HIPAA Privacy, Security, Breach Notification, and Other Administrative Simplification Rules

A Lexis Practice Advisor® Practice Note by
Gabriel S. Marinaro, Katten Muchin Rosenman LLP


Gabriel S. Marinaro

This practice note discusses rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) impacting employers and the group health plans they sponsor. In particular, it covers HIPAA's (1) Privacy Rule and Security Rule, which are designed to ensure the confidentiality and integrity of, respectively, protected health information (PHI) and electronic PHI (ePHI); (2) Breach Notification Rule, which deals with breaches of PHI; and (3) Transactions Rule, which standardizes certain electronic transactions that involve health care data.

These are referred to collectively as the HIPAA Administrative Simplification provisions.

A wide range of parties involved in the provision of health care are subject to these rules, including many health plans, insurers, health care providers, third-party administrators, and others, both within and outside the context of employer group health plans. However, the focus of this note is the impact of these rules on employer-provided group health plans and their sponsoring employers.

This practice note is divided into the following main topics:

- Overview of Administrative Simplification Rules for Employers and Their Group Health Plans
- What Does the HIPAA Privacy Rule Require?
- What Are the Notice Obligations under the Privacy Rule?
- What Safeguards, Policies, and Procedures Are Needed for Privacy Rule Compliance?
- How Can PHI Be Used or Disclosed under the Privacy Rule?
- How Does the Privacy Rule Affect Information Sharing between an Employer and Its Group Health Plan?
- What Rights Do Individuals Have Regarding Their PHI?
- What Does the HIPAA Security Rule Require?
- What Rules Apply for Retaining Business Associates to Provide Services to a Plan?
- What Does the HIPAA Breach Notification Rule Require?
- What Does the HIPAA Transactions Rule Require?
- How Is HIPAA Enforced and What Penalties Apply?

OVERVIEW OF ADMINISTRATIVE SIMPLIFICATION RULES FOR EMPLOYERS AND THEIR GROUP HEALTH PLANS

The passage of HIPAA in 1996 (104 P.L. 191) brought about a host of reforms within the U.S. health care industry. In recognition of increasing threats to the privacy of individuals' health information posed by advances in information technology and the growing number of parties having access to such information, Congress included in HIPAA's Administrative Simplification rules a framework for protecting PHI from unauthorized access and disclosure.

The HIPAA Administrative Simplification rules, implemented under 42 U.S.C. §§ 1320d to 1320d-9, cover the following four areas, in addition to the related enforcement provisions:

- **Privacy standards for PHI.** The Privacy Rule requires implementation of appropriate safeguards to protect the privacy of an individual's PHI. It sets limits and conditions on the uses and disclosures of PHI without the individual's authorization. The Privacy Rule also gives individuals certain rights regarding their PHI. See part 160 and subparts A and E of part 164 of Code of Federal Regulations title 45 (45 C.F.R. §§ 160.101 to 160.550; 45 C.F.R. §§ 164.102 to 164.106; 45 C.F.R. §§ 164.500 to 164.534).
- **Security standards for ePHI.** The Security Rule provides security standards for access to and use of ePHI. See part 160 and subparts A and C of part 164 of Code of Federal Regulations title 45 (45 C.F.R. §§ 160.101 to 160.550; 45 C.F.R. §§ 164.102 to 164.106; 45 C.F.R. §§ 164.302 to 164.318).
- **Breach notification requirements.** The Breach Notification Rule sets forth actions required in the event of certain unauthorized uses or disclosures of unsecured PHI. See part 164, subpart D of Code of Federal Regulations title 45 (45 C.F.R. §§ 164.400 to 164.414).
- **Electronic transactions and code sets standards.** The Transactions Rule imposes standardization guidelines for electronic exchanges of health care data (known as transactions). Such transactions involve, for example, health care claims and payments, enrollment, premium payments, and coordination of benefits. See parts 160 and 162 of Code of Federal Regulations title 45 (45 C.F.R. §§ 160.101 to 160.550; 45 C.F.R. §§ 162.100 to 162.1902).

The U.S. Department of Health and Human Services (HHS) has primary responsibility for implementation and enforcement of the HIPAA Administrative Simplification mandates. HHS most recently revised the Privacy Rule, Security Rule, Breach Notification Rule and enforcement regulations in 2013 under the so-called Omnibus Rule, following legislative changes adopted under the Genetic Information Nondiscrimination Act of 2008 (GINA) and the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act). The Transactions Rule provisions were augmented under the Patient Protection and Affordable Care Act of 2010 (ACA), and rulemaking is still underway. A consolidated version of all Administrative Simplification final regulations issued to date is available on the HHS website.

What Is PHI and ePHI?

The Privacy Rule, Security Rule, and Breach Notification Rule are primarily concerned with PHI and/or ePHI. HIPAA broadly defines PHI as individually identifiable health information that is transmitted or maintained in any medium, and ePHI is a subset that comprises any PHI transmitted by or maintained in electronic media. 45 C.F.R. § 160.103 (definitions of "protected health information" and "electronic protected health information").

Individually identifiable health information is information that:

- Is created or received by a health care provider, health plan, employer, public health authority, life insurer,

school or university, or health care clearinghouse

- Relates to (1) the past, present, or future physical or mental health or condition (including genetic information) of an individual, (2) the provision of health care to an individual, or (3) the past, present, or future payment for the provision of health care to an individual –and–
- Identifies or could reasonably be used to identify the individual

45 C.F.R. § 160.103 (definition of "individually identifiable health information").

The PHI definition also excludes any individually identifiable information that:

- Is held by a covered entity (as defined in the next section) in employment records in its role as employer
- Consists of educational records covered by the Family Educational Rights and Privacy Act (see 20 U.S.C. § 1232g) –or–
- Concerns an individual who has been deceased for 50 or more years

45 C.F.R. § 160.103.

Entities Subject to HIPAA Rules

HIPAA's Administrative Simplification provisions generally apply to so-called covered entities and business associates. Covered entities include group health plans, health care clearinghouses (outside entities that process health information), and most health care providers. Business associates are service providers to covered entities that handle PHI. 45 C.F.R. § 160.103 (definitions of "covered entity" and "business associate").

Application of HIPAA Rules to Employers and the Group Health Plans They Sponsor

Employer sponsors of health plans generally are **not** considered covered entities or business associates under HIPAA. However, the group health plans they sponsor **are** covered entities. An exception applies for self-funded group health plans that do not use a third-party administrator and have fewer than 50 employees eligible to participate in the plan. Such plans are not covered entities because they are carved out from HIPAA's definition of group health plan. 45 C.F.R. § 160.103 (definition of "group health plan").

Employers that sponsor group health plans must ensure their group health plans (as covered entities) comply with applicable HIPAA requirements. Additionally, employers may be directly subject to some HIPAA Administrative Simplification provisions in their role as plan sponsor. For example, if an employer handles PHI to perform administrative functions for its plan(s) (e.g., reviewing benefit claims), then the employer needs to comply with any applicable HIPAA Administrative Simplification requirements, as discussed in this practice note.

HIPAA requirements impact group health plans and their employer sponsors in different ways depending on plan administration and whether the plan is self-funded (i.e., the employer funds benefit claims from its general assets) or is fully insured (i.e., the employer provides coverage through an insurance contract with a health insurance issuer or health maintenance organization (HMO)). For example:

Fully insured plans maintained by an employer with limited access to PHI. If an employer sponsors a fully insured group health plan and the plan and employer do not create or receive PHI, except for the limited information noted below (a so-called hands-off plan), then the plan and employer are exempt from most Privacy Rule requirements. The limited information that can be shared between a hands-off plan and the plan sponsor includes summary health information and participation and enrollment data. These exceptions are described

below in the sections entitled “Plan Enrollment Information” and “Disclosure of Summary Health Information for Settlor Functions” under How Does the Privacy Rule Affect Information Sharing between an Employer and Its Group Health Plan? Compliance with HIPAA Administrative Simplification provisions is significantly less onerous for hands-off plans.

Fully insured plans maintained by an employer with access to PHI. If an employer sponsoring a group health plan has access to PHI for any purpose other than limited participation and enrollment data and the plan has access to PHI, then the employer and the plan must fully comply with the relevant HIPAA Administrative Simplification requirements as a plan sponsor and covered entity, respectively.

Self-funded plans. An employer sponsoring a self-funded group health plan and the plan itself will also need to comply with relevant HIPAA Administrative Simplification provisions, whether or not it handles PHI. Even if the self-funded plan uses a third-party administrator for all plan administration functions, the employer is still obligated, for example, to ensure the plan satisfies applicable HIPAA requirements, such as putting in place HIPAA business associate agreements (described in the following section) with the third-party service provider operating the plan.

Further information on an employer sponsor’s HIPAA responsibilities can be found on the HHS website.

Business Associates

Under HIPAA, a business associate is any person or entity that, on behalf of a covered entity (such as a group health plan):

- Creates, receives, maintains, or transmits PHI for a function regulated by the HIPAA Administrative Simplification provisions, such as claims processing or administration, data analysis or processing, billing, and benefits management –or–
- Receives PHI in connection with providing legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for the covered entity

45 C.F.R. § 160.103 (definition of “business associate”).

However, each of the following persons is excluded from the business associate definition:

- Workforce personnel of the covered entity
- Health care providers receiving PHI concerning the treatment of individuals –and–
- Employer plan sponsors receiving PHI, if the conditions described below under How Does the Privacy Rule Affect Information Sharing between an Employer and Its Group Health Plan? are satisfied

Id.

