

**FORC QUARTERLY JOURNAL
OF
INSURANCE LAW AND REGULATION**

Spring 1998 March 14, 1998 Vol. X, Edition I

PRIVACY PROTECTION FOR HEALTH INSURANCE AND MEDICAL RECORDS - STATE AND FEDERAL REGULATION,

Glennon J. Karr, Esq.
(614) 848-3100

This article will look at the issues involving the confidentiality of patients'/consumers' medical and health insurance records and the handling of those records by providers, health insurance companies, and others. Although the information presented here applies to all medical/health insurance records, some records are obviously more sensitive than others, such as records detailing information on sexually transmitted diseases, or mental health/alcohol and chemical substance abuse records, where release could expose the patient/consumer to loss of a job and other forms of discrimination.

Although the regulation of insurance by the states in the past has concentrated on solvency issues, in recent years greater emphasis has been placed on consumer issues. Market conduct audits now look beyond an insurance company's financial information to make sure that consumers are protected in a number of ways. Unfortunately, not a lot of emphasis has been placed on privacy issues.

People typically go to doctors, psychologists, and other health care providers with the understanding that whatever they tell these providers will be subject to some type of protection. Almost all medical and mental health providers in all states are governed by strict confidentiality requirements resulting in discipline for ethical violation if the professional discloses a confidence. In Ohio, for instance, medical records kept on patients in mental institutions are protected from disclosure [Ohio Revised Code (O.R.C.) Section 5122.31], and information told to psychologists is considered privileged, with the privilege controlled by the patient/consumer and not the psychologist (O.R.C. Section 4732.19). The physician-patient privilege found at O.R.C. Section 2317.02 provides protection of information provided by the patient/consumer or learned during the course of treatment with a physician. There are exceptions to these privileges involving reporting requirements in areas such as child abuse (O.R.C. Section 2151.421), where prevention of child abuse is considered more important than the protection of the patient's/consumer's rights to confidentiality, or where, for instance, the patient/consumer discloses to a health care provider information that suggests that he or she represents a clear and present danger to himself or herself or to others, although each state's provisions must be carefully reviewed and analyzed to ensure that in a particular situation the provider is following the reporting statute and not violating any other statutory or ethical guideline.

Beyond the protection provided to patient/consumer information known to providers, the state of the law varies greatly as to the right of a patient/consumer not to have personal information disclosed by insurance, managed care companies, and others. To its credit, Ohio has recently enacted legislation which makes its laws very comprehensive in this area. In Ohio there is a privacy law which protects State of Ohio records (O.R.C. Chapter 1347 - Personal Information Systems). In addition, there is a whole chapter, O.R.C. Chapter 3904 - Insurance Information Practices, which provides some privacy protection for patients/consumers with regard to how insurance companies and managed care organizations and "Insurance Support Organizations" (The Medical Information Bureau in Massachusetts which stores health and related information on patients/consumers is a prime example of this type of entity) utilize and disclose information. This legislation, passed by Ohio in 1995, is modeled after the National Association of Insurance Commissioner's (NAIC) Model Act entitled "Insurance Information Privacy Protection". It provides for notice to the patient/consumer of the type of information that will be collected and how that information may be accessed and corrected if the patient/consumer feels there is a mistake in the records. Also provided is the right to sue for damages in the event of an unauthorized disclosure and the recovery of attorneys' fees in certain instances. In addition there are even criminal provisions which apply when someone obtains information on an insured person under false pretenses. The model NAIC legislation has been adopted by sixteen (16) states

information on an insured person under false pretenses. The model NAIC legislation has been adopted by sixteen (16) states to date, including Ohio.

The Ohio legislation, unlike even the NAIC model act, applies to all types of managed care organizations. The NAIC model act generally covers only insurance companies, health maintenance organizations (HMO's), and hospital and medical service plans. In Ohio there is new legislation, passed in 1997, Chapter 1751 of the O.R.C., which creates Health Insuring Corporations. That chapter has its own Section 1751.52, which provides that information involving the diagnosis, treatment, or health of any enrollee or applicant that is obtained either from the enrollee or applicant or health care facility or provider must be held in confidence and not disclosed except under a limited set of circumstances. Health Insuring Corporations replace HMO's in Ohio, but also include Preferred Provider Organizations (PPO's) and other arrangements where care is provided and some type of transfer of risk is involved. The remedy for breach of the confidentiality provision appears to be that the Superintendent of Insurance in Ohio may suspend or revoke the license of the Health Insuring Corporation. However, when the Health Insuring Corporation legislation was passed, an amendment was made to the Insurance Information Practices Act, found in Chapter 3904, previously cited, which applied that law to Health Insuring Corporations in addition to insurance companies and HMO's, which had previously been included. Ohio, therefore, has extended the NAIC model legislation beyond insurance companies and HMO's to all types of arrangements, including PPO's.

