

THE REGULATION OF HEALTH INFORMATION PRIVACY – HIPAA AND OTHER RELEVANT LAWS AND LEGAL ACTIONS – THE IMPACT ON INSURANCE AGENTS

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

With the Health Insurance Portability and Accountability Act (“HIPAA”) Privacy Standards¹ finally effective as of April 14, 2003, all types of medical information gained important new protections. Previously medical information was shielded from release under at least one federal privacy law which protects information from disclosure where federal funds are involved with alcohol/substance abuse treatment programs.² That law greatly limited to whom information could be provided and provided a detailed, model Consent to Release form which the HIPAA Authorization to Release form strongly resembles. However, at the federal level, until HIPAA there was no comprehensive regulation which provided privacy protection for the average American’s medical records, although by some estimates almost one half of all health care plans are self-insured and are most likely exempt, at least to some extent, from most state privacy regulation, due largely to Employee Retirement Income Security Act (“ERISA”)³ preemption theories.

The National Association of Insurance Commissioners (“NAIC”) has several model acts and model regulations which apply to insurance information. One of them, entitled “Standards for Safeguarding Customer Information Model Regulation,” deals with implementing safeguards in connection with the Gramm-Leach-Bliley Act⁴ (“Act”). Although some health information may be provided protection under that Act, it is not the intent of this article to deal with those provisions, although obviously a lawyer advising a client subject to the Act should take into account the possible applicability of that law. The NAIC “Insurance Information and Privacy Protection Model Act,” with some modification, became effective in Ohio in 1995 and now has been adopted, in some form, by eighteen states. That model statute allows a person to sue, when their health information is released, which HIPAA does not. However, the NAIC model statute is probably inapplicable under ERISA to self-insured health care plans, although jurisdiction over licensed companies and agents probably remains, allowing at least some form of state regulation. The NAIC “Privacy of Consumer Financial and Health Information Regulation” has been adopted by thirty-eight states in various forms. It specifically references and interrelates with HIPAA. The NAIC “Health Information Privacy Model Act,” similar to HIPAA, has not been adopted by any states to date. It would face the same ERISA preemption issues as the other NAIC model laws and regulations, i.e., there is some question as to their applicability to self-insured plans.

In addition, HIPAA itself has a state preemption feature⁵ which essentially defers to state law where the state law is stricter with regard to releasing information to third parties or where state law allows greater access to an individual to their own/their children’s medical records. This further complicates matters in that each provision of state law which may or may not be applicable must be reviewed in relation to HIPAA provisions in order to determine which provision is applicable in any given situation.

HIPAA specifically exempts from protection Family Educational Rights and Privacy Act (“FERPA”) records⁶ which may contain medical information. If the purpose of the record’s creation was primarily for educational purposes, then FERPA applies and HIPAA doesn’t; and HIPAA specifically exempts employer records.⁷ With FERPA there is a specific set of protections that have been in place for years. The HIPAA law did not provide the government with the power to regulate employment records. The general definition of Protected Health Information (“PHI”) under HIPAA is quite broad and applies to almost all information in any way dealing with a person’s past, present or future mental or physical health, with the exceptions previously listed.⁸

So although there seems to be some floor of protection in place now for almost all types of medical/health information within insurance/self-insurance systems, a lawyer dealing with the different laws needs to review carefully the type of records involved and then determine what laws apply and the requirements involving disclosures under those laws. It is useful to see how a typical health insurance agent might be affected by all of this. Ohio will be used as an example to show the various laws/rules/legal actions that may apply.

One of the first places to check if there are privacy rights is to determine if there is a state law which gives the Insurance Department the right to regulate privacy protection for individuals. Often these are modeled on the NAIC model laws. In 1995 Ohio adopted a form of the “Insurance Information and Privacy Protection Model Act,”⁹ which protects health information collected by agents in connection with life, health and disability policies and which is handled by insurance companies. The Department of Insurance has the ability to obtain a cease and desist order in order to enforce the law,¹⁰ and an individual whose rights are violated under the statute may sue for actual damages.¹¹ The prevailing party, which may include either the person suing or the person/business entity being sued, may be awarded reasonable attorneys fees.¹² This law may not apply, however, to self-insured plans due to ERISA preemption issues. Agents in Ohio need to carefully ensure that they are following this law, however, regardless of the arguments available involving preemption issues, because the agents might be subjected to a lawsuit under the law and the Ohio Department of Insurance could review their actions under the appropriate licensing statute.