A subcontractor of a business associate that handles PHI on behalf of the business associate is also considered a business associate for purposes of the HIPAA Administrative Simplification provisions. Id. However, a covered entity may treat a contractor who works at the covered entity’s facility and has more than incidental access to PHI either as a business associate or as a member of the covered entity’s workforce. 78 Fed. Reg. 5,566, 5,576 (Jan. 25, 2013). In the latter case, the business associate obligations would not apply and the contractor would not be subject to direct liability under HIPAA.

A group health plan (or other covered entity) that engages a third-party administrator or other service provider that will handle plan PHI must enter into a business associate agreement with the service provider. This agreement, among other things, requires the business associate to comply with the Privacy Rule and, to the extent that the PHI will be in electronic form, the Security Rule.

Business associates and business associate agreements are covered in more detail later in this practice note.

WHAT DOES THE HIPAA PRIVACY RULE REQUIRE?

A group health plan (or other covered entity) generally has the following obligations under the Privacy Rule:

- Provide individuals with a notice of privacy practices. 45 C.F.R. § 164.520.
- Adopt appropriate administrative, technical, and physical safeguards to protect the privacy of PHI and implement policies and procedures designed to comply with the Privacy Rule standards. 45 C.F.R. §§ 164.530(c)-(j).
- Designate a privacy officer to develop and implement the PHI policies and procedures. 45 C.F.R. § 164.530(a).
- Train workforce members on the PHI policies and procedures. 45 C.F.R. § 164.530(b).
- Use or disclose PHI only in accordance with the Privacy Rule standards. 45 C.F.R. §§ 164.502, 164.506, 164.508, 164.510, 164.512, 164.514.
- Ensure that all business associates are covered by a compliant business associate agreement. 45 C.F.R. § 164.504(e).
- Grant individuals the right to access their PHI, to amend incorrect PHI, and to receive an accounting of most PHI disclosures. 45 C.F.R. § 164.522, 45 C.F.R. § 164.524, 45 C.F.R. § 164.526, 45 C.F.R. § 164.528.

These rules are discussed in detail below, under What Are the Notice Obligations under the Privacy Rule?, What Safeguards, Policies, and Procedures Are Needed for Privacy Rule Compliance?, How Can PHI Be Used or Disclosed under the Privacy Rule?, How Does the Privacy Rule Affect Information Sharing between an Employer and Its Group Health Plan?, and What Rights Do Individuals Have Regarding Their PHI?

For information on enforcement of the Privacy Rule and the other Administrative Simplification requirements, see How Is HIPAA Enforced and What Penalties Apply?

WHAT ARE THE NOTICE OBLIGATIONS UNDER THE PRIVACY RULE?

Individuals have a right under HIPAA to receive a written notice describing (1) the uses and disclosures of PHI that may be made by a group health plan or other covered entity, (2) the individuals' rights regarding PHI, and (3) the covered entity's legal duties with respect to PHI. 45 C.F.R. § 164.520(a)(1). Specific requirements are described in the following sections.

Responsibility for and Delivery of the Notice

In the context of a group health plan, either the plan or the insurance issuer or HMO administering the plan is responsible for the notice:

- For self-funded plans, the plan must furnish the notice.

- For fully insured plans, the insurer or HMO must furnish the notice, and if the plan has access to PHI (other than summary health information and participation and enrollment data), the plan must maintain the current notice and provide it to covered individuals upon request.
- Hands-off plans (i.e., a fully insured plan where the plan does not create or handle PHI, except for summary health information and participation and enrollment data) do not need to maintain or furnish the notice; the notice obligation falls on the insurance provider or HMO.

45 C.F.R. § 164.520(a)(2).

It is sufficient to deliver the notice of privacy practices only to plan participants, on behalf of themselves and any family members receiving dependent coverage under the plan. 45 C.F.R. § 164.520(c)(1)(iii). The notice may be provided by e-mail to participants who consent to electronic notice in accordance with the rules under 45 C.F.R. § 164.520(c)(3).

Notice Content

The notice must be written in plain language and contain the elements set forth in the following subsections. HHS provides various forms of model notices for plans and for health care providers on its website.

Statement of Purpose

The notice must feature the following statement prominently displayed: “THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.” 45 C.F.R. § 164.520(b)(1)(i).

Description of Permitted Uses and Disclosures of PHI

The notice must describe in sufficient detail to put the individual on notice regarding:

- The types of uses and disclosures of PHI that the covered entity is permitted to make without the individual’s written authorization under the HIPAA Privacy Rule for treatment, payment, and health care operations and include at least one example
- Each of the other circumstances in which the covered entity is permitted or required to use or disclose PHI without the individual’s written authorization
- Any prohibition or material limitation applicable to any of the foregoing permitted uses or disclosures under other applicable law –and–
- Any types of uses and disclosures of PHI that require the individual’s authorization and how the individual can revoke such authorization

45 C.F.R. § 164.520(b)(1)(ii).

Separate statements and descriptions are needed (1) for any disclosures of PHI by the plan, insurer, or HMO to the employer plan sponsor, even if they are limited to disclosures of summary health information and participation and enrollment data, or (2) if the covered entity is permitted to contact participants for fundraising activities.

Additionally, if PHI is intended to be used for underwriting purposes, the notice must state that genetic information cannot be used for such purposes. 45 C.F.R. § 164.520(b)(1)(iii)(A)-(C). For details on the kinds of underwriting

activities that are subject to this prohibition, see the section below entitled "Prohibited Uses and Disclosures of PHI," under How Can PHI Be Used or Disclosed under the Privacy Rule?

Individuals' Rights Regarding PHI

The notice must contain a statement of the individual's rights with respect to PHI and a brief description of how to exercise them, specifically the rights to:

- Request restrictions on certain uses and disclosures of PHI (but not the right to compel the group health plan to agree to a requested restriction)
- Receive communications containing PHI in a manner reasonably requested to ensure confidentiality and safety
- Inspect and copy PHI
- Amend incorrect PHI
- Receive an accounting of certain disclosures of PHI –and–
- Obtain a paper copy of the notice from the group health plan upon request, even if the individual agreed to receive the notice electronically

45 C.F.R. § 164.520(b)(1)(iv).

Covered Entity's Responsibilities Regarding PHI

The notice must contain statements describing the covered entity's legal duties to (1) maintain the privacy of PHI, (2) provide notice of its legal duties and privacy practices regarding PHI, (3) notify individuals following a breach of unsecured PHI, and (4) abide by the terms of the notice currently in effect. In addition, in order to reserve the right to change a privacy policy set forth in the notice, the covered entity must include a statement that it is reserving that right and describe how it will furnish a revised notice in the event of a policy change. 45 C.F.R. § 164.520(b)(1)(v)(A)-(C).

Privacy Complaints and Contact for Further Information

Detailed information on how privacy complaints are handled is required, including a statement that retaliation for making a complaint is prohibited. The notice must also contain the name, title, and telephone number of a person or office to contact for further information about its contents. 45 C.F.R. § 164.520(b)(1)(vi), (vii).

Effective Date

The notice must set forth the date upon which it became effective. 45 C.F.R. § 164.520(b)(1)(viii).

When Does the Notice of Privacy Practices Need to Be Delivered?

Covered entities that are required to deliver the notice must do so to all plan participants at the time of their enrollment. In addition, no less frequently than once every three years, they must notify individuals then covered by the plan of the availability of the notice and how to obtain a copy. 45 C.F.R. § 164.520(c)(1)(i), (ii).

If the covered entity maintains a website for participants, the notice must be prominently posted and made available electronically through the website. 45 C.F.R. § 164.520(c)(3)(i).

In the event the notice is materially modified, the revised notice must be provided to participants within 60 days of the material revision. If the notice is posted on a website, the new notice must be posted as of the effective date of the change. 45 C.F.R. § 164.520(c)(1)(v).

WHAT SAFEGUARDS, POLICIES, AND PROCEDURES ARE NEEDED FOR PRIVACY RULE COMPLIANCE?

Generally, most group health plans must satisfy the Privacy Rule standards listed below. However, these rules do **not** apply to a hands-off plan (i.e., a fully insured plan where the plan does not create or handle PHI, except for summary health information and participation and enrollment data). 45 C.F.R. § 164.530(k).

Note: Although the term "plan" is used in the list because the focus of this practice note is on employer-provided group health plans, these rules apply to all types of covered entities (i.e., health care providers, health care clearinghouses in addition to group health plans) and in most cases business associates.

