Acquiring Pharmaceutical or Medical Device Manufacturers

MICHAEL M. MANNIX AND VALARIE NEY, HOLLAND & KNIGHT LLP AND MICHAEL M. GABA, POLSINELLI PC
WITH PRACTICAL LAW CORPORATE & SECURITIES

This Practice Note explores selected legal and compliance issues for acquirors to focus on when pursuing an M&A transaction involving a target that is a manufacturer of pharmaceuticals or medical devices. In particular, this Note reviews the preliminary goals of effective due diligence, provides guidance on key areas of the investigation, and highlights some of the strategies acquirors can use to mitigate risk in these deals.

The business of health care is evolving, driven in part by increasingly sophisticated information technology, a shift in the method of delivery of health-related services, and the aging of the baby boom population. In addition, the healthcare industry is bracing for changes that may result if the Patient Protection and Affordable Care Act (ACA) is repealed and new health care reform legislation is enacted. For more information on the ACA, see Practice Note, Affordable Care Act (ACA) Overview (7-502-3192) and Affordable Care Act (ACA) Toolkit (9-518-2991).

M&A transactions in the pharmaceutical and medical device industries, in particular, are largely driven by the ever-increasing costs of development, with pharmaceutical and device companies seeking deals to bolster innovation, capitalize on synergies, and realign their product portfolios. As a result of this as well as broader market forces, M&A activity in the healthcare industry has been strong in recent years and the expectation is that M&A activity will stay at the same high level or increase.

However, M&A in the healthcare industry is not without its challenges. The industry operates in a complex scheme of federal and state regulations. Failure to comply with these regulations can result in the loss of authority to deliver products and services. The stakes are especially high, as many industry participants have violated applicable laws or neglected their disclosure obligations.

When considering an M&A transaction, industry-specific compliance issues should be at the forefront of the acquiror's due diligence investigation.

Performing high-quality due diligence is the best way for an acquiror to protect itself against the risks of an M&A transaction. If an acquiror discovers compliance failures and other material risks during the due diligence process, the acquiror must find a method to mitigate the risks or the deal is in peril. Once those risks have been identified, it is crucial for the acquiror to effectively negotiate transaction terms through which the risks between the acquiror and the seller or target are properly allocated.

This Note explores selected legal and compliance issues for acquirors to focus on when pursuing an M&A transaction involving a target that is a manufacturer of pharmaceuticals or medical devices. In particular, this Note both:

- Reviews the preliminary goals of effective due diligence and provides guidance on the most important areas of investigation when acquiring a pharmaceutical or medical device manufacturer.
- Highlights some of the strategies acquirors can use to mitigate risks discovered through the due diligence process.

This Note assumes that there are no distinctions in due diligence and risk mitigation between deals with simultaneous and non-simultaneous signings and closings.

DUE DILIGENCE OF PHARMACEUTICAL AND MEDICAL DEVICE MANUFACTURERS

The preliminary goals of due diligence are to:

- Determine the existence of any "deal stoppers" in the transaction (for example, an ongoing governmental investigation).
- Identify and weigh any facts that require the revision of the original strategic rationale for the transaction.

For more information on due diligence in M&A transactions, see Practice Notes, Due Diligence for Public Mergers and Acquisitions (9-382-1874) and Due Diligence for Private Mergers and Acquisitions (8-381-0512).

Due to the high degree of regulation in the healthcare industry, it is particularly important for the acquiror to confirm that the target has

operated in substantial conformity with the statutes and regulations applicable to the target's business. The starting point for this analysis is the review of the target's business operations and compliance mechanisms. In particular, during the due diligence process acquirors should evaluate:

- The adequacy of the target's compliance programs and systems (see Compliance Programs).
- Risks stemming from the target's business conduct that may be fraudulent or abusive (see Fraud and Abuse).
- Financial risks related to products liability claims, and product labeling and advertising potentially resulting in misbranding and US Food and Drug Administration (FDA) enforcement actions (see Products Liability and FDA Enforcement).
- The target's policies and practices on protecting, exploiting, and prosecuting its intellectual property (see Intellectual Property).
- The impact of burdensome Physician Payment Sunshine Act disclosures (see Physician Payment Sunshine Act Disclosures).
- Whether the target has obtained and maintains all necessary licenses and has followed proper product approval processes (see Required Licenses and Approvals).
- The target's compliance with the requirements of the Health Insurance Portability and Accountability Act (HIPAA) (see HIPAA Requirements).
- The target's vulnerability to and preparedness against cybersecurity attacks (see Cybersecurity).

