affecting the State of Texas, along with specific rulings will be presented to inform the reader of current enforcement trends, and interpretations of the Privacy rule by federal level courts.

5.6 RECOMMENDATIONS

Specific recommendations can be derived from the process of analyzing precedent. For example, since precedent is developing at a rapid rate, stakeholders need to be aware of these developments.

The entire Consumer Work Group will participate in creating these recommendations offered to the HITAC.

5.6.1 THE THIRD CHARGE OR REQUIREMENT STATES:

“Document specific Texas regulations and policies that might impact the adoption of HIT and HIE.”

5.7 METHODOLOGY EMPLOYED ON THE THIRD DELIVERABLE

This deliverable can be satisfied via information gathered from the interview process. Specific Texas regulations will be presented that were a part of the information gathering phase of the project.

5.8 RECOMMENDATIONS

Specific recommendations will be offered as appropriate.

6 APPLICATION OF THE METHODOLOGY TO THE INFORMATION GATHERED

6.1 INTRODUCTION

All participants in this project were candid in their responses. The respondents were willing to share their information on their experiences in implementing federal and state privacy laws. Interviewees were asked a series of general questions; they were told to explain some of the problems they were having in implementing privacy and security laws. Consequently, all interviewees will remain anonymous.

The result of the interviews was positive; interviewees shared their issues and concerns

about complying with medical privacy and security laws. A copy of the questions presented may be reviewed in the Appendix section of this document.

Again the first deliverable requires that the Consumer Workgroup: *“Document real and perceived legal / regulatory / business barriers that could hinder participation in health information exchange.”*

6.2 APPLICATION OF “METHODOLOGY” TO THE FIRST DELIVERABLE:

6.2.1 QUESTION PRESENTED:

Q: What are the most important Privacy laws that your organization recognizes?

6.2.1.1 RESPONSE:

All stakeholders or “interviewees” responded with the Health Insurance Portability and Accountability Act or HIPAA.

One interviewee stated: *“The Health Insurance Portability and Accountability Act (HIPAA) is the only security rule that specifically impacts Healthcare. Within HIPAA, there are the Security Standards and the ‘mini-security rule’ within the Privacy Standards which requires the “appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.”*

Several interviewees, (but not unanimously), mentioned the following State laws:

The Texas Health and Safety Code, specifically sections:

Chapter 81 entitled “Communicable Diseases,” and Chapter 611, entitled, “Mental Health Records.”

One interviewee stated that a problem their organization was having involved *“comparing the federal and state laws on medical information privacy and security.”*

6.2.1.2 CATEGORIZATION: (REAL OR PERCEIVED BARRIER)

The responses would be categorized as real barriers, i.e., stakeholders are complying with both state and federal laws since they face conflicting compliance requirements from two authoritative sources, one on the state level the other on the federal level.

The exception would be the Texas Health and Safety Code Chapter 81. That “issue” would be categorized as a perceived barrier in relation to the comparing of federal and state laws to determine which law to follow, (which was a problem mentioned by one of

the stakeholders), as a response to question number one.

The Federal District Court in Corpus Christi provided a solution between following either section 81.103 or HIPAA. Consequently, this issue would be considered perceived in that the interviewees may be unaware of this recent ruling.

The legal justification that follows does not represent a reason or “legal advice” for stakeholders to disregard any specific State law privacy mandates; however it does provide a potential solution to the issue of conflict between the federal and state law problem expressed by one of the interviewees. This solution would relate to section 81.103 of the Texas Health and Safety Code. *Of course, this analysis is offered for informational purposes only.*

6.2.1.3 LEGAL JUSTIFICATION

There are two sources of legal information in Texas that impact the actions of stakeholders in the state. The first is an existing legal opinion by the State’s Attorney General’s Office that states that individuals and organizations affected by medical privacy laws should follow the state laws in that the state laws preempt the federal laws.⁴⁶

The second source of legal authority is the Federal Health Insurance Portability and Accountability Act of 1996, specifically the Privacy and Security rules and regulations.⁴⁷

Consequently this barrier is a real barrier to the adoption of HIE and HIT, until further clarification on which set of laws to follow in relation to conflicts between the two sets of

⁴⁶ See the “Preemption Analysis of the Texas Laws Relating to the Privacy of Health Information and the Health Insurance Portability and Accountability Act and Privacy Rules, (HIPAA)”

⁴⁷ See the HIPAA regulations and rules generally. 45 Code of Federal Regulations, sections 160 – 164.

laws is offered by judicial authorities, or the State Legislature.