- **Safeguards.** The plan must have appropriate administrative, technical, and physical safeguards to (1) reasonably protect PHI from any intentional or unintentional use or disclosure in violation of the Privacy Rule, and (2) limit incidental uses or disclosures arising from an otherwise permitted use or disclosure. 45 C.F.R. § 164.530(c). These safeguards should be designed to protect PHI throughout its handling by the plan, from receipt or creation to destruction or disposal. Guidance regarding the disposal of PHI can be found on the HHS website.
- **Written privacy policies and procedures.** The plan must implement and maintain up-to-date written policies and procedures setting forth in detail privacy and security practices reasonably designed to ensure compliance with the Privacy Rule, taking into account the size and type of activities relating to PHI undertaken by the plan. The privacy policies and procedures provide detailed instructions for those members of the employer's workforce tasked with handling PHI. 45 C.F.R. § 164.530(i).
- **Privacy officer.** The plan must appoint a privacy official who is responsible for the development and implementation of the privacy policies and procedures and designate a contact person or office for receiving complaints under the Privacy Rule. 45 C.F.R. § 164.530(a).
- **Training.** The plan must train members of the employer's workforce on PHI privacy procedures as necessary and appropriate for them to carry out their functions for the plan. Each employee who will have access to PHI must receive training within a reasonable period of time after obtaining the relevant position. If there is a material change in the policies or procedures, additional training is required within a reasonable period of time after the material change becomes effective. 45 C.F.R. § 164.530(b).
- **Complaints.** The plan must provide a process for individuals to make complaints concerning the plan's privacy policies and procedures and document all complaints received and their disposition, if any. See 45 C.F.R. § 164.530(d).
- **Sanctions.** The plan must apply and document sanctions against workforce members who fail to comply with the privacy policies and procedures of the group health plan. 45 C.F.R. § 164.530(e).
- **Duty to mitigate.** The plan must mitigate any use or disclosure of PHI in violation of its policies and procedures or the Privacy Rule by the group health plan or any of its business associates. 45 C.F.R. § 164.530(f).
- **Documentation.** The plan must maintain written records of its policies and procedures and any communications, actions, activities, or designations required to be in writing under the Privacy Rule for a period of no less than six years. 45 C.F.R. § 164.530(j). Documentation standards also apply to hands-off plans, but only with respect to the plan document requirements described in the section entitled "Plan

Document and Certification Requirements" under How Does the Privacy Rule Affect Information Sharing between an Employer and Its Group Health Plan?

In addition, all group health plans (including hands-off plans) are prohibited from intimidating, coercing, discriminating against, or taking other retaliatory action against an individual for filing a complaint under the Privacy Rule or for exercising any other right granted to the individual under the Privacy Rule or Breach Notification Rule. And no group health plan (including hands-off plans) may require an individual to waive his or her HIPAA rights under the HIPAA Privacy Rule or Breach Notification Rule as a condition to receiving treatment or benefits under a plan or eligibility or participation in the plan. 45 C.F.R. § 164.530(g), (h).

HOW CAN PHI BE USED OR DISCLOSED UNDER THE PRIVACY RULE?

The following sections summarize the general rules for the use and disclosure of PHI under the Privacy Rule.

Permitted, Mandatory, and Prohibited Uses and Disclosures of PHI

The use and disclosure of PHI is strictly regulated so that covered entities and business associates may only use or disclose PHI as permitted or required by the Privacy Rule.

Permitted and Mandatory Uses and Disclosures of PHI

The following are permitted uses and disclosures (see cited regulations for further details on the rules governing the type of use or disclosure):

- Disclosures to the individual of their own PHI (45 C.F.R. § 164.502(a)(1)(i))
- Uses or disclosures for treatment, payment, or health care operations (45 C.F.R. § 164.506)
- Uses or disclosures incidental to a permitted or required use or disclosure (45 C.F.R. § 164.502(a)(1)(iii))
- Uses or disclosures specifically authorized or consented to by the individual (45 C.F.R. §§ 164.508, 164.510, 164.512)
- Certain disclosures for public purposes (e.g., as required by law, to address public health matters, to report on victims of abuse, neglect, or domestic violence, to facilitate authorized health oversight activities, for research, to facilitate military and other specialized government functions, among others) (45 C.F.R. § 164.512(a)-(l))
- Uses or disclosures of limited data sets (PHI that has been stripped of certain identifying information) for research, public health, or health care operations (45 C.F.R. § 164.514(e))
- Uses or disclosures of limited demographic information for certain fundraising activities (45 C.F.R. § 164.514(f))
- Uses and disclosures related to certain underwriting activities (45 C.F.R. § 164.514(g))

See 45 C.F.R. § 164.502(a)(1). For use and disclosure regulations specific to business associates, see 45 C.F.R. §§ 164.502(a)(3), (4).

Some disclosures are mandatory under HIPAA. These include disclosures to individuals exercising their right to access PHI and disclosures requested by HHS for audit reviews and investigations to ensure HIPAA compliance. 45 C.F.R. §§ 164.502(a)(2), (4).

Prohibited Uses and Disclosures of PHI

The following uses and disclosures are always prohibited:

- Uses or disclosures of genetic information for underwriting purposes (described below). 45 C.F.R. § 164.502(a)(5)(i).
- Sale of PHI (except as specifically permitted pursuant to an authorization by the individual). 45 C.F.R. § 164.502(a)(5)(ii).
- Disclosures by a group health plan to a plan sponsor for employment-related actions or decisions or in connection with any other employee benefit, unless an authorization is received from the individual. 45 C.F.R. § 164.504(f)(3)(iv).

The first item in the above list was added under the Genetic Information Nondiscrimination Act (GINA). The prohibition on the use of genetic information for underwriting purposes applies to any group health plan's use or disclosure of such information for the purposes of:

- Establishing rules for, or making determinations regarding, eligibility for participation or benefits under the plan
- The computation of premium or contribution amounts under the plan (including discounts, rebates, payments in kind, or other premium differential mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program)
- The application of any pre-existing condition exclusion under the plan, coverage, or policy –or–
- Other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits

45 C.F.R. § 164.502(a)(5)(i)(A).

Underwriting purposes do **not** include determinations of medical appropriateness where an individual seeks a benefit under the plan. 45 C.F.R. § 164.502(a)(5)(i)(B).

Notification of Uses and Disclosures

The notice of privacy practices (discussed above under What Are the Notice Obligations under the Privacy Rule?) must inform participants of all uses and disclosures of PHI that may be made by or on behalf of the group health plan.

Minimum Necessary Standard

All covered entities and business associates must limit the PHI they use or disclose (or request to be used or disclosed) to the minimum amount necessary to accomplish the intended purpose. 45 C.F.R. §§ 164.502(b), 164.514(d). This minimum necessary standard does not apply to:

- Disclosures requested or authorized by the individual
- Disclosures required by law or to comply with the Privacy Rule –or–
- Uses or disclosures by a health care provider for treatment.

45 C.F.R. § 164.502(b)(2).

Compliance with the minimum necessary standard requires the covered entity or business associate to (1) identify those persons or classes of persons in its workforce who need access to PHI to carry out their duties, (2) identify the specific PHI needed by each such person or class and any conditions appropriate to their access of the relevant PHI, and (3) make reasonable efforts to limit the access of PHI to the appropriate workforce members accordingly. 45 C.F.R. § 164.514(d)(2).

For a routine and recurring use and disclosure of (or request for) PHI, the covered entity or business associate must put in place practices and procedures designed to limit such uses or disclosures (or requests) to the PHI reasonably necessary to accomplish the intended purpose. Other uses and disclosures of (and requests for) PHI need to be evaluated on a case-by-case basis using criteria designed to achieve the same result. 45 C.F.R. § 164.514(d)(3).

Incidental Uses and Disclosures

Although the Privacy Rule allows uses and disclosures of PHI that are incident to a permitted use or disclosure, a group health plan must reasonably safeguard PHI against incidental use or disclosure. 45 C.F.R. § 164.530(c)(2). HIPAA does not define "incidental," but HHS guidance indicates the term includes accidental disclosures that cannot be prevented by reasonable safeguards. HHS HIPAA for Professionals FAQ.

For example, if an employee, in the performance of services for the plan, discusses a claim with a patient on the phone and is overheard by a colleague who is not authorized to handle patient information, such disclosure is a permissible incidental disclosure so long as the employee made reasonable efforts to avoid being overheard and reasonably limited the information shared. HHS HIPAA for Professionals FAQ.

HOW DOES THE PRIVACY RULE AFFECT INFORMATION SHARING BETWEEN AN EMPLOYER AND ITS GROUP HEALTH PLAN?

Group health plans subject to HIPAA are generally prohibited from sharing PHI with a plan sponsor, except in the limited circumstances described in the following sections. As noted below, in many cases, the group health plan must comply with certain plan document and certification requirements for the plan sponsor to be permitted to receive and handle PHI, but there are special cases where these requirements are not needed.

Disclosures for Plan Administrative Functions

Group health plans may disclose PHI to plan sponsor personnel who are involved in plan administration as a permissible use and disclosure—specifically, for treatment, payment, or health care operations. 45 C.F.R. §§ 164.504(f)(3)(i), 164.502(a)(1)(ii). Many employer administrative functions often fall within the payment category. This includes claim adjudication, billing and collection activities, and justification of charges. Others are covered by health care operations, which is defined to include legal and auditing services, management and administrative functions, and quality improvement activities. 45 C.F.R. § 164.501 (definitions of "payment" and "health care operations").

In addition to the generally applicable Privacy Rule regulations (such as the minimum necessary standard), the disclosure of PHI to the plan sponsor for plan administration usually requires that the plan document and certification requirements described in the following section are in place, which significantly increases the Privacy Rule and Security Rule burdens imposed on plan sponsors that handle PHI and ePHI. 45 C.F.R. §§ 164.504(f)(3)(i). Employer plan sponsors are not considered business associates when they perform these functions

(and so they are not subject to the rules for business associates). 45 C.F.R. §§ 160.103 (definition of "business associate").