COMPLIANCE PROGRAMS

Many business practices that are acceptable in other industries are prohibited by regulations specific to the healthcare industry. For example, broadening the marketing and sales of a product beyond its current use may be ordinary course in the telecommunications industry, but marketing a pharmaceutical or medical device outside the specific use for which the item is approved by the FDA violates the Food, Drug, and Cosmetic Act (FDCA) and its implementing regulations (see Box, Examples of Violations of Healthcare Industry Regulations).

Moreover, drug and medical device advertising and labeling regulations expose not only the manufacturer, but its officers and directors, to potential criminal and civil liability under multiple legal theories. Additionally, there are specific requirements for drug advertisements, and FDA regulations spell out a long list of characteristics of advertisements which fail to meet the regulations. If advertising fails to meet the guidelines, it is deemed to be "misbranded."

Interstate commerce in misbranded products is a crime. Labeling is a separate problem for manufacturers. FDA labeling regulations are detailed and cover, for example, the proximity of some information to other information and type size.

Due diligence must focus on the adequacy of the target's compliance programs and systems. These programs and systems are established to monitor the corporate behavior of the target in regulated areas. The success of these measures is critical. In particular, the acquiror's due diligence review should include the assessment of:

- Codes of conduct, policies, and procedures.
- Background and implementing documents.
- Relevant meeting minutes.
- Audit plans.
- Disciplinary measures and corrective action plans.

The acquiror should view the target's failure to meet adequate thresholds in these critical areas as a potential indication that fraudulent or abusive conduct has gone unnoticed and unaddressed.

Standards of Effectiveness

Unlike many other industries, companies in the healthcare industry are required by federal and local governments to implement and maintain a sound compliance program. The Office of Inspector General (OIG) has issued compliance guidelines for many of the types of businesses that are involved in the healthcare industry. The existence of a program meeting minimum compliance standards allows the healthcare company to participate in federal healthcare programs (such as Medicaid and Medicare). Accordingly, the target's compliance program must meet both the acquiror's subjective standards of effectiveness, as well as the more objective standards used by government programs.

During the due diligence process the acquiror should, at the least, examine the:

- Existence and comprehensiveness of the target's policies and practices, including the target's compliance with the requirements imposed by the:
  - Foreign Corrupt Practices Act (FCPA) (15 U.S.C.A. §§ 78dd-1, et seq.);
  - Federal False Claims Act (FCA) (31 U.S.C.A. §§ 3729 to 3733);
  - Civil Monetary Penalty Statute (42 U.S.C.A. § 1320a-7);
  - Robinson-Patman Act (15 U.S.C.A. § 13(c));
  - Patient Protection and Affordable Care Act (Pub. L. No. 11-148, 124 Stat. 119);
  - Food, Drug, and Cosmetic Act (FDCA) (21 U.S.C.A. §§ 301 to 399f);
  - Public Contracts Anti-Kickback Statute (41 U.S.C.A §§ 8701 to 8707);
  - Anti-Kickback Statute (42 U.S.C.A. § 1320a-7b(b));
  - state anti-kickback statutes and false claims acts; and
  - state consumer protection laws and reporting statutes.
- Target's procedures and resources for employees, independent contractors, distributors, suppliers, or customers to disclose any concerns, allegations, or factual evidence of any non-compliance with the applicable regulations and statutes.
- Function, authority, and corporate visibility of the target's division(s) tasked with:
  - conducting internal audits;
  - facilitating external audits; and
  - coordinating the corporate response to any identified deficiencies in compliance programs or allegations of non-compliance.
- Scope and nature of management's control over the target's divisions.
- Nature of the relationships between the target's divisions. Federal regulators and prosecutors have focused investigations on pharmaceutical and medical device manufacturers that appear to have a corporate culture driven by the sales and marketing division.

