Employee-Enforcement of HIPAA Privacy Requirements Under HIPAA and State Common Law & Statutes

By: David Rintoul
Brown, Paindiris & Scott

Introduction. The Health Insurance Portability and Accountability Act, P.L. 104-191, § 1(a), 110 Stat. 1936, ("HIPAA") enacted a variety of provisions regarding heath insurance and the health care industry. One of the four major parts of HIPAA directed the Department of Health and Human Services ("HHS") to develop standards for financial and administrative transactions to permit efficient electronic exchange of administrative health information, generally referred to as the "administrative simplification" provisions.[1]

In directing HHS to develop these standards, HIPAA also directed HHS to make recommendations and issue regulations "with respect to the privacy of individually identifiable health information." P.L. 104-191, Title II l Subtitle F, § 264.[2] HHS has issued regulations that require "health plans" to protect individuals' medical information, called "protected health information" or "PHI" in the regulations. "HIPAA" as used in this article, unless otherwise mentioned, will mean the privacy provisions. These provisions generally come into effect in April 14 2003, with certain small plans subject to a April 14, 2004 effective date.

HIPAA generally exempts employers from the Act. Many employers will be subject to the Act, however. Employers that receive any PHI in connection with a group health plan, such as employers who administer their own plans or participate in administration of health plans, as plan sponsors or otherwise, will have to comply with the HIPAA privacy provisions.[3] Employers who have fully insured health plans and receive no PHI are not subject to the regulations.[4]

This article will provide a brief summary of what HIPAA requires of employers, and then discusses an employer's exposure to actions by employees who claim that the employer violated HIPAA.

Summary of HIPAA Privacy Provisions

HIPAA basically requires that covered entities use or disclose PHI only to provide treatment, for payment purposes or in connection with certain "heath care operations" unless the individual specifically consents to such other use or disclosure.

It is easy to see how employers could violate HIPAA through use of PHI. One clearly invalid use of PHI is to use it to make employment decisions. An employer subject to HIPAA will violate HIPAA if PHI leaks out of the benefits department to a supervisor who then makes an employment decision based on the PHI. Further, a terminated employee may claim that an employer fired him in retaliation for complaints about misuse of PHI. HIPAA's regulations prohibit such retaliation.[5] The question is what the employee can do about it, and what defenses will the employer have to any action alleging either violation of HIPAA, or retaliation for complaining about violation of HIPAA.

Administrative Enforcement of HIPAA

HIPAA establishes no new private right of action. The only direct remedy available to an employee for violation of HIPAA is the administrative procedure established under HIPAA.[6] HHS's Office of Civil Rights ("OCR") is responsible for the administrative process under HIPAA.[7] HHS

has stated that enforcement of HIPAA will primarily be complaint driven rather than by HHS conducting random compliance audits.

It appears unlikely that there will be a large volume of complaints filed, considering the weakness of the administrative procedure under HIPAA.

Administrative Procedures: The administrative procedure resembles other civil rights administrative provisions, requiring that complaints be in writing and filed within 180 days of the date the complainant knew or should have known of the violation.[8] The 180 days period is **not** jurisdictional, however, and will be waived if good cause for delay is shown. **Anyone** can file a complaint; the complainant does not have to be the person who's PHI was disclosed. This means that employers accused of systemic violations of HIPAA could be subject to complaints brought by advocacy groups, or by current or former employees even if the employees' PHI was not involved in the violation.

The regulations provide that OCR *may* investigate complaints, which appears to give OCR the authority to decide whether to investigate a complaint.[9] OCR can investigate the specific complaint, or conduct a general compliance audit. Covered entities are required to cooperate with the complaint investigation, including providing access to policies, procedures or practices of the covered entity to determine compliance.[10]

Remedies: If OCR finds that a violation occurred, it would first attempt to resolve the complaint by informal means, which informal means are not specified.

If it can not resolve the complaint by informal means, OCR "may issue . . . written findings documenting the non-compliance." It can also levy fines, as explained below. OCR apparently has no authority to order any relief, whether monetary or equitable, in favor of the complainant. There are several other potential sources to compel compliance.

