

inside...

.....
Lessons Learned
..... page 4

Q&A
..... page 5

Continuing
Education
..... page 6
.....



Lifespan Risk Management

167 Point Street
Suite 170
Providence, RI 02903

tel: (401) 444-8273
fax: (401) 444-8963

An Introduction to HIPAA

—by Anne-Marie Vigneau, Enterprise-wide Security Officer, IS

Note: HIPAA regulations are undergoing frequent revisions. This article is only meant to act as a guideline for information that was current when this publication went to press in April of 2001. Please check one of the many websites regarding HIPAA for the latest information (for example, <http://aspe.hhs.gov/admsimp/> or <http://www.rmis.com/sites/heahippa.htm>).

Most practitioners have heard something about HIPAA, but may not understand what the implications are for them. The purpose of this article is to give you some general background information about HIPAA and some guidelines as to what it means for you.

What exactly is HIPAA?

HIPAA is the Health Insurance and Portability Act of 1996. Title II of the Act includes a section called Administrative Simplification, which requires:

- improved efficiency in health care delivery by standardizing electronic data interchange, and
- protection of confidentiality and security of health data through setting and enforcing standards.

HIPAA permits the Department of Health and Human Services (DHHS) to promulgate regulations after a certain time period if Congress fails to act under HIPAA. Congress did not meet the deadline set by HIPAA, and DHHS promulgated two sets of regulations and proposed a third set. The first set of regulations published in August 2000 sets uniform standards for electronic transactions, e.g., health care claims, eligibility benefit inquiries. The second set of regulations published in December 2000 sets standards for the privacy of individually identifiable health information. The proposed regulations published in August 1998 addresses security standards for electronic information and provides for electronic signature standards. These security regulations have not been finalized, but are not expected to change significantly from their current form.

Who is covered by HIPAA?

All health care providers who transmit any health information in electronic transactions, including claims for reimbursement, and health care payers and clearinghouses, are covered by the statute and its regulations. Electronic transmission is defined broadly to include dial-up lines that would include telephones and facsimile machines. On the provider side, HIPAA applies to hospitals, multi-physician practices, one-physician offices, behavioral health specialists, pharmacies, public health providers and so forth. HIPAA also applies to relationships that the covered entities have with business associates with whom individually

continued on page 2

identifiable health care information is shared.

What are the privacy and confidentiality standards?

The privacy standards differ from the other HIPAA regulations in that they apply to all records, both electronic and paper. Any health care provider conducting business electronically must apply the privacy standards to all patient identifiable data, regardless of form. Therefore, paper medical records, reports and oral communications containing patient health information are covered as well as e-mails and electronically stored or transmitted information.

What are the key privacy requirements?

The privacy regulation, in its final form is over 1,500 pages long, so a complete summary of the requirements is not possible in an article of this type. However, some of the key features include:

- the need to obtain patient written consent for the use and disclosure of patient information for treatment, payment and health care operations at the patient's first encounter with the provider;
- the need to establish policies regarding the use and disclosure of patient identifiable data and to provide patients with written notice of those policies;
- the requirement for written authorization from patients to for use of their identifiable data for purposes other than treatment, payment and health care operations, including notice that care cannot be denied if authorization is withheld;
- the patient's right to request restrictions on the for use of health information in the provider's treatment, payment or operations or disclosures;

- the patient's right to access and request amendment of his/her health information and the requirement that procedures be in place to respond to these requests in a timely manner;
- the patient's right to a written accounting of all disclosures of his/her health information, requiring procedures to track certain disclosures;
- the patient's right to have reasonable requests for confidential communications accommodated;
- the requirement that only the minimum necessary health information be used or disclosed and the provider must have procedures in place to address use by its work force and disclosure for routine, recurring requests; and
- other certain organizational and administrative requirements which, including designation of a privacy official, training and sanctions of employees, implement a patient complaint process, implement appropriate administrative, technical, and physical safeguards to protect the privacy of health information.

How do the privacy and security requirements affect a physician office?

