HIPAA Privacy Rule / HIPAA Security Rule / HIPAA Enforcement Rule -- Audits by OCR

The impact of the passage of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) has been enormous. Covered entities, business associates and subcontractor business associates are required by law to fully comply with HIPAA's requirements. Should they fail to meet their statutory obligations, they are subject to significant administrative penalties, civil enforcement, and in some cases criminal sanctions. Today, health care providers around the country still struggle to properly implement and comply with the HIPAA Privacy Rule, the HIPAA Security Rule and the HIPAA Enforcement Rule. This article provides an overview of these requirements so that you can be better prepared in the event of an audit by the government.

I. Historical Background of Medical Privacy:

The concept of medical privacy is far from new. Hippocrates, commonly referred to as the "*Father of Medicine*" is credited with first raising the importance of medical confidentiality as part of The Hippocratic Oath:

> *What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself, holding such things shameful to be spoken about.* **[1]** Hippocrates (460 BC – 375 BC).

Over the last 2,400 years, medical privacy has continued to constitute an integral part of the ethical code followed by physicians and other health care professionals. Early efforts by both the federal government and the states to enact medical privacy legislation were typically limited and often provided little, if any, real protection for patients. For example, the Federal Privacy Act of 1974, codified at 5 U.S.C. § 552a, was a significant first step at the Federal level to set up a *"code of fair*

information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records." **[2]** Unfortunately, the Privacy Act of 1974 was quite limited in scope – it only covered health care data maintained in systems of records held by federal agencies.

With the passage of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), **[3]** the protection and confidentiality of medical information was passed and became Federal law. Since its implementation, HIPAA has completely transformed the health care industry's approach toward patient privacy and medical records security. HIPAA arose, at least in part, because of the need to address how the health care industry could safely and efficiently utilize increasingly available electronic resources. The law was intended to address a number of policy goals, including the desire to:

> *(1) Standardize data systems to allow for a more efficient exchange of information among providers and insurers;*
>
> *(2) Improve federal patient privacy protections; and*
>
> *(3) Improve data security, as a complement to improved privacy protections.*

II. Overview of the Implementation of HIPAA's Requirements:

The Department of Health and Human Services (HHS), Office for Civil Rights (OCR) has been tasked with enforcing HIPAA's Privacy, Security, Enforcement and Breach Notification Rules. Subsequent to the enactment of the statute, HHS and its affected agencies have worked to codify the law and establishing regulations. Significant implementation dates have included:

> **April 14, 2003.** Effective date for compliance with the **HIPAA Privacy Rule**. The Privacy Rule is contained in Subpart E (Privacy of Individually Identifiable Information), C.F.R. §164.500-164.534.
>
> **April 21, 2005.** Effective date for compliance with the **HIPAA Security Rule**. The Security Rule sets out the Administrative, Physical and Technical safeguards that must be met by covered entities. A "**Risk Analysis"** of a covered entity's obligations under the Security Rule is required in order to fully comply with requirements of the Security Rule as the "first step" in identifying and complying with the HIPAA Security Rule.
>
> **March 16, 2006.**Effective date for compliance with the **HIPAA Enforcement Rule**. The Enforcement Rule amended existing rules related to the investigation of HIPAA

noncompliance in order to extend them to all of the Administrative Simplification Rules, not merely the Privacy Rule standards. **[4]** The Enforcement Rule also:

(1) Amended existing rules relating to the process for imposition of civil money penalties;

(2) Clarified and elaborated upon the investigation process, bases for liability, determination of the penalty amount, grounds for waiver, conduct of the hearing, and the appeal process.

February 17, 2009. The *Health Information Technology for Economic and Clinical Health* (**HITECH**) **Act**, enacted as part of *the American Recovery and Reinvestment Act of 2009*, was signed into law on this date. Among its provisions, the HITECH Act promoted the adoption and meaningful use of health information technology.

March 26, 2013. Effective date for compliance with the **HIPAA Omnibus Rule**. The HIPAA Omnibus Rule introduced a number of modifications [5] to existing privacy provisions. Covered entities and business associates were given until 180 days beyond the effective date to fully comply with most of the rule's provisions. These included, but were not limited to:

(1) The modification of the HIPAA's Privacy, Security and Enforcement Rules in order to implement the statutory amendments set out under the Health Information Technology for Economic and Clinical Health Act (HITECH). These changes were needed to strengthen the privacy and security protection for individuals' health information;

(2) The modification of Breach Notification Rule for Unsecured Protected Health Information (as provided by HITECH); and

(3) The modification of the HIPAA Privacy Rule in order to strengthen the protections covering genetic information by implementing section 105 of Title I of the Genetic Information Nondiscrimination Act of 2008 (GINA).

