SENATE STAFF ANALYSIS AND ECONOMIC IMPACT STATEMENT

(This document is based on the provisions contained in the legislation as of the latest date listed below.)

Prepared By: Health Care Committee

BILL:	SB 2500
INTRODUCER:	Senator Campbell
SUBJECT:	Patient Records
DATE:	April 3, 2006
REVISED:	

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	Bedford	Wilson	HE	**Favorable**
2.			JU	
3.				
4.				
5.				
6.				

I. Summary:

This bill requires any person or entity that has contracted with a licensed facility as defined in s. 395.002(17), F.S., (hospital, ambulatory surgical center, or mobile surgical facility) to receive individually identifiable health information to disclose to the facility if any of the information is to be transmitted outside the United States. The information must not be transmitted outside the United States unless certain criteria are met. A licensed facility must use a form to obtain written consent from the patient to transmit her or his health information outside the United States. The form must meet certain criteria. The bill provides that a licensed facility may not discriminate against or deny an individual health care services because the person did not provide consent pursuant to this section.

This bill amends s. 395.3025, F.S.

II. Present Situation:

Florida Law Governing Privacy of Health Information

In Florida, patients have a constitutional right to privacy under Article I, Section 23 of the State Constitution, and judicial decisions. Although Florida courts have recognized patients' rights to secure the confidentiality of their health information (medical records) under the right to privacy under the State Constitution, that right must be balanced with and yields to any compelling state interest.[1]

[1] See *State v. Johnso*n, 814 So.2d 390 (Fla.2002) distinguished in *Limbaugh v. State of Florida 2004 WL 2238978* (4th DCA October 6, 2004); and *Rasmussen v. S. Fla. Blood Serv. Inc*., 500 So.2d 533 (Fla.1987) (privacy interests of blood donors defeated AIDS victims claim to obtain via subpoena names and addresses of blood donors who may have contributed the tainted blood).

Since 1951, Florida law (ch. 26684, Laws of Florida) has granted a patient access to his or her own medical records and has required the health care practitioner who created the records to maintain the confidentiality of the records. Two primary sections of Florida law address medical records and grant patients access to their health information, ss. 456.057 and 395.3025, F.S.

Section 456.057, F.S., provides that medical records are confidential and, absent certain exceptions, they cannot be shared with or provided to anyone without the consent of the patient. Subsection (5) identifies the circumstances under which medical records may be released without written authorization from the patient. The circumstances are as follows:

- To any person, firm, or corporation that has procured or furnished such examination or treatment with the patient's consent;

- When compulsory physical examination is made pursuant to Rule 1.360, Florida Rules of Civil Procedure, in which case copies of the medical records shall be furnished to both the defendant and the plaintiff;

- In any civil or criminal action, unless otherwise prohibited by law, upon the issuance of a subpoena from a court of competent jurisdiction and proper notice to the patient or the patient's legal representative by the party seeking such records; or

- For statistical and scientific research, provided the information is abstracted in such a way as to protect the identity of the patient or provided written permission is received from the patient or the patient's legal representative.

The Florida Supreme Court has addressed the issue of whether a health care provider, absent any of the above-referenced circumstances, can disclose confidential information contained in a patient's medical records as part of a medical malpractice action.[2] The court ruled that, pursuant to s. 455.241, F.S., (the predecessor to current s. 456.057(6), F.S.), only a health care provider who is a defendant, or reasonably expects to become a defendant, in a medical malpractice action can discuss a patient's medical condition. The court also held that the health care provider can only discuss the patient's medical condition with his or her attorney in conjunction with the defense of the action. The court determined that a defendant's attorney cannot have ex parte discussions about the patient's medical condition with any other treating health care provider.

Under s. 456.057(16), F.S., a health care practitioner or records owner furnishing copies of reports or records or making the reports or records available for digital scanning must charge no more than the actual cost of copying, including reasonable staff time, or the amount specified in administrative rule by the appropriate board, or the department when there is no board. The Board of Medicine has adopted an administrative rule that imposes a limitation on charges that any person licensed as a medical physician or physician assistant may charge for copying patient records:

- Reasonable costs of reproducing copies of written or typed documents or reports may not be more than $1 per page for the first 25 pages; and 25 cents per page, for each page in

[2] *Acosta v. Richter*, 671 So.2d 149 (Fla. 1996).

> excess of 25 pages. Reasonable costs of reproducing X-rays and other special kinds of records are the actual costs. "Actual costs" means the cost of the material and supplies used to duplicate the record, as well as the labor costs associated with the duplication.[3]

Under s. 395.3025, F.S., licensed facilities under ch. 395, F.S., have the responsibility to furnish patient records, only after discharge and with a written request, to the patient, patient representative, or a few other designated individuals. This information is protected and confidential. There are some exceptions listed in the statute.