The privacy regulations establish standards, but leave specific policies and procedures up to the entity. DHHS has emphasized flexibility and scalability. Implementation will depend on the size and resources of the practice. Therefore, the privacy measures taken in a physician's office may not be the same as required in a large hospital environment. Whereas a large institution may need to institute a formal web-based solution to track employee compliance with privacy training require-

ments, a physician's office may only need to add patient privacy and security discussions to new employee orientation and periodic staff meetings.

The security standards, as currently proposed, apply to all patient specific data that is stored or transmitted electronically; they and have not been finalized to date. However, the privacy regulations require that the provider implement appropriate administrative, technical and physical safeguards to protect the privacy of health information. Therefore, areas that providers need to address include:

- the security of the physical environment, which can be as simple as having locked filing cabinets, fax machines placed in secure locations, and use of shredders to dispose of health information;
- procedures for identifying appropriate users of health information; and
- audit procedures for accounting for disclosures.

With respect the proposed security regulations, DHHS includes the following additional areas for providers to address:

- disaster contingency plans, including backup and recovery procedures for electronically maintained data;
- procedures for the identification and authentication of users accessing data on-line (user ids and passwords being one method), including their access deletion upon termination;
- maintaining an audit trail of individuals using the information for treatment, payment and health

continued next page

care operations, and others to whom the information is disclosed; and

- encryption of patient-identifiable data prior to its transmission.

What steps can a physician take now?

The key to complying with HIPAA is to review the requirements and assess the office's current policies and procedures as they relate to use, maintenance and disclosure of patient information and submission of electronic transactions. The process undertaken should be well documented and time frames for task completion should be established especially where reliance is being placed on a business associate for the organization's compliance. Risk Management would like to point out that even though we realize not all of these recommendations may become part of the final regulations, they are felt to be good practices to adopt.

- Become familiar with the regulations. While the privacy regulation in particular is long and cumbersome, every health care provider, including multi-physician practices and one-physician offices, must be aware of the regulations, have considered the impact on their practice, and must change their policies and procedures accordingly.
- Appoint both a security and privacy officer (who can be the same individual) to also become familiar with the regulations, and can take the lead in the compliance effort.
- Work with professional organizations to determine if model policies and forms are being created which will save the need for development within the practice. There are many web sites which contain information on HIPAA,

including the HHS site at <http://aspe.hhs.gov/admnsimp/>.

- Recognize current policies and procedures within the office that may not comply with the standards and begin identifying alternative ways of accomplishing the same objective (for example, eliminating common sign-ins by patients, staff interviews of patients in waiting areas, leaving detailed messages on answering machines, etc.)
- Begin asking business associates, such as billing companies, collection agencies, etc. what steps they are taking and what their time frame is to become HIPAA compliant. Identify those control elements you require business associates to have in place in determining HIPAA compliance.

Remember, more stringent state laws protecting patient privacy and confidentiality are still in effect. Usually these laws address categories of sensitive information (e.g., HIV, psychiatric, drug and alcohol, genetic information) and address disclosures to state authorities or law enforcement. In developing or revising policies and procedures, you must include procedures for complying with these laws.

When is compliance to these standards required?

As the regulations currently stand, providers are required to comply with the electronic transaction standards by October 16, 2002 and the privacy standards by April 14, 2003. Additional electronic transactions may be added in the future and will require compliance with the electronic transaction standards. The Bush administration reopened the privacy regulations for public comment earlier this year, but no

changes were made prior to the effective date. Guidelines are now being planned to clarify some of the existing requirements and modifications are being considered to ensure the quality of care does not inadvertently suffer as a result of the privacy regulations. In addition, at some point in the near future, DHHS will finalize the security standards and promulgate regulations regarding national identifiers and enforcement — so stay tuned!

What is the penalty for noncompliance?

The civil penalty for noncompliance with HIPAA standards is \$100 per violation, up to a maximum of \$25,000 per year for each type of violation (for example, each impermissible, unauthorized disclosure).

For the privacy standards, criminal penalties also exist, ranging from fines of \$50,000 and/or one year in jail, to \$250,000 and/or to ten years in jail for knowingly using individually identifiable patient data with malicious intent or for financial gain. Further, while there is no recourse for the individual under the federal regulation, patients may sue for invasion of privacy, breach of duty of confidentiality or negligence claims under existing state law; HIPAA and state laws may provide the standard to which the provider is held.