Culture of Compliance

Compliance-related due diligence examines more than just the programs themselves. The acquiror should evaluate the target's culture of compliance, or the degree to which the target's senior management is involved with the implementation of the compliance program. A corporate culture that values ethics and compliance will help the target avoid incurring violations in the first place.

The acquiror should also assess whether the target's employees understand and respect its compliance program. Compliance with and documentation of the target's internal procedures can be a significant deterrent to fraudulent conduct. Good practices in recordkeeping and documentation can help the target's senior management to oversee and control conduct at the division level.

Corporate Integrity Agreements

The acquiror should also analyze any claims or proceedings brought by government agencies or private individuals against the target company, whether for deficiencies in compliance programs or misconduct that compliance programs are intended to prevent. Many pharmaceutical, medical device, and biotechnology manufacturers have been subject to inquiries by the OIG, the Department of Justice, or other enforcement authorities, and have resolved those inquiries by entering into Corporate Integrity Agreements (CIAs) with the government. CIAs can impose a variety of expensive, time-consuming, and restrictive requirements and obligations on a company, such as:

- Limitations on certain business operations and actions.
- Increased oversight.
- Third-party monitoring and auditing.
- Reporting, certifications, and attestations.

When evaluating a CIA, the acquiror should analyze:

- The nature and term of the CIA requirements and obligations.
- Any requirements imposed by the CIA on the transaction.
- Its impact on future business operations and the residual effects on the resulting entity.

The due diligence team should also review any reports previously provided by outside consultants to the target which evaluate the establishment or operation of the compliance program.

FRAUD AND ABUSE

Due diligence should assess the risk to the target of private or government legal actions stemming from fraudulent or abusive business conduct. The acquiror should also review the nature of the target's relationships with third parties. This area of due diligence is especially important (see Box, Identifying Fraudulent or Abusive Conduct).

Existing or Threatened Legal Proceedings

Pharmaceutical and medical device manufacturers are subject to several broad, overlapping federal and state statutes that prohibit fraudulent or abusive conduct, particularly where the manufacturer sells its products directly or indirectly to the federal health care programs. Even if the manufacturer does not directly serve as a health care provider under the federal health care programs, courts have interpreted the statutes to cover conduct that improperly influences the use of medical services by beneficiaries of the programs.

The acquiror's due diligence team should determine the existence of any investigations, such as:

- Civil investigative subpoenas by federal prosecutors under the FCA.
- Requests by current or former employees under the Freedom of Information Act.
- Threatened enforcement proceedings by federal regulators and prosecutors.

Most frequently, lawsuits and enforcement actions against manufacturers allege violations of the FCA, the FDCA, the Anti-Kickback Statute, and the FCPA.

Some potential claims might not be apparent on the first review. For example, manufacturers may hire physicians to market the off-label uses of a product, which is a violation of FDCA and FDA regulations, or may provide an unrestricted grant to a physician group in exchange for prescribing the product, which violates the Anti-Kickback Statute.

However, this same conduct can also serve as a cause of action under the FCA for private individuals, serving as *qui tam* relators (whistleblowers that file suit under the FCA), or the federal government. Some courts have found that the improper conduct of a manufacturer caused the physicians to submit false claims to the federal government. In other words, the manufacturer caused the physicians to misrepresent in their claim for reimbursement that the physicians were in compliance with federal law.

Therefore, the acquiror should carefully review with its counsel all complaints threatened or filed against the target alleging fraudulent or abusive conduct.

Third-Party Relationships

The scope of risk under the fraud and abuse statutes will be determined not just by a review of current federal investigations and civil actions, but also by careful due diligence of the target's corporate conduct. The acquiror should assess the business practices of the target regarding its contractual relationships with third parties. The due diligence team can begin by reviewing the contracts between the target and third parties that pose potential risks, including contracts with:

- Physicians.
- Clinical researchers.
- Hospitals.
- Managed care organizations.
- Group purchasing organizations.
- Distributors and independent contractors.
- Federal health care programs (in some cases).

However, the contracts may not explain the true extent of the relationship between the target and a particular third party. The acquiror should also interview the target's employees about the nature of the target's relationship with referral sources and match any payments made by the target to the payment requirements set out in the contract.

