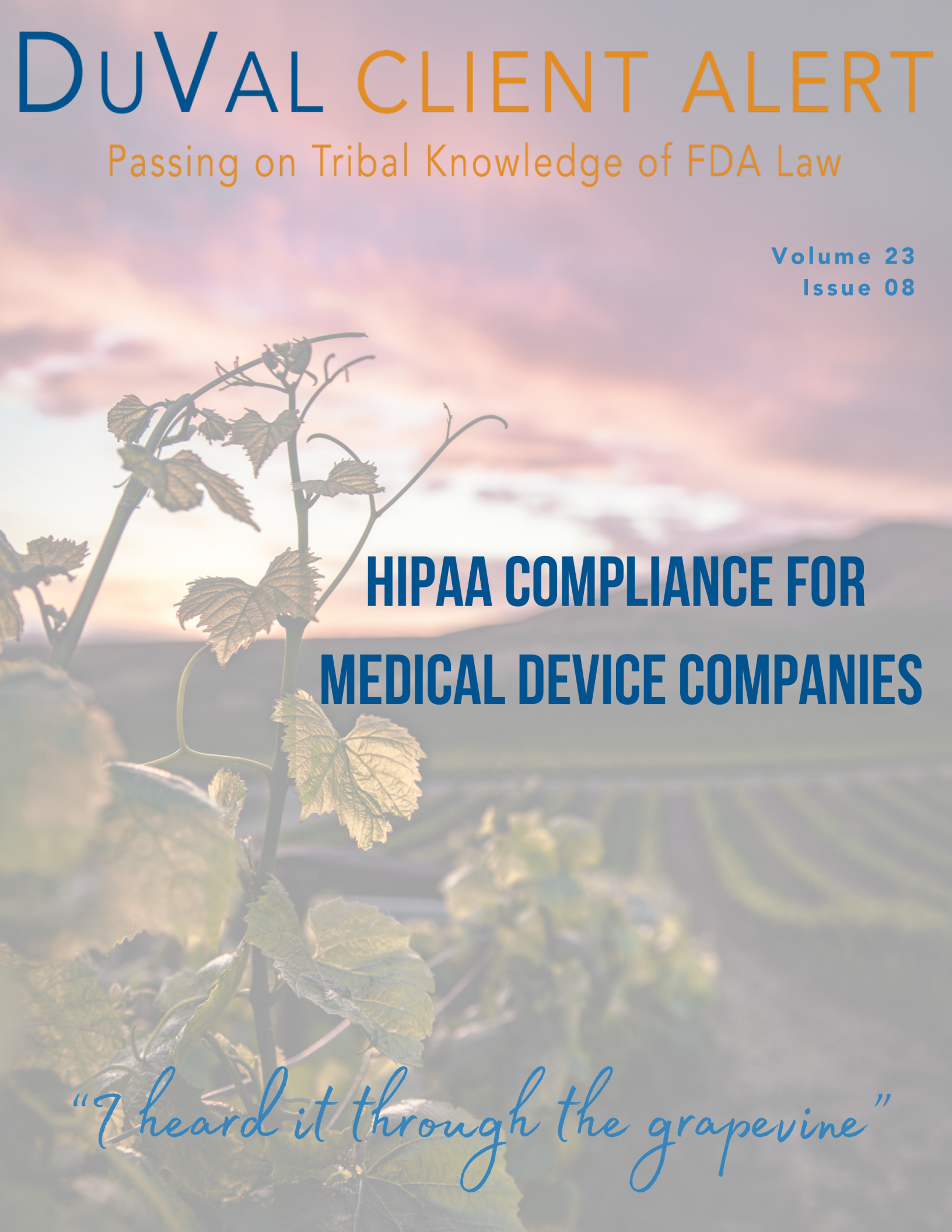
DuVal Client Alert

Passing on Tribal Knowledge of FDA Law

Volume 23
Issue 08



HIPAA Compliance for Medical Device Companies

"I heard it through the grapevine"

Table of Contents

Bryan Feldhaus

Vice President of Legal-Regulatory and Compliance

HIPAA Compliance for Medical Device Companies: "I Heard it Through the Grapevine"

"It took me by surprise I must say,
when I found out yesterday,
don't you know that
I heard it through the grapevine."

