The Florida Senate

Interim Project Report 2005-142 *November 2004*

Committee on Health Care Senator Durell Peaden, Jr., Chair

REVIEW OF STATUTES REGULATING ACCESS TO PATIENT MEDICAL RECORDS

SUMMARY

The purpose of this project is to review the fundamentals of federal preemption of state law and regulations providing for health information privacy and to promote a better understanding of the privacy requirements of the Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, (HIPAA). This report focuses on Florida law that regulates the privacy of and patient access to individual health records.

Covered entities seeking to comply with HIPAA and the federal Privacy Rule must compare applicable state laws relating to privacy with HIPAA and formulate a strategy to comply with any other applicable federal law. A comprehensive interpretation of state laws relating to privacy, for purposes of HIPAA preemption, requires both legal and practical knowledge of how the state laws relating to privacy interplay with HIPAA and applicable federal law. The compliance date for the Privacy Rule was April 14, 2003. There has been very little time for implementation and for affected parties to be fully educated about the Privacy Rule and how it interplays with state law. Due to the complexities of HIPAA preemption analysis, it is recommended that the state encourage collaborative efforts between stakeholders to complete a comprehensive analysis of the effect of HIPAA on state law.

BACKGROUND

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 were originally scheduled to go into effect on February 26, 2001.[1] 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 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

[1] See 45 C.F.R. Parts 160 and 164.

requirements for the use or disclosure of health information that are more protective of privacy.

Preemption

Preemption is a judicial doctrine adopted by the U.S. Supreme Court through its interpretation of the Supremacy Clause, Article VI of the U. S. Constitution, which declares that all laws made in pursuance of the U.S. Constitution and all treaties made under the authority of the United States shall be the supreme law of the land and enjoy legal superiority over any conflicting provision of a State constitution or law.[2]

The Supremacy Clause of the U. S. Constitution invalidates state law that interferes with, or is contrary to, federal law. Federal law generally supercedes state law. Federal preemption arises when Congress expressly states an intention to preempt state law, and when the federal regulatory scheme is so comprehensive that it implies Congressional intent to preclude any supplemental state regulation.

There are two types of preemption: (1) "complete preemption," where competing state laws are invalidated; or (2) "partial preemption," where state and federal law coexist and only require reconciliation between the two bodies of law when any conflict is found. Under partial preemption, a unique hybrid of laws coexists simultaneously. A state law, when partially preempted by a federal law, is still valid but only to the extent permitted by the federal law and when the state law is not otherwise in actual conflict with the federal law. A federal law that provides for partial preemption of state law allows more stringent state law to be followed. The federal law provides a "floor of legal protection" above which a state may adopt more stringent standards.

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.[3]

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.[4]

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;

[2] See Black's Law Dictionary, Abridged 5th Ed. 1983, West Publishing Company.

[3] See 45 C.F.R. 160.202.

[4] 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.[5]

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.[6] 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.[7] 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.[8] 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 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.

---

[5] *Id.*

[6] HHS Final Rule on Standards for Privacy of Individually Identifiable Health Information (December 28, 2004) 65 Fed. Reg. 82462 at 82583.

[7] Id.

[8] 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.

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 are 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 have been referred to the DOJ for investigation and possible criminal prosecution. The majority of complaints allege: 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.[9] The entities most frequently named in complaints include private health care providers, general hospitals, pharmacies, outpatient facilities, and group health plans.[10] 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.[11]

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.[12]

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. Section 456.057, F.S., deals with the confidentiality of, and patient's access to,

[9] Bureau of National Affairs Health Law Reporter, Vol. 13, No. 20, May 13, 2004 p. 712.

[10] Id.

[11] "Health Information," U.S. Gov't Accountability Office Report 04-965, Sept. 2004.

[12] 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).

medical records created by specified health care practitioners, including medical physicians. Section 395.3025, F.S., addresses the confidentiality of, and patient's access to, medical records held by a Florida hospital. In addition to ss. 456.057 and 395.3025, F.S., a number of statutory provisions and administrative agency rules provide additional confidentiality and patient access for specialized individual health information.[13]

METHODOLOGY

Staff researched applicable federal and state laws that regulate the privacy of and access to individual health records. Staff consulted with staff from the State Technology Office, Department of Health, Agency for Health Care Administration, and other state agencies, and interested stakeholders to identify the current laws and to determine the need for any modifications to conform state law with federal requirements for privacy and access to health records.

