

Bloomberg

CORPORATE LAW JOURNAL

Volume 2

Summer 2007

Issue 3

Health Insurance Portability and Accountability Act-Compliant Merger and Acquisition Transactions

Jeffrey C. Johnson and Amanda C. Stevens
Pryor Cashman LLP

Reprinted from
Bloomberg
CORPORATE LAW JOURNAL
Volume 2, Summer 2007, Issue 3

MERGERS & ACQUISITIONS

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT-COMPLIANT MERGER AND ACQUISITION TRANSACTIONS

By Jeffrey C. Johnson* and Amanda C. Stevens**

INTRODUCTION

HIPAA – What Is It?

In recent years, merger and acquisition transactions in the health-care industry have been complicated by the Health Insurance Portability and Accountability Act (HIPAA), which was signed into law on August 21, 1996.¹ This article will briefly explore how HIPAA affects mergers and acquisitions, with a particular focus on databases, which are, with increasing frequency, a critical asset driving the underlying economics of many of these deals. HIPAA's stated purpose was to improve access to group health insurance coverage and guarantee that all coverage in the group market was renewable.² Perhaps more importantly from a legal compliance perspective, HIPAA set up privacy and security standards which protect consumer health information from inappropriate uses and disclosures by those who have access to this data.³ When using or disclosing health information covered by HIPAA's privacy requirement, businesses are required to limit that use and disclosure to the minimum necessary to accomplish the intended purpose.⁴

* Jeffrey C. Johnson is a partner in the New York office of Pryor Cashman LLP. He specializes in the transactional aspects of technology and intellectual property exploitation. In particular, he has significant experience in all aspects of mergers and acquisitions, joint ventures, strategic alliances, private placements and licenses in the biotech, entertainment, Internet, pharmaceutical, software and telecommunications industries. He has been an invited speaker and panelist at a variety of public and private events, including the Digital Commerce Summit in 2006. He is also a co-author of the U.S. Law chapter of the World Online Business Law Digest. Mr. Johnson may be reached at (212) 326-0118 or jjohnson@pryorcashman.com.

** Amanda C. Stevens is a 2007 Summer Associate in the New York office of Pryor Cashman L.L.P. She is also a 2008 J.D. candidate at Cornell University Law School. She is interested in pursuing a career in litigation, with a particular focus on intellectual property matters.

1. Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat 1936 (1996) (codified as amended in scattered sections of 18 U.S.C., 26 U.S.C., 29 U.S.C., and 42 U.S.C.).

2. 45 C.F.R. § 144.101(a) (2005).

3. 45 C.F.R. § 164.502(a) (2005).

4. 45 C.F.R. § 164.502(b)(1) (2005).

What Is Covered?

HIPAA authorized the Department of Health and Human Services (DHHS) to promulgate the Privacy Rule, which established privacy standards for health information.⁵ The HIPAA Privacy Rule regulates how certain entities, called “covered entities,” use and disclose particular individually identifiable health information, called “protected health information” or PHI.⁶ PHI means individually identifiable health information that is transmitted or maintained electronically, or in any other form or medium.⁷ Such information covers demographic data that is collected from an individual by, or that is otherwise created or received by, a covered entity.⁸ It is also information that relates to the health of an individual, the provision of health care to that individual, and any payments for their health care.⁹ Individually identifiable health information can either identify an individual or create a reasonable basis to believe that it could be used to identify an individual.¹⁰ Typically, PHI is aggregated into databases that become an important asset for businesses active in the healthcare industry.

If PHI is de-identified, (i.e., rendered anonymous), the use and disclosure of it is no longer subject to the requirements of HIPAA’s Privacy Rule unless it is, or can easily be, re-identified.¹¹ PHI is de-identified if it no longer identifies an individual and if there is no reasonable basis to believe that it could be used to identify an individual.¹² Under the Privacy Rule a covered entity can use either of two methods to de-identify PHI.¹³ The simplest method is the removal of the eighteen identifiers of an individual or the individual’s relatives, employers, or household members.¹⁴ The Privacy Rule’s eighteen identifiers include basic information such as names, phone numbers, social security numbers and full face photographs.¹⁵ Alternatively, PHI can be de-identified if a person with knowledge and experience of statistical methods determines that the risk is very small that the information could be used alone, or in combination with other reasonably available information, to identify an individual who is a subject of the information.¹⁵ This alternative means of de-identification

5. Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, § 264(c)(1), 1937, 2033-34 (1996).

