



Chapter 1

Health Related Information and Employment Decisions: Is Your ERISA Plan Subject to Privacy Rights Under HIPAA?

By Samuel M. Brock III
Angela F. Hill
Grant P.H. Shuman
Spilman Thomas & Battle, PLLC
Charleston, West Virginia

Synopsis

§ 1.01. Introduction	1
§ 1.02. An Overview of ERISA and Employee Benefit Plans	4
§ 1.03. An Overview of HIPAA's Requirements	7
[1] — Covered Entities Under HIPAA	7
[2] — Protected Health Information Under HIPAA	9
[3] — Use and Disclosure of Protected Health Information	12
[4] — Minimum Necessary Uses and Disclosures	20
[5] — Business Associates of Covered Entities	22
[6] — Enforcement of HIPAA's Privacy Rules	23
§ 1.04. Implementation Issues for Employers	28
[1] — Employers that Sponsor Group Health Plans	29
[2] — Employers that Provide Certain Health Care Services	35
[3] — Other Employer Considerations	37
§ 1.05. Conclusion	39

§ 1.01. Introduction.

When it passed the Health Insurance Portability and Accountability Act of 1996 (HIPAA),¹ “Congress recognized the importance of protecting the privacy of health information given the rapid evolution of health

¹ 42 U.S.C. §§ 1320d - 29d-8 (2000).

information systems”² In reality, Congress enacted “the most significant changes to the health care industry since the passage of Medicare.”³ HIPAA is important in that it provides a reticulated regulatory structure that uniformly governs, with some significant exceptions, the use and disclosure of health information pertaining to most individuals.⁴

HIPAA addresses “four major administrative requirements for private and government-sponsored health plans.”⁵ These requirements include portability, nondiscrimination, fraud and abuse, and administrative simplification. “HIPAA’s administrative simplification provisions require the Secretary [of HHS] to adopt standards for financial and administrative transactions and data elements that are exchanged electronically.”⁶ The administrative simplification provisions also “authorized the Secretary [of HHS] to promulgate standards for the privacy of individually identifiable health information”⁷

The Privacy Rules, which regulate the use, disclosure, and transmission of protected health information (PHI), finally were promulgated on August 14, 2002, after several drafts and a great deal of public comment.⁸ They

² Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53182, 53182 (Aug. 14, 2002).

³ Kathy Bakich and Kaye Pestania, *Employer’s Guide to HIPAA Privacy Requirements*, ¶ 100 (Thompson Pub. Group 2002)(hereafter *Bakich, et al.*).

⁴ According to the U.S. Department of Health and Human Services (HHS), “Congress recognized that advances in electronic technology could erode the privacy of health information. Consequently, Congress incorporated into HIPAA provisions that mandated the adoption of Federal privacy protections for individually identifiable health information.” Office of Civil Rights, U.S. Department of Health and Human Services, *General Overview of Standards for Privacy of Individually Identifiable Health Information*, at 3 (Issued Dec. 3, 2002, Revised Apr. 3, 2003) <<http://www.hhs.gov/ocr/hipaa/>>. HHS also has described HIPAA as establishing “a uniform, federal floor of privacy protections for consumers across the country.” U.S. Department of Health and Human Services, *Fact Sheet: Protecting the Privacy of Patients’ Health Information*, at 1 (Released Apr. 14, 2003) at <<http://www.hhs.gov/news/>>.

⁵ *Id.*

⁶ *Id.* See 42 U.S.C. § 1320d-1(d)(2000).

⁷ Standards for Privacy of Individually Identifiable Health Information, *supra* note 2, at 53182.

⁸ *Id.* at 53183.

are mere one of a “suite” of rules designed to implement HIPAA’s administrative simplification procedures.⁹ As discussed below, these Privacy Rules present a regulatory minefield for the unwary employer.¹⁰

On their face, the Privacy Rules appear to exclude employers from complying with HIPAA’s requirements, but, in practice, there are many ways that employers can be implicated or affected by them.¹¹ The Privacy Rules apply to health plans, health care clearinghouses, and health care providers that transmit health information in electronic form as part of a transaction regulated by HIPAA.¹² The inclusion of health plans as covered entities raises many questions about the potential responsibilities of employers with regard to their employee benefit plans, which already are heavily regulated by the Employee Retirement Income Security Act of 1974, as amended (ERISA),¹³ Moreover, if an employer sponsors a health plan or provides certain health care services to its employees (*e.g.*, in the form of an on-site clinic or an employee assistance program), it may be required to comply with HIPAA’s onerous administrative requirements, in addition to the requirements of the Privacy Rules.

This chapter will address the various ways in which HIPAA may implicate or affect an employer and the steps necessary for employers to comply with HIPAA, where applicable. The following topics will be covered: (1) an overview of ERISA and employee benefit plans; (2) an overview of HIPAA’s privacy requirements; and (3) a discussion of implementation requirements for employers that sponsor covered group health plans or are determined to be health care providers under HIPAA.

⁹ Sheryl T. Dasco, *HIPAA Privacy Rules and Employee Benefit Plans*, 14 No. 2 Health Law. 35, 35 (2002).

¹⁰ HIPAA and the HHS regulations generally have withstood Constitutional challenge in at least one court of appeals. *See South Carolina Med. Ass’n v. Thompson*, 327 F.3d 346 (4th Cir. 2003).

¹¹ *See Bakich, et al., supra* note 3, at ¶ 130.

¹² *See* 45 C.F.R. § 160.102 (2002).

¹³ 29 U.S.C. §§ 1001, *et seq.* (2000).