Due Diligence and HIPAA: Issues Pertaining to Complete Disclosure and the Limitations Imposed to Protect Privacy Considerations

Patrick D. Souter
Jenny G. Givens
Gray Reed & McGraw PC
Dallas, TX

Whether it is a stock or asset purchase, merger, joint venture, or other type of transaction, the main precursor to the parties of a transaction entering into binding agreements pertains to the due diligence disclosures made by the parties. Due diligence allows for the parties to exchange and review the information necessary to provide a level of assurance that the parties' expectations and understandings are supported by tangible information. It also allows for each party to verify to their satisfaction whether the other parties to the transaction have the ability to satisfy any representations and warranties or other underlying terms contained in the transaction's definitive documents. Accordingly, its scope is generally customized to the transaction and the parties' needs.

In non-health care transactions, the scope of due diligence may be straightforward and the disclosure of information and documentation to the other parties sufficiently protected by a confidentiality and nondisclosure agreement. However, in health care transactions, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended, and, in particular, the HIPAA Privacy Rule,[1] imposes impediments to the disclosure of certain patient-related information.

This article describes when HIPAA allows for certain due diligence disclosures and the circumstances when there is not clear guidance on how due diligence may be carried out. Although outside the scope of this article, it also should be noted that there are instances where parties providing due diligence information to competitors as part of a transaction may risk compliance issues under other laws and regulations, such as those governing antitrust.[2]

The Scope of Due Diligence in Health Care Transactions

Due diligence is of utmost importance to health care transactions due to the significant regulatory risks that a party may incur as a result of the previous actions of the other party to the transaction. The areas of information privacy and security, fraud and abuse, billing compliance, antitrust, and licensing and certification are some of the areas of concern to any parties to the transaction. Therefore, due diligence sought in a health care transaction commonly encompasses not only the business information requested in non-health care transactions but also the more expansive information that may address these additional areas of concern.

However, this expansive approach to due diligence may trigger HIPAA compliance concerns.[3] The parties may need to exchange financial information (e.g., including accounts receivable and claims for services rendered), as well as information regarding operational and patient matters such as complaints, adverse events, possible claims or litigation, and compliance matters.

In all of these instances, it may be necessary to disclose patient information that falls within the definition of "Individually Identifiable Health Information" (IIHI)[4] or "Protected Health Information" (PHI).[5] As a general matter, the HIPAA Privacy Rule requires that in the absence of patient authorization for such disclosure, the disclosing "Covered Entity"[6] must establish sufficient safeguards to protect PHI and establishes limits as to what PHI may be disclosed and when.[7]

Due Diligence and Permissible Disclosure Under "Health Care Operations"

In addition to establishing restrictions on the transfer of PHI, the HIPAA Privacy Rule also recognizes the need in certain instances for the Covered Entity to be able to transfer PHI to other parties in the normal course of business. A Covered Entity may disclose PHI without patient authorization in certain instances where it is needed for treatment, payment, or health care operations.[8] Even then, however, the Covered Entity must take sufficient steps to restrict the PHI to be disclosed to what is "minimally necessary" to satisfy the request.[9] Yet, the definition of "Health Care Operations" specifically allows disclosure for:

> "Business management and general administrative activities of the entity, including, but not limited to, … (iv) The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity."[10]

Do You Need an Article?

Would an article on a corporate law issue be interesting to you, but you don't have time to write it? Well, we hear from people who want to write articles, but need topics. Contact Vice Chair of Publications Susan Zinder at szinder@zinderlaw.com or (646) 380-6715 with your ideas, and we'll see if we can get something published on it.

In the preamble to the modifications to the HIPAA Privacy Rule adopted in August 2002,[11] the U.S. Department of Health and Human Services (HHS) expressly stated that the aforementioned definition of Health Care Operations includes not only PHI shared during due diligence but also the physical transferring of such information upon the conclusion of the transaction.

Significantly, HHS also imposed a limitation on transaction-related disclosures. In particular, HHS stated:

> "Under the final definition of "health care operation", a covered entity may use or disclose protected health information in connection with a sale or transfer of assets to, or a consolidation or merger with, ***an entity that is or will be a covered entity upon completion of the transaction***; and to conduct due diligence in connection with such transaction. The modification makes clear it is also a health care operation to transfer records containing protected health information as part of the transaction."[12] (*emphasis added*).

As noted in the emphasized text, HHS limits the definition to the sharing or transferring of PHI to an entity that is or will be a Covered Entity upon completion of the transaction. The example that HHS utilizes to demonstrate the scope of this authority involves a pharmacy that is a Covered Entity buying another pharmacy, which also is a Covered Entity. Under that scenario, PHI may be exchanged between the entities in due diligence and transfer of such records may be made to the new owner upon the completion of the transaction.[13] This authority also allows a Covered Entity to disclose PHI to a party that is not a Covered Entity if it will become a Covered Entity upon consummation of the transaction.[14] The new owner may then use that PHI because it continues to be protected under the HIPAA Privacy Rule as it was prior to the transfer.[15]

The preamble issued by HHS is helpful in some respects, however, this example is very simplistic and leaves many aspects of the due diligence process in a typical health care transaction open for debate. At present, there is little guidance on whether such disclosure fits within the definition of Health Care Operations if in fact the transaction is not consummated or the receiving party is not a Covered Entity and will not be one at the conclusion of the transaction.