Under the federal fraud and abuse statutes, the requisite intent to defraud may be found even where a manufacturer has reasons other than obtaining or inducing referrals to pursue a contractual relationship with the health care provider. Therefore, if any purpose of the transaction is to induce Medicare or Medicaid referrals, the position of the OIG and of the federal courts is that the company has violated the federal statutes. Where there is a purpose by the manufacturer to induce referrals, liability will be found regardless of the nature or importance of the manufacturer's other legitimate purposes. (See *United States v. Borrasi,* 639 F.3d 774, 782 (7th Cir. 2011) (citing *United States v. Greber*, 760 F.2d 68, 69 (3d Cir. 1985)).)

However, there are a number of safe harbors under the Anti-Kickback Statute that protect certain arrangements from prosecution even if the arrangement otherwise might technically constitute a statutory violation. The safe harbors identify arrangements that the OIG, under Congressional authorization, has determined will present little or no risk of fraud or abuse. Under these narrowly circumscribed fact patterns, the OIG will not treat certain conduct as violations of the Anti-Kickback Statute. (42 C.F.R. § 1001.952.)

For instance, certain sales commission agreements, although illegal under a literal reading of the Anti-Kickback Statute, are permissible. Where the conduct does not satisfy each element of the safe harbor, the OIG will employ an analysis to determine whether there is an "improper nexus" between the remuneration in question and the referral of federal health care program business.

PRODUCTS LIABILITY AND FDA ENFORCEMENT

Pharmaceutical and medical device manufacturers must also comply with the labeling and manufacturing standards imposed by FDA regulations and state law-based duties. The FDA can suspend distribution of a product as well as recall the product or, in rare cases, seize or ban "restricted devices" that do not comply with FDA regulations. More significantly, as an alternative to basing a claim on a violation of a state law-based duty, private individuals can claim strict liability and negligence against the manufacturer for harm caused by a drug or Section 510(k) medical device where the manufacturer violated the FDA regulations or the FDA's Current Good Manufacturing Practices (CGMPs). (Section 510(k) requires the medical device manufacturer to register with the FDA, see FDCA, 21 U.S.C.A. § 360(k)). For additional information on FDA regulations applicable to medical devices, including CGMPs, see Practice Note, FDA Medical Devices Regulations (7-613-9907).

In estimating the financial and operational risk of the M&A transaction, the acquiror should closely examine the target's compliance with these federal statutory and state law-based obligations. In particular, the acquiror should assess the degree to which the target has:

- Implemented CGMPs.
- Maintained its obligations under the FDA's applicable reporting obligations.
- Promptly disclosed to the public any adverse findings by the FDA in an administrative hearing. This includes any FDA suspensions or recalls of its products and any adverse administrative determinations by the FDA (such as a notice or warning letter).

Due diligence should also identify which of the target's products are Section 510(k) medical devices "moderate risk" medical devices, as distinguished from Class III "significant risk" devices. State law-based tort claims that allege harm caused by Class III devices that have received premarket approval (PMA) are preempted by the FDA's statutes and regulations when the state regulations impose different or additional requirements than the FDCA does on the manufacturer (see *Riegel v. Medtronic, Inc.*, 552 U.S. 312, at 322 (2008)). Products cleared under Section 510(k) and not approved via a PMA receive no such protection. As "significant risk" devices, Class III devices require higher PMA scrutiny because they are intended to support or sustain human life and therefore pose a greater risk if they malfunction or fail.

In evaluating the risk of future liability, the due diligence team should review the:

- Target's FDA inspection history and preparedness for future inspections.
- Frequency of adverse events reportedly caused by the target's drugs and medical devices.
- Level of communication between the operations managers for each division and the target's compliance staff.

The FDA conducts several types of inspections: preapproval inspections after a company submits a marketing application; routine quality system inspections of a regulated facility; and for-cause inspections to investigate a specific problem that has come to the FDA's attention.

The target may be subject to more potential tort or regulatory risk if the target's employees know of adverse events, but acting independently from the target's compliance officer, have determined that those events did not require disclosure under the statute and associated regulations. For-cause inspections by the FDA can be triggered by not reporting or persistent late reporting of adverse events.