FINDINGS

HIPAA Preemption of Florida Law

Numerous provisions of statutory law and administrative agency rules may be analyzed and found to be more protective of medical privacy than the HIPAA Privacy Rule. The focus of this review has been limited to ss. 456.057 and 395.3025, F.S., which are the two primary statutes in Florida regulating the privacy of and access to individual health information held by certain health care practitioners, hospitals, ambulatory surgical centers, and mobile surgical facilities. The analysis below is illustrative of the detailed analysis that covered entities must complete to be in compliance with the Privacy Rule. To ensure compliance, covered entities must initially perform a review and evaluation of each applicable state law and perform a preemption analysis for each state law. In the completion of such analyses, covered entities will probably render differing conclusions which probably will result in various perspectives and conflicting opinions. The courts are the final arbiter of whether a state law is more stringent.

Confidentiality. Section 456.057(5)(a), F.S., provides a broad and express privilege of confidentiality to medical records and the medical condition of a patient by providing that such records may not be furnished to, and the medical condition discussed with, any person other than the patient or the patient's legal representative or other health care practitioners and providers involved in the care or treatment of the patient, except upon written authorization of the patient.[14] Section 456.057(5)(a), F.S., allows patient records, which are otherwise confidential, to be furnished without written authorization in the following circumstances:

- 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 must be furnished to both the defendant and the plaintiff;
- In any civil or criminal action, unless otherwise prohibited by law, upon 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; and
- For statistical and scientific research, if the information is abstracted in such a way as to protect the identity of the patient or if the patient or patient's legal representative provides written permission.

Section 456.057(5)(a), F.S., is *not contrary* to the Privacy Rule and a covered entity would not find it impossible to comply with both the state and federal requirements. Section 456.057(5)(a), F.S., does not stand as an obstacle to the accomplishment and

[13] See other provisions of Florida statutes providing confidentiality of health information: HIV/AIDS information (ss. 381.004, 627.429, and 641.3007, F.S.); Cancer registry (s. 385.202, F.S.); Mental Health (ss. 394.451 and 394.4615, F.S.); Substance Abuse (s. 397.501, F.S.); Florida Patient's Bill of Rights and Responsibilities (s. 381.026, F.S.); Diseases Reported to DOH (ss. 119.07 and 384.29, F.S.); Genetic Tests (s. 760.40, F.S.); Employers providing health insurance (s. 760.50(5), F.S.); Insurers and HMOs for psychotherapeutic services (ss. 627.4195 and 641.59, F.S.); Medical records held by nursing homes (s. 400.022).

[14] See *Acosta v. Richter* 671 So.2d 149 (Fla.1996). Hospital records, generally, are confidential and may not be disclosed without the consent of the person to whom they pertain with exceptions specified in s. 395.3025(4), F.S.

execution of the full purposes and objectives of HIPAA.[15]

Access. Section 456.057(4), F.S., requires a licensed health care practitioner who performs a physical or mental examination, administers treatment, or dispenses drugs to furnish to a patient upon request copies of all reports and records relating to examination or treatment. If the patient requests psychiatric, psychological, or psychotherapeutic records, the practitioner may provide a report of the examination and treatment instead of copies of the record. Upon the patient's written request, the practitioner must provide complete copies of the patient's psychiatric records to a subsequent treating psychiatrist.[16]

Section 456.057(4), F.S., appears to be *contrary to* HIPAA and is preempted *in part* by 45 C.F.R. 164.524, which provides that an individual has a right of access to inspect and obtain a *complete copy* of PHI except for psychotherapy notes.[17] The Privacy Rule allows an individual access to his or her complete mental health records, excluding psychotherapy notes, unless a determination of harm or other exception applies to allow denial. Under HIPAA preemption, the health care practitioner's discretion in Florida to deny a patient's access to the *complete* PHI would be limited to a determination of harm outlined in the Privacy Rule.

The Privacy Rule allows a covered entity to deny an individual access to PHI after an independent denial review if:

- A licensed health care professional determines that access would "reasonably likely endanger the life or physical safety of the individual or another person;
- The information makes reference to another person and a licensed health care professional has determined that access is reasonably likely to cause substantial harm to such other person; or
- The request for access is made by the individual's personal representative and a licensed health care professional has determined that such access would cause substantial harm to the individual or another person.