Plan Document and Certification Requirements for Sharing PHI with Plan Sponsors

In order for a group health plan to share PHI with a plan sponsor (other than in the circumstances described in the following section), the plan documents must incorporate provisions that require the plan sponsor to do all of the following:

- Provide written certification to the plan prior to the disclosure of any PHI that the plan has been amended in accordance with these documentation requirements and the sponsor agrees to comply with them
- Comply and cause its agents to comply with the terms of the plan and applicable law with respect to the use and disclosure of PHI
- Refrain from using PHI for employment-related actions or decisions
- Report to the plan any use or disclosure other than those uses and disclosures authorized by the plan
- Facilitate the enforcement of individuals' rights regarding their PHI required under Privacy Rule
- Make its internal practices, books, and records relating to PHI available for a compliance audit or investigation by HHS
- Return or destroy PHI when no longer needed, to the extent feasible (and, if not feasible, limit further uses and disclosures of the PHI)
- Provide for adequate separation between the group health plan and the plan sponsor (i.e., "firewall" policies and procedures) to limit unauthorized access of PHI and document those policies and procedures in the plan in accordance with the regulations –and–
- If the sponsor will handle any ePHI, take reasonable steps to safeguard ePHI created, received, maintained, or transmitted to or by the sponsor, including by:
    - Implementing administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of the ePHI
    - Ensuring that the firewall policies and procedures referenced above include adequate ePHI security measures
    - Ensuring that any agents to whom it provides ePHI agree to take reasonable and appropriate security measures to protect the ePHI –and–
    - Reporting to participants any attempted or successful unauthorized access, use, disclosure, modification, or destruction of PHI or interference with system operations in an information system containing PHI

45 C.F.R. § 164.504(f)(2) (PHI provisions), 45 C.F.R. § 164.314(b)(2) (ePHI provisions).

These plan document and certification requirements are not required in certain limited circumstances, described in the following sections.

De-identified Information

De-identified information is not treated as PHI subject to the Privacy Rule restrictions. De-identified information is health information that does not contain (or has been stripped of) 18 specific identifiers relating to the individual

(or relatives, employers, or household members of the individual), such as names; geographic location at or below the level identified by the first three digits of a five-digit ZIP code; age; dates of birth, death, and other identifying events; telephone numbers; Social Security numbers; biometric data; and email and internet protocol addresses. Alternatively, information determined by professional statistical analysis to be de-identified can qualify. In either case, there can be no reasonable basis to believe that the information could be used to identify the individual. 45 C.F.R. §§ 164.502(d), 164.514.

Thus, a group health plan can share de-identified information that was generated from PHI with the plan sponsor without the need to comply with other Privacy Rule provisions, including the plan document and certification requirements discussed above.

Plan Participation and Enrollment Data

Transfer of Participation and Enrollment Data from the Plan (or Issuer or HMO) to the Employer

Enrollment and participation data is PHI subject to the Privacy Rule when it is created or received by a group health plan (or other covered entity) or any business associate. However, the Privacy Rule explicitly permits disclosure of participation and enrollment data by the group health plan (or health insurance issuer or HMO) to the plan sponsor, without the need to comply with the plan document and certification requirements discussed above. 45 C.F.R. § 164.504(f)(1)(iii) (corresponding Security Rule provision at 45 C.F.R. § 164.314(b)(1)). This permitted use is strictly limited to participation and enrollment data that does not include any substantial clinical information about the individual beyond what is situationally required by the electronic data interchange standard transaction for "Benefit Enrollment and Maintenance" (ASC X12B 834) 67 Fed. Reg. 53,181, 53,208 (Aug. 14, 2002).

Transfer of Participation and Enrollment Data from the Employer to the Plan (or Issuer or HMO)

Group health plan enrollment functions are often performed by the employer plan sponsor. In this role, the employer is acting on behalf of the participants, not the plan. Since the enrollment activities are not undertaken by or on behalf of a covered entity in this scenario, the Privacy Rule use and disclosure regulations do not apply when employers perform this function and transfer participation and enrollment data to the plan or health insurance issuer or HMO. 65 Fed. Reg. 82,462, 82,508 (Dec. 28, 2000).

Disclosure of Summary Health Information for Settlor Functions

A group health plan may disclose to the plan sponsor specific types of information that has been substantially de-identified, referred to as **summary health information**, to enable the sponsor to make decisions regarding the nature of coverage to be offered and plan implementation. Such disclosure is permitted, without the need to comply with the plan document and certification requirements discussed above, only for purposes of (1) obtaining insurer premium bids or (2) modifying, amending, or terminating the group health plan (so-called settlor functions). 45 C.F.R. § 164.504(f)(1)(ii) (corresponding Security Rule provision at 45 C.F.R. § 164.314(b)(1)).

Summary health information is defined as information that summarizes the claims history, claims expenses, or types of claims experienced by individuals, but that does not contain any of the 18 specific identifiers that must be removed to render information de-identified (except that geographic location data can be aggregated at the five-digit ZIP code level). 45 C.F.R. § 164.504(a).

Limited Data Sets

Under HIPAA, a limited data set is PHI with 16 specific identifiers removed that relate to the individual or relatives, employers, or household members of the individual. The 16 identifiers are similar to those that must be removed

to de-identify PHI, but limited data sets may include birth dates and other significant dates relating to the individual; geographic location information at the city/town, state or ZIP code level; and identifying numbers or codes that are not otherwise specifically prohibited. 45 C.F.R. § 164.514(e)(2).

Disclosure of limited data sets is permissible only for purposes of research, public health, or, as relevant for employer plan sponsors, health care operations. 45 C.F.R. § 164.514(e)(3). This is another means by which group health plans can disclose information to a plan sponsor that performs administrative functions. The regulations require that a data use agreement be put in place to restrict the use of the limited data set by the recipient. The agreement must meet the requirements set forth in 45 C.F.R. § 164.514(e)(4).

Since limited data sets are still considered PHI, the minimum necessary standard and other relevant Privacy and Security Rule provisions apply. In addition, there is no special exemption for limited data sets, so the plan documentation and certification requirements must be satisfied.

Disclosures of PHI Authorized by the Individual

Unless otherwise prohibited by the HIPAA privacy rule, disclosure of PHI is permissible, including disclosures to the employer plan sponsor, with the signed authorization of the individual to which the PHI relates, if all of the following conditions are met:

- **Form and content.** The authorization is (1) written in plain language, (2) dated, (3) signed by the individual or an authorized representative, (4) adequately describes the information to be used or disclosed, (5) identifies the person(s) or class of persons who are authorized to make the requested use or disclosure and to whom the requested use or disclosure will be made, (6) describes the purpose of the use or disclosure, and (7) sets forth an expiration date or event for the use or disclosure. 45 C.F.R. § 164.508(c)(1), (c)(3).
- **Required statements.** The authorization includes statements regarding (1) the individual's right to revoke the authorization, (2) the ability (if permitted) or inability to condition treatment, payment, enrollment, or eligibility for benefits on the authorization, and (3) the potential for the information to be subject to re-disclosure or to lose the protection of the Privacy Rule. 45 C.F.R. § 164.508(c)(2).
- **Veracity and documentation.** The covered entity is not aware of any fault or inaccuracy that would invalidate the authorization and properly documents and maintains records of the authorization. 45 C.F.R. § 164.508(b)(7).

A covered entity may not require an individual to authorize a use or disclosure of PHI as a condition for providing treatment, payment, enrollment, or eligibility under the plan, except in the very limited circumstances set forth in 45 C.F.R. § 164.508(b)(4). The most common exception provides that enrollment or eligibility for benefits may be conditioned on the individual's authorization of PHI disclosure sought for the purpose of making a relevant determination regarding eligibility, enrollment, underwriting, or risk rating. 45 C.F.R. § 164.508(b)(4)(ii).

WHAT RIGHTS DO INDIVIDUALS HAVE REGARDING THEIR PHI?

The Privacy Rule confers the following affirmative rights to individuals whose PHI is collected by a covered entity or business associate:

Right to request that use and disclosure of PHI be restricted. Individuals have a right to request that PHI not be used and disclosed for purposes of carrying out treatment, payment, or health care operations. Nevertheless, a group health plan generally does not need to agree to the request. One exception is that an individual who pays

for a health care item or service outside of the plan can forbid PHI disclosures pertaining solely to that item or service. 45 C.F.R. § 164.522.

Right to access and amend PHI. Covered entities and business associates must permit individuals to inspect any PHI relating to them that is maintained in the form of a designated record set. Each of the following constitutes a designated record set: (1) medical and billing records about individuals maintained by or for a health care provider, (2) a plan's enrollment, payment, claims adjudication, and case or medical management record systems, or (3) records used by or for a covered entity to make decisions about individuals. 45 C.F.R. § 164.501.

Exceptions to the access right apply for psychotherapy notes and information compiled in connection with a civil, criminal, or administrative action or proceeding. In addition, the covered entity responsible for incorrect PHI in a designated record set must make any amendments necessary to correct errors or omissions. For procedural rules concerning PHI access and amendments, respectively, see 45 C.F.R. §§ 164.524 and 164.526. HHS guidance for compliance with individuals' rights to access PHI can be found on its website.

Right to accounting of disclosures. Individuals have a right to an accounting of disclosures of their PHI made within the previous six years for certain purposes (other than disclosures made to the individual), including, among others, disclosures to carry out treatment, payment, and health care operations. The accounting must contain the date of the disclosure, the recipient of the PHI, a description of the information, and the purpose of the disclosure. Group health plans must maintain adequate records so that they can comply with participants' disclosure accounting requests. For related procedural rules, see 45 C.F.R. § 164.528.

WHAT DOES THE HIPAA SECURITY RULE REQUIRE?

The Security Rule generally requires covered entities and business associates to ensure the confidentiality, integrity, and availability of all ePHI that they create, receive, maintain, or transmit. Specifically, they must (1) protect against any reasonably anticipated threats or hazards to the security or integrity of any PHI that is maintained or transmitted in electronic form, (2) protect against any reasonably anticipated unauthorized uses or disclosures of such information, and (3) ensure compliance with the Security Rule by its workforce. 45 C.F.R. § 164.306.

