Annals of Health Law

Volume 16
Issue 2 *Summer 2007*

Article 9

2007

Private Laws and Their Effect on Healthcare Organizations

Melissa A. Irving
Loyola University Chicago, School of Law

Privacy Laws and Their Effect on Healthcare Organizations

*Introduction by Melissa A. Irving**

I. INTRODUCTION

Those present at the Loyola University Chicago School of Law Beazley Institute for Health Law and Policy's Sixth Annual Health Law and Policy Colloquium had the honor of hearing Stephen J. Weiser, J.D., LL.M., speak about privacy laws and how they affect health plans. Mr. Weiser currently serves as Assistant General Counsel for BlueCross BlueShield of Illinois. Mr. Weiser also has gained experience in private practice through roles as in-house counsel for both Rush University Medical Center and the Michael Reese Hospital and Medical Center. Furthermore, Mr. Weiser was a leader in the American Bar Association's Health Law Section as well as an adjunct professor at DePaul University College of Law's Health Law Institute.

Throughout his career, Mr. Weiser has focused on the corporate and regulatory issues that hospitals, physician groups, managed care providers, and heath insurance companies face. During his presentation, Mr. Weiser spoke about the roles that HIPAA (Health Insurance Portability and Accountability Act), Illinois privacy acts, and federal marketing laws play in the collection of member data by health plans. He concluded his discussion with an analysis of how these laws specifically affect pay-for-performance programs.

II. HIPAA

The Heath Insurance Portability and Accountability Act of 1996, better known as HIPAA, was created to "improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery . . . to

* Student, Loyola University Chicago School of Law, Class of 2008. Ms. Irving is a staff member of the *Annals of Health Law*.

improve access to long-term care services and coverage, [and] to simplify the administration of health insurance . . . ."[1] Clearly, HIPAA plays a large role in the administration of health plans.

One element of health care that HIPAA regulates is health information.[2] HIPAA defines health information as information that is "oral or recorded in any form or medium," and created or received by a healthcare provider, health plan, or public health authority.[3] HIPAA elaborates on this definition by noting that this information can relate to the "past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual . . . [or] payment for the provision of health care to an individual."[4]

Since obtaining personal healthcare information is an essential part of running a health plan, HIPAA applies in many situations that plan administrators face.[5] Transmission of personal health data is necessary because health plans work with billing for procedures, claims, and enrollments among patients.[6] Although HIPAA specifies the protective measures that an individual transmitting personal health data must follow, including consent for use or disclosure of information,[7] HIPAA does not require authorization for transfers that pertain to payment, claims, eligibility for a health plan, or enrollment in a health plan.[8] Due to this leniency, many states have enacted stricter privacy laws.[9]

Creating stringent privacy laws is an effective method for legislators to protect their consumers, as state law trumps HIPAA when the state law is stricter.[10] However, in order to meet the "more stringent" criterion, the law must relate to protection of "individually identifiable health information."[11] A law "'relates to the privacy of individually identifiable health information' when 'the state law has the specific purpose of protecting the

1. *See* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936, 1936 (1996) (Introduction of Act).

2. § 262, 110 Stat. at 2022.

3. *Id.*

4. *Id.*

5. Stephen J. Weiser, Assistant General Counsel for BlueCross BlueShield of Illinois, Address at the Loyola University Chicago School of Law Beazley Institute for Health Law and Policy's Sixth Annual Health Law and Policy Colloquium (Dec. 5, 2006) (at PowerPoint presentation slide 3).

6. *See* § 262, 110 Stat. at 2025.

7. *Id.*

8. *Id.*

9. *See* Weiser, *supra* note 5 (at PowerPoint presentation slide 8).

10. Judith A. Langer, *The HIPAA Privacy Rules: Disclosures of Protected Health Information in Legal Proceedings*, 78 WIS. L. REV. 14, 16 (2005).