There is an exception to this problem as provided for by the Federal District Court in Corpus Christ. That court offered a solution to the overall issue of which set of laws to follow in one specific area of medical privacy that happens to involve the disclosure of a “Communicable Diseases” specifically AIDS / HIV. For example, that court offered the following solution in a section of the Zamora case entitled: “B. Preemption of Texas Health and Safety Code Section 81.103.”

In the Zamora case the Bay Area Health Group contended that the government was not entitled to receive the results of a blood test done upon the defendant Zamora due to section 81.103 of the Texas Health and Safety Code. Zamora was on trial for driving while intoxicated.

The court offered a solution after questioning whether section 81.103 ⁴⁸ is even

⁴⁸ § 81.103. CONFIDENTIALITY; CRIMINAL PENALTY. (a) A test result is confidential. A person that possesses or has knowledge of a test result may not release or disclose the test result or allow the test result to become known except as provided by this section. (b) A test result may be released to: (1) the department under this chapter; (2) a local health authority if reporting is required under this chapter; (3) the Centers for Disease Control of the United States Public Health Service if reporting is required by federal law or regulation; (4) the physician or other person authorized by law who ordered the test; (5) a physician, nurse, or other health care personnel who have a legitimate need to know the test result in order to provide for their protection and to provide for the patient's health and welfare; (6) the person tested or a person legally authorized to consent to the test on the person's behalf;(7) the spouse of the person tested if the person tests positive for AIDS or HIV infection, antibodies to HIV, or infection with any other probable causative agent of AIDS;(8) a person authorized to receive test results under Article 21.31, Code of Criminal Procedure, concerning a person who is tested as required or authorized under that article; and (9) a person exposed to HIV infection as provided by Section 81.050. (c) The court shall notify persons receiving test results under Subsection (b) (8) of the requirements of this section. (d) A person tested or a person legally authorized to consent to the test on the person's behalf may voluntarily release or disclose that person's test results to any other person, and may authorize the release or disclosure of the test results. An authorization under this subsection must be in writing and signed by the person tested or the person legally authorized to consent to the test on the person's behalf. The authorization must state the person or class of persons to whom the test results may be released or disclosed. (e) A person may release or disclose a test result for statistical summary purposes only without the written consent of the person tested if information that could identify the person is removed from the report. (f) A

applicable in this case;” they stated: “even assuming that defendant did undergo HIV testing as part of her hospital visit, any results would not be relevant to the medical records that the government seeks. **As such, the appropriate remedy would be to redact any references to HIV testing.** Consequently, Bay Area’s arguments regarding the applicability of § 81.103 in this case must fail.” Ultimately the court ruled that disclosure was permissible, after offering the solution mentioned directly above involving section 81.103 of the Texas Health and Safety Code.

Consequently stakeholders have a potential solution on what law to follow and how to follow that law in relation to HIPAA and section 81.103. This specific barrier may be classified as a perceived barrier based the facts and the fact that a federal legal solution does exist, at least for the present time.

6.2.1.4 RECOMMENDATION

20.Reduce the Confusion on what set of laws to follow:

blood bank may report positive blood test results indicating the name of a donor with a possible infectious disease to other blood banks if the blood bank does not disclose the infectious disease that the donor has or is suspected of having. A report under this subsection is not a breach of any confidential relationship. (g) A blood bank may report blood test results to the hospitals where the blood was transfused, to the physician who transfused the infected blood, and to the recipient of the blood. A blood bank may also report blood test results for statistical purposes. A report under this subsection may not disclose the name of the donor or person tested or any information that could result in the disclosure of the donor's or person's name, including an address, social security number, a designated recipient, or replacement information. (h) A blood bank may provide blood samples to hospitals, laboratories, and other blood banks for additional, repetitive, or different testing. (i) An employee of a health care facility whose job requires the employee to deal with permanent medical records may view test results in the performance of the employee's duties under reasonable health care facility practices. The test results viewed are confidential under this chapter. (j) A person commits an offense if, with criminal negligence and in violation of this section, the person releases or discloses a test result or other information or allows a test result or other information to become known. An offense under this subsection is a Class A misdemeanor.