However, even Ohio has a substantial gap in records protection in that self-insured employers and third party administrators handling self-insured plan information are not covered by any privacy protection law. It is important in analyzing protection provided to health care data to consider the question of federal Employee Retirement Income Security Act of 1974 (ERISA) (29 U.S.C. Sec. 1001 *et. seq.*) preemption where a self-insured employer's plan is involved. Without going into a lot of detail, because the extent of the preemption is a favorite topic for U.S. Supreme Court decisions every year or two and the rules seem to change depending on the Court's composition, a question arises as to whether the state may even regulate how health care records are handled where a self-insurance plan is involved and no insurance is involved. Arguably, if a health plan is pure self-insurance, then handling of the employer's records probably cannot be regulated by a state law protecting privacy. An argument can be made that where a third party administrator or other entity regulated by state law is involved, then the state may regulate how that entity handles medical/insurance/self-insurance information. However, the Ohio Third Party Administrator statute, found in Chapter 3959 of the O.R.C., does not provide statutory protection to records handled by licensed third party administrators. Currently, with potentially fifty percent (50%) of all health insurance handled on a self-insured basis, and with ERISA preemption still a threat to any state legislation which attempts to regulate self-insurers, there is a tremendous lack of regulation of health care information involving patients/consumers, even in the sixteen (16) states which have adopted the NAIC model privacy legislation.

Two states, Montana and Washington, have adopted the Uniform Health-Care Information Act, proposed in 1985 by the National Conference of Commissioners on Uniform State Laws. That legislation provides protection to patients/consumers involving provider records, including criminal and civil sanctions and penalties for the improper disclosing of information. It does not address, however, the handling of health care information by insurers/managed care companies and/or third party administrators. (Montana, in addition to adopting the Uniform Health-Care Information Act has adopted the NAIC model privacy legislation; Washington has not.) In thirty-four (34) states there is no NAIC model privacy legislation, meaning even the insurance companies, HMO's and medical and hospital service plans aren't regulated as to what they can disclose. The most effective way, therefore, to guarantee privacy protection to all medical records seems to be by means of federal regulation, where even employers could be held accountable for health records handling or mishandling.

Another consideration is the rise of the computerization of records. It is one thing when a record is maintained in a paper format and can be locked in a file cabinet. A whole new set of problems arises with protecting individual privacy when records are computerized and access is greatly expanded. Talk of a computer smart card containing each individual's entire medical, psychiatric and dental history is not just a dream, but could become a reality in a short period of time. If someone had his wallet stolen and the card was missing with that person's entire medical and mental health history encoded on it, currently, there would not be a lot of protection available.

Standards rating organizations are seeking to fill a void in this area. For instance, if a managed care plan qualifies for National Committee for Quality Assurance (NCQA) certification, it must follow strict guidelines regarding the protection of patient/consumer information. No remedies are provided, however, to consumers for a breach of these provisions.

At the federal level there are various provisions which regulate privacy in certain instances. The federal Privacy Act of 1974 (5 U.S.C. Section 552a) provides extensive protection to consumers where federal government records are involved. The law

(5 U.S.C. Section 552a) provides extensive protection to consumers where federal government records are involved. The law has no applicability, however, to private companies. There are some protections built into regulations involving consumer medical records used by Peer Review Organizations [42 C.F.R. 476.101(1)-(4) and 42 C.F.R. 476.115(a)]. Medicare regulations provide [42 C.F.R. 482.24(b)(3)] that hospitals must set up systems to protect the confidentiality of existing records and prevent their unauthorized release in order to participate in the Medicare system. Of major significance also in this area is the special treatment given to information involving alcohol and substance abuse treatment, but this applies only where federal funds are involved. Federal law and regulations providing protection in this area may be found at 42 U.S.C. Sections 290dd-3, 290ee-3, and 42 C.F.R. Section 2.1 *et. seq.*