Any misrepresentations by the target to the FDA in connection with the drug or medical device approval process may serve as a basis for a relator's claim under the FCA. However, these violations of the FDA labeling requirements could also serve as a basis for individuals claiming tort liability due to harm caused by off-label use of the target's drugs or medical devices. The acquiror should examine the target's disclosures to the FDA during the PMA processes to determine if the target made any misrepresentations about the potential use of its products.

INTELLECTUAL PROPERTY

When conducting due diligence on pharmaceutical and medical device manufacturing companies, which operate in a sector marked by rapid technological change and high margins, the acquiror must review the target's documentation, policies, and practices related to protecting, exploiting and prosecuting its intellectual property. A review of the target's portfolio of trade secrets and issued patents will reveal the rights of the target in its patent assets and the target's competitive advantage within the relevant market. An understanding of the target's patents and related disclosures will also allow the acquiror to value the target's patent portfolio.

As part of a comprehensive plan to protect a company's intellectual property, the target should have in place:

- Assignment agreements with its employees and consultants who are inventors of important company technology and know-how.
- Processes for maintaining the confidentiality of its trade secret information.

Documentation of the target's patent portfolio may reveal weaknesses in its competitive advantage. Therefore, the acquiror should review:

- The validity, exclusivity, and enforceability of the issued patents.
- The policies and practices of the target in disclosing its patent rights, prosecuting its patent portfolio, and licensing its technology.
- The extent of the target's efforts to create contractual safeguards (whether through confidentiality or non-competition agreements) to prevent the disclosure of its trade secrets and to ensure the assignment of patent ownership rights.
- Any exploitation and infringement of the target's patents by third parties or by the target regarding the patents of third parties.

For more information on issues to consider when conducting intellectual property due diligence for an M&A transaction, see Checklist, IP Due Diligence Issues in M&A Transactions Checklist (3-501-1681).

PHYSICIAN PAYMENT SUNSHINE ACT DISCLOSURES

As part of the ACA, Congress included the Physician Payment Sunshine Act which directed the Centers for Medicare and Medicaid Services (CMS) to adopt rules implementing the transparency provisions of the ACA. CMS adopted the final rule in 2013, which requires reports under burdensome disclosure obligations, and applies to pharmaceutical, medical device, biotechnology, and other medical supply companies. In light of the requirements under the rule, acquirors should determine the impact on the target's compliance program and the heightened enforcement risk posed by the target's business relationships.

The statute requires annual reporting of direct and indirect payments or other "transfers of value" to physicians and teaching hospitals by manufacturers of drugs, biologicals, and devices covered under Medicare, Medicaid, or the Children's Health Insurance Program (CMS includes manufacturers that license the applicable products for production, distribution, and sale in this definition). Where a covered entity (manufacturer) transfers to a physician, group of physicians, or teaching hospital anything of value above a nominal threshold, the covered entity must publicly disclose:

- The name and address of the recipient and certain identifiers if the recipient is a physician.
- The amount of payment or other transfer of value.
- The date of payment or transfer of value.
- The form of the payment or transfer of value, for example:
  - cash or cash equivalents;
  - in-kind services or goods;
  - stock, stock option. or any other ownership interests; or
  - dividends, profits, and other returns on investment.
- Nature of payment or transfer of value.
- The name(s) of the related covered drugs, devices, biologicals, or medical supplies.
- The purpose of the transfer, including:
  - research;
  - clinical investigations;
  - grants; or
  - charitable contributions.
- The covered entity's product that is "reasonably associated" with the transfer.

(42 U.S.C.A. § 1320a-7h.)

These disclosure requirements pose significant risks for covered entities. Non-compliance with the disclosure requirements can result in civil monetary penalties of $1 million or more per year. The covered entity must also pay for the cost of a compliance audit conducted by the Department of Health and Human Services (DHS). However, most concerning is the heightened risk of liability under the Anti-Kickback Statute and the FCA, especially in cases where the manufacturer discloses questionable financial relationships with physicians and teaching hospitals.

The acquiror should therefore review:

- The enforcement risks posed by material financial relationships with physicians, particularly those that sponsor pharmaceutical products or medical devices or serve as principal investigators in clinical trials funded by the manufacturer.
- The technical ability of the manufacturer to meet the requirements of the implementing regulation issued by CMS, which requires the aggregation of information that is likely not shared between divisions of the company.