6. 45 C.F.R. § 160.103 (2005); 45 C.F.R. § 164.302 (2005).

7. 45 C.F.R. § 160.103 (2005).

8. *Id.*

9. *Id.*

10. *Id.*

11. 45 C.F.R. § 164.514 (2005); Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,499 (Dec. 28, 2000).

12. 45 C.F.R. § 164.514(a) (2005).

13. 45 C.F.R. § 164.514(b) (2005).

14. 45 C.F.R. § 164.514(b)(2)(i) (2005).

15. 45 C.F.R. § 164.514(b)(2)(i)(A), (D), (G), (Q) (2005).

16. 45 C.F.R. § 164.514(b)(1) (2005).

also requires that the person making the determination document the methods and results of his or her determination.¹⁷

Who Is Covered?

Covered entities who must comply with the Privacy Rule are defined as health plans, healthcare clearinghouses, and healthcare providers who transmit any health information in electronic form in connection with certain covered transactions.¹⁸ Covered entities frequently use “business associates” to perform certain administrative operations in an effort to reduce costs.¹⁹ Business associates are defined as a business or individual that contracts to perform certain administrative functions or services that require the disclosure of PHI.²⁰ A good example of a business associate is a billing service.²¹ HIPAA requires that covered entities must enter into contracts with business associates to safeguard PHI used by or disclosed to the business associate.²² The business associate contract, commonly known as a Business Associate Agreement, must establish the permitted and required uses and disclosures of PHI by the business associate.²³ Under these contracts, business associates take on several responsibilities, including a commitment to not use or disclose PHI in a way that would violate their contract or the law.²⁴ Without a Business Associate Agreement, a business associate has no right to receive PHI from a particular covered entity. This means that even if a business associate has a contract to handle billing for one doctor, the business associate is not necessarily authorized to receive PHI from another doctor’s office unless it also has a Business Associate Agreement with that other doctor.

The requirements for business associates trigger important considerations for covered entities. A covered entity is not in compliance with HIPAA if it knows of a pattern of activity by its business associate that violates the Privacy Rule.²⁵ Covered entities need not actively monitor their business associates; however, a covered entity nonetheless is expected to investigate when they receive complaints or substantial and credible evidence of violations by a business associate.²⁶ Furthermore, the covered entity must act upon any knowledge of any such violation that it

17. *Id.*

18. 45 C.F.R. § 160.103 (2005).

19. Matthew B. Drexler, *Health Law – Privacy in Medical Research: A Botched Experiment*, 29 W. NEW ENG. L. REV. 535, 546 (2007).

20. 45 C.F.R. § 160.103 (2005).

21. *Id.*

22. 45 C.F.R. § 164.502(e)(2) (2005); 45 C.F.R. § 164.504(e)(1) (2005).

23. 45 C.F.R. §§ 164.504(e)(2), (e)(2)(i) (2005).

24. 45 C.F.R. § 164.504(e)(ii)(A) (2005).

25. 45 C.F.R. § 164.504(e)(1)(ii); Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,505 (Dec. 28, 2000).

26. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,505 (Dec. 28, 2000).

possesses.²⁷ A covered entity must terminate its contract if it (i) determines that its business associate has breached a material term of the contract and (ii) an action to cure such a breach has failed.²⁸

In order to comply with HIPAA, covered entities and business associates must have in place adequate administrative, physical, and technical safeguards to protect the privacy of PHI from any intentional or unintentional disclosure that would violate the Privacy Rule.²⁹ Examples of such safeguards are staff training and modifying procedures as necessary to comply with changes in the law.³⁰ Additionally, covered entities and their business associates must take reasonable steps to safeguard PHI to limit incidental uses and disclosures made pursuant to an otherwise permissible use or disclosure.³¹

What Are the Penalties for Violations?