Since the majority of states lack laws allowing patients/consumers to sue for unauthorized access or disclosure of their medical/mental health information, the patients/consumers are left to common law. Actions for invasion of privacy, defamation, and/or breach of physician/psychologist-patient privilege are available. The NAIC model privacy legislation specifically prohibits causes of action based on these common law principles where the legislation allows for disclosure, but, in many instances does allow for lawsuits and the recovery of attorney's fees where provisions of the law have been violated. As mentioned previously, however, there are still thirty-four (34) states where no privacy protection exists and even in those states where it does exist, self-insured plans are generally not covered and neither, typically, are many managed care organizations, such as PPO's or third party administrators.

Given this background, and given the increasing ability on the part of many people to access, store and retrieve information from computers, the Health and Human Services Department of the federal government in the Kennedy Kassenbaum legislation passed in September 1996 and otherwise known as the Health Insurance Portability and Accountability Act of 1996 (29 U.S.C. 1181 *et. seq.* and 42 U.S.C. 300gg *et. seq.*) was charged with reviewing this problem. On September 11, 1997, the Secretary of Health and Human Services provided a report to Congress suggesting that health care records be protected. That report may be found at <http://aspe.os.dhhs.gov/admnsimp/index.htm> on the world wide web.

Basically, the Secretary of Health and Human Services is attempting to balance the interests of promoting society's need to obtain access to health information, including research and the prevention of the spread of infectious diseases, with the need for an individual's right to privacy. To replace the use of broad authorization forms whereby consumers now sign a waiver allowing the medical record to be disclosed to any number of people, the Secretary of Health and Human Services is proposing that a new privacy law be passed which provides protection for all medical information.

Under the proposal, payers and providers, including employers when they act as payers for self-insurance plans, would have access to the minimum amount of health care data that they need to pay claims or treat the patient. They would be required to inform the patient/consumer how they protect records, how the patient/consumer could correct errors in their records, and how the patient/consumer could access records and the names of all entities to which the information was released. There would be limitations on the patient/consumer accessing information in their own records, such as where it would endanger the physical health of the patient/consumer or another person, although there is no consideration given to how it would affect the mental health of that patient/consumer.

There would be criminal sanctions for anyone accessing a patient's/consumer's records for other than legitimate purposes, and civil remedies available where, for instance, an insurance company has repeated violations. Further, a patient/consumer would be able to sue for actual damages where their records had been disclosed in violation of the new privacy law and would be able to obtain attorneys' fees and punitive damages where the violation was willful.

Service organizations or third parties having access to the information, such as third party administrators acting on behalf of a self-insured employer, would have to follow disclosure safeguards, but would not have mandatory notification or correction requirements applied to them.

Research organizations or entities would have access to information in files to promote public health and research and an individual's approval would not have to be obtained to gain access to the records. Law enforcement agencies could gain access to records the same way they do now, under current laws allowing access for limited purposes. Wherever individual state privacy laws were stricter, those laws would apply, as the federal privacy law would merely provide a minimum level of safeguarding for health records.

Conclusion

The protection of health insurance and medical records is an issue that will be actively debated as long as little protection is provided by law or there are gaps in the protection that is provided. Now that health and insurance records are routinely transmitted electronically across state lines and unauthorized persons may be able to tap into those records from a home computer, something must be done. The states, lacking the ability to regulate self-insured plans to a great extent, and not a very good record of providing protection in this area since thirty-four (34) states have failed to adopt the model NAIC legislation even though it has been in existence since the early 1980's, may have basically forfeited their chance to legislate at least minimum protection levels in this area. (It should be pointed out that the Secretary of Health and Human Services, in her report to Congress, previously cited, stated that only two (2) states had adopted the Uniform Health-Care Information Act recommended by the National Conference of Commissioners on Uniform States Laws in 1985. No mention was made in the Secretary's report of the NAIC model act on records confidentiality which has been discussed in this article and has been adopted by sixteen (16) states as of 1997. This omission suggests that the Secretary is giving less credit to the states than they actually deserve. In any event, federal legislation appears to be the only effective way to regulate all plans unless the states can convince Congress to allow them to regulate all plans, include self-insured ERISA exempt plans, and then, after having obtained the ability to regulate all plans, all the states effectively follow through with implementing legislation.