Conclusion

DHHS, has indicated that HIPAA compliance is based on reasonableness, flexibility and scalability. What steps would a reasonable person expect a health care provider or plan take to ensure the privacy and security of the patient's identifiable health information? The objective of HIPAA is to ensure that the same standard of care is applied wherever the information might reside or be used.



Lessons Learned

The purpose of this section is to share summaries of closed cases that have occurred in the New England area and represent real life issues that provide proactive risk management educational opportunities. The cases used may come from Lifespan affiliates, or other institutions or practices, but should have some relevance to situations that you may encounter.

—by William J. Daley, Jr. of of Sloane & Walsh

Case:

This case involved a hospital, a pulmonologist and a six-year-old child. The child presented at the hospital with congestive heart failure, pleural and pericardial effusions. The findings on cardiac examination were at the child's baseline. Due to a complaint of headache, a head CT was performed which was negative. A sleep study was also performed revealing prolonged central apnea during sleep.

A cranial MRI was performed and this disclosed an area of increased T2 signal involving the cervicomedullary junction at the caudal pole of the 4th ventricle. The mass that was identified on the MRI was thought to be responsible for the child's cardiorespiratory symptoms. A resection of the tumor was performed but, unfortunately, only a portion could be excised because of its location.

The pediatric pulmonologist instituted a number of therapies to assist the patient included medication and ultimately BiPAP. Over a period of approximately one year, the child was maintained at home.

Approximately 12 months after the initial visit, the mother called the pulmonologist on succeeding days to report that her son was having increased breathing difficulties. The doctor and the mother spoke at length regarding her concerns. The

mother inquired whether she should bring the child to the hospital, but she was reassured and recommendations were made with regard to adjustments in both the medication and the BiPAP therapy. The child was found deceased in the family's apartment approximately 12 hours after the second call was made by the mother to the pulmonologist.

Damages:

The child's mother brought a claim for wrongful death damages alleging that the pulmonologist was negligent in failing to see the child with the result that appropriate therapies were not instituted and the child subsequently died.

Liability:

It was claimed that the pulmonologist failed to give proper attention to the observations made by the mother at the time she communicated the child's increasing problems during the telephone conversations. One of the causes of death was determined to be respiratory failure secondary to severe bronchiolitis. A treating physician testified at deposition that some patients with severe sleep apnea secondary to a brainstem tumor have been known to live 8 to 10 years. The family's expert medical witness testified that had the child

been seen by the pulmonologist at the time the symptoms were worsening, it would have been possible to control the bronchiolitis through the use of medications and ventilatory assistance in a hospital setting, possibly avoiding the patient's untimely death.

Risk Management Issues:

When multiple medical specialties are involved in the care of a patient, it is important that good communication occur among the various clinicians involved in the care of said patient. From a claims handling perspective, it is important that communication be documented. The pulmonologist was in contact with both the neurosurgeons and the oncologists and the interrelated problems were being discussed, but not documented. Documentation as to the seriousness of the problem is helpful to the defense of the claim.

In this case, the pulmonologist had a clear memory of the conversations that he had with the child's mother. It was apparent that each conversation probably lasted approximately 15-20 minutes. The child's condition was discussed in detail, the symptoms were reviewed, and recom-

continued page 5

Lessons Learned continued from page 4

recommendations were made for adjustments in the care being provided at home by the mother. Unfortunately, the detail of the conversation, both as to complaints being made and recommendations being given, were not captured in the brief notes that were placed in the chart. Very often one or two sentences commemorate a lengthy conversation. From a medical stand point the two sentences may be entirely adequate, but when defending a malpractice claim, more is usually better.

When a mother calls twice, on succeeding days, and registers concern regarding her child's condition, a jury can perceive a lack of attention on the part of a doctor who does not see the child. It is very important that a jury understand that the complaints were taken seriously, the

physician had available the information he needed in order to give advice and a physical examination would probably not have caused a significant change in the medical therapies prescribed. There was no reason to believe it was necessary to see the child and perform a physical examination at that time.

