The HIPAA Privacy Rule has had a notable impact on the manner in which health care transactions that involve the “covered entities” regulated by HIPAA are conducted. The Privacy Rule’s restrictions on the flow of protected health information (PHI) create a host of unique considerations and concerns for parties to any sale, merger, acquisition or other corporate transaction involving one or more covered entities.

Use and Disclosure of PHI in Health Care Transactions

Preserving the Ability to Transfer PHI
As a threshold matter, a covered entity should ensure that it preserves the right to sell PHI, if it ever intends to do so, whether in the context of a sale of all or part of its business. For many covered entities, PHI contained in such varied forms as patient lists, databases of clinical trial information and accounts receivable information, may constitute the covered entity’s most valuable assets. However, covered entities do not always take steps necessary to preserve the right to transfer such PHI, and may even take deliberate steps that can jeopardize this right.

The Privacy Rule requires a covered entity to have a “notice of privacy practices.” Such notice includes a description of the types of uses and disclosures of PHI the covered entity may make (consistent with the Privacy Rule’s requirements) and establishes the standard by which the covered entity’s activities will be measured. This description in the covered entity’s notice of privacy practices should include a statement that PHI may be used or disclosed in connection with the sale of all or part of its business. Moreover, the covered entity should ensure that any other privacy policy the covered entity may establish, such as on such entity’s website, similarly preserves this right.

So as to mitigate the public’s concerns regarding the use of PHI in marketing activities, many companies have made the mistake of asserting that they will never sell a patient’s information without that patient’s prior authorization, unwittingly preventing those companies from transferring such information upon the sale of all or part of their business in a manner that might otherwise be permitted under the Privacy Rule.

Restrictions on Transfer of PHI
As a general matter, unless one of the specific exceptions set forth in the Privacy Rule is satisfied, prior patient authorization is required to use and disclose PHI. The administrative burden of acquiring individual authorizations from each individual whose medical records are maintained by a covered entity and segregating the records of those individuals who refused to
provide an authorization would, in most cases, be impractical. Accordingly, the covered entity’s ability to meet an exception to the general rule is critical to the exchange of PHI in the context of a health care transaction.

Under one exception to the Privacy Rule, a covered entity may use and disclose PHI without patient authorization for purposes of treatment, payment, or health care operations.¹ The health care operations exception is critical to a covered entity’s ability to disclose PHI in health care transactions. A covered entity’s health care operations include, among other things:

- the sale, transfer, merger or consolidation of all or part of the covered entity to or with another covered entity, or an entity that following such activity will become a covered entity; and
- due diligence related to such activity.²

When discussing the scope of permissible health care operations, the Department of Health and Human Services (HHS) has explained that this definition includes both the use and disclosure of PHI to conduct due diligence and the actual physical transfer of patient records upon the consummation of the transaction.³ The following example provided by HHS provides further clarity to the intent of the agency in adopting this provision of the Privacy Rule:

> if a pharmacy which is a covered entity buys another pharmacy which is also a covered entity, [PHI] can be exchanged between the two entities for purposes of conducting due diligence, and the selling entity may transfer any records containing [PHI] to the new owner upon completion of the transaction. The new owner may then immediately use and disclose those records to provide health care services to the individuals, as well as for payment and health care operations purposes. Since the information would continue to be subject to the Privacy Rule, any other use or disclosure of the information would require an authorization unless otherwise permitted without authorization by the Rule, and the new owner would be obligated to observe the individual’s rights of access, amendment, and accounting.⁴

Thus, the agency’s position attempts to strike a necessary balance between the realities of corporate transactions and maintaining the privacy of patients’ medical records.