REQUIRED LICENSES AND APPROVALS

Depending on the particular business involved, healthcare companies are regulated by a broad range of both federal and state agencies (for example, Medicaid, state regulatory boards, and state public health agencies). There are also professional and accrediting organizations that have authority over some healthcare companies. Many of these organizations require licenses, permits, registrations, or accreditations for companies (and for individuals) to conduct certain activities. During the due diligence review, the acquiror must identify all of the necessary licenses required of the target. The acquiror must then determine:

- Whether the target maintains the most current versions of the required licenses.
- Whether there have been any lapses in licensure during times in which claims were submitted.
- What actions are necessary to transfer any licenses before or after the M&A transaction.

Medical devices and pharmaceutical products go through a rigorous approval process that requires clinical trials, including human testing and publication of results. Counsel should focus (sometimes with the help of a clinical auditor) on the manufacturer's efforts from the period of drug discovery through FDA approval.

Of special note for due diligence purposes is the Section 510(k) clearance process applicable to medical devices. Under this process, companies can request a shortcut to approval if the product is deemed "substantially equivalent" to another product which already has FDA clearance (a specific type of approval). It is inexpensive and does not require testing which might identify material flaws in the product. The process was created for products that are identical to those previously approved to enhance FDA efficiency in reviews but it is up to the medical device manufacturer to claim substantially equivalent status.

Any shortcuts could result in a large financial burden on the acquiror if there is a recall, removal from the market by the FDA, or some other regulatory action by the FDA that limits the prescription of the products being purchased. Additionally, if any mistakes were made in the medical device approval process and individual patients are harmed as a result, the acquiror could face significant financial liability.

HIPAA REQUIREMENTS

Under the HIPAA Privacy Rule for "covered entities" and "business associates" (such as independent contractors of covered entities), the Department of Health and Human Services Office of Civil Rights (OCR) regulates the corporate procedures for the use and corporate response to the misuse or mishandling of certain Protected Health Information (PHI) (45 C.F.R. §§ 160.101 to 160.552). For additional information regarding the HIPAA Privacy Rule, see Practice Note, HIPAA Privacy Rule (4-501-7220).

OCR has increased its enforcement efforts related to HIPAA in recent years. There have been a number of enforcement actions against healthcare providers, including medical device companies.

The acquiror should therefore identify whether the target has:

- Experienced any security breaches of PHI, including cybersecurity breaches, especially with respect to unencrypted laptops and other portable media, and, if so, has disclosed the form and type of PHI.
- Promptly notified the appropriate government entities, individuals and, in some cases, the media after experiencing a security breach.
- Promptly corrected either the cause of any security breach or any deficiencies identified by the OCR in connection with select post-breach audits.
- Recovered any PHI prior to misuse.
- Developed and maintained appropriate systems for documentation of:
  - the target's compliance with HIPAA and the Health Information Technology for Economic and Clinical Health (HITECH) Act;
  - any security breaches; and
  - corporate responses to breaches.

CYBERSECURITY

Pharmaceutical and medical device manufacturers are an attractive target of cyberattacks. The purpose of the intrusion might be to misappropriate intellectual property or confidential data, including PHI.

A breach into a drug manufacturing system might also lead to a range of operational disruptions including disruption to industrial control systems that manage and automate drug manufacturing processes. Any incident that compromises such systems can result in large losses. Months of data re-validation may be required before resuming operations, which may result in major financial losses as well as damage to the company's reputation.

Medical devices are increasingly connected to the internet, external networks, and other medical devices, which increase the cybersecurity risk. Medical devices can be susceptible to security breaches which may impact the safety and effectiveness of the device.

The FDA has the power to dictate cybersecurity and privacy requirements for regulated medical devices. The FDA has provided some guidance on medical device cybersecurity. The FDA's recommendations for mitigating and managing cybersecurity threats include:

- **Ensuring safeguards are in place.** "Medical device manufacturers should take steps to ensure appropriate safeguards are in place. Manufacturers are responsible for remaining vigilant about identifying risks and hazards associated with their medical devices, including risks related to cybersecurity. These organizations are responsible for putting appropriate mitigations in place to address patient safety risks and ensure proper device performance."
- **Network security evaluations.** "Health care delivery organizations should evaluate their network security and protect their hospital systems."