Under s. 395.3025(7), F.S., the recipient of any confidential information, other than the patient or patient's representative, cannot use the information for any purpose other than what was provided and cannot disclose the information to anyone else, unless the patient gives written consent. A general authorization is not sufficient for this purpose. The contents of the patient treatment record is confidential and exempt from the provisions of s. 119.07(1), F.S., and s. 24(a), Art. I of the Florida State Constitution. Patient information cannot be used for solicitation or marketing the sale of goods or services without specific written release or authorization.

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Sections 261-264 of the "Administrative Simplification" provisions of HIPAA, enacted August 21, 1996, relate to health information privacy. In addition to protecting the privacy of health information, HIPAA encourages the electronic transfer of health information and requires the development of standards for electronic transactions. The United States Department of Health and Human Services (HHS) issued Standards for Privacy of Individually Identifiable Health Information (Privacy Rule) on December 28, 2000, which was originally scheduled to go into effect on February 26, 2001.[4] The effective date for the Privacy Rule was delayed and the rule took effect on April 14, 2003. The regulations only apply to covered entities (health providers who engage in certain electronic transactions, health plans, and health care clearinghouses). HHS issued transaction and code sets rules for which the compliance date was October 16, 2003. Compliance with a security rule under HIPAA is not mandated until April 2005.

The United States Supreme Court has recognized a limited constitutional protection of personal health information. The United States Supreme Court in *Whalen v. Roe*, 429 U.S. 589 (1977) upheld a state law that created a database of persons who obtained certain controlled substances, and the court recognized an individual's interest in avoiding the disclosure of personal matters within the context of medical information. Although *Whalen* and subsequent federal judicial decisions recognized medical information privacy, the cases had not articulated safeguards that custodians could use to protect the privacy of sensitive information such as medical records. HIPAA and the Privacy Rule provide uniform federal protection for the privacy rights of individuals over their health information.

HIPAA and the Privacy Rule protect the privacy rights of individuals over their health information, grant individuals access to their health information, and allow individuals to amend

[3] See Rule 64B8-10.003, Florida Administrative Code.
[4] See 45 C.F.R. Parts 160 and 164.

their health information under specified circumstances. HIPAA serves as a floor of privacy rights for certain health information, and states are free to adopt laws providing more stringent requirements for the use or disclosure of health information that are more protective of privacy.

Preemption under HIPAA and the Privacy Rule

HIPAA provides for partial preemption of state law. The Privacy Rule does not preempt existing state laws that are more stringent than HIPAA by providing greater confidentiality to protected health information (PHI). To trigger preemption by HIPAA, a state law must relate to *privacy*, and be *contrary* to HIPAA. If the state law is more stringent than the HIPAA standard to which it corresponds, the state law will prevail. If not, then the state law is preempted. HIPAA does not provide for complete preemption whereby competing state law is invalidated. The term "contrary," when used to compare a provision of state law to a HIPAA standard, requirement, or implementation, means that a covered entity would find it impossible to comply with both the state and federal requirements, or the provisions of state law stand as an obstacle to the accomplishment and execution of the full purposes and objectives of HIPAA.[5]

Any state law that is contrary to a standard, requirement, or implementation under the Privacy Rule is preempted, unless an exception applies. Exceptions apply to (1) state laws that affirmatively require the HHS Secretary to officially determine that they are not to be preempted; and (2) those state laws that are "more stringent" which do not require a determination to avoid preemption. Under the first exception, laws that require the HHS Secretary to make an official determination that they are not to be preempted include laws dealing with a State's authority to regulate certain areas. Such laws include those that are needed: to prevent fraud and abuse; to ensure appropriate state regulation of insurance and health plans; for state reporting on health care delivery costs; or for serving a compelling need related to public health, safety or welfare when the HHS Secretary has made a determination that the intrusion is warranted, when balanced against the needs that are served.

State laws or portions of state law can be preserved and followed under that type of preemption analysis. The Privacy Rule and HIPAA define "state law" to include the State Constitution, statutes, regulations, rules, common law, or other state action having the force and effect of law.[6]

In the context of a comparison of a state law and a HIPAA standard, "more stringent" means that the state law meets one or more of the following criteria:

- Prohibits or further limits the use or disclosure of PHI, with exceptions, if the disclosure is required by the HHS Secretary in connection with determining whether a covered entity is in compliance with HIPAA or if the disclosure is to the individual who is the subject of the individually identifiable health information;

- Provides individuals with greater rights or access to, or amendment of, their individually identifiable health information;

[5] See 45 C.F.R. 160.202.
[6] See 45 C.F.R. 160.202.

