-Related Liability for Employers?

by Mark Barnes, Patrik S. Florencio, and Brian M. Wyatt

Introduction

The greatest impact, in terms of number of businesses and organizations affected, of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its associated regulations (the "Privacy Rule")[1] may be on employers outside of the healthcare industry. Although the Privacy Rule directly regulates only healthcare providers who electronically transmit health information in connection with a transaction that is covered by the Rule (e.g., certain electronic billing and referral transactions), health plans, and health clearinghouses (collectively "covered entities"),[2] employer-sponsored employee health benefit plans that have 50 or more participants (or that are administered by an entity other than the employer-sponsor) are regulated as group health plans under the Rule.[3] Additionally, on-site medical clinics, such as employee health services, are also covered by the Rule if they electronically conduct any of the HIPAA-covered transactions. Thus, the number of employers outside of the healthcare industry with covered group health plans and/or covered on-site medical clinics may greatly outweigh the number of entities within the healthcare industry that must comply.

Many nonhealthcare-related businesses seem unaware of the fact that, because of one or more covered group health plans or on-site medical clinics, they may have certain obligations under the Privacy Rule. Because the Rule's jurisdiction attaches to the group health plan and/or on-site medical clinic, rather than to the employer directly, the Rule's regulation of employers is largely indirect. While the vast majority of the employer's operations will not be covered by the Rule, employers are nevertheless practically responsible for group health plan compliance, and legally responsible for on-site medical clinic compliance.

Because group health plans are separate legal entities from the employers that sponsor them for HIPAA and Employee Retirement Income and Security Act of 1974 (ERISA) purposes, they are theoretically responsible for satisfying their own Privacy Rule compliance obligations. However, the separate status of group health plans, legal or otherwise, is by and large a fiction. The group health plan certainly does not possess a separate corporate status, and typically is managed or administered by employees of the sponsor. Therefore, even if group health plan administrators are charged with responsibility for complying with the Privacy Rule, it is really the employer-sponsor that is supporting the compliance effort. Similarly, even though the Privacy Rule applies only to the on-site medical clinic of an employer, rather than to the employer's operations entirely, the legal responsibility for ensuring the clinic's compliance rests with the employer.

Another way that employers are indirectly regulated by the Privacy Rule is through the certification that they provide to their group health plan(s). A group health plan may not disclose any protected health information (PHI) to its employer-sponsor, unless the employer-sponsor has provided the group health plan with a certification that attests to the fact that the plan documents have been amended as required by the Rule.[4] The amendments to the plan documents impose a number of substantive obligations on the employer-sponsor.[5] Thus, if an employer-sponsor wants to receive any PHI from one or more of its group health plans, it must first agree through the certification process to comply with the obligations imposed on it through the plan document amendments. The regulation of employer-sponsors is indirect because, whereas the source of the group health plan's obligations is the Privacy Rule itself, the source of the employer-sponsor's obligations is the certification.

Mr. Barnes is a Partner in the Health Care Group in the law firm of Ropes & Gray, New York, NY.

Mr. Florencio is an Associate in the Health Care Group in the law firm of Ropes & Gray, New York, NY.

Mr. Wyatt is an Associate in the Health Care Group in the law firm of Ropes & Gray, New York, NY.

Nature and Scope of Employer-Sponsor Obligations

The foremost of the employer-sponsor's obligations with respect to PHI that it receives from one or more of its group health plans is to use and disclose only such PHI as permitted by the Privacy Rule or as required by law.[6] This obligation derives from the fact that the plan documents must be amended to ensure that the permitted uses and disclosures of PHI by the employer-sponsor under the plan documents are consistent with what is permitted under the Rule. In addition, the employer-sponsor must agree to abide by the Privacy Rule's provisions on access of individuals to PHI, amendment of PHI, and accounting of disclosures of PHI.[7] This entails, for example, making available to the group health plan such PHI as is necessary for the group health plan to provide employees/enrollees with access to their PHI.[8] Thus, the employer-sponsor is indirectly regulated through the certification and plan document amendments in largely the same way as the group health plan is directly regulated by the Privacy Rule. The employer-sponsor must even report to the group health plan any uses or disclosures of PHI that deviate from the permitted uses and disclosures of PHI enumerated in the plan documents.[9]

But if employer-sponsors are out of harm's way in relation to HIPAA-imposed sanctions, what incentive is there for them to comply with the obligations that they accrue by amending the plan documents?