Under 45 C.F.R. 164.524(2)(v), a covered entity may deny an individual access to his or her PHI *without providing the individual an opportunity for review,* if the PHI was obtained from *someone other than a health care provider under a promise of confidentiality* and the access requested would be reasonably likely to reveal the source of the information.[18]

The Privacy Rule permits, but does not require, a covered entity to provide the individual with a summary of the PHI requested. In lieu of providing access to the PHI, the covered entity may provide an explanation of the PHI to which access has been requested, if: the individual agrees, in advance, to such a summary or explanation; and the individual agrees in advance to the fees imposed, if any, by the covered entity for such summary or explanation.[19] The provisions of s. 456.057(4), F.S., that allow, rather than require, a health care practitioner to provide a report of examination in lieu of copies of the record appear to be *preempted* in part by 45 C.F.R 164.524.

The Board of Psychology has adopted an administrative rule (64B19-19.005, Florida Administrative Code), providing requirements on licensed psychologists for the release of records and reports. The administrative rule is *preempted* in part by 45 C.F.R. 164.524 to the extent that the rule authorizes a licensed psychologist to release a report or summary in lieu of the record of the PHI.[20]

Use/Disclosure For Research. 45 C.F.R. 164.512(i) allows a covered entity to use or disclose PHI for research if the covered entity obtains documentation that an alteration to, or waiver of, the individual's authorization has been approved by either an Institutional Review Board or a privacy board.

[15] See 45 C.F.R. 160.202.

[16] Hospital records must be furnished, upon written request and only after discharge, and in a timely manner, to patients without delays for legal review under s. 395.3025(1), F.S.

[17] A similar HIPAA Privacy Rule preemption issue exists in s. 394.4615(10), F.S. Section 394.4615(10), F.S., is pre-empted in part by 45 C.F.R. 164.524 to the extent that it requires a physician in a facility to give the individual access to his or her clinical records unless the physician determines that release would be harmful to the patient.

[18] Other authorized denials include: the PHI was compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative action; the request is by an inmate of a correctional facility and, if disclosed to the inmate, could place at risk the health, safety, security, or custody of the inmate or others; or the right to access has been suspended pursuant to the Clinical Laboratory Improvement Amendments of 1988.

[19] See 45 C.F.R. 164.524(c)(2)(i).

[20] See also s. 394.4615(10), F.S., relating to clinical records held by mental health treatment facilities.

Section 456.057(5)(a)4., F.S., allows patient records to be furnished without a patient's written authorization for statistical and scientific research if the information is abstracted in such a way as to protect the identity of the patient, or the patient or the patient's legal representative provides written permission.[21] Section 456.057(5)(a)4., F.S., is *more stringent* than and is not *preempted* by 45 C.F.R. 164.512(i) to the extent that it requires written authorization for disclosure of PHI for research purposes unless the patient's identity is protected. Section 456.057(5)(a)4., F.S., is *more stringent* than 45 C.F.R. 164.512(i) because it prohibits or further limits the use or disclosure of PHI; 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; and increases record-keeping or accounting of disclosures of PHI.[22]

Use/Disclosure For Marketing. Section 456.057(5)(b), F.S., provides that absent a specific written release or authorization permitting utilization of patient information for solicitation or marketing the sale of goods or services, any use of that information for those purposes is prohibited.[23] 45 C.F.R. 164.508(a)(3) requires a covered entity to obtain an authorization for any use or disclosure of PHI for marketing, except if the communication is in the form of: a face-to-face communication made by a covered entity to an individual; or a promotional gift of nominal value provided by a covered entity. Section 456.057(5)(b), F.S., is *more stringent than* and is not preempted by 45 C.F.R. 164.508(a)(3) to the extent that it prohibits disclosure or use of individual identifiable health information for marketing the sale of goods or services unless the patient provides written authorization and does not provide an exception for face-to-face communication made by a covered entity to an individual or for the giving of a promotional gift of nominal value provided by a covered entity.