III. Relationship Between Federal and State Privacy Laws:

The provisions of HIPAA preempt contrary state laws, meaning that HIPAA rules apply when it would be impossible for a covered entity to comply with both the state and federal requirements. **[6]** HIPAA rules also apply when a certain state law is "an obstacle" to fully accomplishing the full purposes and objectives of the Administrative Simplification provisions of HIPAA.[7] However, HIPAA is intended to be a floor, not a ceiling, to patient privacy and information security. If state medical privacy requirements and standards are more stringent than those imposed under HIPAA, state law applies.**[8]** For instance, the State of Texas has enacted

H.B. 300**,** which is more restrictive in several respects than HIPAA. More stringent laws are those that might provide more restricted third-party access to protected health information, greater patient access to information, more information about privacy, greater protections when express legal permission is required, or longer or more detailed record retention. A state law cannot, however, prevent the HHS Secretary from verifying compliance with HIPAA. **[9]**

There are several other exceptions to the general rule that Federal law preempts state law. State law may be applied if the HHS Secretary determines that the state law is necessary: (a) to prevent health care fraud and abuse; (b) to ensure appropriate state regulation of insurance and health plans as authorized; (c) for state reporting on health care delivery or costs; or d) to serve a compelling public health, safety, or welfare need. Other instances in which state law controls include if the Secretary determines that its principal purpose is the regulation of controlled substances or if the law requires health plans to meet certain informational requirements. **[10]**

IV. Entities Covered Under HIPAA:

The Security and Privacy Rules of HIPAA apply to "covered entities," meaning a health plan, a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a standard transaction.**[11]** Health care providers include all***"providers of service"*** **and** ***"providers of medical or health services"***as defined by Medicare, and any other person or organization that furnishes, bills, or is paid for health care.**[12]** The provider may be any size and is still covered whether the provider transmits the health care information directly or through a third party (such as a billing service). Merely using electronic technology, like e-mail, does not mean a health care provider is a covered entity—the transmission must be in connection with a standard transaction.

If an entity is a hybrid entity, meaning that the entity's business activities include both covered and non-covered functions, the Security and Privacy Rules only apply to the health care components of the entity. **[13]** The Centers for Medicare and Medicaid Services (CMS) has developed extensive charts describing who is a covered entity. **[14]**

Additionally, if a covered entity engages a "business associate" to help it carry out its health care activities and functions, the Security and Privacy Rules of HIPAA also apply to these entities. HHS has gone to great length in discussing who is, and who is not, considered a business associate. **[15]** However, not all of the Privacy Rule obligations are imposed on business associates. A business associate is subject to direct enforcement of the HIPAA Privacy obligations and penalties in the same manner as a covered entity, but only to the extent required under the HITECH Act (discussed below) – not the HIPAA Privacy Rule itself.

V. Scope of Information Under the HIPAA Privacy Rule:

While the Security Rule deals with electronic information, the Privacy Rule defines *"Health*

Information" as any information whether oral or recorded in any form or medium, that:

> (1) Relates to the past, present, or future physical or mental health or condition of an individual;
>
> (2) Related to the he provision of health care to an individual; or
>
> (3) Relates to the past, present, or future payment for the provision of health care to an individual. **[16]**

In contrast, the term "*Individually Identifiable Health Information*" is a subset of the term "*Health Information*" and is limited to information that identifies an individual or is information that reasonably could serve as the basis to identify an individual. Finally, the term *"Protected Health Information"* (PHI) covers individually identifiable health information that is transmitted by electronic media, maintained in electronic media or transmitted or maintained in any other form or medium. The rules do not include "de-identified information," individually identifiable information where all 18 identifiers have been removed. Such information can be used without restriction or patient authorization. **[17]**

VI. HIPAA Privacy Rule Considerations for Small and Mid-Sized Providers:

Importantly, under HIPAA, small and mid-sized providers are not treated the same as large, institutional providers (such as hospitals). The law allows for scalability, which can keep added compliance expenses lower and reflect the operational reality of a smaller office. However, there are some additional challenges that come with maintaining privacy and security in a smaller office setting. For instance, it may be harder to dedicate the physical space necessary to keep unauthorized persons from areas where PHI is accessible.

Small and mid-sized providers should also be aware that scalability does not allow for major reductions in some areas. For instance, providers must still comply with the Privacy Rule. However, the procedures associated with such compliance may be simplified, such as appointing a privacy official who also has other office or clinical duties rather than hiring a dedicated Compliance Officer.

