

IN THIS ISSUE

An Overview of HIPAA

1

What is Protected Health Information?

2

HIPAA Pre-Emption Standards

3

Identifying Business Associates and Protecting the Health Information to Which They Have Access

4

HEALTH LAW UPDATE: SPOTLIGHT ON HIPAA

Summer 2002

BOCA RATON / FT. LAUDERDALE / MIAMI / ORLANDO / TALLAHASSEE / TAMPA / WEST PALM BEACH

Are Your Covered Entities Subject to HIPAA?

JOANNE B. ERDE AND MIKE SEGAL

Only "Covered Entities" must comply with the standards imposed by HIPAA. What is a Covered Entity? The term is very broad; it includes all health plans, health care clearinghouses, and all health care providers who transmit Protected Health Information (PHI) in electronic form in connection with a Designated Transaction. A provider is also a Covered Entity if it causes other entities to submit electronic claims on its behalf. The Final Regulations contain detailed definitions of all of these three types of entities.

The Act and Final Regulations define a "health plan" very broadly, including, among others, (a) a group health plan, which is essentially any ERISA (Employee Retirement Income

COVERED ENTITIES continued on page 6

COVER STORY:

An Overview of HIPAA

ROY HARRIS

Congress enacted the Health Insurance Portability and Accountability Act (HIPAA) in 1996. HIPAA calls for regulations promoting the administrative simplification of electronic healthcare transactions and regulations ensuring the privacy and security of patient information. HIPAA required Congress to enact laws implementing these goals by 1999. However, Congress failed to do so and the Department of Health and Human Services (HHS) stepped in and disseminated the regulations. The regulations are made up of four separate parts: (1) transaction

standards, (2) identifiers, (3) security and (4) privacy. These standards apply to "covered entities" as defined by HIPAA. Covered entities are generally defined to include healthcare providers, health plans and healthcare clearinghouses that transmit any health information in electronic form in connection with a "transaction" as defined by HIPAA.

The transaction standards require the use of common electronic claim standards, common code sets and unique health identifiers. The transaction standards

HIPAA OVERVIEW continued on back

ADVERTISEMENT

What is Protected Health Information?

Protected Health Information (PHI) is individually identifiable health information, maintained or transmitted, in whatever form the information exists, including oral communications.

Does the information (can be written or oral) contain any of the following identifiers?

- Name
- Address, including city, county and zip code
- Dates, including birthdate, admission date, discharge date and date of death
- Telephone and Fax numbers
- Electronic Mail (E-Mail) addresses
- Social Security numbers
- Health plan beneficiary number
- Account number
- Certificate/License number
- Vehicle or other device serial number
- Web URL
- Internet Protocol Address
- Finger or voice prints
- Likeness of photographic images
- Patient identification number, account number, or any other unique identifying number, characteristic or code

▼
If YES, continue

Is there a reasonable basis to believe that the information can be used to identify the individual?

▼
If YES, continue

Does the information relate to the past, present or future physical or mental health or condition of an individual, or the past, present or future payment for the provision of health care? NOTE: "Individual" includes deceased persons and minors.

▼
If YES, continue

Was information created or received by a health care provider, health plan, employer, or health care clearing house (i.e., billing company)?

▼
If YES, it is PHI

► **If NO, not PHI**

► **If NO, not PHI**

► **If NO, not PHI**

► **If NO, not PHI**

Examples of PHI:

- Physician dictation that has yet to be transcribed
- Patient status boards
- Eligibility printout from managed care companies outlining covered health care services
- Financial records
- Hospital face sheets, cover sheets, and head sheets
- Copies of patient demographic information used on files by large health care organizations to avoid collecting the same information over and over again
- Fax sheets
- Test results

Computerized PHI can include:

- Data appearing on computer monitors and screens
- Information transferred by magnetic or optical devices from one location to another
- Data stored or communicated on the Internet, extranet, or an intranet
- Data stored on electronic memory chips, magnetic tapes, discs, or CDs.