For information on enforcement of the Security Rule and the other Administrative Simplification requirements, see How Is HIPAA Enforced and What Penalties Apply?

Note: Although the following discussion refers to plans because the focus of this practice note is on employer-provided group health plans, these rules apply to all types of covered entities as well as business associates.

Security Measures for Protecting ePHI

Group health plans may use any security measures that allow them to reasonably and appropriately implement the standards of the Security Rule. The following factors must be taken into account when determining what security measures are reasonable and appropriate:

- Size, complexity, and capabilities of the plan
- Technical infrastructure, hardware, and software security capabilities of the plan
- Costs of security measures –and–
- Probability and importance of potential risks to ePHI

The Security Rule sets forth standards for the protection of ePHI in the following areas: (1) administrative safeguards, (2) physical safeguards, (3) technical safeguards, (4) organizational requirements, and (5) policies and procedures. Each of these is briefly described in the following sections. Consult the relevant regulatory provisions for further details.

Most of the Security Rule standards have implementation specifications, which are categorized either as required or addressable. Required specifications are mandatory. For addressable specifications, the group health plan must assess whether the implementation specification is a reasonable and appropriate safeguard in its environment. An addressable implementation specification must be adopted if it is determined to be reasonable and appropriate; otherwise, the plan must document why it would not be reasonable and appropriate and implement an equivalent alternative measure if it would be reasonable and appropriate to do so.

Administrative Safeguards

- **Security management process.** Plans must implement policies and procedures to prevent, detect, contain, and correct security violations. The four implementation specifications are all required: (1) risk analysis to identify risks to ePHI, (2) risk management to reduce identified vulnerabilities, (3) sanctions policy enforcement to induce compliance by the workforce, and (4) periodic review of information system activity, such as audit logs, access reports, and security incident tracking. 45 C.F.R. § 164.308(a)(1); see also OCR, Risk Analyses vs. Gap Analyses—What Is the difference? for guidance on HIPAA risk analysis.
- **Security officer.** One required implementation specification for this standard requires plans to designate a security official responsible for the development and implementation of the security rule policies and procedures 45 C.F.R. § 164.308(a)(2).
- **Workforce security.** Plans must adopt policies and procedures to manage access to ePHI, including preventing access by individuals who do not have the requisite authority. The three implementation specifications are each classified as addressable. They relate to authorization and supervision of personnel who work with ePHI, personnel clearance procedures, and termination procedures when an individual's access to ePHI ends (e.g., at the end of employment). 45 C.F.R. § 164.308(a)(3).
- **Information access management.** Two addressable implementation specifications pertain to policies and procedures for authorizing access to ePHI (e.g., by establishing access via a computer workstation, program, or other mechanism and monitoring users' right to access). 45 C.F.R. § 164.308(a)(4).
- **Security awareness and training.** Four addressable implementation specifications regarding security awareness and training include (1) periodic security updates, (2) dealing with malicious software, (3) monitoring log-in attempts and reporting discrepancies, and (4) changing, creating, and safeguarding passwords. 45 C.F.R. § 164.308(a)(5).
- **Security incident procedures.** The single required implementation specification is to identify and respond to suspected and known security incidents, including mitigation of harm as well as documentation of security incidents and their outcomes. 45 C.F.R. § 164.308(a)(6).
- **Contingency planning.** Plans must establish policies and procedures for responding to events that could damage systems that contain ePHI. Required implementation specifications apply for data backup and recovery and emergency mode operation. Addressable specifications cover periodic testing and assessment of systemic functionality. 45 C.F.R. § 164.308(a)(7).
- **Evaluation.** This standard calls for periodic technical and nontechnical evaluation of the standards implemented under the Security Rule and in response to environmental or operational challenges affecting the security of ePHI. 45 C.F.R. § 164.308(a)(8). No implementation specifications are given for

this standard.

- **Business associates.** Plans may permit a business associate to create, receive, maintain, or transmit ePHI on the plan's behalf only after obtaining satisfactory assurances that the business associate will appropriately safeguard the ePHI, as documented in a business associate agreement. 45 C.F.R. § 164.308(b).

Physical Safeguards

- **Facility access and controls.** This standard deals with limiting physical access to ePHI and the facilities in which it is housed. Four addressable implementation specifications concern facility access during contingency plan operations, facility security, access control and validation, and maintenance of records relating to physical facilities. 45 C.F.R. § 164.310(a).
- **Workstation use and workstation security.** These standards concern policies and procedures regarding the nature and attributes of workstation(s) to be used to access ePHI and physical safeguards for such workstations. 45 C.F.R. § 164.310(b), (c). No implementation specifications are given for these standards.
- **Device and media controls.** Policies and procedures are required that govern the hardware and electronic media that contain ePHI. Two required implementation specifications address the final disposition of ePHI and the hardware or electronic media on which it is stored and the removal of ePHI from electronic media before the media are made available for re-use. Two addressable specifications concern tracking of hardware and electronic media used to access ePHI and data backup and storage. 45 C.F.R. § 164.310(d).

Technical Safeguards

- **Access control.** Technical policies and procedures are required for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights. Two required implementation specifications require unique user identification (e.g., traceable password protection) and emergency access procedures. Two addressable specifications cover automatic logoff and encryption of ePHI. 45 C.F.R. § 164.312(a).
- **Audit controls.** This standard calls for hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI. 45 C.F.R. § 164.312(b). No implementation specifications are given for this standard.
- **Integrity.** Electronic PHI must be protected from improper alteration or destruction. The single addressable implementation specification concerns electronic monitoring to corroborate the integrity of ePHI. 45 C.F.R. § 164.312(c).
- **Person or entity authentication.** This standard requires procedures to verify that a person or entity seeking access to ePHI is the one claimed. 45 C.F.R. § 164.312(d). No implementation specifications are given for this standard.
- **Transmission security.** Plans must implement technical security measures to guard against unauthorized access to ePHI that is transmitted over electronic communications networks. Two addressable implantation specifications concern prevention of improper modification and data encryption for ePHI transmission. 45 C.F.R. § 164.312(e).

Organizational Requirements

- **Business associate agreements.** This required implementation specification for this standard governs the mandatory provisions for such agreements. 45 C.F.R. § 164.314(a).
- **Plan document requirements.** As noted in the discussion under How Does the Privacy Rule Affect Information Sharing between an Employer and Its Group Health Plan? above, the plan documents of a group health plan must include certain provisions as a prerequisite before the plan is permitted to share PHI with the plan sponsor unless an exception applies. The required implementation specification here sets forth the plan documentation and certification requirements if the sponsor will receive or handle ePHI. 45 C.F.R. § 164.314(b).

Policies and Procedures and Documentation Requirements

- **Security Rule documentation.** Plans must maintain up-to-date written policies and procedures that are reasonable and appropriate to ensure Security Rule compliance, along with records of actions, activities, and assessments required by the Security Rule. The implementation specifications are required and provide that such records must be kept for at least six years after the last date they are in effect and be made available to HHS upon request as the agency determines is necessary in its compliance oversight role. 45 C.F.R. § 164.316.

WHAT RULES APPLY FOR RETAINING BUSINESS ASSOCIATES TO PROVIDE SERVICES TO A PLAN?

Under the Privacy Rule, covered entities may disclose PHI to a business associate (BA)—and may allow a BA to create, receive, maintain, or transmit PHI on its behalf—only if the covered entity obtains satisfactory assurances that the BA will appropriately safeguard the information. 45 C.F.R. § 164.502(e)(1). The Security Rule contains similar provisions for BAs that handle ePHI on behalf of a group health plan. 45 C.F.R. § 164.308(b).

Note: Although the following discussion refers to plans because the focus of this practice note is on employer-provided group health plans, these rules apply to all types of covered entities.

Business Associate Agreements

Group health plans must enter into a written business associate agreement (BAA) with their BAs that satisfies the Privacy Rule and Security Rule requirements summarized below. A plan is not required to obtain such assurances from a subcontractor to a BA (instead, the BA must represent that it will ensure that any of its subcontractors will comply with the applicable HIPAA regulations through a separate agreement between the BA and the subcontractor). 45 C.F.R. § 164.502(e)(1)(i), (ii).

The BAA must establish the exclusive uses and disclosures of PHI permitted and required by the BA and prohibit any others. This authorization may not exceed the scope of the Privacy Rule's permitted uses and disclosures discussed above, except the BAA may permit uses and disclosures (1) that are required for the BA's own proper management and administration, and/or (2) to provide data aggregation services relating to the health care operations of the group health plan. 45 C.F.R. § 164.504(e)(2)(i), (ii)(A).

The BAA must also provide that the BA will:

- Use appropriate safeguards for ePHI and comply with the Security Rule
- Report to the group health plan any use or disclosure of the information not provided for by the BAA of

which it becomes aware

- Ensure that any subcontractors that handles the plan's PHI on behalf of the BA observe the same restrictions and conditions that apply to the BA with respect to such information
- Facilitate compliance with individuals' rights under HIPAA to access and amend their PHI, and receive an accounting of PHI disclosures, with respect to PHI created or maintained by the BA
- To the extent the BA is to carry out a HIPAA obligation of the plan, comply with the requirements of Privacy and Security Rule provisions that apply to the plan
- Make available to HHS the BA's internal practices, books, and records relating to the use and disclosure of relevant PHI for purposes of the agency's HIPAA compliance oversight role –and–
- At termination of the contract, return or destroy all relevant PHI that the BA still maintains, and if such return or destruction is not feasible, then extend the protections of the contact to the information and limit any further uses and disclosures that make the return or destruction of the information infeasible

45 C.F.R. § 164.504(e)(2)(ii)(B)-(J).

BAA provisions must also authorize the termination of the contract by the group health plan if the plan determines that the BA has violated a material term of the contract. In fact, if the group health plan knows of a pattern of activity or practice of the BA that constitutes a material breach or violation of the BA's obligation under the BAA, the group health plan must take reasonable steps to cure the breach or end the violation. If such steps are unsuccessful, the plan must terminate the BAA, if feasible. 45 C.F.R. § 164.504(e)(1), (e)(2)(iii).