Civil Penalties: OCR can impose a civil penalty of up to $100 per violation on any "person" who violates HIPAA, with a maximum of $25,000 for separate instances of the identical requirement or violation.[11] The penalties cannot be imposed if the person liable did not know of the violation and would not have known of it in the exercise of reasonable diligence, or the compliance failure is the result of reasonable cause and not willful neglect, and the failure is cured within thirty days of when the liable person knew or should have known of the compliance failure occurred.

Criminal Penalties: A person who obtains PHI of an individual or discloses the information can be fined up to $50,000, imprisoned for a year, or both. A person who knowingly violates HIPAA can be fined up to $100,000, imprisoned for five years, or both. A person who knowingly violates HIPAA with intent to sell or use the information for commercial advantage can be fined up to $250,000, imprisoned for ten years, or both.

Anti-Retaliation Provisions: The regulations do state that a covered entity cannot retaliate against or intimidate an individual for exercising HIPAA rights, filing a complaint under HIPAA, testifying or cooperating in the investigation of a complaint, or opposing any act that is unlawful under HIPAA, or that the individual believes in good faith to constitute a violation, and the manner of the opposition is reasonable and does not involve the disclosure of PHI.[12]

In addition to prohibiting retaliation, the regulations require that an entity must mitigate, to the extent practicable, the harmful effect of any violations of HIPAA policies or procedures.[13] Presumably, this could include the obligation to rehire an employee who was dismissed in violation of the anti-retaliation provisions. It is unclear, however, how this obligation could be enforced, since it does not appear that OCR has the power to order covered employees to do anything other than pay civil penalties.

HIPAA Violation as a Violation of ERISA or the ADA

Violations of HIPAA are potential violations of ERISA as well. ERISA and HIPAA both generally apply to group health plans. Further, HIPAA requires that ERISA plan documents be amended in certain respects to establish permitted and required PHI uses and disclosures. For instance, a plan cannot release PHI to a plan sponsor unless the plan documents require the plan sponsor to comply with HIPAA's privacy rules in using the information.[14] Under ERISA §502(a)(3), failure to administer the plan in accordance with the plan documents is a breach of fiduciary duty.[15] Failure to comply with the HIPAA-mandated plan provisions could therefore be a breach of fiduciary duty. However, considering the current inability to recover any type of money damages for violation of ERISA, ERISA will probably be only a theoretical method for an individual to enforce HIPAA.[16]

The ADA also requires that an employee's medical information be kept from the employee's supervisors, other than as is necessary to disclose job restrictions or accommodations. In Fitch v. Continental Casualty Co., 2002 U.S. Dist. LEXIS 24269 (N.D. Ill., Dec. 16, 2002), an EAP counselor, who had counseled an employee, told the employee's supervisors that he believed the employee was mentally ill, could not control her impulses, and would not get better. The employee alleged violation of the ADA and state law handbook contract and misrepresentation claims based on violation of the employer's promises that EAP matters would remain confidential. The court denied the employer's motion for summary judgment on both claims.

Common Law Enforcement of HIPAA

There is no direct action that an employee can bring for violation of HIPAA. The question is whether an individual can maintain any state law causes of action, including a Sheets public policy wrongful discharge claim, alleging retaliation for exercising one's rights under HIPAA or complaining about violations of HIPAA.

Preemption of State Laws. HIPAA preemption makes ERISA preemption look easy. See, for instance, U.S. ex re. Stewart v. The Louisiana Clinic, No. Civ.A. 99-1767 (E.D. La. Dec. 12, 2002)[17] The full scope of HIPAA preemption is beyond the scope of this article, but basically, state laws are preempted if they are contrary to a requirement or provision of HIPAA.

The privacy rules state that a state law is contrary to HIPAA if a covered entity would find it impossible to comply with both, or the state law is an obstacle to accomplishing the full purpose of HIPAA's goal of promoting administrative simplification.[18] To avoid preemption on grounds that the law is stricter than HIPAA, a law that conflicts with HIPAA must be specifically designed to protect the privacy of individually identifiable medical information, and the state law must be more

stringent in certain specified ways set forth in the regulations.[19]

Whether a particular state law will be preempted must be done on a section-by-section basis: the fact that one provision will be preempted does not mean that other sections of the same law will be preempted.[20] Therefore, it is difficult to determine preemption without reference to a specific law, but in general:

- Employee counsel will argue that allowing state law causes of action that grant employees greater remedies for unauthorized disclosures of medical information, or for retaliation, is not contrary to HIPAA, since affording such remedies does not make it impossible for the covered entity to comply with HIPAA, and in fact furthers HIPAA's interest in by providing additional incentives to protect private medical information.