HIPAA Pre-Emption Standards

GABRIEL L. IMPERATO

The development of regulations in line with the privacy provisions of the Health Insurance Portability and Accountability Act (HIPAA) provide a Federal or national standard for the use and dissemination of personal health information. This area of the law has traditionally been regulated on a state-by-state basis, but the onset of dissemination of personal health information through electronic means, and the increase of this exchange of information by large managed care organizations, highlighted the need for national standards in this area. The development of the final regulations, which are to become effective in 2003, has created a dynamic interaction between Federal and state law in the regulation of the dissemination of personal health information.

The General Rule

The general rule under the Federal privacy regulations states that a provision of the HIPAA regulations pre-empt contrary state laws. At the same time, the regulations exempt many state laws from this general HIPAA pre-emption requirement. A state law includes any constitutional or statutory provision, rules or regulations, or the law detailed in a case or other judicial proceeding. Accordingly, when contemplating whether a state law is contrary to the HIPAA regulations or is exempt from HIPAA preemption, one must examine all relevant sources of state law.

The Regulations

The regulations discuss in some detail what is meant by a regulatory provision which would be deemed "contrary" to state law under the regulations. A law that would prevent a health care provider from complying with both the HIPAA

regulations and state law at the same time, or a provision of state law that is contrary to HIPAA's purposes and objectives, is pre-empted by the HIPAA regulations. There are, however, several important provisions in the regulations which are exceptions to this pre-emption requirement. The regulations create an exception to pre-emption for state laws which the Department of Health and Human Services determines are necessary to:

- prevent fraud and abuse regarding the provision of or payment for health care services;
- ensure appropriate state regulation of insurance and health plans;
- serve a compelling need related to public health, safety or welfare;
- address the use or prescription of controlled substances;
- address the reporting of disease or injury (i.e., HIV);
- laws that impose certain requirements on health plans (i.e., financial audits, monitoring and evaluation, licensure and certification);
- prohibit the disclosure of health information about minors to their parents, guardians or legal representatives;
- protect the privacy of health information that are more stringent than the standards under the HIPAA regulations.

This final area of exemption from the HIPAA requirements will clearly create

the most need for analysis and clarification in applying the Federal privacy standards.

Compare: State Law vs. HIPAA

The framework for such an analysis requires one to determine what HIPAA regulations may apply to the state law in question and compare the state law and HIPAA regulations to determine whether the substance of the state law is contrary to or more stringent than the HIPAA reg-

ulations. If the state law is contrary to the HIPAA provisions (i.e., one that prevents a provider from complying with both Federal and state law), then the regulations require adherence to the Federal standard. If the state law and the HIPAA regulations address the same subject and the state law is stricter, then the state

law will pre-empt the Federal regulatory scheme.

Conclusion

A determination of whether state or Federal law controls will not always be clear or obvious. Accordingly, the HIPAA regulations provide for affected parties to request clarification through an advisory opinion process before the Secretary of Health and Human Services to make a determination regarding pre-emption and whether the Federal regulations or the state law will apply in any given situation. **BC**

**A DETERMINATION
OF WHETHER STATE OR
FEDERAL LAW CONTROLS
WILL NOT ALWAYS
BE CLEAR OR OBVIOUS.**

SPOTLIGHT:

Identifying Business Associates and Protecting the Health Information

LESTER J. PERLING

The privacy rule, published in accordance with the Health Insurance Portability and Accountability Act (HIPAA), requires that covered entities (physicians, hospitals, long-term care facilities, ambulatory surgery centers, managed care organizations, insurers, HMOs, and self-insured employers) protect individuals' medical records and other personal health information. Covered entities may disclose protected health information (individually identifiable health information that is transmitted or maintained in any form or medium) to a business associate or allow it to create or receive protected health information if it obtains reasonable assurance that the business associate will adequately protect the information.

Who Are Your Business Associates?

A business associate is an entity that performs or assists in the performance of a function or service on a covered entity's behalf that involves the use or disclosure of protected health information. Entities that provide legal, actuarial, accounting, consulting, data aggregation, management, accreditation, administrative, or financial services would likely be considered business associates if the entity receives protected health information. Services that typically involve protected



is to look at the nature of the transactions between the covered entity and the third party. If the transactions involve the sharing, disclosing or creating of protected health information either between the covered entity and the third party or by the third party on behalf of the covered entity, then the third party is likely a business associate. However, if the interaction between the covered entity and the third party or by the third party on the covered entity's behalf does not involve the use of protected health information, then most likely a business associate relationship does not exist.