Use/Disclosure Required By Law. Subsections 456.057(6) - (8), F.S., impose legal requirements on covered entities to use or disclose PHI. Section 456.057(6), F.S., provides that information disclosed to a health care practitioner by a patient in the care and treatment of the patient is confidential. Section 456.057(6), F.S., provides a waiver of the confidentiality of the patient's medical information in only four circumstances:

- In a medical negligence action or administrative proceeding when a health care practitioner or provider reasonably expects to be named as a defendant;
- Discussions only to other health care practitioners and providers *involved in the care or treatment of the patient*;
- By written authorization of the patient; or
- When compelled by subpoena at a deposition, evidentiary hearing, or trial for which proper notice has been given.

Section 456.057(7), F.S., authorizes the Department of Health (DOH) to obtain patient records by subpoena without the patient's written authorization when investigating professional disciplinary cases. Section 456.057(8), F.S., makes all patient records obtained by DOH and any other documents maintained by DOH which identify the patient by name confidential and exempt from the Public Records Law, and provides that such records may be used solely for the purpose of DOH and its regulatory boards in the investigation, prosecution, and appeal of disciplinary proceedings. Upon request of the Medicaid Fraud Control Unit in the Department of Legal Affairs, DOH must make all patient records and other documents which relate to a Medicaid recipient available to the Medicaid Fraud Control Unit.

Subsections 456.057(6) – (8), F.S., are *not contrary* to the Privacy Rule and a covered entity would not find it

[21] CS/SB 2170 (2004) included a provision amending s. 395.3025, F.S., that would allow patient records to be disclosed without patient consent to researchers or to facility personnel for research purposes if the researchers demonstrate compliance with the requirements of federal privacy regulations. 45 C.F.R. 164.501 defines "research" to mean a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

[22] Also see 45 C.F.R. 164.514, which provides that health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not subject to HIPAA.

[23] Section 456.057(5)(b), F.S., and a comparable provision in s. 395.3025(7)(b), F.S., applicable to hospitals, were both created by ch. 2001-222, L.O.F. Section 395.3025(7)(b), F.S., prohibits the use of a patient's hospital records for solicitation or marketing unless the patient or the patient's legal representative provides written permission.

impossible to comply with both the state and federal requirements. Subsections 456.057(6) – (8), F.S., do not stand as an obstacle to the accomplishment and execution of the full purposes and objectives of HIPAA. For purposes of s. 456.057(7), F.S., covered entities may disclose PHI to DOH in conjunction with certain health oversight activities.[24]

Responsibilities Of Records Owner. Section 456.057(9), F.S., requires all "records owners" to develop and implement policies, standards, and procedures to protect the confidentiality and security of medical records. Employees of "records owners" must be trained in these policies, standards, and procedures. 45 C.F.R. 164.530 requires a covered entity to designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity. A covered entity must train all members of its workforce on the policies and procedures with respect to PHI to carry out their function within the entity. A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of PHI. Section 456.057(9), F.S., is *consistent* with 45 C.F.R. 164.530.

Accounting For Disclosures. Section 456.057(10), F.S., provides that records owners are responsible for maintaining a record of all disclosures of information contained in the medical record to a third party, including the purpose of the disclosure request. The record of disclosure may be maintained in the medical record. The third party to whom information is disclosed is prohibited from further disclosing any information in the medical record without the express written consent of the patient or the patient's legal representative. 45 C.F.R. 164.528(a) provides an individual with the right to receive an accounting of disclosures of PHI made by a covered entity in the 6 years prior to the date on which the accounting is requested, with specified exceptions.

Section 456.057(10), F.S., is *more stringent* than 45 C.F.R. 164.528 to the extent that it does not provide any exceptions to an accounting for disclosures to third parties. Section 456.057(10), F.S**.** is *more stringent* than 45 C.F.R. 164.528 because it prohibits or further limits the use or disclosure of PHI; 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; and increases record-keeping or accounting of disclosures of PHI.

Copying Fees. 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 DOH when there is no board.[25] 45 C.F.R. 164.524(c)(4) provides that if an individual requests a copy of his or her PHI or agrees to a summary or explanation of such information, the covered entity *may* impose a reasonable, cost-based fee. 45 C.F.R. 164.524(c)(4) *permits, but does not require,* a covered entity to charge a reasonable fee for copying and mailing PHI. If a state imposes additional requirements or limits on what may be charged and under what circumstances covered entities may charge patients for copies to the patient records, then the state law is *not contrary* to the Privacy Rule and state law will govern.