VII. Goal of the HIPAA Privacy Rule:

A major goal of the Privacy Rule is to ensure that an individual's health information is properly protected while still allowing for the sharing of information needed to provide high quality health care and to protect the public. The Rule applies to health plans, health care clearing houses, and those health care providers (of any size) that conduct certain health care transactions electronically. It also applies to business associates that perform certain activities on behalf the

provider which requires the use or disclosure of individually identifiable information. The Rule requires appropriate safeguards to protect the privacy of personal health information, and it sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Privacy Rule also covers the rights of patients over their health information, including the right to examine and obtain a copy of their health records and to request corrections. **[18]**

HIPAA's Privacy Rule attempts to strike a balance between an individual's right to keep personal health information private and the needs of the health care system. This section will describe: (a) the basic rule and its exceptions; (b) the steps required for developing and implementing policies and procedures required under the rule; and (c) notice requirements.

A basic mandate of the Privacy Rule is that organizations may only release PHI as explicitly permitted by the rule or with the prior written consent of the individual who is the subject of the records. Moreover, when access is permitted or required, the **"*minimum necessary standard*"** applies. The minimum necessary standard dictates that when a covered entity uses, accesses, or discloses PHI or requests health information from another covered entity, the entity must make reasonable efforts to limit PHI use or disclosure to that which is reasonably necessary to accomplish the intended purpose. **[19]**

> ***The key question for compliance with the minimum necessary standard is whether the use or disclosure is necessary for the employee to do his or her job. For example, does a billing clerk really need access to a patient's entire medical record?***

(A) Business Associates / Business Associate Agreements. When a patient authorizes a covered entity to collect, maintain and have access to their individually-identifiable health information, the covered entity is effectively holding this medical information in trust. More often than not, the covered entity contracts with one or more outside entities to perform ancillary services (such as billing, IT support, consulting, etc.) which requires that patient information be shared. The entities are known as "business associates." Under the Privacy Rule, a covered entity must ensure that these entities fully understand their obligations under HIPAA to protect individually-identifiable health information from improper access, use and disclosure that would be in violation of HIPAA. You must ensure that any outside entities with whom you share such information has executed a "Business Associate Agreement" which outlines the business associate's obligations and the safeguards that the entity must have in place, prior to sharing this protected information.

(B) Patient Rights. The Privacy Rule focuses, to a large part, on achieving a reasonable balance between protecting patient rights of confidentiality and allowing health care providers to do their jobs. Importantly, patients have a number of rights that impact a provider's compliance plan, including the right:

- To know when and to whom there has been a disclosure for the six years prior to the request. **[20]**
- To request restrictions in how the provider communicates information, especially to health plans when the patient has paid for services out-of-pocket. **[21]**
- To make copies of privacy notices. **[22]**
- To access records, except in limited instances. **[23]**
- To amend his or her file. **[24]**
- To complain of violations. **[25]**

It is essential that staff be cognizant of these rights and be trained to respect patients and their privacy. While the provider's policies and procedures should take all of these rights into account, the provider must explicitly plan for tracking disclosures and patient communication protocols on a regular basis. For the former, the provider is obliged to keep a log of any and all disclosures of each patient's information. Where a large institutional provider might implement a complex logging system, a small provider may find it appropriate to keep a pen and paper list in the patient's file or other similarly straightforward documentation. Regarding the latter, the provider must have a procedure in place to determine if the patient prefers phone calls, whether it is acceptable to leave a voicemail, if emails are preferred, etc., and then must strictly adhere to that preference.

(C) Authorized Uses and Disclosures.

All covered entities must obtain a patient's written authorization for any use or disclosure of PHI that is not for treatment, payment or health care operations or otherwise permitted or required by the Privacy Rule. **[26]** A covered entity may also use certain information for patient directories—name, location in hospital, condition (good, fair, critical), and religious affiliation—for use by clergy or those asking for the patient. **[27]**

However, there are restrictions with regards to a disclosure to a patient's health plan. Notably, a covered entity ***must*** abide by a patient's request not to disclose PHI about the patient if the disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law, and the PHI pertains solely to a health care item or service for which the patient has paid the physician in full. **[28]** This rule is an update under the new HIPAA Omnibus Rule. Previously, while physicians could refuse to abide by any such request, the new rule ***requires*** physicians and other health care providers to abide by a patient's request not to disclose PHI to a health plan for those services for which the patient has paid out-of-pocket and requests the restriction.