The definition of a business associate does not include the covered entity's workforce (employees, volunteers, trainees, and other persons who do work for the covered entity and are under its direct control, regardless of whether or not they are paid). Additionally, a medical staff based solely on staff privileges is not considered a business

THE KEY TO IDENTIFYING IF A THIRD PARTY IS A BUSINESS ASSOCIATE IS TO LOOK AT THE NATURE OF THE TRANSACTIONS BETWEEN THE COVERED ENTITY AND THE THIRD PARTY.

Before a covered entity releases any protected health information, however, it should determine 1) who its business associates are, and 2) what provisions should be in place to ensure the safety of the protected health information.

health information include claims processing or administration, data analysis, utilization review, quality assurance, billing, benefit management, practice management and repricing. The key to identifying if a third party is a business associate

associate. However, if one party is providing additional services for another, then a business associate relationship might exist (e.g. when a hospital provides billing services for physicians with staff privileges).

Transactions with third parties that serve only to transmit information are generally not considered business associate relationships. For example, using the U.S. Postal Service or other delivery company will not likely implicate a business associate relationship with the “messenger,” because no disclosure to the messenger is intended and the probability of disclosure is small.

Certain disclosures, while involving protected health information, DO NOT create a business associate relationship. Disclosures made as part of an Organized Health Care Arrangement in which participants need to share protected health information about their patients are not considered business associate relationships. These arrangements involve clinical or operational integration among legally separate entities in which it is often necessary to share protected health information for the joint management and operations of the arrangement. Disclosures between a hospital and physician regarding the treatment of an individual, disclosures of protected health information to health plans for payment purposes, and disclosures to agencies providing oversight of federal programs and the health care system (e.g., a Medicare carrier or intermediary) are not considered business associate relationships.

Ensuring the Safety of Protected Health Information

Every covered entity must enter into a written contract with each of its business associates. If the covered entity has an existing service agreement with a

business associate, then it is possible to amend the existing agreement to add the business associate provisions. Creating a separate agreement is also an option.

Business associate agreements should 1) set permissible uses and disclosures of protected health information that the business associate may undertake, and 2) allow the covered entity to terminate the contract if the business associate commits a serious violation or material breach of the contract. Additionally, the business associate agreements should require business associates to:

- not use or disclose health information except as permitted by the contract or required by law;
- have appropriate safeguards in place to prevent misuse and inappropriate disclosure of health information;
- report unauthorized uses and disclosures of health information to your organization;
- require the same disclosure conditions/restrictions on the agents and subcontractors of each business associate;
- make a patient’s protected health information available to him or her for access and copying;
- make protected health information available so that amendments to protected health information can be made, as needed, and update protected health information to include any such amendments;
- make available information to the covered entity needed to provide patients with an accounting of disclosures of their protected health information;
- make practices, books, and records available to the Department of Health and Human Services (HHS); and
- return or destroy protected health

information on termination of the contract or, if that is not possible, limit disclosures of protected health information beyond the termination date of the contract.

Covered entities are not required to actively monitor compliance or investigate the practices of their business associates. They are required to take action if they know or have substantial credible evidence of a material violation of the business associate agreement. Under these circumstances, the covered entity must take steps to lessen the harmful effects of the breach. If the steps to lessen the effects fail, the covered entity must terminate the underlying contract with the business associate. The underlying contract should be amended to allow termination in this circumstance or the separate business associate contract should provide for it.