However, many health care transactions are not as simple as the HHS example and not easily addressed given the dearth of guidance regarding the application of this exception to various health care transactions. In particular, disclosures of PHI to individuals or entities that are not and would not, as a result of the transaction, become covered entities are not included in the definition of health care operations. For example, it is not clear that this exception would apply where a covered entity would seek to disclose PHI to multiple bidders who are not covered entities (e.g., private equity or venture capital firms) in the context of a competitive bid to acquire the covered entity, where only one of the bidders will consummate a transaction and become a covered entity. Moreover, it is not clear that this exception would allow PHI to be shared with affiliates of the acquiring party or with entities serving the acquiring party (e.g., law firms, accountants advisors, and sources of financing) in the transaction before the acquiring party becomes a covered entity.

Disclosures of PHI by the covered entity to its advisors in the context of a deal are permitted, provided the covered entity enters a business associate agreement meeting the Privacy Rule’s requirements with each advisor. Such agreement requires these entities that are not otherwise subject to the Privacy Rule to contractually agree to comply with many of its provisions.
In addition, even where disclosure of PHI is permitted by the Privacy Rule, there are other constraints that complicate health care transactions. Notably, like most other uses and disclosures of PHI, uses and disclosures for health care operations are subject to the so-called “minimum necessary” rule. This rule requires a covered entity to reasonably limit the PHI that it uses and discloses and that it requests from another covered entity to the minimum amount of information necessary to accomplish the intended purpose of the use, disclosure or request. Accordingly, even where disclosure is permitted, such as in the due diligence process, the covered entity disclosing PHI must assess what constitutes the minimum amount of PHI necessary to permit the recipient to conduct due diligence.

Other Restrictions
Notwithstanding the latitude afforded to covered entities under the Privacy Rule for health care operations, uses and disclosures under this provision are not without risk. For example, HHS has emphasized that even if a covered entity complies with the health care operations rule, it must still be mindful of other “legal or ethical obligations” that may arise out of the nature of its business or relationship with customers or patients. This is significant because the Privacy Rule merely establishes a uniform federal floor for protecting the privacy of PHI, but does not preempt state laws that are more protective of the privacy of individuals’ medical records. As a result, before engaging in uses or disclosures of PHI otherwise permitted under the Privacy Rule as health care operations, covered entities must identify state laws which limit the manner in which such uses and disclosures may be made. Examples of such state laws include those requiring notice of an impending transfer of PHI to affected individuals and an opportunity to object, or which prohibit transfers altogether in the absence of a signed authorization or other mandatory form of consent.

In addition, the Privacy Rule permits an individual to request that a covered entity restrict routine uses or disclosures that the covered entity may make about the individual, including those made under the guise of health care operations. Although the rule does not require a covered entity to agree to these requests, if the entity does, it could be exposed to liability for violation of the agreed-upon restrictions.

Conducting Privacy Rule Due Diligence
In addition to imposing restrictions on the disclosure of PHI in health care transactions, the Privacy Rule creates a need for due diligence of the target covered entity’s compliance with the Privacy Rule’s various organizational and administrative requirements. Each covered entity and each transaction will present unique issues that must be addressed in due diligence. However, at a minimum, the due diligence review should verify that the covered entity has taken the following measures:

- preserved the ability to transfer PHI in connection with the proposed transaction;
- designated a privacy officer who is responsible for developing and implementing its privacy policies and procedures, overseeing workforce training, and addressing complaints involving the covered entity’s use and disclosure of PHI;
- developed and implemented written privacy policies and procedures consistent with the Privacy Rule which demonstrate that the covered entity has in place appropriate administrative, technical and physical safeguards to prevent the use or disclosure of PHI in violation of the Privacy Rule;
- trained and periodically retrained members of its workforce on its privacy policies and procedures as necessary for them to perform their employment functions;
- implemented procedures addressing the provision of access, amendments
to, or an accounting of disclosures of PHI that it maintains;

• entered into business associate agreements, as necessary, with third parties performing services on its behalf;

• prepared and disseminated a HIPAA-compliant notice of privacy practices;

• has and uses when required, a HIPAA-compliant form of authorization;

• implemented a system to document uses and disclosures of PHI, the disposition of complaints involving the use or disclosure of PHI, and to maintain its privacy policies and procedures, notice of privacy practices and other related items as required by the Privacy Rule;

• if the covered entity maintains PHI in electronic format, established (or will have in place no later than April 21, 2005) safeguards, as required by the HIPAA Security Rule, to protect against reasonably anticipated threats or hazards to the security and integrity of electronic PHI, including having in place an information systems infrastructure capable of ensuring that these safeguard are consistently employed; and

• if the covered entity engages in standard transactions addressed in the HIPAA Transactions Rule, implemented appropriate policies for the proper processing of these transactions, including ensuring compliance by third parties engaged to process these transactions on the covered entity’s behalf.