HHS has provided sample language for BAAs on its website.

Recent Changes in Business Associate Rules

The Omnibus Rule expanded the scope and obligations of BAs as of 2013, pursuant to the HITECH Act. See 78 Fed. Reg. 5,566, 5,570 (Jan. 25, 2013). Notably:

- The definition of business associate was clarified and certain entities expressly included (e.g., a data transmission service acting for a covered entity if the service has routine access to PHI). 45 C.F.R. § 160.103.
- All BAs are now directly subject to all aspects of the Security Rule, specified provisions of the Privacy Rule (including the minimum necessary standard), and new Breach Notification Rule requirements (previously, their obligations were predominately contractual under the BAA), and are therefore subject to compliance audits and potentially liable for civil money penalties and other enforcement measures for noncompliance. 45 C.F.R. §§ 164.104(b), 164.302, 164.500(c).
- Any subcontractor that creates, receives, maintains, or transmits PHI on behalf of a BA is now treated a BA in its own right. As a result:
    - BAs must enter into a BAA with such subcontractors similar to those between a covered entity and the BA. 45 C.F.R. §§ 164.314(a)(2)(iii), 164.504(e)(2).
    - The subcontractor is directly regulated as a BA and is therefore subject to compliance audits and potentially liable for civil money penalties and other enforcement measures for noncompliance. 45 C.F.R. § 160.103 (definition of "business associate").
    - If the subcontractor retains a second subcontractor that creates, receives, maintains, or transmits PHI

on behalf of the first subcontractor, the second subcontractor would also be a BA (and so on down the line). 45 C.F.R. § 160.103 (definition of "subcontractor").

WHAT DOES THE HIPAA BREACH NOTIFICATION RULE REQUIRE?

The HITECH Act established breach notification requirements for covered entities and business associates. See 45 C.F.R. §§ 164.400 to 164.414. In the event of certain breaches of unsecured PHI (generally meaning PHI that has not been encrypted), the covered entity must notify the individual(s) whose PHI has been compromised, report the breach to HHS, and, in case of a large breach, notify the media. In 2013, HHS issued final regulations for the Breach Notification Rule, modifying and supplementing the 2009 interim final regulations. 78 Fed. Reg. 5,638.

For information on enforcement of the Breach Notification Rule and the other Administrative Simplification requirements, see How Is HIPAA Enforced and What Penalties Apply?

Determining Whether the Breach Notification Rules Are Triggered

A "breach" is defined as the use or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule, unless one of three exceptions applies (described under "Step 2" below), and the security or privacy of the PHI is compromised as a result. 45 C.F.R. § 164.402. Therefore, when dealing with a potential breach of PHI or ePHI, work through the following questions to determine if the notification requirements are triggered:

(1) Has there been an unauthorized use or disclosure of unsecured PHI?

(2) If so, is there an applicable exception?

(3) If there is no exception, did the use or disclosure cause the PHI to be compromised, applying a risk assessment as described below?

Step 1. Determine whether PHI has been acquired, accessed, used, or disclosed other than in accordance with the privacy rule. For example, some incidental uses and disclosures are treated as permitted under these rules. Remember that PHI that has been encrypted is not considered unsecured PHI, so disclosures of encrypted PHI do not trigger the notice requirements.

Even if an incident does not constitute a breach for purposes of the Breach Notification Rule, actions may be required by a covered entity or business associate to comply with policies and procedures adopted in accordance with the Privacy Rule or Security Rule.

Step 2. Determine whether any of the following exceptions to the HIPAA breach definition apply:

- **Unintentional internal acquisition, access, or use.** Any unintentional acquisition, access, or use of PHI by a workforce member of a covered entity or business associate that is made in good faith and within the individual's scope of authority and does not result in further unauthorized use or disclosure.
- **Inadvertent internal disclosure.** Any inadvertent PHI disclosure by a person who is authorized to access the PHI at a covered entity or business associate to another person authorized to access PHI (of the same or a different type as the disclosed PHI) at the same group health plan or business associate (or pursuant to an organized health care arrangement in which the covered entity participates), and the information received as a result of such disclosure is not further used or disclosed.

- **Disclosure without reasonable opportunity for retention.** A disclosure of PHI where the relevant covered entity or business associate has a good faith belief that the unauthorized person(s) to whom the disclosure was made would not reasonably have been able to retain such information. In addition to fleeting disclosures, the preamble to the final regulations suggests this exception could apply if PHI were mailed to an incorrect address and returned unopened so that no unauthorized person would reasonably be able to retain the information.

45 C.F.R. § 164.402(1)(i)-(iii); 78 Fed. Reg. 5,640.

Step 3. If there has been an unauthorized use or disclosure and none of the exceptions apply, Step 3 is to determine whether the PHI has been compromised. Any unauthorized use or disclosure of unsecured PHI is presumed to be a breach under the Breach Notification Rule unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

(1) The nature and extent of the PHI involved, including the types of identifiers and the likelihood for re-identification

(2) The unauthorized person who used the PHI or to whom the disclosure was made

(3) Whether the PHI was actually acquired or viewed

(4) The extent to which the risk to the PHI has been mitigated

45 C.F.R. § 164.402(2).

This “low probability of compromise” standard replaces the “significant risk of harm” standard applicable under the superseded interim final regulations. The following paragraphs provide guidance on the four factors noted above. For more information, see 78 Fed. Reg. 5,639.

First factor: nature and extent of the PHI involved. Consider the type of data in the PHI involved in the impermissible use or disclosure and whether the disclosure involved information that is of a more sensitive nature (sensitive information may include, e.g., financial information, certain medical diagnoses, history of substance abuse, etc.). Also consider the type of identifiers in the PHI and the likelihood that it can be linked to the individual, using not only the data in the PHI but also any other available information.

Second factor: unauthorized recipients of the PHI. Who impermissibly used or received the PHI? Consider whether the unauthorized recipient has obligations to protect the privacy and security of the information. For example, if PHI is impermissibly disclosed to another entity required to abide by the HIPAA Privacy and Security Rules, there may be a lower probability that the PHI has been compromised since the recipient of the information is obligated to protect the privacy and security of the information in a similar manner as the disclosing entity. This factor should also be considered with regard to the risk of re-identification. If the information impermissibly used or disclosed is not immediately identifiable, determine whether the unauthorized person who received the PHI could reasonably be able to link the information to the individual, using not only the data in the PHI but also any other available information.

Third factor: was the PHI acquired or viewed? Did the impermissible use or disclosure result in PHI actually being acquired or viewed by an unauthorized person or was there only an opportunity to do so? For example, if a

stolen laptop computer is later recovered and a forensic analysis shows that the PHI on the computer was never accessed, viewed, acquired, transferred, or otherwise compromised, the entity might reasonably conclude there is a low probability that PHI was compromised.

Fourth factor: to what extent has risk to the PHI been mitigated? When a PHI breach or other security incident occurs, it is often necessary to attempt to mitigate the risks of harm arising from the incident in accordance with the Privacy and Security Rules. This might include obtaining the unauthorized recipient's satisfactory assurances (e.g., through a confidentiality agreement) that the information will not be further used or disclosed and will be or has been returned or destroyed. Consider the extent and efficacy of all mitigation efforts when determining the probability that the PHI has been compromised.

Adequate documentation of the breach assessment procedures is important since the covered entity or business associate has the burden of proof in the event the determination that an incident does not constitute a breach is challenged. Also, if there is a breach of PHI, the covered entity or business associate must retain records sufficient to demonstrate its compliance with the applicable notification requirements discussed in the following subsections.

Notification Requirements upon Discovery of a Breach of PHI

The covered entity is responsible for fulfilling the notification requirements described in this section following the discovery of a breach of unsecured PHI. Covered entities must be vigilant in their PHI privacy and security procedures because they are deemed to have discovered a breach if the breach would have become known to them through the exercise of reasonable diligence by the covered entity or any of its workforce members or agents (other than the person committing the breach). 45 C.F.R. § 164.404(a)(2). Therefore, penalties may be imposed in cases where a breach is not actually known to the covered entity or the covered entity improperly determines that an incident does not constitute a breach under the Breach Notification Rule.

Note: Although the term "plan" is used in the following discussion because the focus of this practice note is on employer-provided group health plans, these rules apply to all types of covered entities.

Notice to Individuals

In all cases, the plan must notify each individual whose unsecured PHI has been, or is reasonably believed to have been, used or disclosed as a result of the breach. The notice must be made without unreasonable delay and in no case later than 60 days after discovery (unless otherwise ordered by law enforcement officials). 45 C.F.R. § 164.404(b).