If a proposed use or disclosure of information is ***not*** for treatment, payment, or operations, as required by law, or as allowed for the directory, the provider ***must obtain written*** authorization ***prior*** to access or disclosure. Additionally, although there are exceptions to the general rule, a patient's authorization must be obtained to use or disclose psychotherapy notes. **[29]**

The information may only be sold or used for fundraising with specific authorization. **[30]** The HIPAA Omnibus Rule further clarifies that the prohibition on the sale of PHI in the absence of the patient's written authorization extends to licenses or lease agreements. It also extends to the receipt of financial or in-kind benefits. It also includes disclosures in conjunction with research if the remuneration received includes any profit margin.

Another significant change to patients' rights as to the use of their PHI relates to marketing and subsidized communication of that information. The HIPAA Privacy Rule defines marketing as making "*a communication about a product or service that encourages recipients of the communication to purchase or use the product or service*." **[31]** Previously, this form of communication required a prior authorization from the intended recipient of the communication, with some exceptions. Now, however, the Final Rule requires authorization for ***all*** treatment and health care operations communications where the covered entity receives financial remuneration from the third party whose products or services are being marketed.

The Privacy Rule is not intended to impede customary and essential communications and practices. HIPAA permits certain incidental uses and disclosures of PHI to occur when the covered entity has in place reasonable safeguards and "minimum necessary" policies and procedures to protect an individual's privacy. Reasonable safeguards might include avoiding the use of patients' names, speaking softly when discussing a patient in a public area, locking file cabinets, or using passwords for computers. An incidental use or disclosure is a secondary use or disclosure that cannot reasonably be prevented is limited in nature, and that occurs as a result of another use or disclosure that is permitted by the rule. For instance, if a person inadvertently overhears a provider's confidential conversation with a patient or colleague or sees a name on a sign-in sheet, this may be an incidental use. Disclosure is not permitted if it is a by-product of an underlying use or disclosure that violates the rule.

Nevertheless, if a patient requests that a covered entity restrict certain disclosures of PHI to a health plan, the covered entity ***must*** ensure that he or she complies with this request. **[32]** The covered entity must employ some method to flag or make a notation in a patient's medical with respect to the PHI that has been restricted so that the information is not sent to a health plan. In those situations where an individual wants to restrict disclosures to a health plan concerning a prescribed medication, the prescribing provider may provide the patient with a paper prescription to allow the individual an opportunity to request a restriction and pay for the prescription with the pharmacy *before* the pharmacy has submitted the bill to the patient's health plan.

(D) Personal Representatives and Unemancipated Minors.

A "*personal representative*" is someone who is legally authorized to make health care decisions on an individual's behalf (or on behalf of a deceased individual's estate). A covered entity is required under the Privacy Rule to treat a personal representative the same as the individual, with respect to uses and disclosures of the individual's PHI. **[33]**

When dealing with unemancipated minors, the Privacy Rule defers to state law to determine the extent of parents to make medical decisions on behalf of their children. To the extent that state law is silent, the Privacy Rule does authorize parents to serve as a child's personal representatives and legally authorizes them to make health care decisions on their child's behalf. **[34]**

(E) Public Interest Disclosures of Protected Health Information.

Importantly, the Privacy Rule permits the use and disclosure of PHI, without a patient's authorization or permission, for a number of specific purposes that are mandated by law **[35].** This is in recognition of the important uses made of health information outside of the health care context.

Uses and disclosures required by law. **[36]**

Uses and disclosures for public health activities. **[37]**

Disclosures about victims of abuse, neglect or domestic violence. **[38]**

Uses and disclosures for health oversight activities. **[39]**

Disclosures for judicial and administrative proceedings. **[40]**

Disclosures for law enforcement purposes. **[41]**

Uses and disclosures about decedents. **[42]**

Uses and disclosures for cadaveric organ, eye or tissue donation purposes. **[43]**

Uses and disclosures for research purposes. **[44]**

Uses and disclosures to avert a serious threat to health or safety. **[45]**

Uses and disclosures for specialized government functions. **[46]** and

Disclosures for worker's compensation. **[47]**

(F) Notice of Privacy Practices.

A covered entity must give patients a notice that tells them how the entity may use and share health information and how patients can exercise their health privacy rights.**[48]** In most cases, you should give this notice to the patient on the patient's first visit to the provider, and be ready to

provide a copy at any time to anyone who asks for one. It is also required that you make a good faith effort to obtain written acknowledgement of receipt of the notice from your patients.**[49]** When drafting a Notice of Privacy Practices, it is imperative that providers incorporate both Federal and state privacy laws. If a covered entity has a website for customers, it must post its notice in an obvious spot on the site. The provider or health plan cannot use or disclose information in a way that is not consistent with its notice.