In any transaction, if the target covered entity has not undertaken these basic obligations, it will become necessary to include the cost of post-closing compliance efforts in assessing the economic benefits of the transaction. Beyond diligence of the covered entity’s basic compliance efforts, the due diligence effort should include a review of the covered entity’s complaint history and any litigation relating to privacy issues, as well as any contractual arrangement under which the covered entity has agreed to indemnify third parties for its failure to comply with HIPAA. An acquirer must carefully assess the potential liability that it will incur as a result of the covered entity’s compliance deficiencies and the costs likely to be incurred to ensure compliance after the transaction is consummated, and determine how such liability should be reflected in the terms of the deal documents.

The Ongoing Impact of the Privacy Rule

The Privacy Rule’s impact on transactions involving covered entities does not end with a signature on the dotted line. These transactions will frequently be subject to post-closing indemnification and other related obligations that may require the use or disclosure of PHI between an individual or entity and its successor in interest. In many cases, a business associate agreement will be necessary in order to ensure that these obligations do not run afoul of the requirements of the Privacy Rule. In addition, the Privacy Rule may require business associate agreements with lenders who hold a security interest in accounts receivable or who maintain rights of audit and inspection under credit and related agreements if these rights will expose the lenders to PHI. The obligations of being a business associate could present risk management, operational and financial concerns for a lender who is not familiar with the Privacy Rule or accustomed to the requirements imposed upon business associates.

Conclusion

The inception of the Privacy Rule resulted in a fundamental shift in the way that covered entities use and disclose PHI. As a result, covered entities now must expend considerable time and resources to ensure that their activities do not expose them to potential civil and criminal liability. These concerns are not without significance for individuals and entities involved in corporate transactions.
involving covered entities. Under the paradigm created by the Privacy Rule, parties to a transaction must be mindful of the rule’s provisions and also of the consequences, economic and otherwise, of both compliance and non-compliance. From understanding the conditions under which PHI may be transferred and used for due diligence purposes, to the evaluation of an entity’s compliance activities and potential liability exposure, to post-closing operational issues, the Privacy Rule has injected an entirely new set of issues that must be addressed by all parties, whether or not they are covered entities, in connection with transactions involving entities in the health care industry.

Andrew Gantt is a partner in Latham & Watkins’ Washington, D.C., office, where he is a member of the firm’s Health Care Practice Group. Mr. Gantt represents a wide variety of health care providers, manufacturers, suppliers and health care e-commerce companies in corporate and regulatory matters, including compliance with the Health Insurance Portability and Accountability Act of 1996. In addition, Mr. Gantt advises venture capital groups, private equity funds and underwriters on a variety of health care regulatory issues in connection with health care transactions.

Anthony Casarona is an associate in Latham & Watkins’ Washington, D.C., office, where he is a member of the firm’s Health Care Practice Group. Mr. Casarona provides corporate, transactional, and regulatory advice to a wide range of individuals and entities involved in the health care industry. In addition, Mr. Casarona represents health care service providers in matters related to their compliance with the Health Insurance Portability and Accountability Act of 1996.

1 45 C.F.R. § 164.502(a).
2 Id. at § 164.501.
4 Id. at 53190-91.
5 45 C.F.R. § 164.502(b).
7 45 C.F.R. § 164.522(a).
8 45 C.F.R. Part 160 and Part 164, Subpart C.
9 45 C.F.R. Part 162.