(see Cybersecurity, U.S. Food & Drug Administration).

The FTC has the power to hold organizations responsible for their cybersecurity and privacy practices under Section 5 of the Federal Trade Commission Act (Section 5) which covers unfair and deceptive practices. The FTC has used this power to initiate a number of civil enforcement actions in recent years. Under Section 5, data security liability is governed by a reasonableness test. The FTC has also provided guidance on cybersecurity measures, including advice for businesses about building security into products connected to the internet by using, among others, proper authentication, reasonable security measures, and carefully considered default settings. This guidance also addresses the steps to take once a breach has occurred. The FTC has considered whether or not the company has followed this guidance as a factor in determining liability in enforcement actions.

The DHS has also recently released a publication entitled: "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients," that provides a voluntary call to action to make cybersecurity a "priority for patient safety." The Health Industry Cybersecurity Practices publication focuses on five primary cybersecurity threats to health industry organizations and identifies some of the best practices to address each threat, including:

- **E-mail Phishing Attacks.** Suggested practices include a focus on staff training, implementing multifactor authentication, and technical screening tools for malicious content/links.
- **Ransomware Attacks**. Suggested practices include regular and secure data backups, segmenting networks to protect critical data and systems, and using anti-malware detection and remediation tools.

- **Loss or Theft of Equipment or Data.** Suggested practices include encryption of sensitive data, and ensuring an organization has an up-to-date asset inventory to be able to benchmark losses in an incident.
- **Insider Threats, Accidental, or Intentional Data Loss.** Suggested practices include audits of those who have access to sensitive data, implementing access control tools, as well as tools to report unauthorized access to critical technology systems, PHI, and personal identifiable information.
- **Attacks Against Connected Medical Devices.** Suggested practices include secure device patching, security risk assessments for devices and vendors, and using device security language in contracts.

Although these suggested practices and guidelines are meant to serve as a resource and are voluntary, they could potentially lead to a new standard of care for healthcare entities and may well have implications for an organization's legal liability for a cybersecurity or data privacy incident.

RISK MITIGATION STRATEGIES

After risks are identified through the due diligence process, the acquiror's counsel must determine an appropriate risk mitigation strategy. In cases of substantial risk, the conclusion may be that the proposed transaction should be abandoned. Most often, the parties will consider changes to the transaction structure or to the terms in the definitive documentation to mitigate the risks.

TRANSACTION STRUCTURE

The transaction might be restructured into an asset purchase in which the acquiror does not purchase the higher risk portion of the target's business or assets. This alternative is only feasible if the parties can achieve their goals on the tax and accounting aspects of the deal and if the target's key contracts and other rights can be effectively transferred at the closing to the acquiror.

For more information on asset purchases, see Practice Note, Asset Acquisitions: Overview (6-380-7695).

RISK ALLOCATION PROVISIONS

The acquiror's counsel may also try to mitigate the risks of expensive or indeterminate post-closing liabilities by using some of the risk protection provisions commonly available in transaction documents related to the purchase of private companies, such as:

- Indemnification provisions.
- Acquiror escrows.
- Holdbacks.
- Representation and warranties insurance.

Indemnification

Special indemnifications provide for more extensive liability for the seller for known risks which are considered by the acquiror to be above the normal business risk in operating the target. For example, terminated employee litigation is frequently considered routine while litigation over the FDA approval process or intellectual property is probably not considered routine and would be the subject of special indemnification provisions.

The indemnification provisions are among the most important covenants in the transaction documents because they are most often the sole remedy for breaches of the purchase agreement. However, there is a delicate balance to be struck when negotiating these provisions. When a party perceives that the other side is attempting to disproportionately shift the risk in the transaction documents, the negotiations may become strained and the deal may fail to close.

For more information on indemnification provisions, see Practice Note, What's Market: Indemnification Provisions in Acquisition Agreements (3-504-8533).

Escrows and Holdbacks

The traditional methods of addressing indemnification risks in M&A transactions are through an indemnification escrow account and a holdback of the purchase price. An indemnification escrow account is a fund created at the closing from which the seller's indemnification obligations are paid. The escrow is typically administered by an independent third party, usually a bank or financial institution. Alternatively, a buyer may hold back a portion of the purchase price to cover the seller's indemnification obligations for a certain period of time post-closing. Holdback funds (unlike funds held in indemnification escrow accounts) are not secured in a special account. As a result, sellers generally prefer the use of an escrow account over a holdback, as it reduces the control the buyer has over the funds and may increase the likelihood that funds remaining after the payment of indemnification claims is promptly released to the seller after the applicable release date.