In 1968, Marvin Gaye released the acclaimed soul classic, "***I Heard It Through the Grapevine***," in which he sings about his surprise when learning about a lover's infidelity "through the grapevine."

The phrase "through the grapevine" dates to the Civil War era and refers to rumor-prone communications overhead through rudimentary telegraph lines, which is more recently and colloquially referred to as the "rumor mill".

While Gaye's lyrics in "***I Heard It Through the Grapevine***," regarding the rumor mill were (likely) unrelated to compliance requirements for medical device companies, the lyrics are a useful surrogate for training clients regarding obligations imposed under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and, specifically, the HIPAA Privacy Rule and the HIPAA Security Rule. After all, many HIPAA concerns for medical device companies arise from "grapevine" disclosures (i.e., the rumor mill), such as sharing favorable patient results for an investigational device via social media.

This DuVal Client Alert will provide an overview of the HIPAA Privacy Rule and its applicability to medical device companies, distinguish device manufacturers from "Business Associates," itemize exceptions to the HIPAA Privacy Rule for device manufacturers including the Public Health Exception under 45 C.F.R. § 164.512(b)(1)(iii), and the "Treatment, Payment, and Health Care Operations" exception under 45 C.F.R. § 164.506(c), and identify HIPAA best practices that medical device companies should implement to prevent "grapevine" disclosures, improve privacy in an increasingly digital industry, and avoid being taken by a HIPAA "surprise".

HIPAA BACKGROUND

Prior to HIPAA, no generally accepted set of security standards or general requirements for protecting health information existed within the healthcare industry. At the same time, new technologies were evolving, and the healthcare industry began to use electronic information systems to complete several administrative and clinical functions, such as sharing patient information for clinical treatment and paying healthcare claims.

As a result, HIPAA was signed into law in 1996 and required the Secretary of the U.S. Department of Health and Human Services (HHS) to develop regulations protecting the privacy and security of certain health information. To do so, HHS published national standards to protect patient information. Originally, HHS published the Privacy Rule and the Security Rule, which are more fully described below. Since that original enactment, the requirements under HIPAA have evolved significantly to address changes in technology and usage.

HIPAA was enacted to improve the portability and accountability of health insurance coverage and to combat waste, fraud, and abuse in health insurance and healthcare delivery. The procedures for simplifying the administration of health insurance became a vehicle for encouraging the healthcare industry to move to electronic health records. HIPAA and the subsequent Health Information Technology for Economic and Clinical Health Act of 2009 are designed to extend rights to patients regarding their protected health information (PHI) and ensure health information is kept secure. To this end, HIPAA also required the Secretary to issue privacy regulations governing individually identifiable health information if Congress did not enact legislation within three years of the passage of HIPAA. Because Congress did not enact such legislation, the U.S. Department of Health and Human Services ("HHS") enacted the Privacy Rule to implement the requirements of HIPAA.

HIPAA RULES

HIPAA is a collection of rules governing the privacy and security of patient information. Although the Privacy Rule is the most well-known HIPAA obligation, there are five separate rules imposed under HIPAA that govern the protection of patient information.

1. ***The Privacy Rule*** addresses the use and disclosure of individuals' health information by organizations – called "covered entities," as well as standards for individuals' privacy rights to understand and control how their health information is used. The Privacy Rule protects all "*individually identifiable health information*" held or transmitted by a Covered Entity or its Business Associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "protected health information (PHI)."

2. ***The Security Rule*** sets the minimum standards to safeguard electronic PHI (ePHI), which is PHI that is held or transferred in electronic form. The Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that covered entities must put in place to secure individuals' ePHI. The goal of the Security Rule is to protect the privacy of individuals' health information while allowing covered entities to adopt new technologies to improve the quality and efficiency of patient care. Given that the health care marketplace is diverse, the Security Rule is designed to be flexible and scalable so a Covered Entity can implement policies, procedures, and technologies that are appropriate for the entity's particular size, organizational structure, and risks to consumers' ePHI.

3. ***The Breach Notification Rule*** requires covered entities to provide notification to affected individuals, the Department of Health & Human Services (HHS) Secretary, and the media (under specific circumstances) if there is a breach of unsecured PHI; and Business Associates must notify covered entities if a breach occurs at or by the associates.