Another of the employer-sponsor's obligations is to refrain from using or disclosing PHI when taking employment-related actions or making employment-related decisions, and to refrain from using or disclosing PHI in connection with any other benefit or employee benefit plan of the employer-sponsor.[10] While it is important for this obligation to be clearly articulated in the plan documents, and for the employer-sponsor to abide by this obligation pursuant to its certification, it will be very difficult for an employee/enrollee to prove that the reason for the employment-related action taken against him or her was based wholly or partially upon information derived from his or her PHI (e.g., a propensity to develop a costly future illness). For this reason, it has been posited that the law should impose greater restrictions on the collection of employee PHI, rather than regulate the subsequent use and disclosure of PHI by employers.[11]

In addition to the foregoing obligations, an employer-sponsor also must certify that it will: 1) make its internal practices, books, and records relating to the use and disclosure of PHI available to the Secretary of the Department of Health and Human Services for the purposes of determining compliance by the group health plan(s) (e.g., the Secretary may wish to audit the employer-sponsor's records to ascertain whether the group health plan is indiscriminately disclosing PHI to the employer-sponsor in violation of the amended plan documents);[12] 2) return or destroy all PHI, where feasible, when such PHI is no longer needed for the purpose for which the disclosure was originally made (where such return or destruction is not feasible, the employer-sponsor must agree to limit further uses and disclosures to those purposes that make the return or destruction of the PHI infeasible);[13] 3) establish adequate firewalls to prevent PHI from the group health plan from flowing to the employer-sponsor in circumstances that are not permitted by the plan documents;[14] and 4) ensure that any subcontractors or other agents to whom it discloses PHI acquiesce to the same restrictions and conditions upon the use and disclosure of PHI that are stipulated by the plan documents.[15]

Liability of Employer-Sponsor for Breach of Obligation?

While the Privacy Rule sets forth the aforementioned scheme for indirectly regulating the PHI that employer-sponsors receive from their group health plans, it does not specify what sanctions, if any, might be imposed on employer-sponsors who breach one or more of their obligations. The civil and criminal sanctions available under HIPAA[16] would not seem to apply to employer-sponsors, as these latter are not covered entities, and thus not technically covered by HIPAA. But if employer-sponsors are out of harm's way in relation to HIPAA-imposed sanctions, what incentive is there for them to comply with the obligations that they accrue by amending the plan documents? Are there any other sources of liability that might apply to employer-sponsors that violate one or more of their obligations?

To date, little to no scholarship exists on the HIPAA-related liability of employer-sponsors, making it unclear whether employer-sponsors could be subject to potential liability for failing to comply with their obligations, or whether no such liability will attach to employer-sponsors

(making it possible for them to breach their obligations with impunity).

The most obvious potential source of liability is the law of contracts. Could the certification provided by the employer-sponsor to the group health plan—first to amend the plan documents as required by the Rule, and then to abide by those amendments—be regarded as a contract between the employer-sponsor and the group health plan? If the certification can be considered a promise in consideration of the benefit of having access to PHI collected from employees/enrollees by the group health plan, then a contract may well exist. But who is likely to want to enforce that contract? Certainly not the group health plan whose managers and administrators are salaried employees of the employer-sponsor. The harm, if any, of a breach of contract (i.e., breach of the certification through a violation of one or more of the employer-sponsor's obligations under the amended plan documents) is likely to befall employees/enrollees, who may, for instance, suffer a loss of privacy through the inappropriate disclosure of their PHI, or who may have inappropriate employment-related action taken against them. Unless these employees/enrollees are considered to be third-party beneficiaries of the contract, however, they will be unable to enforce the contract (i.e., the certification), making its protective effects illusory.

Another potential source of liability for employer-sponsors is tort law. If certain portions of the Privacy Rule, or the Privacy Rule as a whole, become recognized as industry standards of care, those standards also may become recognized as legal standards of care in tort cases. Employees/enrollees who suffer a loss—particularly an economic loss—as a result of breach by the employer-sponsor of one or more standard of care, may then have a private right of action against the offending employer-sponsor. Yet another potential source of liability for employer-sponsors is fiduciary law. If a fiduciary relationship between the employer-sponsor and employees/enrollees can be established for these purposes, then a breach of the amended plan documents may be construed as a violation of that relationship.