- Employer counsel will argue that the limited non-criminal enforcement of HIPAA is in fact a "provision" of HIPAA. By imposing greater consequences for violating HIPAA than HIPAA provides itself, applying greater sanctions under state law would by an obstacle to achieving HIPAA's purpose of promoting administrative simplification. If the state law is found to conflict with HIPAA, employer counsel will argue that laws such as common law retaliation claims are not primarily intended to protect medical privacy, and so will not qualify for the preemption exemption.

State Laws That Could Apply to HIPAA Violations

Common Law Wrongful Discharge. A claim of public policy wrongful discharge based on the public policy embodied in HIPAA would be a great test of how far the Connecticut Supreme Court is willing to go in applying its holding in Burnham v. Gelb, 252 Conn. 153 (2000). In that case, among other things, the Court held that the existence of an administrative remedy under the Occupational Safety and Health Act (at 29 U.S.C. § 660) precluded the plaintiff from bringing a Sheets claim. The OSHA regulations provided that the Secretary of Labor determines if a violation took place. If it found that a violation existed, the statute provides that the Secretary "shall" bring suit on behalf of the employee. In such a suit, the Secretary is authorized to obtain reinstatement with back pay. 252 Conn. at 181, n. 2. If the Secretary did not find a violation, the employee would have no further remedy. 252 Conn. at 183. The Court held that even though the administrative remedies were not equivalent to the common law remedies, the existence of an administrative remedy precluded a common law cause of action, applying the reasoning of Atkins v. Bridgeport Hydraulic Co., 5 Conn. App. 643 (1985).

The remedies available under HIPAA for an employee who is retaliatorily discharged make the OSHA remedies look generous. Essentially, there is no remedy under HIPAA for retaliatory discharge in favor of the discharged employee, since the only consequence of OCR finding that a violation of HIPAA occurred is to issue a written finding to that effect and levy civil fines. While the Court in Burnham held that the administrative remedy does not have to be equivalent to preclude a common law cause of action, the effective absence of **any** remedy under HIPAA may cause the Court to allow such a cause of action for

retaliatory discharges that violate HIPAA's public policy.

If the preemption battle does not defeat such a claim, it may be that the mere existence of any administrative procedures might be sufficient for the Connecticut Supreme Court to hold that any public policy wrongful discharge claim is precluded by the administrative procedures.

Common Law Invasion of Privacy. Connecticut recognizes the tort of invasion of privacy, including the "intrusion upon seclusion" part of the tort. Goodrich v. Waterbury Republican-American, Inc., 188 Conn. 107, 128, 448 A.2d 1317 (1982). The elements of a claim for intrusion upon seclusion are that there has been an intrusion upon the seclusion of an individuals that would be highly offensive to a reasonable person. Id. Violation of HIPAA's requirements could be used to establish a claim of intrusion upon seclusion. In Fallstrom v. L.K. Comstock & Co., 2001 Conn. Super. LEXIS 129, the court held that the violation of the confidentiality provisions of C.G.S. §31-51u, Connecticut's drug testing statute, established that an intrusion occurred, leaving only the issue of whether the intrusion would be highly objectionable to a reasonable person. Violations of HIPAA by an employer subject to HIPAA could be used in the same manner.

Connecticut Statutory Remedies for Violations of Medical Privacy. The provisions of the Connecticut Personnel Files Act, C.G.S. §31-128A et seq., apply as well to medical files.[21] The statute general prohibits disclosure of individually identified information from an employee's medical file unless the employee consents.[22] There is unlikely any direct cause of action exists for violation of 31-128a, since Superior Courts that have considered the issue have found no private right of action under the statute, though an appellate court has not yet addressed the issue. *E.g.* Esposito v. Connecticut College, 2000 Conn. Super. LEXIS 2305 (September 1, 2000). Since there is no administrative remedy under the state statute, a discharge in retaliation for actions taken to protect an employee's medical information would presumably support a public policy wrongful discharge claim.