4. ***The Omnibus Rule*** made clarifications to the HIPAA Privacy and Security rules and improved the ability of the Office for Civil Rights (OCR) to enforce HIPAA requirements, while also implementing the mandates of the Health Information Technology for Economic and Clinical Health (HITECH Act).

5. Finally, ***the Enforcement Rule*** established how the OCR can determine liability and impose civil monetary penalties for HIPAA violations.

This Client Alert will specifically focus on the HIPAA Privacy Rule as it relates to device manufacturers.

HIPAA PRIVACY RULE

The HIPAA Privacy Rule is intended to assure individuals' health information is protected while allowing the flow of health information needed to provide and promote high-quality health care and to protect the public's health and well-being. Thus, the Privacy Rule is designed to define and limit the circumstances in which an individual's protected health information may be used or disclosed by covered entities. However, often times device manufacturers fall outside the scope of the Privacy Rule because they do not meet the definition of a Covered Entity and should be aware of unnecessarily engaging in Business Associate agreements.

A. Individually Identifiable Health Information and Protected Health Information

To understand the obligations imposed under the HIPAA Privacy Rule, it is important to first discern what information is protected by the Privacy Rule. ***As a general matter, the Privacy Rule protects individually identifiable health information held or transmitted by a Covered Entity or its Business Associate, in any form or media, whether electronic, paper, or oral***. The information protected by the Privacy Rule includes information across several data categories including, without limitation, the individual's past, present, or future physical or mental health or condition; the provision of health care to the individual, or; the past, present, or future payment for the provision of health care to the individual, and which identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers, such as name, address, birth date, and Social Security Number.

Protected health information (PHI) is defined to include individually identifiable health information that is (i) transmitted by electronic media; (ii) maintained in electronic media; or (iii) transmitted or maintained in any other form or medium, 45 C.F.R. § 160.103, and, therefore, broadly includes all individually identifiable health information transmitted or maintained in any form or medium. Thus, personal or demographic data that relates to an individual's physical or mental health, or the provision of or payment for health care, that identifies the individual is considered PHI. PHI also includes any data that can be used to identify an individual such as private information, facial images, fingerprints, and voiceprints, which can be associated with medical records, biological specimens, biometrics, data sets, as well as other direct identifiers of patients. Finally, PHI also includes personal information or identifiers in

electronic format and consists of data within emails, stored in the cloud, on a physical server, or in an electronic database.

However, not all individually identifiable health information is considered protected health information under HIPAA. In fact, there are several exceptions that may apply to a device manufacturer based upon specific factual circumstances. For example, identifying information alone (i.e., names, residential addresses, or phone numbers) is not necessarily designated as PHI if it is not related to health data. Additionally, protected health information does not include individually identified health information in (i) education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. § 1232g; (ii) in federally funded educational agencies described at 20 U.S.C. § 1232g(a)(4)(B)(iv); (iii) in employment records held by a Covered Entity in its role as employer; and (iv) information regarding a person who has been deceased for more than 50 years. Further, the Department of Health and Human Services has specifically clarified that the Privacy Rules do not protect employment records, even if such information is health-related:

> *"The Privacy Rule excludes from protected health information employment records that a Covered Entity maintains in its capacity as an employer and education and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g."*

See https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

Finally, information that is deidentified pursuant to HIPAA regulations, including 45 C.F.R. §§ 164.502(d) and 164.514(a)-(b), is not PHI. The Privacy Rule permits a Covered Entity or its Business Associate to create information that is not individually identifiable by following the de-identification standard and implementation specifications in § 164.514(a)-(b). There are two deidentification methods under the Privacy Rule: (1) a formal determination by a qualified expert; or (2) the removal of specified individual identifiers as well as an absence of actual knowledge by the Covered Entity that the remaining information could be used alone or in combination with other information to identify the individual. ***Information that is properly deidentified under the Privacy Rule can be used and disclosed by an entity because it is not PHI.*** It should be noted, however, that even if an information set is deidentified, there is still a remote possibility the information could be linked back to the identity of a patient and, therefore, deidentified information should be used with caution.

