# The Security of Your Medical Records

## *From HIPAA to the Health Information Technology for Economic and Clinical Health Act*

BY RICHARD T. O'CONNOR

Your medical record is full of very personal information. It is not unusual that such a repository of confidential information may be of great interest to others — relatives, employers, and health insurance companies, to name a few. It is well-documented that decisions regarding hiring and promotions have been made after reviewing the information in a medical record. State and federal governments have addressed the concerns of their constituents by passing legislation establishing standards of privacy and security applicable to medical information.

In 1996, the federal government enacted the Health Insurance Portability and Accountability Act (HIPAA). Although the privacy rule of HIPAA did not impact physician offices until 2003, the legislation was aimed at promoting standardization, efficiency, and privacy regarding the transmission, disclosure, and confidentiality of patient information. The HIPAA privacy rules apply strict standards of privacy and security to all entities electronically transmitting patient information. Hospitals, physician offices, and health insurance companies electronically transmit patient medical information and billing information, and, consequently, must comply with the standards of privacy and security established by HIPAA. With few exceptions, your authorization is required before such organizations may release your medical information to others.

The information in your medical records is referred to as "protected health information," (PHI) and is to be stored, accessed, transmitted, and disclosed in compliance with the HIPAA regulations.

You will experience the impact HIPAA has on the administration of medical records on the very first visit to your physician. A member of the office staff will ask you to complete a very detailed questionnaire as well as provide you with a copy of their HIPAA office policy concerning the protection of your health information. You will be informed that the information in your medical record will be secure, confidential, and released to other entities or persons in compliance with the parameters established by state and federal legislation. The questionnaire will ask you to designate a person or persons authorized to inquire and receive information concerning your medical care. Be prepared to let the office staff know if you are willing to have information regarding your medical care left on your answering machine.

Richard O'Connor

*With few exceptions, your authorization is required before certain organizations may release your medical information to others.*

The staff of your physician's office will also ask you if you have a health care proxy. The person you designate as your health care proxy also has access to your medical record and is authorized to discuss your care and treatment with your physician when you are incapable of doing so. The office HIPAA policy statement will inform you that the office has designated a member of the staff to be a compliance officer charged with monitoring HIPAA regulations and that you are encouraged to contact this person with any concerns.

Although your physician may authorize disclosure of your health information for treatment, payment or operational reasons, under the HIPAA regulations, access to such information by relatives, employees, and health insurance companies is strictly regulated. After completing the questionnaire and reading the confidentiality policy, you should have a greater sense of confidence that access to your medical record is restricted.

A more recent federal regulation, the Fair and Accurate Credit Transactions Act, requires all financial institutions and creditors to create and implement a written program for the "detection, prevention, and mitigation of identify theft." This legislation, under the auspices of the Federal Trace Commission, was directed toward businesses that regularly extend credit to consumers. It has been decided that physician offices qualify as creditors and, as such, are expected to comply with the regulations of the act.

Your physician's office must identify warning signs, or red flags, of identity theft in their day-to-day operations. The physician's staff may implement procedures requiring patients to verify their address as well as produce a picture identification along with an insurance card at each visit. The 'Red Flag' legislation is aimed at preventing your medical information from being released to an unauthorized individual.

While recent legislation has greatly enhanced the security regarding access by others to your medical record, your personal access is well established by the regulations of the Commonwealth of Massachusetts. You have the right to view and to obtain a copy of your records. Hospitals are required to respond to your request within 30 days, and physician offices are required to respond within 14 to 21 days.

Should you request a copy of your records, be prepared to pay a fee. The regulations state that a fee of more than 25 cents per page or a clerical fee of more than $20 per hour is considered unreasonable. Also, please be aware that a charge may be added for postage expense. No fee may be charged if you request a copy of your medical records for the purpose of supporting a claim or appeal under any provision of the Social Security Act (SSA) or any state or federal financial needs-based benefit program.

You also have the right to amend your medical record by adding information to it. The

office staff will instruct you how to go about that. While you have access to view your records and obtain a copy, your physician is responsible for the maintenance and ownership of your medical record.

There are instances where your medical record will be released against your express wishes. For example, your physician must release your medical record upon a subpoena from a court stating that your record is important in a legal proceeding, and it may also be released upon a request by your health insurance company conducting an audit of services rendered by your physician.

Expect regulations to continue to impact the security and privacy of your medical information. This year, the Health Information Technology for Economic and Clinical Health Act (HITECH) became effective. It extends the security and privacy provisions of HIPAA and requires that appropriate notice be given when there is a security breach of patient information.

Regulations will likely continue to evolve and impact the security and privacy of your medical information, so don't hesitate to seek the assistance of your physician's office staff in your quest to remain informed of the latest developments in protecting your health information. ❖

*Attorney Richard T. O'Connor serves as counsel with the law firm of Bacon Wilson. He is a member of the firm's Health Care Department and has experience in working with physicians and hospitals on business transactions, physician recruitment, and managed-care contracts with third-party payers; (413) 781-0560.*