The notice must be written in plain language and include:

- A brief description of what happened, including the date of the breach and the date of the discovery of the breach
- A description of the types of unsecured PHI that were involved in the breach
- Any steps individuals should take to protect themselves from potential harm resulting from the breach
- A brief description of what the group health plan is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches –and–
- Contact procedures for individuals to ask questions or learn additional information

45 C.F.R. § 164.404(c).

Notice must be provided by first-class mail at the last known address of the individual or may be sent by e-mail if the individual agrees to electronic notice. If the individual is deceased, notice is to be sent to the individual's next of kin or personal representative if the plan has their address. 45 C.F.R. § 164.404(d)(1).

For special rules allowing a substitute form of notice when insufficient or out-of-date address information precludes written notification, see 45 C.F.R. § 164.404(d)(2).

Notification to the Media

For a breach of unsecured PHI involving more than 500 residents of a state or jurisdiction, the plan must notify prominent media outlets serving the state or jurisdiction in accordance with the timing and contents requirements described above for the notice sent to affected individuals. 45 C.F.R. § 164.406.

Notification to HHS

For breaches of unsecured PHI involving 500 or more individuals, the plan must notify HHS contemporaneously with the notification made to the affected individual(s). Breaches of unsecured PHI involving fewer than 500 individuals must be reported annually by the plan within 60 days after the end of each calendar year. HHS notification is to be furnished in the manner specified on the agency's website. 45 C.F.R. § 164.408.

If a Business Associate Discovers a Breach of PHI

If a business associate discovers a breach of unsecured PHI that it is handling on behalf of a group health plan (or other covered entity), the business associate is required to notify the plan without unreasonable delay and in no case later than 60 days after discovery of the breach. 45 C.F.R. § 164.410(b).

The notification by the business associate must include the identification of each individual whose unsecured PHI has been or is reasonably believed to have been impermissibly used or disclosed. The business associate must also provide the plan any other information the plan is required to include in its notification to affected individuals. 45 C.F.R. § 164.410(c).

Business associates, like covered entities, are deemed to have discovered a breach if the breach would have become known to them through the exercise of reasonable diligence by the business associate or any of its employees, officers, or agents (other than the person committing the breach). 45 C.F.R. § 164.410(a)(2).

WHAT DOES THE HIPAA TRANSACTIONS RULE REQUIRE?

The Transactions Rule requires covered entities and their business associates to comply with rules to facilitate the electronic data interchange (EDI) of health care data when conducting certain transactions (so-called standard transactions). Standard transactions involve the electronic exchange of health care data among covered entities (or business associates), e.g., when a health care provider sends a claim via e-mail or the internet to a health plan or insurance company to request payment for medical services. Among the purposes of the Transactions Rule is to improve the efficiency and effectiveness of health care delivery by encouraging the widespread use of standardized EDI formats and procedures.

As described in further detail below, the Transactions Rule requirements cover the following areas (as updated under the ACA):

- **Standard transactions and operating rules.** Identification of standard transactions and adoption of standards (including applicable implementation specifications) and operating rules for each of the standard transactions.
- **Code sets.** Establishment of uniform code sets for diagnoses, procedures, prescription drugs, and other data elements to be used in the standard transactions.
- **Standard identifiers.** A system for assigning unique identifiers for health plans and health care providers, which must be used for all standard transactions.
- **Compliance certification for health plans.** Plan certification procedures regarding compliance with certain standards and operating rules.
- **Certification noncompliance penalties.** Penalties for health plans that fail to comply with the Transactions Rule certification compliance.

45 C.F.R. §§ 162.100 to 162.1902; 42 U.S.C. § 1320d-2(j).

The Centers for Medicare & Medicaid Services (CMS) has been charged with the administration and enforcement of the Transactions Rule provisions. 68 Fed. Reg. 60,694 (Oct. 23, 2003).

Standard Transactions and Operating Rules

Standard Transactions

The currently identified standard transactions are:

- Health claims or encounter information (see 45 C.F.R. part 162, subpart K)
- Eligibility for a health plan (see 45 C.F.R. part 162, subpart L)
- Referral certification and authorization (see 45 C.F.R. part 162, subpart M)
- Health claim status (see 45 C.F.R. part 162, subpart N)
- Enrollment and disenrollment in a health plan (see 45 C.F.R. part 162, subpart O)
- Electronic funds transfers and remittance advice (modified under the ACA, includes payments by plans to providers and related information) (see 45 C.F.R. part 162, subpart P)
- Health plan premium payments (see 45 C.F.R. part 162, subpart Q)
- Coordination of benefits (see 45 C.F.R. part 162, subpart R)
- Medicaid pharmacy subrogation (see 45 C.F.R. part 162, subpart S)
- Health claims attachments (standards yet to be adopted)
- First report of injury (standards yet to be adopted)

42 U.S.C. § 1320d-2(a)(2).

The mandatory standards for the standard transactions may contain rules for data content limitations, data condition requirements (i.e., circumstances where specific data elements must be used), and format requirements. 42 U.S.C. § 1320d(7). A process for covered entities to request permission to test a proposed modification to a standard is also available. 45 C.F.R. § 162.940.

Operating Rules

To further the uniformity goals of the Transactions Rule, the ACA required HHS to establish "operating rules" for each of the standard transactions. Operating rules set forth business rules and guidelines for the electronic exchange of information not defined by the standards or their implementation specifications. 42 U.S.C. § 1320d(9).

HHS assigned the task of developing the operating rules to the Counsel for Affordable Quality Healthcare Committee on Operating Rules for Information Exchange (CAQH CORE), a collaboration of more than 130 stakeholder organizations. See 79 Fed. Reg. 298, 299 (Jan. 2, 2014). CAQH CORE's Phase I-III operating rules have been finalized, and the compliance deadlines for those rules have passed

On September 23, 2015, CAQH CORE announced its adoption of the Phase IV CAQH CORE operating rules, which focus on infrastructure requirements for data exchange relating to the standard transactions for health claims or encounter information; referral certification and authorization; health plan premium payments; and enrollment and disenrollment in a health plan. HHS is expected to issue a proposed rule for Phase IV operating rules in 2016.

See the CAQH CORE website for further information.

Code Sets

Code sets are standardized codes and descriptors for various elements used in the standard transactions. The code sets adopted by HHS include standardization systems established and maintained by various entities, such as CMS (the Health Care Common Procedure Coding System), the American Medical Association (Current Procedure Terminology codes), and the CDC (International Classification of Diseases), among others. For more information, see the CMS website.

Standard Identifiers

Health Plan Identifier

Final regulations adopted in 2012 require all controlling health plans (i.e., plans that control their own business activities, actions, or policies, or are controlled by entities that are not health plans) to obtain a ten-digit Health Plan Identifier (HPID) and use their HPID for all standard transactions. 45 C.F.R. §§ 162.510, 162.512. HPIDs can be obtained from the CMS enterprise portal website by registering for the Health Insurance Oversight System (HIOS).

However, in 2014, the HHS advisory body, the National Committee on Vital and Health Statistics, recommended that HHS revisit the HPID policy and not require HPIDs for standard transactions in light of the national payer identifier system that has become widespread in the industry. CMS announced a delay in the enforcement of the HPID standards until further notice while HHS reconsiders the current rules.

Other Identifiers

The Transactions Rule establishes a separate identifier—the national provider identifier (NPI)—for health care providers and health care clearinghouses. 45 C.F.R. §§ 162.406, 162.408. Employers are identified by their Employer Identification Number (EIN) issued by the Internal Revenue Service. 45 C.F.R. § 162.605. Other entities may use an Other Entity Identifier (OEID). 45 C.F.R. § 162.514.

Compliance Certification for Health Plans

The ACA requires all controlling health plans to attest to HHS that they have obtained certification of compliance with seven standard transactions. These include standard transactions for electronic funds transfers, eligibility for a health plan, health claim status, and health care payment and remittance advice. 42 U.S.C. § 1320d-2(h)(1)(A). The statutory penalty for failing to comply with the certification requirement is $1 (adjusted as noted below) per covered life for each day that the plan is not in compliance until certification is complete, capped at $20 per covered life under the plan. The amount is increased annually by the percentage increase in total national health care expenditures, as determined by HHS. 42 U.S.C. § 1320d-2(j)(1)(A) to (E).

However, no certification program has yet been implemented and the rule remains unenforced pending further agency action. HHS issued proposed regulations for the certification process in 2014 (79 Fed. Reg. 298), but subsequently withdrew them to further examine issues raised in the public comment process and investigate alternative approaches. 82 Fed. Reg. 46,182 (Oct. 4, 2017).

The proposed regulations would have established two options to meet the certification requirements: obtaining a "HIPAA Credential" under a process to be administered by CAQH CORE, or receiving "CORE Certification" from CAQH CORE under its existing "CORE Seal" program. As mentioned above, CAQH CORE currently offers CORE Seal certification for Phase I, II, and III. Phase IV is currently under development. For more information, see the CAQH CORE website.

Group health plans will need to monitor additional guidance from HHS and CMS regarding certification compliance.

The statutory penalty fee is $1 (adjusted as noted below) per covered life for each day that the plan is not in compliance with the requirement until certification is complete, not to exceed $20 per covered life under the plan. The $1 penalty fee amount is increased on an annual basis by the annual percentage increase in total national health care expenditures, as determined by HHS. 42 U.S.C. § 1320d-2(j)(1)(A) to (E).

A health plan that knowingly provides inaccurate or incomplete information in a statement, certification, or documentation of compliance is subject to a penalty of double the amount that would otherwise apply (with a cap of $40 per covered life under the plan). 42 U.S.C. § 1320d-2(j)(1)(C).