B. Covered Entities and Business Associates

In addition to understanding the scope of information protected by the HIPAA Privacy Rule, it is also important to understand to whom the Privacy Rule applies. As a general matter, the HIPAA Privacy Rule directly affects only those who meet the definition of a "Covered Entity." ***A "Covered Entity" includes (i) health care providers who conduct certain financial and administrative transactions electronically, (ii) health care clearinghouses, and (iii) health plans.*** In general, covered entities include individuals and organizations like health care practitioners, hospitals and insurance companies who engage in covered transactions, and clinicians or organizations who engage in electronic billing or who check eligibility for insurance coverage using a computer and web-based system. The Privacy Rule precludes a Covered Entity from using or disclosing protected health information, except either: as the Privacy Rule permits or requires, or as the individual who is the subject of the information (or the individual's personal representative) authorizes in writing, provided such use or disclosure is consistent with applicable HIPAA standards, including the "minimum necessary" standard.[1]

Most device manufacturers are not covered entities. This is because device manufacturers are neither health care providers, health care clearinghouses, or health plans. Instead, most device manufacturers solely operate in the limited capacity of a vendor or distributor of medical products.

A health care provider includes all "providers of services" (e.g., institutional providers such as hospitals) and "providers of medical or health services" (e.g., non-institutional providers such as physicians, dentists, and other practitioners) as defined by Medicare, and any other person or organization that furnishes, bills, or is paid for health care. A health care provider also includes any provider that electronically transmits health information with certain transactions, such as benefit eligibility issues, referral authorization requests, or other transactions for which HHS has established standards under the HIPAA Transactions Rule.

---

[1] 45 C.F.R. § 164.502(b). ***Under HIPAA, the "minimum necessary" standard applies when using or disclosing protected health information or when requesting protected health information from another Covered Entity.*** Under the minimum necessary standard, a Covered Entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

Further, the Privacy Rule applies to a provider whether it electronically transmits these transactions or uses a billing service or third party to do so on its behalf. Health care clearinghouses are entities that process nonstandard information they receive from another entity, or vice versa, into a standard (i.e., standard format or data content) for the purpose of processing healthcare services. Health care clearinghouses generally include billing services, repricing companies, and community health management information systems.

Finally, health plans generally include those individual and group plans that provide or pay the cost of medical care and include but are not limited to health, dental, vision, and prescription drug insurers, health maintenance organizations ("HMOs"), Medicare, Medicaid, and Medicare supplement insurers, and long-term care insurers (excluding nursing home fixed-indemnity policies).

Covered entities are also bound by HIPAA privacy standards even if they contract with others (i.e., "Business Associates") to perform some of their essential functions. A Business Associate is a person or organization, other than a member of a Covered Entity's workforce, that performs certain functions or activities on behalf of, or provides certain services to, a Covered Entity that involve the use or disclosure of individually identifiable health information. Specifically, the HIPAA regulations describe a "Business Associate" as one who:

> (i) On behalf of such Covered Entity or of an organized health care arrangement (as defined in this section) in which the Covered Entity participates, but other than in the capacity of a member of the workforce of such Covered Entity or arrangement, ***creates, receives, maintains, or transmits protected health information*** for a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing; or
>
> (ii) Provides, other than in the capacity of a member of the workforce of such Covered Entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such Covered Entity, or to or for an organized health care arrangement in which the Covered Entity participates, where the ***provision of the service involves the disclosure of protected health***

information from such Covered Entity or arrangement, or from another Business Associate of such Covered Entity or arrangement, to the person.

See 45 C.F.R. § 164.103. (Emphasis added in bold). Our medical device clients frequently inquire whether they are Business Associates under HIPAA. ***As a general matter, most device manufacturers are not Business Associates because they do not perform any of the regulated functions or activities on behalf of, or provide services to, a Covered Entity.*** Further, most device manufacturers do not create, receive, maintain, or transmit protected health information on behalf of a Covered Entity. If a healthcare provider requests a device manufacturer to sign a Business Associate agreement, we recommend the device manufacturer consult with legal counsel to determine whether the functions to be performed by the manufacturer render it a Business Associate under HIPAA and, if not, provide a declination letter to the healthcare provider declining the Business Associate Agreement. This can often be accomplished by invoking the HIPAA Privacy Rule exceptions set forth in the succeeding section, which except certain functions from the scope of the HIPAA Privacy Rule.