In the case of employment-related action based inappropriately on information derived from an employee's/enrollee's PHI, a potential source of liability for employer-sponsors is federal and state antidiscrimination laws, including the Americans with Disabilities Act of 1990 (ADA). This recourse may avail employees/enrollees only in the most egregious cases. In addition to the problem of proof noted above, employer-sponsors have available to them a number of defenses to discrimination, such as the threat-to-others defense and the threat-to-self defense, which recently was upheld by the U.S. Supreme Court in *Chevron U.S.A Inc. v. Echazabal*.[17]

Conclusion

It remains uncertain whether the indirect regulatory scheme designed to subject employer-sponsors to many of the same obligations imposed on group health plans under the Privacy Rule will be capable of enforcement, directly by federal regulators and prosecutors or indirectly by aggrieved employees/enrollees citing common law principles of contract or tort, and/or other laws. If the scheme is unenforceable, one wonders how many employer-sponsors will abide by the relatively onerous obligations imposed by that scheme. As with other comprehensive regulatory schemes promulgated in recent years, such as the ADA, one might expect HIPAA-related employer-sponsor liability to become clear in ensuing years when addressed by the courts.

---

1 Standards for Privacy of Individually Identifiable Health Information; Final Rule, 65 Fed. Reg. 82,462 (2000), as amended at 67 Fed. Reg. 53,182 (2002). All citations to the regulations are referenced to 45 C.F.R.

2 45 C.F.R. § 160.103 (defining the term "covered entity").

3 *Id.* (defining the term "group health plan"). Group health plans are a covered form of health plan. *See id.* (defining the term "health plan").

4 *Id.* § 164.504(f)(1)(i) & (f)(2)(ii). The group health plan may nevertheless disclose summary health information, as well as enrollment/disenrollment information, to the employer-sponsor in the absence of certification from the employer-sponsor that the plan documents have been amended. *See id.* § 164.504(f)(1)(ii), (iii).

5 *Id.* § 164.504(f)(2).

6 *Id.* § 164.504(f)(2)(i), (f)(2)(ii)(A).

7 *Id.* § 164.504(f)(2)(ii)(E), (F), (G).

8 While the Privacy Rule could be read as requiring the plan documents to be amended so as to impose an obligation on employer-sponsors to themselves comply with the access, amendment, and accounting standards of the Rule, the better interpretation is that the documents impose on employer-sponsors the obligation of making available to the group health plan such PHI as is necessary for the group health plan to abide by those standards. A similar issue arose with respect to whether business associates must personally comply with these standards, or whether they must simply facilitate compliance with these standards by the covered entity. The preamble to the August 14, 2002 Rule clarified that the obligation of complying with the standards rests with the covered entity, but that the business associate is expected—by virtue of having entered into a business associate agreement with the covered entity—to assist the covered entity as necessary to carry out the covered entity's obligations under the Rule.

9 45 C.F.R. § 164.504(f)(2)(ii)(D).

10 *Id.* § 164.504(f)(2)(ii)(C).

11 P.S. Florencio & E.D. Ramanathan, *Secret Code: The Need for Enhanced Privacy Protections in the United States and Canada to Prevent Employment Discrimination Based on Genetic and Health Information*, 39 OSGOODE HALL L.J. 77 (2001).

12 45 C.F.R. § 164.504(f)(2)(ii)(H).

13 *Id.* § 164.504(f)(2)(ii)(I).

14 *Id.* § 164.504(f)(2)(ii)(J) & (f)(2)(iii).

15 *Id.* § 164.504(f)(2)(ii)(B).

16 42 U.S.C. §§ 1320d-5, 1320d-6.

17 122 S. Ct. 2045 (2002). For a review of this case, see M. Barnes, K.A. Cleaveland & P.S. Florencio, Chevron v. Echazabal: *Public Health Issues Raised by the 'Threat-to-Self' Defense to Adverse Employment Actions,* AM. J. PUB. HEALTH [forthcoming].