The ACA also provides that HHS shall conduct periodic audits to ensure that health plans are in compliance with the Transactions Rule's standards and operating rules. 42 U.S.C. § 1320d-2(h)(6).

CMS has been delegated the authority to investigate complaints of noncompliance with, and to make decisions regarding the interpretation, implementation, and enforcement of, Transactions Rule provisions. To date, the CMS enforcement strategy has been to provide technical assistance and seek the cooperation of all parties to the complaint, to help achieve compliance. CMS is still in the process of developing compliance audit processes and potential non-compliance penalties. See CMS Website.

Basic Transactions Rule Requirements for Health Plans

Following is a summary of the principal Transaction Rule obligations for health plans:

- Obtain an HPID if it is a "controlling health plan" (enforcement delayed pending further HHS action). 45 C.F.R. § 162.512.

- Conduct transactions among covered entities as a standard transaction. 45 C.F.R. § 162.923(a).
- Comply with a covered entity's request to conduct a transaction as a standard transaction. 45 C.F.R. § 162.925(a)(1).
- Not delay or reject a transaction, or attempt to adversely affect another entity or the transaction, because the transaction is a standard transaction. 45 C.F.R. § 162.925(a)(2).
- Not reject a standard transaction on the basis that it contains data elements not needed or used by the health plan (e.g., coordination of benefits information). 45 C.F.R. § 162.925(a)(3).
- Not offer an incentive for a health care provider to conduct a standard transaction as a direct data entry transaction described under 45 C.F.R. § 162.923(b), which permits an exception to the format requirements for standard transactions. 45 C.F.R. § 162.925(a)(4).
- Store any coordination-of-benefits data it needs to forward to another health plan (or other payer) to undertake a standard transaction where benefits are coordinated with them. 45 C.F.R. § 162.925(b).
- Not enter an agreement with another covered entity that would (1) change the definition, data condition, or use of a data element or segment in a standard or operating rule, (2) add any data elements or segments to the maximum defined data set for a transaction, (3) use any code or data elements that are not used in an implementation specification, or (4) change the meaning or intent of an implementation specification. 45 C.F.R. § 162.915(a).
- Keep code sets for the current billing period and appeals periods still open to processing under the plan's terms of coverage. 45 C.F.R. § 162.925(c)(1).
- Use the data code sets that are valid at the time the health care is furnished (for medical data) or the time the data exchange transaction is initiated (for non-medical data). 45 C.F.R. § 162.925(c)(2).
- Require any business associate used to conduct its standard transactions (and any subcontractor of the business associate) to comply with all applicable HIPAA Administrative Simplification requirements. 45 C.F.R. § 162.923(c).
- Certify compliance with certain standard transaction standards and operating rules, as described above (enforcement delayed pending issuance of final regulations). 42 U.S.C. § 1320d-2(h)(6).

Group health plans commonly use business associates to handle standard transactions or utilize a clearinghouse to assist in Transactions Rule compliance. Nevertheless, as noted above, the plan itself will have responsibilities under these provisions, including obtaining a HPID and compliance certification.

Transaction Rule Enforcement

CMS has been delegated the authority to investigate complaints of noncompliance with, and to make decisions regarding the interpretation, implementation, and enforcement of, Transactions Rule provisions. To date, the CMS enforcement strategy has been to provide technical assistance and seek the cooperation of all parties to the complaint, to help achieve compliance. See the CMS website.

HOW IS HIPAA ENFORCED AND WHAT PENALTIES APPLY?

Administrative Simplification enforcement provisions are found in 45 C.F.R. part 160, subparts C, D, and E.

The Office for Civil Rights at HHS (OCR) is responsible for enforcing the Privacy, Security, and Breach Notification Rules. Enforcement authority and penalties were increased under the HITECH Act, and OCR investigative activity has increased since that time. While the general rules governing enforcement discussed below also cover

Transaction Rule violations, oversight and enforcement of those rules has been delegated to CMS, as noted in the previous section.

OCR Investigations

Enforcement action by OCR can arise from complaints made to HHS or from a compliance review initiated by OCR. HIPAA grants individuals a right to file complaints regarding compliance with the Administrative Simplification rules. 45 C.F.R. § 160.306. The HHS website contains helpful information on the complaint process and OCR investigations, summarized in the following paragraphs.

An OCR investigation may include a review of the pertinent policies, procedures, or practices of the group health plan (or other covered entity or business associate) and of the circumstances regarding any alleged violation. Covered entities and business associates are required to cooperate with complaint and compliance investigations, including by making available their facilities, books, records, accounts, and other sources of information that are pertinent to the investigations. HHS may issue subpoenas to require the attendance and testimony of witnesses and the production of any other evidence during an investigation or compliance review. OCR may refer the complaint to the department of justice if the investigation reveals a violation of the criminal provisions of HIPAA.

Upon determining that a HIPAA violation occurred, OCR will attempt to resolve the case. Most privacy and security rule violations are resolved through an arrangement between OCR and the covered entity or business associate providing for voluntary compliance, corrective action, and/or entering into a resolution agreement.

If the non-compliant party does not take action to resolve the matter in a manner satisfactory to OCR, OCR may decide to impose civil money penalties after providing the covered entity or business associate an opportunity to submit written evidence of any mitigating factors or affirmative defenses. The covered entity or business associate may request a hearing to object to the imposition of penalties, in which case an HHS administrative law judge decides if the penalties are supported by the evidence.

HHS must bring an action under the HIPAA Administrative Simplification provisions within six years from the date of the occurrence of the violation. 45 C.F.R. § 160.414.

For examples of OCR investigations and resolutions, see the HHS Website.

Civil Money Penalties

The amount of a civil money penalty that may be imposed is subject to the rules noted below and must be determined by considering (1) the nature and extent of the violation, (2) the nature and extent of any resulting harm, (3) the history of prior HIPAA compliance, (4) the financial condition of the covered entity or business associate, and (5) such other matters as justice may require. 45 C.F.R. § 160.408.

Limitations on civil money penalties apply based on the establishment of certain circumstances:

- If the covered entity or business associate did not know and, by exercising reasonable diligence, would not have known that it violated the HIPAA rules, then the penalty must be no less than $100 or more than $50,000 for each violation.
- If the violation was due to reasonable cause and not willful neglect, then the penalty must be no less than $1,000 or more than $50,000 for each violation.
- If the violation was due to willful neglect and was 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, then the penalty must be no less than $10,000 or more than $50,000 for each violation.

- If the violation was due to willful neglect and was not corrected during the 30-day period described above, then the penalty must be no less than $50,000 for each violation.

45 C.F.R. § 160.404(b)(2).

However, in each of the above four scenarios, the civil money penalty may not exceed $1,500,000 for identical violations during a calendar year. Id.

A civil money penalty may be imposed for a violation of only a single Administrative Simplification violation even if the provision's requirement or prohibition is repeated in a more general form in another privacy or security rule. 45 C.F.R. § 160.404(b)(3).

Affirmative Defenses

HHS may not impose a civil money penalty on a covered entity or business associate for:

- An act that violates the HIPAA Privacy or Security Rule if a penalty for that violation has been imposed under the HIPAA criminal liability provisions –or–
- A violation if the covered entity or business associate establishes that the violation is not due to willful neglect and is corrected during the 30-day period beginning on the first date it knew (or, by exercising reasonable diligence, would have known) that the violation occurred, or such additional period as HHS determines to be appropriate

45 C.F.R. §§ 160.410(a)(2), (c).

Criminal Penalties

The U.S. Department of Justice (DOJ) has jurisdiction to enforce criminal penalties for violations of the HIPAA Administrative Simplification provisions under 42 U.S.C. § 1320d-6. Such penalties may apply to persons who knowingly (1) use or cause to be used a unique health identifier, (2) obtain individually identifiable health information, or (3) disclose individually identifiable health information, in each case in a manner that violates HIPAA requirements. 42 U.S.C. § 1320d-6(a).

According to a DOJ memorandum, the knowing standard used in that statute requires only that the person have knowledge of the facts that constitute the offense, not knowledge that the act is a violation of HIPAA.

Criminal penalties are:

- A fine of not more than $50,000, imprisonment of not more than one year, or both for knowing violations
- A fine not to exceed $100,000, imprisonment of not more than five years, or both if the offense is committed under false pretenses –or–
- A fine up to $250,000, imprisonment of up to ten years, or both if the offense is with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm

42 U.S.C. § 1320d-6(b).

Gabriel S. Marinaro
Special Counsel, Katten Muchin Rosenman LLP

Gabriel Marinaro serves as special counsel in the Employee Benefits and Executive Compensation group. His practice focuses on all aspects of employee benefits and executive compensation. He regularly counsels publicly traded and privately held companies, tax-exempt organizations, and governmental entities on a variety of employee benefits and executive compensation matters. Gabe regularly advises both employers and executives on a wide range of executive compensation matters, including drafting employment agreements, equity compensation arrangements, severance agreements and bonus plans. Gabe provides guidance on nonqualified deferred compensation plans both for for-profit companies and tax-exempt clients. Gabe regularly drafts nonqualified deferred compensation arrangements, including supplemental executive retirement plans, and change in control agreements. Additionally, Gabe advises employers and executives on issues under Code Sections 409A, 457(f), 457A, 162(m), 280G and 83 regarding compensation arrangements for executives.

Gabe assists both publicly traded and privately held companies with equity compensation matters, including drafting equity incentive plans, securities filings, award agreements, and other documentation surrounding the implementation of an equity incentive plan and the underlying awards. Gabe also has drafted and advised on profits interests plans and unit appreciation rights plans for limited liability companies.