C. HIPAA Privacy Rule Exceptions

Finally, it is necessary to understand the exceptions to the HIPAA Privacy Rule. We frequently receive questions from medical device clients about whether they are obligated to comply with the HIPAA Privacy Rule or execute a Business Associate Agreement to transact business with a Covered Entity. The answer to this question largely depends upon the specific factual circumstances presented. ***However, in many instances, a device manufacturer is not required to comply with the Privacy Rule obligations or enter into a Business Associate Agreement based on several exceptions to the HIPAA Privacy Rule that generally cover the functions of a device manufacturer.*** The most notable exceptions are the Public Health Exception and the Treatment, Payment, and Operations (TPO) Exception.

The Public Health Exception to the HIPAA Privacy Rule is located at 45 C.F.R. § 164.512(b)(1)(iii) and provides that a Covered Entity may use or disclose protected health information, without patient authorization, in certain instances. Specifically, the exception permits the use or disclosure of PHI to "[a] person subject to the jurisdiction of the Food and Drug Administration (FDA) with respect to an FDA-regulated product or activity for which that person has responsibility, for the purpose of activities related to the quality, safety or effectiveness of such FDA-regulated product or activity," including "(i) to collect or report adverse events (or similar activities

with respect to food or dietary supplements), product defects or problems (including problems with the use or labeling of a product), or biological product deviations; (ii) to track FDA-regulated products; (iii) to enable product recalls, repairs, or replacement, or lookback (including locating and notifying individuals who have received products that have been recalled, withdrawn, or are the subject of lookback); or (iv) to conduct post marketing surveillance." See 45 C.F.R. § 164.512(b)(1)(iii).

While the Public Health Exception to the Privacy Rule addresses many of the post-market activities that apply to device manufacturers and explicitly permits a Covered Entity to disclose PHI to a device manufacturer for the purpose of adverse event reporting, tracking regulated products (i.e., cleared or approved medical devices), enable repairs or replacement of devices, or for the purpose of post-market surveillance, the Public Health Exception is limited to disclosures for those stated purposes. As a result, the Public Health Exception does not apply to disclosures from a Covered Entity to a device manufacturer for other purposes, such as the disclosure of PHI for future device innovation or development, the disclosure of PHI through a cloud-based system for analytical purposes, or the disclosure of PHI for marketing or other commercial activities.

The other common HIPAA exception for device manufacturers is the Treatment, Payment and Operations (TPO) Exception. Under the TPO Exception, "[a] Covered Entity may disclose protected health information for treatment activities of a health care provider" without authorization ***provided that*** the healthcare provider uses reasonable safeguards when doing so to protect the information from inappropriate use or disclosure. 45 C.F.R. § 164.506(c)(2). A medical device company meets the Privacy Rule's definition of "health care provider" if it furnishes, bills, or is paid for "health care" in the normal course of business. "Health care" under the Rule means care, services, or supplies related to the health of an individual. Additionally, HHS has clarified that a manufacturer's services in supporting the appropriate use of its product for a patient are part of the patient's treatment. Thus, the TPO exception provides substantial leeway for disclosures of PHI from a healthcare provider to a device manufacturer.

The core health care activities of "Treatment," "Payment," and "Health Care Operations" are defined in the Privacy Rule at 45 C.F.R. § 164.501. "Treatment" generally means the provision, coordination, or management of health care and related services among health care providers or by a health care provider with a third party, consultation between health care providers regarding a patient, or the referral of a patient from one health care provider to another. "Payment" encompasses the

various activities of health care providers to obtain payment or be reimbursed for their services and of a health plan to obtain premiums, fulfill their coverage responsibilities and provide benefits under the plan, and obtain or provide reimbursement for the provision of health care. Finally, "Health care operations" are certain administrative, financial, legal, and quality improvement activities of a Covered Entity that are necessary to run its business and to support the core functions of treatment and payment.