(G) Developing Policies and Procedures.

A covered entity must develop and implement written privacy policies and procedures that are consistent with the Privacy Rule. **[50]** As a first step, a covered entity must assign a Privacy Officer or HIPAA Compliance Contact to be responsible for HIPAA compliance. **[51]** This can be a person hired specifically for this purpose or someone with other duties, such as the office manager. The person will need to be given the authority, resources, and time to ensure the entity is HIPAA compliant. Job responsibilities of a Privacy Officer might include:

Performing initial and periodic privacy risk assessments;

Working with legal counsel and others to ensure the organization has and maintains appropriate, up-to-date privacy and confidentiality forms and notices;

Ensuring privacy training and orientation to all workforce personnel, business associates, and other appropriate third parties;

Participating in the development, implementation, and ongoing compliance monitoring of all trading partner and business associate agreements;

Establishing a mechanism to track access to PHI and to allow qualified individuals to review or receive a report on such activity;

Establishing and administering a process for addressing all complaints concerning privacy policies and procedures;

Ensuring compliance with privacy practices and consistent application of sanctions for failure to comply with privacy policies;

Ensuring alignment between security and privacy practices;

Maintaining current knowledge of applicable federal and state privacy laws and other standards;

Monitoring advancements in information privacy technologies; and

Cooperating with law enforcement and other governmental agencies in any compliance reviews or investigations.

Once appointed, your organization's Privacy Officer should review any procedures and policies that may already be in place and identify where additional policies and procedures are needed. Your Privacy Officer should be closely involved in developing and implementing privacy rules and procedures.

After policies and procedures have been determined, your staff must be trained regarding both the rules and their obligations under the law. This training must include anyone who may see or work with health, financial, or confidential information involving PHI identifiers and everyone who uses a computer or other device that stores or transmits information having anything to do with patient health. The covered entity must train all workforce members on privacy policies and procedures "*as necessary and appropriate for them to carry out their functions*." **[52]** In a small practice, the training may be uniform for all employees and somewhat less formal than what might take place for a major institutional provider. The training should be updated as necessary to ensure compliance.

Finally, the Privacy Officer should pay careful attention to records retention policies. A provider must maintain privacy records for at least six years. **[53]**

VIII. HIPAA Security Rule:

Designed to complement the Privacy Rule, the Security Rule established national standards to protect an individual's electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronically protected health information. **[54]**

The Security Rule provides that covered entities may use any security measures that allow the covered entity to reasonably and appropriately implement its requirements. *"In deciding which security measures to use, a covered entity must take into account the following factors: (i) the size, complexity, and capabilities of the covered entity; (ii) the covered entity's technical infrastructure, hardware, and software security capabilities; (iii) the cost of security measures; (iv) the probability and criticality of potential risks to electronic protected health information*." **[55]** As a result, a small to mid-sized practice may be able to implement more limited security policies and less intricate procedures than the government would typically expect from a hospital or other institutional provider. For instance, the physical safeguards might include using locked rooms/closets for equipment and media, as opposed to installing an electronic access system to data rooms. Training might entail reviewing a copy of policies and procedures with new hires and documenting the event, rather than holding a formal presentation.

A covered entity's obligation to implement security standards extends to its entire workforce, including individuals who perform billing functions (either in the practice or from home). These security restrictions must also be met by primary business associates and any subcontractor business associates.

(A) Protection of Electronic PHI.

The Security Rule works with the Privacy Rule by requiring a covered entity to assess the potential disclosure risks of **electronic** PHI (ePHI) and to maintain appropriate data security measures. The rule requires covered entities to:

> Ensure the confidentiality, integrity, and availability of all ePHI that the covered entity creates, receives, maintains, or transmits;
>
> Protect against any reasonably anticipated threats for hazards to the security or integrity of such ePHI;
>
> Protect against any reasonably anticipated, non-permitted uses, or disclosures of ePHI; and
>
> Ensure compliance with the rule by its workforce. **[56]**

As noted, the rule incorporates a flexible approach (scalability), allowing a covered entity to use any security measures that allow it to reasonably and appropriately implement the standards based on the size and infrastructure of the entity and a cost-risk analysis. **[57]**

Therefore, the first step in developing any security compliance plan is appointing a Security Officer. **[58]** Like the Privacy Officer, this person may have other duties or may exclusively function as the Privacy Officer. Next, the Security Officer must assess security needs and security gaps. Such a review, which may or may not require the assistance of an outside consultant, should examine the provider's practices for:

- The existence of policies;
- Compliance with policies;
- How information is shared;
- Who has access to information;
- Whether information is regularly backed-up;
- Whether proper contracts with business associates are in place; and

- How employees are trained, monitored, and sanctioned.