HIPAA creates civil penalties for the improper use and disclosure of PHI.³² Civil penalties may not be imposed if the noncompliance was not discovered because the person liable for the penalty did not know, and by exercising reasonable diligence would not have known, of the violation.³³ Furthermore, a civil penalty may not be imposed if the failure to comply was due to reasonable cause, not to willful neglect, and the failure to comply was corrected within thirty days of either discovering the violation or within thirty days of the date that, by exercising reasonable diligence, the failure to comply would have been discovered.³⁴

The civil penalty may not be more than \$100 per violation, except that the total penalty imposed for all violations of an identical requirement or prohibition may not exceed \$25,000 in a calendar year.³⁵ However, there is no limit on the number of standards that may be violated and on which the civil monetary penalty may be assessed.³⁶ As a result, fines can add up quickly, particularly for entities that process large volumes of data.

Criminal sanctions will be imposed if someone knowingly and without proper authorization uses a unique health identifier or obtains or discloses individually identifiable health information relating to an individual.³⁷ The penalties vary depending upon the severity of the criminal

27. *Id.*

28. *Id.*

29. 45 C.F.R. § 164.530(c) (2005); 45 C.F.R. § 164.502(e)(1) (2005); 45 C.F.R. § 164.504(e)(2) (2005).

30. 45 C.F.R. § 164.530(i)(1) (2005); 45 C.F.R. § 164.530(i)(2)(i) (2005).

31. 45 C.F.R. § 164.530(c)(2)(ii) (2005).

32. 42 U.S.C.A. § 1320d-5(a)(1) (2003).

33. 42 U.S.C.A. § 1320d-5(b)(2) (2003).

34. 42 U.S.C.A. § 1320d-5(b)(3)(A) (2003).

35. 42 U.S.C.A. § 1320d-5(a)(1) (2003).

36. Greta C. Cowart, *Retiree Medical Benefits and HIPAA Privacy and Security in Mergers and Acquisitions*, 2007 A.L.I. & A.B.A. CONTINUING LEGAL EDUC., COURSE OF STUDY, 961.

37. 42 U.S.C.A. § 1320d-6(a) (2003).

act.³⁸ The maximum penalties are a fine of up to \$250,000 or imprisonment of up to ten years, or in some cases both.³⁹

DHHS has agreed that individuals should be able to sue for breaches of privacy.⁴⁰ Accordingly, it has taken the view that state laws which are more protective of privacy than contrary federal standards will continue to exist under, and are not superseded by, HIPAA, and will continue to provide the maximum legal protection for individual's health information privacy.⁴¹

HIPAA-COMPLIANT TRANSACTIONS

What Should the Seller Worry About?

The advent of HIPAA has imposed upon seller's counsel a new and critical element of the "pre-deal" due diligence process: to determine whether the assets of the business being sold include PHI. In most instances, the seller will be aware that it owns PHI and that the PHI will be included in the assets of the business being sold; however, there may be instances where a business that is not traditionally thought of as a "business associate" subject to the Privacy Rule is, in fact, just that.

A good example is a collection agency. If seller is a collection agency with clients that are mostly traditional businesses rather than healthcare providers, but which has a few clients that are healthcare providers, that seller may be receiving PHI without even being aware of it. Ordinarily, the healthcare provider client will have made the seller aware that by providing services to the healthcare provider, it has become a business associate subject to the Privacy Rule, but the significance of that fact may not be fully appreciated by the seller. Simply put, the seller may innocently fail to disclose this information to its counsel because it does not appreciate its significance. Alternatively, the seller's health-care provider client may have itself failed to comply with HIPAA and provided PHI to the seller without ever entering into a business associate agreement. Again, in such circumstances it is likely the seller will have failed to appreciate the significance of the information it is receiving from its client.

If seller is a covered entity, and the assets of the business being sold include PHI, then a second level of inquiry must be pursued once the prospective buyer has been identified. Specifically, in order to comply with HIPAA in connection with a sale of a business that has, or assets that include, PHI, the seller must take reasonable steps to satisfy itself that the buyer is in fact a covered entity or business associate that can be trusted to properly handle the PHI. Recall that PHI cannot be disclosed to anyone other than a covered entity or a business associate contractually

38. 42 U.S.C.A. § 1320d-6(b) (2003).

39. 42 U.S.C.A. § 1320d-6(b)(3) (2003).

40. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,566 (Dec. 28, 2000).

41. *Id.*

bound to comply with the Privacy Rule. It is important to appreciate that this analysis can be complicated, particularly if the buyer is not simply assuming control of a going concern.