For example, the TPO Exception would apply if a manufacturer or its representative is present in the operating room, as requested by the surgeon, to provide support and guidance regarding the appropriate use, implantation, calibration, or adjustment of a medical device for that particular patient because this would constitute "treatment" by the company. The TPO exception also permits a covered provider to allow a representative of a device manufacturer to view protected health information, such as films or patient records, to provide consultation, advice, or assistance where the provider, in her professional judgment, believes that this will assist with a particular patient's treatment. Finally, a covered provider may share protected health information with a device manufacturer under the TPO Exception for the device manufacturer to receive payment for the health care it provides.

The HHS website serves as a helpful resource when evaluating whether an anticipated disclosure of PHI from a Covered Entity to a device manufacturer is subject to either the Public Health Exception or the TPO Exception. Additionally, the website provides several useful examples for device manufacturers concerning the application of those exceptions, including the following, ***all of which permit the disclosure of PHI without patient authorization or a Business Associate Agreement:***

- A covered provider may disclose protected health information needed for an orthopedic device manufacturer or its representative to determine and deliver the appropriate range of sizes of a prosthesis for the surgeon to use during a particular patient's surgery. (This would be a treatment disclosure to the device company as a health care provider. Exchanges of protected health information between health care providers for the treatment of the individual are not subject to the minimum necessary standards. 45 C.F.R. § 164.502(b).)

- The device manufacturer or its representative may be present in the operating room, as requested by the surgeon, to provide support and guidance regarding the appropriate use, implantation, calibration, or adjustment of a medical device

for that particular patient. (This would be treatment by the device company as a health care provider. As noted in the prior example, treatment disclosures between health care providers are not subject to the minimum necessary standards.)

- A covered provider may allow a representative of a device manufacturer to view protected health information, such as films or patient records, to provide consultation, advice, or assistance where the provider, in her professional judgment, believes that this will assist with a particular patient's treatment. (This would also be a treatment disclosure and the minimum necessary would not apply.)

- A covered provider may share protected health information with a medical device company as necessary for the device company to receive payment for the health care it provides. (This would be a disclosure for payment of a health care provider and subject to minimum necessary standards.)

- A covered provider may disclose protected health information to a device manufacturer that is subject to FDA jurisdiction to report an adverse event, to track an FDA-regulated product, or for other purposes related to the quality, safety, or effectiveness of an FDA-regulated product (This would be a public health disclosure and subject to minimum necessary standards).

(*See* https://www.hhs.gov/hipaa/for-professionals/faq/490/.)

In other instances, disclosure of PHI between a Covered Entity and a device manufacturer requires a Business Associate Agreement. For example, the HHS website clarifies that a Business Associate agreement would be required if a Covered Entity asked the medical device company to provide an estimate of the cost savings it might expect from the use of a particular medical device; and to do so, the device company needed access to the Covered Entity's protected health information. In this case, the medical device company is performing a health care operations function (business planning and development) on behalf of the covered provider, which requires a Business Associate agreement even though the disclosure is permitted without an authorization. (*See id.*)

In addition to the guidance by HHS, the American Hospital Association and the Healthcare Leadership Council have provided helpful guidance for device manufacturers when navigating HIPAA privacy concerns. For example, in the

Frequently Asked Question entitled "Covered Entity – Manufacturer Relationships Under HIPAA", ***the American Hospital Association and the Healthcare Leadership Council clarify when a Business Associate Agreement is required between a Covered Entity and a device manufacturer***:

> *Do I need a Business Associate agreement with manufacturers from whom I obtain drugs and supplies? A Business Associate agreement should be used only when you intend the other party to have access to patient-identifiable information in order to perform some service for you. This is not what occurs when a Covered Entity is buying items or accepting samples from a vendor. It is generally not advisable for a provider or health plan to enter into a Business Associate agreement with a manufacturer or other vendor from whom it purchases drugs, devices, or supplies, unless the provider or plan also provides patient-identifiable information to the manufacturer in order to perform some other service. Examples of services that might require a Business Associate agreement (or perhaps a data use agreement) include patient outcomes analysis, archiving or processing of medical images, quality improvement analyses, benchmarking against standards of care, and so forth.*