The Security Officer should then work with the appropriate parties to develop policies and procedures needed to implement the safeguards and to train the workforce accordingly. A covered entity must maintain, until six (6) years after the date of their creation or last effective date, written security policies and procedures, as well as written records of required actions, activities, or assessments. The covered entity must review and modify its security measures as needed to continue to provide reasonable and appropriate protection of ePHI. **[59]**

IX. HIPAA Enforcement Rule:

The Enforcement Rule contains provisions relating to compliance and investigations, the imposition of civil monetary penalties for violations of the HIPAA Administrative Simplification Rules, and procedures for hearings. **[60]**

HHS oversees compliance and enforces HIPAA's sanctions for noncompliance through Office for Civil Rights (OCR) and works with the Department of Justice (DOJ) for criminal sanctions. The beginning of the process is a complaint or compliance audit. A patient has a right to complain to the Secretary that a covered entity is not complying with HIPAA rules; however, this right is within the patient's discretion. **[61]** Yet, even without a complaint, the Secretary must conduct compliance reviews. **[62]**

The HIPAA Omnibus Rule has changed the enforcement provisions. Previously, the agency had discretion in choosing whether to investigate complaints or potential violation in cases where the Agency's preliminary review reveals a *possible* violation due to willful neglect. Now, the agency is ***required*** to initiate a formal investigation when a party appears to have exhibited willful neglect. If an investigation is performed, it may include a review of pertinent policies, procedures, or practices of the covered entity and the circumstances of the alleged violation. Documentation and evidence of compliance are key to ensuring no penalties and violations.

A review may determine that there was no violation, indicate a need to negotiate an informal resolution, or find there was a violation. If there is a violation and a civil monetary penalty is issued, the covered entity can seek an administrative appeal. If OCR finds evidence of potential criminal violations, the case will refer a matter to the DOJ for further investigation and possible criminal enforcement. Notably, HITECH strengthened HIPAA by extending penalties to business associates who are in violation of their business association agreements.

(A) Provider Cooperation is Required.

HIPAA requires cooperation if a covered entity is investigated for compliance or a complaint. First, a covered entity must provide records and compliance reports as necessary to enable the Secretary to determine if it has complied or is complying with the Act. Next, a covered entity must

cooperate with the Secretary's investigation. In this instance, it is often wise to involve counsel as early as possible. Finally, the entity must permit access during normal business hours to its pertinent facilities, books, records, accounts, and other sources of information. If there are exigent circumstances, such as records being hidden or destroyed, the Secretary does not need to wait for normal business hours. If information is exclusively controlled by another entity, the covered entity must make documented efforts to obtain the information. **[63]**

(B) Civil Money Penalties (CMPs):

The Secretary may impose civil money penalties (CMPs) on a covered entity if he or she determines that the entity has violated an Administrative Simplification Rule. **[64]** The action must commence within 6 years of the violation or the Secretary is barred from entertaining it. **[65]** A CMP is not an exclusive penalty. The HIPAA Omnibus Rule also makes a covered entity liable for the violations of its business associates that are its agents. It also adds a parallel provision providing for the liability of business associates for the acts of their subcontracting agents.

(C) Potential Civil Penalties and Criminal Sanctions.

HITECH amended HIPAA enforcement violations to include a tiered penalty structure and mandatory penalties for "willful neglect." As of 2009, HHS must base its penalty determination on the nature and extent of the violation and whether the violation has been corrected. HHS must also consider whether the violator knew he or she was committing a violation and the level of correction within the organization. The range of CMPs depends on whether an individual is a first time or a repeat violator. Agencies sometimes may waive or reduce an excessive penalty or may settle a case if the entity becomes compliant.

A	**45 C.F.R. § 160.404 (b)(2)(i): No Knowledge.** Applies if the covered entity or business associate did not know, and by exercising reasonable diligence would not have known, that the covered entity or business associate violated the law. The penalty ranges from $100 to $50,000 per violation, except that the total imposed on the person for all such violations of an identical requirement or prohibition during a calendar year may not exceed $25,000.
B	**45 C.F.R. § 160.404 (b)(2)(ii): Reasonable Cause.** Applies if the violation was due to reasonable cause and not to willful neglect. The penalty is $1,000 to $50,000 per violation, except that the total amount imposed on the person for all such violations of

an identical requirement or prohibition during a calendar year may not exceed $100,000.