11. Keith E. Emmons et al., *Survey of Illinois Law: Health Care*, 27 S. ILL. U. L.J. 817, 832 (2003).

privacy of health information or affects the privacy of health information in a direct, clear and substantial way."'[12] Conflicts typically arise as states often prohibit the use or sharing of health information in situations where HIPAA allows the release of this data.[13] Furthermore, states often increase the privacy rights of an individual in relation to private health information.[14] As such, health plan administrators must be aware of both federal and state privacy regulations.[15]

III. STRICTER STATE LAWS

A. Illinois AIDS Confidentiality Act

Stringent state statutes often control the dissemination of personal health information pertaining to diseases such as HIV and AIDS.[16] The Illinois AIDS Confidentiality Act is one such law.[17] In order for a physician to order an HIV test, she must first obtain the consent of the patient;[18] however, authorization is not required if the test is for research purposes, the identity of the test subject is not known, and the subject is not informed of the results of the test.[19] Furthermore, outside of a few specific exceptions, any person to whom the results are disclosed is prohibited from passing that information on to anyone else.[20] Moreover, consent is required for disclosures related to payment and the general operation of a health plan, therefore increasing the regulations a health plan must follow.[21]

B. Illinois Insurance Code

State insurance codes also build upon the regulations put in place by HIPAA.[22] For example, the Illinois Insurance Code specifically outlines what an insurance company must include on personal information disclosure forms.[23] Although some aspects of HIPAA and the Illinois Insurance Code requirements overlap, the laws differ in the length of time

12. *Id.*
13. Langer, *supra* note 10, at 16.
14. *Id.*
15. *See* Emmons et al., *supra* note 11, at 835.
16. *See* 410 ILL. COMP. STAT. 305 (2004).
17. *Id.*
18. 305/4.
19. 305/8.
20. 305/10.
21. Weiser, *supra* note 5 (at PowerPoint presentation slide 17).
22. *See* 215 ILL. COMP. STAT. 5/1007 (2004).
23. *See id.*

that an authorization remains valid.[24] The Illinois law requires an insurance company to list a precise time period on the form, and also restricts the duration of the validity; if the authorization involves health insurance, it is only valid for a maximum of thirty months.[25] Since HIPAA only requires an expiration date, healthcare organizations must provide more structured authorization forms when working in Illinois.[26]

IV. OTHER FEDERAL LAWS REGULATING HEALTH CARE ORGANIZATIONS

A. ECPA

In addition to state laws strengthening HIPAA, federal regulations affect the way heath plans obtain and use personal health information. For example, the Federal Electronic Communications Privacy Act (ECPA) regulates how phone conversations are monitored and recorded.[27] The ECPA specifies that in order to "intercept a wire, oral, or electronic communication," either the person recording it must be "a party to the communication," or the consent of the other party needs to be obtained prior to the interception.[28] Therefore, healthcare organizations must comply with this law when they are surveying customers, offering customer service, or marketing their products.[29]

Not only does the ECPA add to the privacy regulations of HIPAA, it also creates a private right of action.[30] HIPAA currently does not allow an individual to file a lawsuit for a HIPAA privacy violation; instead, enforcement of HIPAA is left to the Office of Civil Rights (OCR).[31] Once an individual files a complaint with the OCR, the OCR pursues the complaint.[32] If the OCR believes a violation has occurred, it will then prosecute the violating entity.[33] Unfortunately, this is not an effective method of recourse for victims of privacy violations—as of April 2005, the federal government had only prosecuted one case under HIPAA.[34] However, the ECPA "contains express language creating a private right of

24. Weiser, *supra* note 5 (at PowerPoint presentation slide 15).
25. 5/1007.
26. Weiser, *supra* note 5 (at PowerPoint presentation slide 15).
27. *See* 18 U.S.C. § 2511 (2006).
28. *Id.*
29. Weiser, *supra* note 5 (at PowerPoint presentation slide 24).
30. Sonia W. Nath, *Relief for the E-Patient? Legislative and Judicial Remedies to Fill HIPAA's Privacy Gaps*, 74 GEO. WASH. L. REV. 529, 548 (2006).
31. *Id.* at 540.
32. *Id.*
33. *Id.*
34. *Id.* at 541.

action."[35] Therefore, the ECPA is more likely to affect the healthcare industry because a consumer can sue a healthcare provider over a privacy violation, which is something that rarely occurs under HIPAA.[36]