- Allows for greater disclosure of information regarding the use of an individual's health information;

- Imposes tighter requirements for authorizing or consenting to disclosure of individually identifiable health information or reduces the coercive effect of the circumstances surrounding the authorization or consent;

- Increases record-keeping or accounting of disclosures of PHI; or

- Strengthens privacy protection for individuals who are the subject of individually identifiable health information.[7]

To avoid being preempted, state laws that are "more stringent" than the Privacy Rule do not require a determination by the HHS Secretary. The courts are the final arbiter of whether a state law is more stringent. Health care providers and others who provided comments to the proposed Privacy Rule recommended that a process be established under which HHS would be required to perform an initial state-by-state critical analysis to provide guidance on which state laws will not be preempted.[8] Many commenters argued that the HHS Secretary should complete the analysis before the compliance date and that the HHS Secretary should bear the cost of the analysis of state laws.[9] The preamble of the proposed Privacy Rule recognized that the private sector, in the context of individual markets, could more efficiently complete an analysis of applicable state medical privacy laws to determine preemption issues which may arise in implementing the Privacy Rule.

The Privacy Rule appears to impose a duty on covered entities, which include health plans, health clearinghouses, and health care providers, to initially perform a review and evaluation of each applicable state law and perform a preemption analysis for each state law. Various opinions regarding HIPAA preemption probably will exist. Under the Privacy Rule, any person may request that the HHS Secretary grant an exception determination from HIPAA preemption for particular state laws.[10] In addition to a state law review, some entities covered by the Privacy Rule will also have to comply with other federal laws and regulations and must formulate an analysis as to the appropriate procedure to follow that would allow the entity to comply with applicable federal law and the Privacy Rule.

HIPAA Privacy Rule

*Uses and Disclosures Allowed under the Privacy Rule***.**
The Privacy Rule addresses the use and disclosure of PHI and establishes a floor of rights to allow individuals to obtain and control access to their health information. The Privacy Rule covers individually identifiable health information that is transmitted or maintained in any form

[7] Id.
[8] HHS Final Rule on Standards for Privacy of Individually Identifiable Health Information (December 28, 2004) 65 Fed. Reg. 82462 at 82583.
[9] Id.
[10] See 45 C.F.R. 160.204 (a) which provides that a request to except a provision of state law from preemption under 45 C.F.R. 160.203 (a) may be submitted to the Secretary. If a State makes a request, then it must be submitted through its chief elected official.

by a covered entity. Covered entities may use and disclose an individual's PHI for treatment, payment, or health care operations in accordance with the Privacy Rule, without obtaining the individual's authorization.

The Privacy Rule does not affect an individual's right to execute a written authorization for the release of medical records and data. A covered entity may disclose an individual's PHI without an authorization for certain public health and law enforcement activities, and for judicial and administrative proceedings required by law. If a waiver of authorization is obtained from an Institutional Review Board or a privacy board, and other requirements are met, an individual's authorization is not required for disclosures for research purposes. In the absence of an executed authorization by the individual who is the subject of the PHI, the Privacy Rule gives discretion to covered entities, in various circumstances, to disclose PHI to family and friends, public health authorities, and health researchers.

Rights of Access, Amendment, Disclosure, and Complaint. Individuals who are the subject of PHI are afforded rights relating to their access to, and the use of their PHI by covered entities. Under the Privacy Rule, individuals have the right to inspect and copy their PHI, and to request amendments to such records. PHI excludes psychotherapy notes. If an individual agrees, in advance, a covered entity may provide a summary or report of the PHI in lieu of actual copies of the records. Covered entities must give individuals a notice of privacy which outlines the uses and disclosures of their PHI and informs individuals regarding their rights and the responsibilities of the covered entity. *Covered entities must provide individuals the right to request and receive a list of any disclosures of their PHI that have been shared with others for any purpose other than treatment, payment, or health care operations.* The Privacy Rule does not create a private cause of action to allow a person to sue for violations of the rule. Any person who believes that a covered entity has not complied with the Privacy Rule may file a complaint with the HHS Office of Civil Rights.

Covered Entities' Responsibilities. The Privacy Rule directly regulates health care providers, health plans, and health care clearinghouses (covered entities) that bill or transmit other information electronically with certain transactions. Covered entities must adopt, implement, monitor and maintain compliance programs to ensure that the Privacy Rule's requirements for PHI are followed. Each covered entity must designate a privacy officer, and establish safeguards to ensure that its staff is in compliance with the Privacy Rule.