C **45 C.F.R. § 160.404 (b)(2)(iii): Willful Neglect -- Corrected.** Applies for a violation in which it is established that the violation was due to willful neglect and was corrected during the 30-day period beginning the first date that the covered entity or business associate liable for the penalty knew, or, by exercising reasonable diligence, would have known that the violation occurred. The penalty is $10,000 to $50,000 per violation, except that the total amount imposed on the person for all such violations of an identical requirement or prohibition during a calendar year may not exceed $250,000.

D **45 C.F.R. § 160.404 (b)(2)(iii): Willful Neglect -- Not Corrected.** Applies if the violation was due to willful neglect and was not corrected during the 30-day period beginning on the first date the covered entity or business associate liable for the penalty knew, or, by exercising reasonable diligence, would have known that the violation occurred. The penalty is at least $50,000 per violation, except that the total amount imposed on the person for all such violations of an identical requirement or prohibition during a calendar year may not exceed $1.5 million.

Under the HIPAA Omnibus Rule, HHS does not have the authority to automatically impose the maximum CMP for any given violation. Rather, the Secretary may consider aggravating or mitigating factors when determining the penalty, including: **[66]**

(1) The nature of the violation, in light of the purpose of the rule violated;

(2) The circumstances, including the consequences of the violation, including:

The time period during which the violation occurred,
The number of individuals affected;
Whether the violation caused physical harm;
Whether the violation hindered or facilitated an individual's ability to obtain health care; and
Whether the violation resulted in financial harm;

(3) The degree of culpability of the covered entity, including but not limited to:

Whether the violation was intentional; and
Whether the violation was beyond the direct control of the covered entity;

(4) Any history of prior compliance with the Administrative Simplification provisions, including violations by the covered entity, including:

Whether the current violation is the same or similar to prior violations;
Whether and to what extent the covered entity has attempted to correct previous violations;
How the covered entity has responded to technical assistance from the Secretary provided in the context of the compliance effort; and
How the covered entity has responded to prior complaints;

(5) The financial condition of the covered entity, including:

Whether the covered entity had financial difficulties that affected its ability to comply;
Whether the imposition of CMPs would jeopardize the ability of the covered entity to continue to provide, or to pay for, health care; and
The size of the covered entity;

(6) Such other matters as justice may require.

X. Criminal Penalties Under HIPAA:

Depending on the facts, the wrongful use or disclosure of individually identifiable health information may give rise to criminal liability. Potential criminal cases are reviewed and prosecuted by the Department of Justice. Under the law, if a person knowingly and in violation of HIPAA:

(1) uses or causes to be used a unique health identifier;

(2) obtains individually identifiable health information relating to an individual; or

(3) discloses individually identifiable health information to another person, shall be punished as provided in subsection (b) of this section. For purposes of the previous sentence, a person (including an employee or other individual) shall be considered to have obtained or disclosed individually identifiable health information in violation of this part if the information is maintained by a covered entity (as defined in the HIPAA privacy regulation described in section 1320d-9 (b)(3) of this title) and the individual obtained or disclosed such information without authorization.**[67]**

Criminal penalties for a knowingly, wrongful disclosure of individually identifiable health information can include fines of not more than $50,000, imprisonment of not more than 1 year, or both. Additionally, if the offense is committed under false pretenses, a person can be fined not more than $100,000, imprisoned not more than 5 years, or both. If the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, a person may be fined not more than $250,000, imprisoned not more than 10 years, or both. **[68]**

If your organization is investigated by the OCR (or by a state entity charged with enforcing state privacy laws), it is essential that you engage qualified health care legal counsel to assist you in navigating through the complex response and settlement process. For a free consultation, give us a call at: (202) 298-8750.

[1] Ludwig Edelstein, The Hippocratic Oath: Text, Translation, and Interpretation (Johns Hopkins Press, 1943).

[2] The Privacy Act of 1974, codified at 5 U.S.C. § 552a, is discussed in detail on the U.S. Department of Justice website. It can be found at: https://www.justice.gov/opcl/privacy-act-1974

[3]The Health Insurance Portability and Accountability Act of 1996 (HIPAA), P.L. 104-191, 42 U.S.C. 1320d, available at https://www.gpo.gov/fdsys/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf. Although the initial driving impetus behind the passage of HIPAA was the need to improve the portability and continuity of health insurance coverage for individuals who change or lose their job, the statute is now generally thought of as medical privacy legislation. Less overtly, but with a substantial impact on the health care community, HIPAA allocated significant funding for the detection and deterrence of fraud, waste, and abuse in federal health care programs.

[4] 71 Fed. Reg. 8390, (Feb. 16, 2006), available at https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/privacyrule/finalenforcementrule06.pdf.