Model provisions of business associate agreements are becoming more prevalent, including those published by DHHS. Care must be taken to ensure that each business associate agreement is tightly tailored to the relationship between your organization and each particular business associate. It is a mistake to assume that one generic business associate agreement can be used for every business associate relationship. Each relationship is unique and may include some disclosures that are permissible, and some that are not, depending on the circumstances of the relationship and the types of interactions between your organization and that particular business associate. Covered entities are advised to retain competent counsel to assist them in identifying business associates and drafting the business associate agreements that are specifically tailored to the wide variety of third parties with which the organization interacts. **BC**

COVERED ENTITIES

continued from cover

Security Act) employee welfare benefit plan (even self-insured) that either has more than 50 participants or is administered by someone other than the employer; (b) insurance companies who issue health insurance (including life, disability, casualty, and most types of long-term care insurance); (c) Medicare and Medicaid, including any issuer of a Medicare supplemental policy, and the Medicare + Choice program; (d) an HMO; (e) any employee welfare benefit plan established or maintained to offer or provide health benefits to the employees of two or more employers; and (f) any other individual or group plan, or combination of them, that provides or pays for the cost of medical care.

The term “health care clearing-house” is defined in the Act and Final Regulations as including *any* public or private entity that either (a) converts information received in a nonstandard format or containing nonstandard data, and converts that information into standard data elements or a standard transaction, or (b) in the reverse, takes standard transaction from one entity and converts it into information in a

nonstandard format or nonstandard data content for a receiving entity.

“Health Care Provider” generally includes any provider of medical or other health services, and any other person or organization who bills, or is paid for, health care in the normal course of business. An entity involved in health care service case management is, according to the Final Regulations, generally considered to be a Health Care Provider.

In addition to the three basic categories, a “Business Associate” (a lawyer, a billing company, accountant or consultant involved in the creation or transmission of PHI for a Covered Entity) may also be considered to be a Covered Entity. A Business Associate is an entity that performs an activity for a Covered Entity that involves the use or disclosure of PHI. Except for disclosures between health care providers for consultation and referral purposes, a Covered Entity may not disclose PHI to a business associate without satisfactory assurance (i.e., a written agreement) that information will be appropriately safeguarded. HCFA has recently published suggested language for such an agreement. Among the elements that must be included in such an Agreement are limits on the use and

disclosure of PHI and the establishment of appropriate safeguards to prevent disclosure, (1) requirements regarding the reporting of any violations to the Covered Entity, (2) making its records available to the Secretary of HHS, and (3) returning or destroying all PHI at the termination of any Business Associate agreement. If a Business Associate violates any HIPAA rules, the Covered Entity can be held liable, if it were aware of the Business Associate pattern of activity in breach of its agreement.

Not all transactions will cause an entity to become a Covered Entity. For example, if a provider who merely engages in basic faxes or emails between itself and a patient or an insurance company will not be engaged in a covered electronic transaction and this will not make the provider a Covered Entity. Similarly, if a provider performs all of its transactions in paper or via hard copy and does not transmit information electronically, it will not be a Covered Entity. But if as little as five percent of a provider’s PHI is transmitted electronically and 95 percent is transmitted through hard copy, all of the provider’s PHI is subject to HIPAA — the provider is a Covered Entity. **BC**

Save the Date – September 25, 2002

Broad and Cassel’s Tampa Office will be hosting a health law seminar and presentations will be made on the following topics:

- **Asset Protection**
- **Medicare Reimbursement**
- **and Fraud and Abuse Audits**

Watch your mail for more information, or call (813) 225-3020.

Edward Hopkins Selected to Speak at 2002 Florida Hospices and Palliative Care Annual Symposium

Edward Hopkins, Partner in the West Palm Beach Office, will speak at the 2002 Annual Symposium sponsored by Florida Hospices and Palliative Care Association on August 26 to 28, 2002, in Fort Lauderdale. His topic will be "The Impact of HIPAA on End-of-Life Care."

Mr. Hopkins is a member of the Firm's Health Law Practice Group. He received his B.A., Magna Cum Laude, in 1970 from Xavier University and his J.D. from Duke University School of Law in 1973.



Edward Hopkins

Mr. Hopkins is a member of the American Bar Association's Health Law Section; American Health Lawyers Association; Health Care Compliance Association, and the Health Care Financial Management Association. He focuses his practice in the areas of Fraud and Abuse, Compliance, Part A Medicare and Medicaid Reimbursement, and Reimbursement Appeals.

2002 Florida Legislative Report Highlighted on Broad and Cassel's website

Health care issues were again very important topics before the 2002 Florida Legislature. More than 100 bills were introduced regarding health care. A very brief summary of some of the bills which passed the Legislature is provided on Broad and Cassel's website at

<http://www.broadandcassel.com/pub.htm>.