B. Restrictions of Telemarketing, Telephone Solicitation, and Facsimile Advertising

Moreover, federal restrictions regarding the use of automatic calls and automated voice recordings affect telephone conversations between customers and health plan organizations.[37] *The Restrictions of Telemarketing, Telephone Solicitation, and Facsimile Advertising* affect the marketing side of health plans by specifically restricting automated and recorded calls to any patient in a hospital, nursing home, healthcare facility, or the like.[38] Furthermore, a call cannot be placed to any person on a "do-not-call" list.[39] Due to this law, health plans must pay attention to whom they are calling and how they are placing the calls.[40] Although the government does allow some leniency on this issue if a group with the proper implementation of policies and procedures makes a mistake,[41] health plans still need to be sure they are following federal regulations.

IV. EFFECT ON PAY-FOR-PERFORMANCE PROGRAMS

The above-mentioned privacy laws not only affect health plan organizations, but also concern their pay-for-performance programs (PFPs).[42] PFPs were created to aid healthcare providers in cutting costs while improving the quality of care they give, and to ultimately reward providers based on performance.[43] There are four attributes commonly shared by PFPs: "(1) adherence to clinical guidelines; (2) collection of data from the healthcare provider; (3) measurement of the provider's performance; and (4) acknowledgement of the provider's performance with recognition and pay."[44]

---

35. *Id.*
36. Nath, *supra* note 30, at 541, 548.
37. Weiser, *supra* note 5 (at PowerPoint presentation slide 24); 47 C.F.R. § 64.1200 (2006).
38. § 64.1200.
39. *Id.*
40. Weiser, *supra* note 5 (at PowerPoint presentation slide 27).
41. *Id.*
42. *Id.*
43. Stacy L. Cook, *Will Pay for Performance Be Worth the Price to Medical Providers? A Look at Pay for Performance and Its Legal Implications for Providers*, 16 ANNALS HEALTH L. 163, 163 (2007).
44. *Id.* at 164.

Due to the extensive data needed for these programs, HIPAA and the other privacy laws play a large role in the management of PFPs.[45] The American Medical Association (AMA) has issued guidelines to aid in the administration of PFPs, which require that "[p]atient privacy . . . be protected in all data collection, analysis, and reporting."[46] These guiding principles assert that "[d]ata collection must be administratively simple and consistent with [HIPAA]."[47] Furthermore, physicians and plan administrators must pay careful attention to state legislation, as that often addresses the privacy of personal health information.[48]

V. CONCLUSION

As there are no uniform methods or rules for sharing personal health information, PFP administrators face a daunting task when establishing a legal method for analyzing data. These health plans need to look at what HIPAA permits while also abiding by the sometimes more stringent state laws.[49] If the healthcare organization covers PFPs in multiple states, it must develop several policies and procedures to satisfy the diverse laws.[50] Furthermore, management must look at other regulations affecting its practices, such as rules governing research design and research purposes, as well as the communications and marketing laws that come into play when communicating with its customers.[51] Privacy laws encompass many aspects of health care, thus requiring healthcare organizations to fully comprehend and research all applicable federal and state laws when establishing their policies and procedures.

In the following transcript, Mr. Weiser addresses the effect that these state and federal regulations have on the managing of health plans. He also explores the effects of the laws on the PFP movement and the data requests embedded in PFP programs. Finally, Mr. Weiser discusses the actions taken by health plans to work and comply with both federal and state privacy laws.

45. Weiser, *supra* note 5 (at PowerPoint presentation slide 28).

46. AMERICAN MEDICAL ASSOCIATION, AMA PRINCIPLES FOR PAY-FOR-PERFORMANCE PROGRAMS, http://www.ama-assn.org/ama1/pub/upload/mm/368/principles4pay62705.pdf, at 4 (last visited February 2, 2007).

47. *Id.*

48. *See* Emmons et al., *supra* note 11, at 835.

49. *See id.*

50. *Weiser*, *supra* note 5 (at PowerPoint presentation slide 37).

51. *Id.* (at PowerPoint presentation slide 24, 37).