The next place to check is case law for the state, which will generally provide a right to sue to individuals whose information has been disclosed without a proper release. In a landmark decision in September 1999, the Ohio Supreme Court ruled in *Biddle v. Warren General Hospital*,¹³ that instead of using various theories, which are still in use in one form or another in many states, like invasion of privacy, defamation, implied breach of contract, intentional and negligent infliction of emotional distress, implied private statutory cause of action, breach of trust, detrimental reliance, negligence and medical malpractice, it would create new torts to cover the release of medical information. It created an independent tort for the unauthorized, unprivileged disclosure of nonpublic medical information and a second tort for inducing the unauthorized, unprivileged disclosure of nonpublic medical information. Although the Court’s ruling was limited to the disclosure of information subject to the physician-patient privilege, it is reasonable to assume that the Court would apply the same reasoning to the release of information in other settings where the information is being obtained for some specific purpose and where the party obtaining the information is subject to some duty to use the information only for that purpose, such as an agent acquiring medical information in connection with a health insurance product. At the very least, the right to sue under the Ohio Insurance Information Practices Act, which is Ohio’s form of the NAIC’s Insurance Information and Privacy Protection Model Act, would probably apply.

Therefore, in most states, in one various form or another, there are rights that an individual has to file suit against a person or entity which releases otherwise nonpublic medical information. These rights would appear to apply regardless of whether or not a self-funded ERISA plan is involved in the disclosure, although there are arguably less rights available with regard to self-funded plans. Unless there is some public policy exception allowing for the release of the information, disclosure of the information is allowed only after the disclosing party obtains the permission of the person whose information is involved to release the information. Further, at least in Ohio, inducing the release of the information may also give rise to a second cause of action.

Now that the HIPAA Privacy Rule has become effective, there is another layer of protection provided to all types of medical records. There is no private right to sue under the HIPAA Privacy Rule, meaning a person injured may not use HIPAA to sue the person releasing the information. Rather, enforcement comes through fines and even possible criminal penalties.¹⁴ The law is enforced by the Secretary of Health and Human Services.

Insurance companies, medical offices, hospitals and self-insured health care plans are all directly impacted by HIPAA as “Covered Entities.”¹⁵ However, in order to ensure that privacy protection was spread to a greater number of people/entities dealing with protected health information, the Privacy Rule developed the concept of a Business Associate.¹⁶ Essentially, a Business Associate is a person/entity that performs services on behalf of a Covered Entity. Typical examples would be lawyers to whom protected health information is disclosed, billing companies, accountants if they have access to protected health information, and to some extent, insurance agents and brokers for insurance companies.

A Covered Entity, i.e. the insurance companies, medical offices, and hospitals, are required by the HIPAA Privacy Rule to have contracts in place with their Business Associates which effectively require the Business Associate to follow the HIPAA Privacy Rule. Although there is no direct penalty that the Secretary of Health and Human Services may impose on a Business Associate for violation of their contract obligations, the Covered Entity is required to take certain actions to ensure that problems are corrected, or it must terminate the contract with the Business Associate¹⁷

if the problems cannot be corrected.

If an insurance agent works solely on behalf of one insurance company there is no problem in determining whether or not the HIPAA Privacy Rule applies; it does apply simply because the agent is acting solely on behalf of that insurance company, which is a Covered Entity. In order to make sure that they have the proper contracts in place, insurance companies are sending out Business Associate contracts routinely to all of the agents that they license. However, various other legal principals apply as to whether or not the agent is acting as the agent of the employer which is seeking insurance in the group health market or the agent of the company which may be offering the insurance. In some cases there may be a statute which clarifies the situation to some extent, as does an Ohio statute which states that once licensed by a company, the acts of that agent become the acts of the insurer to the extent that the agent is working within actual or apparent authority.¹⁸ However, where an agent, acting on behalf of an employer, is approaching several insurance companies for quotes and it is licensed by all of those companies, the problem presents itself as to which Business Associate contract applies to the information obtained, including the multiple quotes obtained. Further, as stated earlier, employer employment records are not covered by HIPAA.¹⁹ So if an insurance agent is contacted by an employer to act on its behalf in procuring insurance, there is some question as to the applicability of HIPAA because the agent may not be acting as the agent of the insurance company, a Covered Entity under HIPAA, but for the employer, which is not being covered by HIPAA unless it is operating a self-insured plan. And, if the agent is deemed to be the agent of a Covered Entity, the question arises as to which Covered Entity is involved, i.e. which insurer, for purposes of compliance as a Business Associate of that insurer. If the employer is also a Plan Sponsor of a self-insured plan, then as a Covered Entity the employer might have to have the agent sign a Business Associate contract if the agent will be provided with PHI.