When using or disclosing PHI or when requesting PHI from another covered entity, a covered entity must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. The Privacy Rule permits an entire medical record to be disclosed or requested by a health care provider for purposes of treatment.

The Privacy Rule requires covered entities to account to individuals for disclosures, but they do not have to account for disclosures made for treatment, payment, or health care operations. Covered entities are not required to account for disclosures to law enforcement as required by law, disclosures compelled by court order, or disclosures made for compliance with certain health care oversight agency activities such as the tracking of births or deaths.

Enforcement of the Privacy Rule. The HHS Office of Civil Rights enforces the Privacy Rule through a complaint-driven mechanism and provides guidance to common questions regarding the rule. Congress gave HHS jurisdiction over civil enforcement and the U.S. Department of Justice (DOJ) jurisdiction over criminal investigations and prosecutions. Congress mandated that the agency charged with the civil enforcement of the HIPAA Privacy Rule do so by resolving complaints through informal means before levying any fines. The required intent for a violation under the HIPAA Privacy Rule is that a person knew or should have known that he or she was violating the rule. HHS encourages covered entities and patients to try to resolve their differences before resorting to the complaint process.

Over half of about 5,000 complaints filed in the first year of the Privacy Rule had been resolved as of May, 2004. Fifty of those complaints had been referred to the DOJ for investigation and possible criminal prosecution. The majority of complaints alleged: impermissible use or disclosure of PHI; lack of adequate safeguards to prevent such use or disclosure; failure to provide access to PHI; disclosure of PHI that exceeds the 'minimum necessary' standards; and failure to provide notice of privacy practices.[11] The entities most frequently named in complaints include private health care providers, general hospitals, pharmacies, outpatient facilities, and group health plans.[12] A recent report found that nearly two-thirds of the privacy complaints closed during the Privacy Rule's first year of operation fell outside the scope or time frame of the rule.[13]

III. Effect of Proposed Changes:

Section 1. Amends s. 395.3025(7), F.S., relating to release of medical information by licensed facilities, to require a person or entity that has contracted or subcontracted with a licensed facility to receive health information to disclose to the licensed facility if any of the information will be transmitted out of the United States. A licensed facility or a person or entity that has contracted with a licensed facility cannot transmit health information outside the United States unless all of the following apply:

- The licensed facility has disclosed to the patient upon admission, or as soon as practicable after admission, that her or his health information may be transmitted to a site outside the United States.
- The licensed facility has obtained written consent from the patient to transmit her or his health information outside the United States.
- The consent of the patient has been granted or renewed on an annual basis.
- The patient has been informed that she or he can withdraw consent at any time.

[11] Bureau of National Affairs Health Law Reporter, Vol. 13, No. 20, May 13, 2004 p. 712.
[12] Id.
[13] "Health Information," U.S. Gov't Accountability Office Report 04-965, Sept. 2004.

A form meeting the following criteria must be used to obtain the consent to transmit health information to a site outside the United States (unless it is a request for health care services initiated by a person seeking diagnosis or treatment outside the United States):

- The form must be a separate document.
- It must be dated and signed by the patient whose information is being transmitted.
- It must clearly state all of the following:
    - That by signing, the patient is consenting to the transmission of her or his individually identifiable health information to a site outside the United States where the information is not protected by confidentiality laws.
    - That the licensed facility must get the consent annually.
    - That the patient may revoke consent at any time using a procedure specified on the form.

A licensed facility cannot discriminate against someone or deny health care services to them if they refuse to consent pursuant to this subsection.

Section 2. Provides that this bill take effect on July 1, 2006.

IV. Constitutional Issues:

A. Municipality/County Mandates Restrictions:

The provisions of this bill have no impact on municipalities and the counties under the requirements of Article VII, Section 18 of the Florida Constitution.

B. Public Records/Open Meetings Issues:

The provisions of this bill have no impact on public records or open meetings issues under the requirements of Art. I, s. 24(a) and (b) of the Florida Constitution.

C. Trust Funds Restrictions:

The provisions of this bill have no impact on the trust fund restrictions under the requirements of Article III, Subsection 19(f) of the Florida Constitution.

V. Economic Impact and Fiscal Note:

A. Tax/Fee Issues:

None.

B. Private Sector Impact:

To the extent that facilities licensed under ch. 395, F.S., provide individually identifiable health information to entities that transmit such information outside of the United States, the facilities will incur costs to implement this bill.

C. Government Sector Impact:

None.

VI. Technical Deficiencies:

None.

VII. Related Issues:

None.

VIII. Summary of Amendments:

None.