As stated above, we are frequently asked to advise device manufacturers to evaluate the need for a Business Associate Agreement based upon the Public Health Exception and the TPO Exception. ***In many instances, either the Public Health Exception or the TPO Exception apply to permit the disclosure without the need for patient authorization or a Business Associate Agreement***. In those instances, we frequently draft Business Associate Agreement declination letters for clients that identify the reasons why a Business Associate Agreement is not required for the disclosure of information from a Covered Entity to a device manufacturer. A declination letter may be predicated upon the Public Health Exception or TPO Exception, or upon the fact there will not be any use or disclosure of protected health information or would be covered by a patient authorization. For example, in the pre-and post-operative context in which a medical device will be utilized for a clinical procedure, the provision of patient information from the Covered Entity to a device manufacturer may be considered part of the provision or management of health care and related service within the scope of the TPO Exception.

Finally, in other instances, device manufacturers choose to voluntarily enter into a Business Associate Agreement in deference to the HIPAA obligations of their customers, which are covered entities, and the privacy interests of patients. While we generally counsel clients to avoid voluntarily accepting unnecessary contractual

and regulatory obligations, this approach may enhance the relationship between a device manufacturer and its customers if necessary. For example, we recently had one medical device client that voluntarily enter into a Business Associate Agreement in deference to its customer's obligations and to illustrate its commitment and compliance with the HIPAA Privacy Rule and the Security Rules. That client was willing to voluntarily assume the risks and obligations as a Business Associate because the client had previously established vigorous security protocols consistent with ISO certifications, an experienced privacy and security compliance team, and a robust infrastructure to protect the disclosure of PHI from its customers to the client. Although that particular client was comfortable with entering into the Business Associate Agreement, doing so does impose additional obligations and risks. Accordingly, the decision by a device manufacturer to voluntarily enter into a Business Associate Agreement should be made only after a careful consideration of all the applicable facts, circumstances, and legal requirements.

HIPAA ENFORCEMENT

In his song, *"I Heard it Through the Grapevine,"* Marvin Gaye's surprise occurred when he learned of his lover's infidelity through the rumor mill. With respect to HIPAA, a device manufacturer could be surprised by an enforcement action commenced by the Department of Health & Human Services, Office for Civil Rights (OCR) due to a HIPAA violation. The HHS-OCR is responsible for providing education and outreach, investigating patients' complaints, and conducting compliance reviews of covered entities with respect to HIPAA. Further, OCR has the authority to levy civil and criminal fines and penalties for violations of HIPAA.

Since 2003, the U.S. Department of Health & Human Services Office for Civil Rights (OCR) has imposed more than 100 civil monetary penalties, totaling over $131 million, for violations of the HIPAA. Additionally, under the Health Information Technology for Economic and Clinical Health Act, states may bring enforcement actions on behalf of their residents for HIPAA violations. Recently, multistate actions have been on the rise, with state attorneys general working cooperatively to investigate and enforce violations more efficiently, often resulting in financial penalties for covered entities and Business Associates. ***Additionally, due to an increasingly digitized healthcare industry, it is expected that HIPAA enforcement will continue to increase or adapt based upon novel privacy concerns***.

Finally, in cases of HIPAA noncompliance, the OCR may decide to impose civil money penalties (CMPs) on the Covered Entity or the DOJ may impose criminal penalties.

CMPs for HIPAA violations are determined based on a tiered civil penalty structure. The Secretary of HHS has discretion in determining the amount of the penalty based on the nature and extent of the violation and the nature and extent of the harm resulting from the violation. For example, HIPAA penalties may range from $100 - $50,000 per violation, with an annual maximum of $25,000 for repeat violations that resulted from inadvertence, to $50,000 per violation, with an annual maximum of $1.5 million, for violations caused by willful neglect. It is important to note that individuals such as directors, employees, or officers may also be directly criminally liable under HIPAA in accordance with "corporate criminal liability," or may be charged with conspiracy or aiding and abetting based on the factual circumstances.

HIPAA COMPLIANCE BEST PRACTICES

In our experience, HIPAA violations that affect device manufacturers are generally inadvertent and unexpected, and/or arise "through the grapevine," such as the inadvertent sharing of favorable patient results for an investigational device via social media, or other similar acts. Indeed, the most common HIPAA Privacy Rule compliance risks fall within one of three risk categories: ***(i) inadequate access, identification and operations; (ii) lack of visibility or oversight of user activity; and (iii) inadequate compliance training.*** Inadequate access, identification and operations refers to those HIPAA violations that arise from inappropriate credentialing, user privileges, access, and authorization to protected health information. Lack of visibility or oversights refers to inadequate monitoring of user access in a digital environment. Finally, inadequate compliance training refers to improper training provided by an employer regarding the employer's HIPAA obligations and risks.