CONCLUSIONS

The completion of a HIPAA preemption analysis is a complex and difficult legal task. Covered entities seeking to comply with HIPAA and the Privacy Rule must compare applicable state laws relating to privacy with HIPAA, and formulate a strategy to comply with any other applicable federal law. A comprehensive interpretation of state laws relating to privacy, for purposes of HIPAA preemption, requires legal and practical knowledge of how the state laws relating to privacy interplay with HIPAA and applicable federal law. The compliance date for the Privacy Rule was April 14, 2003. There has been very little time for implementation, and for affected parties to be fully educated about the Privacy Rule and how it interplays with state law. Legal staff in the Governor's office are only aware of one request for guidance regarding state law relating to privacy. The Florida Hospital Association reports that the association has not heard from any members that have requested an exception determination or preemption interpretation from HHS, or that have had HIPAA complaints filed against them. The Florida Legislature has provided for the statewide coordination of state agencies' compliance with

[24] See 45 C.F.R. 164.512(d).

[25] Pursuant to s. 456.057(16), F.S., the Board of Medicine has adopted an administrative rule (Rule 64B8-10.003, F.A.C.) that imposes a limitation on charges that any person licensed as a medical physician or physician assistant may charge for copying patient records.

HIPAA. Chapter 2001-261, L.O.F., requires the State Technology Office (STO) to designate a State Chief Privacy Officer to be responsible for continually reviewing policies, laws, rules, and practices of state agencies that may affect the privacy concerns of state residents. The STO has coordinated the HIPAA compliance activities of state agencies. Although covered entities and others have engaged in HIPAA compliance activities, committee staff is not aware of any entity that has formed a coalition of stakeholders in Florida to review the Privacy Rule and make publicly available a comprehensive HIPAA preemption analysis for educational use or for use to revise incompatible state law for harmonization with HIPAA.

Various collaborative efforts between other state governments and interested stakeholders have resulted in the completion of comprehensive HIPAA preemption analyses which have been used for educational purposes or have provided the basis for revision of state laws that were found to be inconsistent with the intent of HIPAA's privacy protections.[26]

RECOMMENDATIONS

Due to the complexities of HIPAA preemption analysis, it is recommended that the state encourage collaborative efforts between stakeholders to complete a comprehensive analysis of the effect of HIPAA on state law. Such collaborative efforts in Florida would require consensus building among stakeholders to ensure that consistent interpretation occurs regarding HIPAA preemption of state law. Collaborative efforts resulting in a comparative HIPAA preemption analysis may allow parties to more efficiently ask HHS to provide guidance or a determination that one or more state laws are not preempted by HIPAA.

The Legislature may consider the following options:

- Encourage voluntary collaborative efforts between stakeholders to complete a comprehensive analysis of the effect of HIPAA and the Privacy Rule on state law and to make recommendations for any revisions to the Legislature in an informal manner.
- Create an advisory council whose duties would include an examination of state law and the Privacy Rule, an identification of state laws affected by the Privacy Rule, and the completion of a comprehensive HIPAA preemption analysis that includes recommendations to the Legislature for any revisions of incompatible state laws for harmonization with HIPAA.
- Require the State Privacy Officer, by statute, to coordinate efforts with interested stakeholders, including those in the private sector, to identify state laws affected by the Privacy Rule, and complete a comprehensive HIPAA preemption analysis that includes recommendations to the Legislature for any revisions of incompatible state laws for harmonization with HIPAA and to make electronically available a matrix of state laws preempted by HIPAA for educational use. The State Privacy Officer could be required to update the matrix as needed to accommodate any changes in state and federal law.[27]

[26] See Iowa HIPAA Preemption Analysis (2003); Utah HIPAA State Guide; Maryland Health Commission and other parties have created a HIPAA Preemption Analysis that is updated periodically for guidance.

[27] The State Privacy Officer pursuant to s. 282.102, F.S., is working on the development of a Privacy Workgroup made up of HIPAA privacy officers and representatives from other interested state executive branch agencies to identify privacy issues. One immediate goal of the workgroup will be to finalize an inventory of statutes, rules and agency practices impacting privacy, along with legislative recommendations. The workgroup could also identify what types of information are stored in databases and how such information should be shared with other state agencies, shared with third parties and provided online. Also, the group could assist in the development of risk assessment tools and methodologies to identify risks to privacy, work with state agencies to implement the appropriate operational controls and ensure the existence and effectiveness of operational controls (audits).