For example, while a business associate may possess and use PHI that it must necessarily use in order to properly provide its services, that business associate is not necessarily authorized to possess or use other PHI that is not required to be used in connection with the services it provides.⁴² Accordingly, if a buyer intends to recast the business it is purchasing so that it will no longer provide the same services the seller provided, the seller may violate the Privacy Rule by selling and subsequently revealing to buyer PHI included in the assets being sold.

In this era of large databases, it is not unusual for data, including PHI, to have value in a de-identified form. For example, a statistically meaningful amount of de-identified data regarding the habits of prescription drug users may provide valuable marketing information to a drug manufacturer, such as whether patients are taking the recommended doses, which can be gleaned from information about refill frequency. As a result, even if a buyer is not a covered entity, and does not otherwise have a right to possess PHI, it may still want to purchase assets of the seller consisting of PHI.

In these circumstances, the seller can still structure a HIPAA-compliant transaction by de-identifying the relevant PHI. Typically, the method of de-identification relying on statistical analysis (as opposed to actual removal of the eighteen specific identifiers) can be acceptable to buyer. In these circumstances, the relevant PHI may be encrypted using a sophisticated encryption algorithm; so long as a properly qualified statistician will certify for seller that the risk is "very small" that the resulting encrypted data can be unencrypted or otherwise used (either alone or in combination with other readily available information) to identify an individual who is the subject of the information,⁴³ the seller can deliver the de-identified data to the buyer without violating the Privacy Rule.

In these circumstances, seller's counsel must also ensure that the encryption algorithm used to de-identify the PHI will not be accessible to or otherwise used by the buyer to re-identify the PHI. Ordinarily, a covenant to that effect can be included in the agreement(s) documenting the relevant transaction.

What Should the Buyer Worry About?

As with seller's counsel, the advent of HIPAA has imposed upon buyer's counsel new and critical elements of the due diligence process. In particular, a buyer needs to be wary of inadvertently buying PHI. If the

42. 45 C.F.R. § 164.504(e)(ii)(A) (2005) (A contract . . . must . . . provide that the business associate will not use or further disclose the information other than as permitted or required by the contract. . .).

43. 45 C.F.R. § 164.514(b)(1) (2005).

assets of the business being acquired include PHI, then the buyer must either qualify as a "covered entity" in respect of such PHI, or it must arrange for that PHI to be de-identified.

A buyer who is not familiar with HIPAA compliance may well be surprised by the cost of establishing an adequate infrastructure for protecting and otherwise managing the PHI it possesses. Similarly, a buyer may expect to be able to use the PHI for particular commercial purposes, only to find that the Privacy Rule prohibits such activities. For instance, a buyer can't simply buy a healthcare provider's database containing the names and addresses of diabetes patients and then use that information to send them marketing materials for sugar-free foods.

While a well prepared and well counseled seller will ordinarily know, and make any prospective buyer aware of, the fact that the assets of the business being sold include PHI, the buyer should not assume this to be the case. If a seller's business consists (whether in large part or small) of being a business associate, there may well be significant HIPAA compliance costs associated with that fact, and buyer needs to account for these costs in its pre-deal due diligence. In short, uninitiated buyers need to be well educated about the consequences of owning PHI and what can and can't be done with that PHI.

Another significant risk arises in the context of restructuring a business, particularly in this era of information technology services. When a buyer restructures that business as planned, the restructured business may necessarily possess PHI that, under the old business model, it did not possess.

For example, a software business that sells customized office management software to doctors and other healthcare providers will not possess PHI if it simply licenses its software on disks that are then loaded onto the licensee's hardware. If that same business is recast as an application service provider or is similarly restructured so that the software owner sells a service allowing the healthcare provider clients to remotely access the software and store PHI on its servers, the buyer now possesses PHI and must necessarily be a business associate that complies with HIPAA's Privacy Rule.

CONCLUSION

As the use of databases proliferates, so too do attendant privacy concerns. HIPAA was in large part enacted to address some of these concerns. In HIPAA's wake new concerns regarding the commercial use of databases including (or derived from) PHI have arisen. It is increasingly important for transactional attorneys to be aware of these concerns and to provide their client with well-thought out guidance regarding HIPAA compliance, taking into account not just the technical requirements of HIPAA's regulatory scheme, but the client's practical commercial requirements as well.