To mitigate against these common HIPAA risks, there are several best practices a device manufacturer can implement (which are in addition to avoiding any regulated activities or functions under HIPAA).[2]

1. **Executive Leadership**: Tone from the top of an organization is critical to establishing a culture of compliance, especially as it relates to HIPAA privacy concerns. By providing an executive commitment for the implementation of HIPAA policies, compliance training, and a privacy and security infrastructure, a

[2] Implementation of a commercially reasonable security architecture and information and event management solution consistent with ISO certifications and/or other privacy and security standards is also advisable, but beyond the scope of this Client Alert.

company can better position itself to comply with its HIPAA obligations and avoid being surprised "through the grapevine";

2. **Policies & Procedures**: Documentation is key to HIPAA compliance and includes the use of enterprise-wide policies and procedures that conform to federal standards, including the minimum necessary standard. Policies and procedures are often an area of focus in OCR resolution agreements. Additionally, OCR and state agencies may require HIPAA violators to submit their policies and procedures for review and approval as part of resolution agreements. Covered entities and Business Associates should, therefore, adopt an appropriate HIPAA policy to govern information flow. An appropriate policy should have at least four, central components: (1) an obligation to protect and safeguard privacy and security of PHI in accordance with HIPAA; (2) an obligation to train staff regarding the protection and safeguarding of PHI; (3) an obligation to inform customers, partners, consultants and vendors of the HIPAA policy and a review of the HIPAA policies of those third-parties, and (4) an obligation to limit the amount of PHI that is used and/or disclosed consistent with the "minimum necessary" standard. In addition to implementing a policy, a company should assess, update, and make necessary revisions to its policies and procedures at least annually. Changes to an organization's privacy and security practices and environmental changes should be reflected with immediate revisions. Additionally, an appropriate HIPAA Policy should specify requirements for the routine and timely disposal of PHI.

3. **Access Management & Tools**: To promote HIPAA compliance a company must strategically address access, privileges and credentialing for information databases. Such access, privileges and credentialing should be explained to all employees to ensure information is only shared on a "need-to-know" basis. Additionally, a company should also implement other efforts to improve the privacy and security of its information, through administrative safeguards, such as access management tools and security awareness training, reducing the number of recipients on communications containing PHI, removal of all unnecessary PHI in communications, the evaluation of employee utilization of mobile electronic devices enhancing restrictions on unapproved applications that may involve PHI; physical safeguards, such as facility controls, and workstation/device/media security; and technical safeguards, such as access control, audit control and transmission security.

4. **Risk Analysis**: When a Covered Entity or Business Associate reports a breach, the subsequent investigation will invariably include an examination of the organization's risk analysis and risk management plan. As such, failure to conduct an accurate, enterprise-wide risk analysis or implement risk-mitigating measures are two of the most common HIPAA violations in both OCR and state enforcement actions. An adequate risk audit and analysis should identify all risks to the security, privacy, and integrity of protected health information.

5. **Compliance Training**: In several recent HIPAA enforcement actions, the conduct of individual workforce members was the primary cause of the resulting breach of PHI. As such, the requirement that covered entities and Business Associates provide privacy and security awareness training for all workforce members is crucial. It is best practice that workforce members who have access to PHI receive training at least annually, with new workforce members receiving training as soon as possible upon hire, preferably within 14 days but no later than 30 days of hire. Similar to the requirements for distributing policies and procedures, organizations should require their workforce members to certify, either in electronic or written form, that they attended and completed training. The content of the training should be reviewed at least annually and updated, as needed, to address changes in federal law or agency guidance.

As Marvin Gaye sang, it took him by surprise when he "heard it through the grapevine." Implementing the above best practices, among others, will help a device manufacturer improve its HIPAA compliance and avoid potential "grapevine" surprises based on the use and disclosure of PHI protected by HIPAA.