This recommendation takes several parts; each part is intended to provide a potential solution for the HITAC to recommend to the State Legislature.

The first recommendation or solution would be for the HITAC to recommend to the State Legislature that an official statement be issued by the appropriate State agency that all organizations and individuals in the State of Texas that are subject to the HIPAA rules, need to understand and comply with all federal HIPAA regulations, including keeping up with changes in the law, also required specifically by the HIPAA regulations themselves.⁴⁹

The second part of this recommendation would be for the HITAC to recommend to the State Legislature that an independent research group be commissioned that is devoted to keeping up with the changes in the federal HIPAA regulations as interpreted by the federal courts. Likewise this group would need to issue pronouncements to all stakeholders of changes that affect stakeholders similar to the analysis of the Zamora case mentioned above.

OR

In the alternative to commissioning an independent study group, the HITAC should recommend to the State Legislature that they adopt a mirror set of HIPAA rules and regulations including a mirror set of enforcement rules. Also, that the State Legislature ensure that these mirror rules actually get enforced. This would solve the problem that stakeholders are having with discerning between two sets of laws, in that the State of Texas would require that all stakeholders that use or share medical information, or PHI, follow both sets of laws on the State level. Enforcement is the key to this recommendation. Without enforcement, most organizations are not willing to spend the time and effort to become truly

⁴⁹ 45 CFR § 164.530 (i) (3), entitled "Changes in the Law."

compliant with either State or Federal privacy rules. For example please see the statement by the Secretary of the Veterans Administration on this issue cited in the footnote below.⁵⁰ In fact, this suggestion was made by an interviewee that

⁵⁰ **VA Secretary Wants Penalties for Mishandling Personal Data**

By [Stephen Barr](#)

Friday, June 9, 2006; Page D04

<http://www.washingtonpost.com/wp-dyn/content/article/2006/06/08/AR2006060801806.html>

The secretary of veterans affairs, *R. James Nicholson*, in the spotlight because of a breakdown in data security, called yesterday for tougher penalties on federal employees who mishandle sensitive information.

Nicholson told the House Government Reform Committee that it is "too hard, in my opinion, to discipline people in the civil service -- it's too hard to impose sanctions."

He recommended that the committee look at the 1996 Health Insurance Portability and Accountability Act, or HIPAA, as a model. The law allows the government to levy fines against individuals, doctors and hospitals that violate patient privacy rules and, in cases of intentional violations, permits the Justice Department to pursue criminal penalties.

"I think we should consider putting the same kind of teeth into an enforcement mechanism for the compromising and the careless and negligent handling of personal information," Nicholson said.

In early May, a career employee of the Veterans Affairs Department reported the theft from his Maryland home of a laptop computer and a hard drive containing names, Social Security numbers and dates of birth of at least 26.5 million veterans and active-duty members of the armed forces, including the National Guard and reserves.

The employee was not authorized to work on the files at home, the VA said. Officials have placed the employee on administrative leave and started the process that leads to a firing. Two superiors, including a political appointee, have been "let go," Nicholson testified.

Nicholson said the government conducts background investigations on employees who are given access to classified information but said "we do not have a similar screen for those to whom we will give enormous amounts of data."

The employee who took the data home has worked at the VA for 34 years but had not had a background check in 32, Nicholson said. The employee had signed this year's form on security awareness, he said.

wished to remain anonymous. Finally this recommendation would assist the HITAC in fulfilling their statutory responsibilities associated with developing a “long range plan for health information technology.” For example, all stakeholders affected by state and federal laws regulating the use and sharing of health information would be required to comply with the law so long as

Members of the House Government Reform Committee, chaired by Rep. *Thomas M. Davis III* (R-Va.), did not directly address Nicholson's suggestion that Congress move to provide additional sanctions against federal employees who compromise personal information and put citizens at risk of identity theft.