The death certificate listed severe bronchiolitis and recurrent brainstem tumor as the causes of death. It was necessary that testimony be available from an oncologist and a neuropathologist to explain that the advancing tumor can result in a sudden death of a child with these comorbid conditions. It is easy for a layperson to quickly conclude that severe bronchiolitis could cause sudden death; in fact, the sud-

den death was caused by the tumor shutting down the respiratory or cardiac system which can occur quite rapidly. In this case, it was important to have expert testimony to establish that bronchiolitis is quite a different problem for a child as opposed to an older person. This particular child was very obese and typically such children can be chronically hypoxemic. It was important that the oncologist, the pulmonologist and the neuropathologist all explain to the jury, within their particular disciplines and areas of expertise, that bronchiolitis normally does not cause sudden death in a child. Rather, the advancing tumor, located within a critical area of the brain, is known to cause sudden death.

Appropriate documentation relating to the medical condition, the treatment plan, conversations with the patient and family members, and interactions with other caregivers can go a long way in assisting a physician to explain and defend his position. The fact that the doctor took the time to enter the note often impresses a jury who interpret this as a sign of the doctor's thoroughness.

Risk Management Q&A

Q If I am deposed and I am not the defendant, is my deposition really important?

A Yes. There are various reasons for being deposed. The reason healthcare professionals are deposed is to ascertain their knowledge as providers, whether it is in a Worker's Compensation case, Child Abuse issue, Motor Vehicle Accident claim or Medical Malpractice Suit, to name a few. In almost any deposition, regardless of the type of suit, the deposed could create liability for his/herself, depending how the questions are answered. It is imperative to answer only the questions asked and as briefly as possible, without speculation. Stick to the facts of the case and do not volunteer any information beyond that which was solicited.

During a deposition involving a medical malpractice case, both the defendant's and plaintiff's legal counsel are collecting salient information regarding the malpractice lawsuit. It is extremely important to listen care-

Outcome:

Fortunately, the jury found in favor of the physician. When the verdict was received, the physician pledged that he would share his experience with his colleagues and advise everyone of the importance of appropriate documentation. A few extra words can go a long way when you are called upon to explain what you were thinking.

continued page 6



Lifespan Risk Services

Continuing Ed

**"Back to Basics:
Liability Trends, Informed Consent and Documentation
Do's and Don'ts"**

Wednesday, June 6, 2001 from 6 pm to 8 pm

Presenter: Virginia Fleming, Esq. and Angela Vieira, Esq.

Location: Arthur M. Sackler Center for Health
Communications, 145 Harrison Avenue, Boston

Pre-registration is required by calling 1-617-636-6579

Lifespan is accredited by the Rhode Island Medical Society
to sponsor intrastate continuing medical education for
physicians.

Lifespan designates each of these education activities for a
maximum of 1 hour in Category 1 credit towards the AMA
Physician's Recognition Award. Each physician should claim
only those hours or credit that he/she actually spent in the edu-
cation activity.

Risk Management

Q&A

continued from page 3

fully to the question and answer only what is being asked without lengthy explanations which may then could trigger additional questions that may be harmful to you or to the defense of the party's whose case you are advocating. Information provided may actually prove fodder for the plaintiff's attorney to name you as a codefendant, or be detrimental to the defendant's defense. If you are deposed and have a concern, whether it is a malpractice suit or not, you should immediately contact the institution's risk manager or your insurance carrier immediately. They will work with you and if it is felt exposure exists for you, they will seek legal representation to advise you and accompany you to the deposition.



Insights is published quarterly by Lifespan Risk Management department. Submissions and ideas are welcome and may be submitted to Rosemary Silvia via e-mail: rsilvia@lifespan.org or fax: (401) 845-1065.

editorial committee chairperson: Rosemary Silvia

committee members: Paul Adler, Joan Flynn, Virginia Fleming, Kathy Lavallee, Joseph Melino and Roland C. Loranger

design: Ellen Watt/IGN

Lifespan
Risk Management
167 Point Street
Suite 170
Providence, RI 02903