Areas of Uncertainty Involving Disclosure of PHI in Due Diligence

In its pharmacy transaction example, HHS addresses only the disclosure of PHI between two Covered Entities and a Covered Entity's disclosure of information to an acquiring entity that will become a Covered Entity at the conclusion of the transaction. This approach assumes that the transaction will essentially be seamless and that the protections required by the HIPAA Privacy Rule have been maintained during diligence. However, many questions remain. For example, would a disclosure comply with the HIPAA Privacy Rule if:

- The PHI is disclosed to a non-Covered Entity that is a party to the transaction but the transaction is not consummated.
- A Covered Entity provides information to multiple non-Covered Entity suitors as part of a Request for Proposal or other type of bidding process with only one or no successful bidders.
- The PHI is provided directly or indirectly to financial, professional, or other advisors associated with the acquiring party.
- The PHI is provided to a non-Covered Entity party that upon closing will become an owner in the acquiring Covered Entity but remain a non-Covered Entity.

In these four examples, there is no clear answer on what steps should be taken to satisfy the HIPAA Privacy Rule.

As to the first example, it is arguable that the definition of "Health Care Operations" provides legal authority to disclose PHI, even if the transaction is not consummated. However, HHS' statement as to due diligence and the pharmacy transaction example in the August 2002 preamble do not provide clear guidance as to the authority derived from Health Care Operations.

The other three examples are more problematic. If a Covered Entity tenders PHI to multiple bidding entities, only one of which will ultimately be party to the transaction, the guidance does not address how the PHI may be protected. In this instance the disclosing Covered Entity should take proactive steps to attempt to satisfy the HIPAA Privacy Rule. For example, the information should be redacted so there is no individually identifiable health information provided to the recipients. If it is necessary to provide PHI in a non-redacted format, the disclosing Covered Entity should enter into a separate agreement meeting those elements of a Business Associate Agreement but specifically tailored to fit the disclosure.

Can We Publish Your Article?

What have you worked on recently? Is it interesting? Why not tell us about it? The BLG PG needs volunteers to draft newsletter articles, Executive Summaries, and Member Briefings for PG members. We are currently especially interested in governance-related topics. Contact Vice Chair of Publications Susan Zinder at szinder@zinderlaw.com or (646) 380-6715 for more information about how we can convert your recent work into an informative publication for your colleagues.

If the PHI is going to be disclosed to the acquiring party's financial, professional, or other advisors, the disclosing Covered Entity should never disclose directly to these third parties. Rather, the PHI should be disclosed to the acquiring party who then may share the PHI with its advisors, subject to the ultimate recipient executing a Business Associate Agreement with the receiving party. If the PHI is disclosed to a non-Covered Entity party who ultimately upon closing is an owner in the acquiring Covered Entity, it does not give that owner any right to PHI after the transaction is consummated. Rather, the owner's right to access and use terminates upon closing. Any post-closing rights to PHI would require that such access or disclosure fall within the scope of payment, treatment, and operations; be permitted by an authorization; or fall within some other permitted use.

Considerations Prior to Disclosing PHI in Due Diligence

Whether it is permissible under the definition of "Health Care Operations" or falls within the areas of uncertainty, there are issues that should be addressed prior to disclosing PHI in connection with a transaction.

- It is advisable that the disclosing Covered Entity's Notice of Privacy Practices (NPP)[16] contain a provision whereby the patient allows for the sharing of PHI in the event of a sale, merger, or other similar transaction involving the Covered Entity. Therefore, by signing the NPP, the patient will have acknowledged the ability of the Covered Entity to disclose the information in due diligence.
- Prior to moving into the disclosing phase of due diligence, the parties should negotiate what information will be needed, in what format it is needed, what components of the information may be redacted, and which parties and advisors will have access to the information. The parties should then reduce this understanding into a Letter Agreement, Confidentiality Agreement, or Non-Disclosure Agreement that incorporates the parties' respective rights and obligations under the HIPAA Privacy Rule.
- The disclosing party should provide only the minimum PHI necessary to satisfy the due diligence request. It is not uncommon for a due diligence checklist to be overly broad and request information in terms of general categories. The disclosing party should seek clarification on exactly what the receiving party needs to satisfy its due diligence requirements. PHI and IIHI that is not absolutely required, as part of the requesting party's due diligence activities, should be redacted.
- The parties should include within the Non-Disclosure or other Confidentiality Agreement how the information will be handled in the event the transaction is not consummated so as to ensure prompt return and/or destruction of the information, and the maintenance (without use) of any information that cannot be returned or destroyed.
- The disclosing party should require that its Business Associate Agreement be used by the receiving party or that it has the opportunity to review and accept the receiving party's Business Associate Agreement should it disclose the information to an outside party. However, Business Associate Agreements are general in their terms, so it is imperative that the agreement entered into by the parties specifically reference the contemplated transaction. The parties should negotiate what additional terms should be included in the Business Associate Agreement and set forth in its recitals a description of the circumstances for the disclosure. As there is uncertainty regarding disclosure, indemnification language in favor of the disclosing Covered Entity should be included in the negotiated Business Associate Agreement. This proactive step will ensure that the PHI is protected to the satisfaction of the disclosing party, and the disclosing party is adequately protected in event of a breach.
- Ascertain if there are any state confidentiality or privacy laws that may restrict or otherwise limit disclosure.