"It is beyond stupid to take out sensitive documents," Rep. *Christopher Shays* (R-Conn.) said. "But I have a sense that this is a common practice."

Clay Johnson III, a deputy director at the Office of Management and Budget, said there are dozens of security breaches involving laptops each year. In the VA case, he said, "the magnitude of it is the alarming thing."

Johnson said he thinks federal laws, policies and standards are sound, "but we can and must do a much, much better job of implementing them." He said federal policy calls for data encryption and the use of passwords to protect data taken out of the office on laptops. The information on the stolen VA laptop was not encrypted, officials have said.

As part of an effort to strengthen data security at the VA, Nicholson said he has instructed the department's 235,000 employees to complete privacy and cybersecurity training by June 30.

During the week of June 26, VA employees across the nation will "stand down" so managers can review information security and reinforce privacy obligations with their staffs, Nicholson said.

He also has banned employees who adjudicate benefit claims from taking files from regular workstations to alternative locations or to their homes for processing. He also has prohibited employees from using personal laptops or computers for VA business, including for access to the department's "virtual private network." About 35,000 VA employees have access to the department's secure network.

Nicholson said the department has an obligation to ensure that employees "have the right training, that they have been instilled with the sense of discipline and the commitment to be careful in their trusteeship of this data."

enforcement occurred.

21. Enforcement Recommendation

As previously stated, enforcement of the privacy regulations must be promoted. Consequently the HITAC should recommend that the State legislature require the enforcement of the law particularly if they adopt the mirror HIPAA provision on the State level.

6.2.2 QUESTION PRESENTED

Can you specify one rule or a set of rules that your organizations is specifically aware of? For example, is your organization aware of the minimum necessary rule? Is that an important one to your organization?

6.2.2.1 RESPONSE

The majority of the responses indicated that the “**minimum necessary**” rule was considered an important rule. One stakeholder indicated that their organization was aware of this rule as it pertains to disclosures of PHI. Several educational institutions mentioned a concern over confusion related to which law to follow involving HIPAA and FERPA. In fact one of the stakeholders specifically requested clarification on this issue.

6.2.2.2 CATEGORIZATION, (REAL OR PERCEIVED BARRIERS)

These responses would be categorized as real barriers to the adoption of HIT and HIE. Almost all of these organizations indicated that they attempt to follow the minimum necessary rule. Consequently, with the adoption of more technology in the form of EMR's and uniform network security protocols, organizations “may” view the minimum necessary rule as a barrier to the free use of PHI via technology.

It must be noted that all of the organizations interviewed were large with adequate resources to devote to becoming HIPAA compliant. Generally, smaller organizations do not have the resource nor experience to devote to comprehensive HIPAA compliance.

Consequently, with the adoption of EMR's, those organizations that understand the impact of the “minimum necessary” rule would view it as a barrier to the adoption of HIE and HIT. However, smaller organizations may not understand how this rule impacts the use of technology in medicine, thus they “may” or “may not” view it as a barrier to the adoption of HIE and HIT.

The exception to the categorization as “real” would be the confusion over which set of

laws to follow as it relates to FERPA and HIPAA. That barrier would be classified as a perceived barrier. The legal justification that follows will provide the reasoning for this classification.

6.2.2.3 LEGAL JUSTIFICATION

Much of the confusion surrounding which law to follow relating to HIPAA and FERPA involves a narrow exception to the definition of PHI, which states, *“protected health information excludes individually identifiable health information in: (i) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g.”*

FERPA educational records have been defined very narrowly by the United States Supreme court in OWASSO INDEP. SCHOOL DIST. NO. I-011 v. FALVO, 122 S.Ct. 934 (2002), 939 – 940.