This report was compiled by Douglas Mannheimer, a partner in the Tallahassee office of Broad and Cassel. He heads the firm's legislative practice and has represented health care providers before the Legislature for the past 15 years. He is a former chairman of the Florida Commission on Integrated Health Care Delivery Systems, was a co-chair of the Florida Health Care Association's Legislative Tort Reform Committee, and has an extensive regulatory practice representing health care providers.



Douglas Mannheimer

This report does not summarize every piece of legislation enacted, nor is it meant to provide a detailed analysis of those bills. The complete version of bills can be found under the Legislature's web site:

<http://www.leg.state.fl.us/Welcome/index.cfm>, looking for the "enrolled" (ER) version of a bill.

For more information on our health law services, contact the Broad and Cassel office nearest you:

FORT LAUDERDALE

Gabriel Imperato

Broward Financial Centre
500 E. Broward Blvd.
Suite 1130
Ft. Lauderdale, FL 33394
Phone: (954) 764-7060
Fax: (954) 761-8135

MIAMI

Mike Segal

Miami Center
201 South Biscayne Blvd.
Suite 3000
Miami, FL 33131
Phone: (305) 373-9400
Fax: (305) 373-9443

WEST PALM BEACH

Edward Hopkins

One North Clematis
Suite 500
West Palm Beach, FL 33401
Phone: (561) 832-3300
Fax: (561) 655-1109

TAMPA

Lester Perling

100 North Tampa Street
Suite 3500
Tampa, FL 33602
Phone: (813) 225-3020
Fax: (813) 225-3039

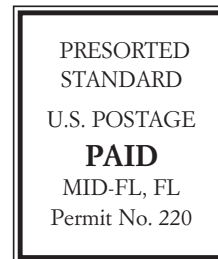
TALLAHASSEE

Douglas Mannheimer

215 South Monroe Street
Suite 400
Tallahassee, FL 32301
Phone: (850) 681-6810
Fax: (850) 681-9792



Health Law Department
Bank of America Center
390 North Orange Avenue
Suite 1100
Orlando, FL 32801



ADVERTISEMENT

The hiring of a lawyer is an important decision that should not be based solely upon advertisements. Before you decide, ask us to send you free written information about our qualifications and experience.

HIPAA OVERVIEW *con't from front*

became effective on October 16, 2000 and covered entities have until October 16, 2002 to comply. However, HHS will grant a covered entity until October 16, 2003 to comply if it files a proper compliance plan by October 15, 2002.

Additionally, HIPAA proposes the creation of national health care provider identifiers, national standard employer identifiers and national health plan identifiers. These identification standards will also set requirements concerning the use of the identifiers by health plans, health care clearinghouses, and health care providers. Health plans, health care clearinghouses, and health care providers would use the identifiers, among other uses, in connection with certain electronic transactions. These standards have not been finalized but are expected to be finalized this year.

HIPAA contains security regulations developed to govern the type of administrative procedures and physical safeguards covered entities must have in place to ensure the confidentiality, integrity and availability of protected health information, as defined by HIPAA. The security regulations have also not been finalized but are expected to be finalized sometime this year.

Finally, privacy regulations will likely have the greatest affect on a covered entity's day-to-day-operations. The privacy regulations address how protected health information is shared, accessed by patients and released to third parties. The privacy regulations became effective April 14, 2001, and covered entities must comply with the privacy regulations by April 14, 2003. Under the law, small health plans have until April 14, 2003 to come into compliance with these standards.

Currently, changes have been proposed to the privacy regulations, but those proposed changes have not been adopted. The Office of Civil Rights is responsible for enforcing the HIPAA privacy regulations. Penalties range from \$100 per patient per violation for minor violations up to \$250,000 and 10 years in prison for criminal violations.

HIPAA will deeply and broadly affect healthcare organizations. Each organization's required compliance response will vary because each organization is unique. Implementation of HIPAA's requirements will take the time, cooperation and coordination of numerous divisions of covered entities. Covered entities must immediately begin the process of implementing HIPAA's standards where appropriate to ensure that they meet the compliance deadlines. **BC**