By taking these steps prior to assembling and disclosing any type of due diligence, it will ensure that the disclosure of PHI has been contemplated and planned for in advance by the disclosing party.

---

1 *See* Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Part 160 and Part 164, Subparts A and E.

2 *For examples of other concerns, see* Krul, S., & Joseph, A. "Navigating due diligence: Sensitive information and pitfalls." *Compliance Today*, 69-75 (April 2015).

3 The American Health Lawyers Association Business Law and Governance Practice Group has created due diligence checklists based upon the type of transaction in its Due Diligence Checklist Toolkit. This information may be found at www.healthlawyers.org/Members/PracticeGroups/blg/Toolkits/Pages/DueDiligenceToolkit.aspx.

4 "Individually Identifiable Health Information" is information that is a subset of health information, including demographic information collected from an individual, and:

Dealmakers Needed

The Transactions AG is seeking dealmakers to share their experiences with their colleagues. We need volunteers to share their knowledge by writing email alerts, Executive Summaries, and Member Briefings on hot, newsworthy business transactions or transaction-related topics throughout the year. We also need people who are interested in leading educational sessions. Interested? Please contact Transactions AG Co-Chairs Judy Mayer at mayej@ihn.org or (856) 853-2115 or Joel Rush at jrush@mwe.com or (202) 756-8659, and we'll work together to share your wisdom with your colleagues.

(1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
(i) That identifies the individual; or
(ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

5 Pursuant to 45 C.F.R. § 160.103, Protected Health Information is defined as individually identifiable health information that is: (a) transmitted by electronic media; (b) maintained in electronic media; or (c) transmitted or maintained in any other form or medium but does not include individually identifiable health information: (w) in education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. § 1232g; (x) in records described at 20 U.S.C. § 1232g(a)(4)(B)(iv); (y) in employment records held by a covered entity in its role as employer; and (z) regarding a person who has been deceased for more than 50 years.

6 Pursuant to 45 C.F.R. § 160.103, "*covered entity*" means a health plan, a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

7 *See* Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Part 160 and Part 164, Subparts A and E.

8 45 C.F.R. § 164.502(a).

9 *Id.* at § 164.502(b).

10 *Id.* at § 164.501.

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

12 *Id.* at 53190.

13 *Id.* at 53190 – 53191.

14 *Id.*

15 *Id.* at 53191.

16 45 C.F.R. § 160.520.

Business Law and Governance Practice Group Leadership

Jay A. Martus, Chair
Advantia Health
Washington, DC
(954) 881-9623
jay.martus@advantiahealth.com

Jeffrey L. Kapp, Vice Chair – Research and Website
Jones Day
Cleveland, OH
(216) 586-7230
jlkapp@jonesday.com

Carolyn V. Metnick, Vice Chair – Educational Programs
Akerman LLP
Chicago, IL
(312) 634-5719
carolyn.metnick@akerman.com

Glenn P. Prives, Vice Chair – Membership
McElroy Deutsch Mulvaney & Carpenter LLP
Morristown, NJ
(973) 425-4179
gprives@mdmc-law.com

Lisa D. Taylor, Vice Chair – Strategic Planning and Special Projects
Inglesino Webster Wyciskala & Taylor LLC
Parsippany, NJ
(973) 947-7135
ltaylor@iwt-law.com

Susan F. Zinder, Vice Chair – Publications
The Law Office of Susan F. Zinder PLLC
New York, NY
(646) 380-6715
szinder@zinderlaw.com

Reema Sultan, Social Media Coordinator
Rivkin Radler LLP
Uniondale, NY
(516) 357-3295
reema.sultan@rivkin.com

Judy W. Mayer, Co-Chair–
Transactions Affinity Group
Inspira Health Network
Woodbury, NJ
(856) 853-2115
mayerj@ihn.org

Joel C. Rush, Co-Chair–
Transactions Affinity Group
McDermott Will & Emery LLP
Washington, DC
(202) 756-8659
jrush@mwe.com