- Employee counsel would argue that statute should not be preempted by HIPAA, and therefore a public policy claim based on the statute should not be preempted, either. It appears that nothing in the statute conflicts with HIPAA. To the extent there is a conflict resulting from the statute imposing more stringent requirements than HIPAA, the statute probably complies with the exemption from preemption set forth in the rules: the law is specifically concerned with protecting the privacy of medical information and neither conflicts with HIPAA nor is an obstacle to accomplishing HIPAA's purpose of promoting administrative simplification.

- Considering the extensive privacy provisions of the HIPAA regulations, employer counsel will argue that the Connecticut Personnel Files Act does conflict with HIPAA. The privacy regulations of HIPAA are so comprehensive that conflicts will exists to the extent HIPAA requires covered entities to take some action that is not required by the Connecticut Personnel Files Act.

They would argue that the preemption exemption would not save the Act from preemption, since the Act is in fact **less** stringent than HIPAA as a result of the extensive privacy regulations of HIPAA. They would argue that since the statute itself is preempted, any wrongful discharge claim based on the public policy embodied in the statute would be preempted as well.

Conclusion

Efforts to comply with HIPAA by health plans and employers subject to HIPAA has created an industry of consultants and advisors seeking to help covered entities to comply with the extensive, but still incomplete, HIPAA regulations. While the compliance work is extensive for many employment lawyers, determining whether HIPAA will lead to significant employment litigation will be unknown until the privacy regulations come into effect, and courts determine what sort of remedy employees can obtain for violations of HIPAA.

David Rintoul is a partner in Brown, Paindiris & Scott's Glastonbury office. He represents individuals and employers in all areas of employment law, and individuals in all aspects of ERISA litigation. He can be reached at (860) 659-0700 or drintoul@bpslawyers.com

[1] The other three major parts of HIPAA provide for: portability of group health coverage; non-discrimination in benefits eligibility and premiums based on certain health conditions; and measures to fight and punish fraud and abuse. These other three parts are beyond the scope of this article.
[2] Text of public act contained in the notes to 42 U.S.C.S. 1320d-2.
[3] A group health plan administered and established by an employer with fewer than fifty participants is exempt from the HIPAA privacy requirements. 45 C.F.R. § 160.103.
[4] 45 C.F.R. §164.530(k).
[5] 42 C.F.R. § 164.530(g).
[6] The administrative provisions are set forth at 45 C.F.R. §160.300 et seq. with additional provisions at 45 C.F.R. §160.530.
[7] Located on the web at http://www.hhs.gov/ocr/index.html.
[8] 45 C.F.R. §160.306. Complainants can, but are not required, to use OCR's Health Information Privacy Complaint Form, to be available at http://www.hhs.gov/ocr/hipaa. Complaints from Connecticut should be filed at the following address: Region I, Office for Civil Rights,
U.S. Department of Health and Human Services,
Government Center,
J.F. Kennedy Federal Building—Room 1875,
Boston, Massachusetts 02203. Voice phone (617) 565–1340. FAX (617) 565–3809.
[9] 45 C.F.R. § 160.306(c).
[10] 45 C.F.R. §160.310.
[11] 42 C.F.R. § 1320d-5(a)(1).
[12] 45 C.F.R. § 164.530(g).
[13] 45 C.F.R. § 164.530(f).
[14] 45 C.F.R. §164.504(f).
[15] 29 U.S.C. §1132(a)(3).
[16] Mertens v. Hewitt Associates, 508 U.S. 248, 113 S. Ct. 2063, 124 L. Ed. 2d 161 (1993).
[17] (holding that HIPAA preempted Louisiana's medical privacy rules, and allowed production in litigation of individually identifiable medical information pursuant to procedures under HIPAA, rather than pursuant to procedures under the Louisiana statute).
[18] 64 Fed. Reg. 59997 (Nov. 3, 1999).
[19] 64 Fed. Reg. 59996 (Nov. 3, 1999).
[20] 64 Fed. Reg. 59995 (Nov. 3, 1999)
[21] C.G.S. § 31-128f.
[22] The statute allows disclosure: to a third party that performs employment-related services for the employer; pursuant to a subpoena; pursuant to a law enforcement agency's request for a home address and dates of employment; in response to a medical emergency; to comply with law; or pursuant to a collective bargaining agreement. C.G.S. § 31-128f.