For example the Court stated, *“It is a fundamental canon of statutory construction that the words of a statute must be read in their context and with a view to their place in the overall statutory scheme”*). FERPA, for example, requires educational institutions to *“maintain a record, kept with the education records of each student.”* § 1232g(b)(4)(A). *This record must list those who have requested access to a student’s education records and their reasons for doing so. Ibid. The record of access “shall be available only to parents, [and] to the school official and his assistants who are responsible for the custody of such records.”*

Also, *“FERPA requires “a record” of access for each pupil. This single record must be kept “with the education records.” This suggests Congress contemplated that education records would be kept in one place with a single record of access. By describing a “school official” and “his assistants” as the personnel responsible for the custody of the records, FERPA implies that education records are institutional records kept by a single central custodian, such as a registrar, not individual assignments handled by many student graders in their separate classrooms.”*

Obviously a FERPA record cannot be construed as all of the medical information recorded by a school or university regarding their students. There are many other departments within Independent School Districts and Universities in the State of Texas that record or utilize PHI relating to students for a wide variety of reasons. For example, nursing departments, along with trainers, special education personnel, counselors, risk management, and human resources personnel might all use or record PHI on a regular basis.

As stated the definition of a FERPA, a student record is a *“single”* record or a static record that is created, added to and changed according to a formal process that may involve an attorney. Again the United States Supreme court stated, *“FERPA also*

requires recipients of federal funds to provide parents with a hearing at which they may contest the accuracy of their child's education records. § 1232g(a)(2). The hearings must be conducted "in accordance with regulations of the Secretary," ibid., which in turn require adjudication by a disinterested official and the opportunity for parents to be represented by an attorney. 34 CFR § 99.22 (2001). It is doubtful Congress would have provided parents with this elaborate procedural machinery to challenge the accuracy of the grade on every spelling test and art project the child completes." Id at 940.

The same can be said of medical records, they are similar to "*spelling test grades and art projects.*" It is not feasible that Congress would have contemplated that every medical record be subject to a parental challenge "adjudicated" by an disinterested official...with the child's and the parent's attorney present. Nurses in universities and schools create student medical records regularly without going through the process described as legally mandated by the United States Supreme Court.

Likewise there are many authoritative organizations that have stated that schools and universities in the State of Texas are subject to the HIPAA rules and regulations relating to privacy and security.

The National School Board Administration or NSBA characterized the Owasso holding as follows: "*The United States Supreme Court's narrow interpretation of the term "education records" in Owasso Ind. School Dist. v. Falvo, also likely decreases the FERPA exemption, leaving more student records with health information potentially subject to the HIPAA Privacy Rule.*" The NSBA recommends that schools classify themselves as HIPAA "Hybrid Entities." Please see "Inquiry and Analysis, what to do when the HIPAA Beast is at Your Door." See the January 2003 newsletter, provided by the National School Board's Association's Council of School Attorneys.

In addition, the Texas Department of State Health Services offers schools guidance for HIPAA on their "School Health Information" web site. Please refer to the University of North Carolina or UNC HIPAA Health Information for Schools authored by Jill Moore and Aimee Wall.

That site can be found at <http://www.dshs.state.tx.us/hipaa/schoolhlthinfo.shtm>. The information provided in document can also assist universities in the State of Texas understand how HIPAA applies to them as well.

6.2.2.4 RECOMMENDATION

Communications is a critical part of getting Independent School Districts and Universities in the State of Texas to comply with HIPAA. As stated above, these organizations have received mixed messages from different departments within the State of Texas regarding their need to comply with HIPAA.

The first step toward getting organizations to comply with HIPAA would be to clearly inform them that compliance is a legal requirement.

22. Targeted Communications

Consequently the HITAC needs to recommend that the State Legislature require an authoritative source within the State of Texas, to inform Independent School Districts, and Universities that they need to comply with HIPAA and all other appropriate medical privacy laws on the state level.

The next step involves ensuring that these organizations actually comply with the law. Motivating organizations to take the necessary steps towards complying with HIPAA and state privacy laws can come from monetary rewards or sanctions or audits and enforcement on the state level. Consequently the HITAC should recommend that the State Legislature utilize these tactics to motivate ISDs and universities to comply with the law.