[5] 78 Fed. Reg. 5566, (Jan. 25, 2013), available at https://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf.

[6] 45 C.F.R. § 160.203.

[7] 45 C.F.R. § 160.202.

[8] 45 C.F.R. § 160.203(b). For example, under the Texas Medical Privacy Act (Chapter 181, Texas Health and Safety Code), the definition of “covered entity” is considerably more expansive than it is under HIPAA. Health care providers must review the medical privacy statutes in their

state to determine whether more stringent requirements may apply.

[9] 45 C.F.R. § 160.202.

[10] 45 C.F.R. § 160.203.

[11] 45 C.F.R. § 164.104.

[12] For additional information, see the Summary of the HIPAA Privacy Rule, available at **https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.**

[13] 45 C.F.R. § 164.105(a)(1).

[14] For a guide to entities covered under HIPAA, see https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/Downloads/CoveredEntitiesChart20160617.pdf.

[15] See 45 C.F.R. § 160.103.

[16] Id.

[17] 45 C.F.R. § 164.514(b).

[18] 45 C.F.R. § 164.500 *et seq.*

[19] 45 C.F.R. §§ 164.502(b) and 164.514 (d).

[20] 45 C.F.R. § 164.528(a). Please note that the Privacy Rule does not require accounting for disclosures either (a) for treatment, payment, or health care operations, or (b) to the individual or the individual's personal representative.

[21] 45 C.F.R. § 164.522.

[22] 45 C.F.R. § 164.520(b)(1)(iv).

[23] 45 C.F.R. § 164.524(a)(1). With the exception of psychotherapy notes and information complied in anticipation of a civil, criminal or administrative proceeding, an individual has a right of access to inspect and obtain a copy of protected health information about the individual that is in a designated records set, for as long as the information is maintained in the designated record set.

[24] 45 C.F.R. § 164.526.

[25] 45 C.F.R.§ 164.520(b)(1)(vi). A provider's Notice of Privacy Practices must include a

statement that individuals may complain to the covered entity and to the Secretary, HHS, if they believe their privacy rights have been violated. The notice must also include a brief description of how the individual may file a complaint with the covered entity, along with a statement that the individual will not be retaliated against for filing a complaint.

[26] 45 C.F.R. § 164.506(a).

[27] 45 C.F.R. § 164.510(a)(1)(i).

[28] 45 C.F.R. § 164.522(a)(1)(iv).

[29] 45 C.F.R. § 164.508(a)(2).

[30] 45 C.F.R. § 164.508.

[31] 45 C.F.R. § 164.501.

[32] 45 C.F.R. § 164.522(a)(1)(iv).

[33] 45 C.F.R. § 164.502(g)(1).

[34] 45 C.F.R. § 164.502(g)(3).

[35] 45 C.F.R. § 160.103.

[36] 45 C.F.R. § 164.512(a).

[37] 45 C.F.R. § 164.512(b).

[38] 45 C.F.R. § 164.512(c).

[39] 45 C.F.R. § 164.512(d).

[40] 45 C.F.R. § 164.512(e).

[41] 45 C.F.R. § 164.512(f).

[42] 45 C.F.R. § 164.512(g).

[43] 45 C.F.R. § 164.512(h).

[44] 45 C.F.R. § 164.512(i).

[45] 45 C.F.R. § 164.512(j).

[46] 45 C.F.R. § 164.512(k).

[47] 45 C.F.R. § 164.512(l).

[48] 45 C.F.R. § 164.520.

[49] 45 C.F.R. § 164.520(e).

[50] 45 C.F.R. § 164.530(i).

[51] 45 C.F.R. § 164.530(a)(1)(i).

[52] 45 C.F.R. § 164.530(b, e).

[53] 45 C.F.R. § 164.530(j)(2).

[54] 45 C.F.R. § 164.302 *et seq.*

[55] 45 C.F.R. § 164.306(b)(2).

[56] 45 C.F.R. § 164.306.

[57] 45 C.F.R. § 164.306.

[58] 45 C.F.R. § 164.308(2).

[59] 45 C.F.R. § 164.306(e).

[60] 45 C.F.R. § 160.300 *et seq.*

[61] 45 C.F.R. § 160.306.

[62] 45 C.F.R. § 160.308.

[63] 45 C.F.R. § 160.310.

[64] 45 C.F.R. § 160.402.

[65] 45 C.F.R. § 160.414.

[66] 45 C.F.R. § 160.408.

[67] 42 U.S.C. § 1320d–6(a).

[68] 42 U.S.C. § 1320d–6(b).