Representation and Warranty Insurance

A newer method of addressing indemnification risks that is becoming increasingly popular in M&A transactions is a buy-side representations and warranties insurance (RWI) policy. Under a RWI policy, the buyer in an M&A transaction can recover directly from an insurer for losses arising from certain breaches of the seller's representations and warranties in the acquisition agreement. By shifting the risk of these losses from the seller to an insurer, the buyer and seller can limit the seller's liability for breaches of certain representations and provide the seller with a clean exit by reducing the need to establish escrows or holdbacks. A RWI policy also provides the buyer with protection against collectability and solvency risks of an unsecured indemnity from the seller. Use of a RWI policy can also distinguish a buyer's bid in a competitive auction process by allowing shorter survival periods, lower liability caps, and reduced escrow amounts for breaches of representations and warranties in the buyer's draft purchase agreement.

For more information on indemnification provisions, including holdbacks and escrows see Practice Note, Indemnification Clauses in Private M&A Agreements (4-568-4787). For more information on RWI, see Practice Notes, Representation and Warranty Insurance for

M&A Transactions (w-000-4767) and Incorporating Representation and Warranty Insurance into M&A Transactions (w-003-3851).

The authors gratefully acknowledge the assistance of Ariel Stevenson of Holland & Knight LLP in the preparation of this Note.

EXAMPLES OF VIOLATIONS OF HEALTHCARE INDUSTRY REGULATIONS

Some years ago, makers of biliary stents began marketing them for uses for which they are not approved. A *qui tam* suit was filed accusing three companies of encouraging physicians to use the biliary stents to treat blocked blood vessels. The stents are designed to treat bile duct cancers and the FDA has not approved them for other uses. The whistleblower lawsuit allowed the plaintiff to file suit on behalf of the government and to collect one-third of any monetary judgment resulting from the case.

Violations of applicable laws and regulations can result in significant whistleblower and other civil suits and criminal sanctions. For example, in July 2012, a prominent pharmaceutical company pled guilty and agreed to pay $3 billion to resolve its criminal and civil liability arising from the company's unlawful promotion of certain prescription drugs, its failure to report certain safety data, and its civil liability for alleged false price reporting practices. The fine is the second largest payment by a pharmaceutical company in history. It is comprised of a criminal fine and forfeiture totaling $1 billion and civil settlements totaling $2 billion with the federal government under the False Claims Act, as well as the states. The company is also subject to court-supervised probation and reporting obligations for its chief executive officer and board of directors. (DOJ 12-842 (D.O.J.).)

IDENTIFYING FRAUDULENT OR ABUSIVE CONDUCT

The acquisition of a well-known pharmaceutical company provides a cautionary tale for potential acquirors. After closing the transaction, the acquiror voluntarily disclosed to federal officials potential violations of federal statutes by the target company it had acquired. The target allegedly violated the Anti-Kickback Statute by offering to make improper payments on a distribution contract to a subsidiary of a pharmacy benefits manager. The payment was made with the expectation of obtaining improved positioning for the products and improved ancillary benefits from that pharmacy benefits manager for the target's drug products.

A pharmacy benefits manager often acts as a middleman between pharmaceutical companies and health insurers and recommends pharmaceutical products to health plans. In this case, the target offered to make payments under a drug distribution contract with the expectation that the pharmacy benefits manager would recommend the target's drug products to certain of its health plan clients.

The acquiror's due diligence should include a review of material contracts of the target. The acquiror's team might have reviewed the target's contract with the pharmacy benefits manager if it were a material contract. If so, the due diligence team might have uncovered the improper payment as outside the ordinary terms of the contract prior to closing. However, generally, acquirors cannot review all material contracts and to some degree can rely upon the presence of a robust compliance program. An effective compliance program at work in the target would raise the acquiror's comfort level on matters relating to the compliance and monitoring of fraud and abuse and other prohibited business conduct.

03-19