As problematic as it is to determine whether or not HIPAA applies in a particular agency situation, the best way to ensure protection is to assume that it does apply and to limit the amount of individually identifiable information that is collected by the agent and to then limit how that information is distributed once it is obtained. For instance, if the agent is solely the agent of the insurance company, and therefore a Business Associate of that company, the only way any health information the broker obtains can be released to the employer is pursuant to an authorization signed by the person whose information is involved.²⁰

HIPAA provides for a process of “de-identification.”²¹ That process involves removing all of eighteen specific identifiers, such as name, social security number, etc., from the information, so long as the information isn’t capable of being recognized as identifiable in any other way. Once de-identified, the information can then be used in almost any form. Because it no longer is individually identifiable information it is no longer protected by HIPAA, and presumably it doesn’t come under any other law or protection which might give rise to liability if it is released. HIPAA also provides a process where the information may be “re-identified” with the use of code words or by other means which would protect the confidentiality of the information.²²

In the event that it is going to be impossible to de-identify the information, then the agent should ensure that he or she has obtained the appropriate authorization from the person whose information is being used, to distribute the information in a specific way, such as to the employer if the employer is going to place the information in an employment or non-HIPAA protected file. The authorization under HIPAA²³ is specific, time-limited, and provides detailed information on how the information will be used and disclosed. It should meet almost any standard under any state law which governs the release of medical information, although again, the attorney recommending the use of the form should check to see if a particular state’s law provides for a more stringent authorization form than the one called for under HIPAA. In Ohio there is no more stringent form required.

The end result of all of this is that the agent, or anyone else dealing with the information, should take all necessary steps to follow the most stringent rules that apply and then limit as much as possible how the information is released to various parties. If, for instance, the information is being released by the agent to an insurance company the agent may assume that a number of laws apply. In Ohio the *Biddle* case²⁴ would arguably provide a cause of action if the insurance company released the information, the Insurance Information Practices Act²⁵ would provide a cause of action against the insurance company if it released the information, and HIPAA would provide penalties, as the insurance company would be a Covered Entity. Where there is any question as to whether or not the agent is a Business Associate of the entity to which he or she is releasing information, then the agent should attempt to get

written assurance from the insurance company that the information released to it, if it is in identifiable form, will be protected.

Endnotes

1. 42 U.S.C. §§1320d-1329d-8.
2. §408 of the Drug Abuse Prevention, Treatment, and Rehabilitation Act, 21 U.S.C. §1175, which was amended and transferred to 42 U.S.C. §290ee-3, with implementing regulations found at 42 C.F.R. Ch. 1, Part 2.
3. 29 U.S.C. §1002.
4. 15 U.S.C. §§6801-6827.
5. 45 C.F.R. §160 Subpart B.
6. 45 C.F.R. §164.501.
7. 45 C.F.R. §164.501.
8. 45 C.F.R. §160.103 and 45 C.F.R. §164.501.
9. Chapter 3904 of the Ohio Revised Code.
10. §3904.18 of the Ohio Revised Code.
11. §3904.21(B) of the Ohio Revised Code.
12. §3904.21(C) of the Ohio Revised Code.
13. *Biddle v. Warren Gen. Hosp.*, 698 N.E.2d 1007 (1999).
14. Interim Rule published in the Federal Register April 17, 2003 (Vol. 68, No. 74, 18895-18906).
15. 45 C.F.R. §160.103.
16. 45 C.F.R. §164.504(e)(1).
17. 45 C.F.R. §164.504(e)(2).
18. §3905.20 of the Ohio Revised Code.
19. 45 C.F.R. §164.501.
20. 45 C.F.R. §164.508.
21. 45 C.F.R. §164.514.
22. 45 C.F.R. §164.514(c).
23. 45 C.F.R. §164.508.
24. *Biddle v. Warren Gen. Hosp.*, 698 N.E.2d 1007 (1999).

25. §3904.21(B) of the Ohio Revised Code. 
