23RD NATIONAL HIPAA SUMMIT

OMNI SHOREHAM HOTEL | WASHINGTON, D.C.

MARCH 16 – 18, 2015

The HIPAA Privacy and Security Rules from the Employer's/Group Health Plan Sponsor's Perspective

Prepared by

Alden J. Bianchi, Esq.
Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, P.C.
One Financial Center
Boston, MA 02111

The HIPAA Privacy and Security Rules from the Employer's/Group Health Plan Sponsor's Perspective

Alden J. Bianchi, Esq.

Explaining the administrative simplification provisions of Title II, Subpart F of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) evokes the plight of the blind man asked to describe an elephant: the description will vary depending on where the listener stands in relationship to the animal. In particular, the privacy and security provisions included in these rules affect different stakeholders in different ways. For purposes of gaining even a working knowledge of these rules, however, there is no more precarious perch than that occupied by an employer-sponsored group health plan.

A comprehensive treatment of the HIPAA administrative simplification rules is beyond both the scope of this paper and the competence of the author. This paper instead endeavors to shed some light on what employers, in their capacities as sponsors of group health plans (or, in the parlance of HIPAA, "covered entities"), must do to comply. The concerns of employers differ from those of other covered entities, i.e., providers, health care clearing houses, and other health plans. As a result, broad statements about the HIPAA administrative simplification rule (e.g., "employers are not covered entities") tend to mislead. Context is critical. It is not enough to ask how the rules work; rather, one must in each instance ask, how does the rule work in this particular instance with these particular parties given these particular facts?

I. Background

HIPAA regulates only "covered entities." The term "Covered Entity" is defined to include only (i) health plans, (ii) health care clearinghouses, and (iii) health care providers (other than those that do not transmit protected health information electronically). The exception for information that is not transmitted electronically applies only to providers. Employers that operate group health plans using only paper are subject to the privacy rule. Health plans include employer-sponsored group health plans as well as a host of other arrangements such as HMOs, insurers that provide medical coverage. This also includes Medicare and Medicaid, and state "high risk" pools, among others. The definition of what constitutes a health plan covers two uniquely different entities.

Covered entities typically enlist the aid of so-called "business associates" to assist them. A business associate is a person or entity that assists a covered entity with a function or activity that involves the use or disclosure of "individually identifiable health information." This includes claims processing and administration. From the employer's perspective, the most commonly encountered business associate is a third-party administrator or administrative-services-only provider. In some instances, consultants, brokers and other professionals who advise the employer regarding its health plan can also be business associates.

(a) *Congress's Road to HIPAA*

The policy goal of Administrative Simplification is to streamline the administrative and claims processing components of the U.S. health care system. Congress was aware of the extent to which the Internet and electronic media had transformed the claims processing landscape. With more than 400 different health care coding, billing and reporting formats in use by the various providers and payers, among others, unnecessary delays and costs were inevitable. But the private sector was unable or unwilling to adopt uniform standards, so the job was left to Congress. By prescribing uniform standards—which in the parlance of Administrative Simplification are referred to as "transactions and code sets"—Congress expects annual savings on the order of $5 billion. The transaction and code set rules prescribe data content, code and format standards for "covered transactions"—i.e., transactions that are covered by the rule.

Although the transaction and code set rules hold out the promise of substantial savings, other protections relating to privacy and security were needed for the rule to work. In the days when most medical records were in paper form and safely locked up in physicians' offices, privacy was not typically thought to be a problem. But once those same records were converted to electronic form and transmitted nearly instantaneously over the Internet, privacy became very much a concern. The preamble to the final privacy rule describes some particularly egregious privacy violations in support of the need for a set of comprehensive privacy protections. The HIPAA privacy standards are designed to ensure that the savings resulting from standardized electronic claims processing would not be accompanied by a wholesale loss of privacy.

The promise of privacy rings hollow without also ensuring security. So Congress included a security component as a part of Administrative Simplification. While the privacy rules determine who should have access to medical records, the security provisions establish the manner in which medical records must be protected from inappropriate access. Rounding out the Administrative Simplification suite, Congress lastly mandated the adoption and use of "unique health identifiers." These are identification numbers that apply to employers, individuals, providers and health plans. They must be used in connection with covered transactions.

(b) *Protected Health Information*

HIPAA does not extend regulatory protection to all health information; rather, it governs only "protected health information" or "PHI." Health information that is not PHI might still be protected, but not by HIPAA. Rather, those protections must be found under state law or other Federal laws. To understand what constitutes PHI, it helps to break the definition down into three, successively narrower components beginning with health information:

"Health information" means any information, whether oral or recorded in any form or medium that (i) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university or health care clearinghouse, and (ii) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or past, present or future payment for the provision of health care to an individual.

Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and is (i) created or received by a health care provider, health plan, employer, or health care clearinghouse; and

(ii) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (A) that identifies the individual; or (B) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

PHI is defined to mean and include "individually identifiable health information" that is transmitted or maintained in any form or medium (electronic, oral or written). Though the definition of PHI is complex and relies on and refers to defined terms, it generally means and includes any information about health status, provision of health care, or payment for health care that can be linked to a specific individual. Medical records, for example, clearly include PHI.

(c) *The Medical Privacy Rule*

A basic (though somewhat simplified) statement of the HIPAA medical privacy rule is as follows:

> "A Covered Entity may not use or disclose Protected Health Information except as (i) authorized by the individual who is the subject of the information or (ii) explicitly required or permitted by the rule."

As the basic statement of the privacy rule suggests, there are instances where PHI may be used or disclosed without the need for an authorization. The most important of the permitted uses and disclosures is for purposes of "treatment, payment and health care operations." Essentially, this exception allows the U.S. health care system to continue to operate without the need to get a signed authorization for every routine transaction. There are other exceptions for such things as incidental uses and disclosures, as well as certain permitted "public interest activities that include (i) items that are required by law, (ii) public health activities, (iii) victim abuse, neglect or domestic violence, (iv) health oversight, (v) judicial and administrative proceedings, (vi) law enforcement purposes, (vii) decedents, (viii) cadaveric organ, eye or tissue donations, (ix) research, (x) serious threat to health or safety, (xi) essential government functions, and (xii) workers' compensation.

There are also instances where disclosure is required. A covered entity must disclose PHI to an individual upon request, to HHS in the case of an investigation, or pursuant to a court order or a warrant.

Where there is no express exception provided under the privacy rule, an individual must give his or her consent before a covered entity can release PHI. Since disclosures for treatment, payment or health care operations are allowed under the rule, there is no need to get an authorization under these circumstances. Employers (and other covered entities) may not condition treatment, payment, or enrollment on whether or not an employee signs an authorization. To be valid, an authorization must include: a description of the information that will be used and disclosed (and for what purposes); a description of any information that may not be disclosed, if applicable; a list of who will disclose the information and to whom it will be disclosed; an expiration date; a statement that the authorization can be revoked; a statement that

disclosed information may be re-disclosed and no longer protected; and the individual's signature and date.

(d) *Employment Records*

Plan sponsors get sensitive medical information from many sources, some plan-related and others not. While the definition of PHI is strikingly broad, there is an important exception for "employment records." The preamble to the final modifications to the final privacy rule issued in August 2002 makes clear that employment records held by an employer in its capacity as an employer are not PHI. This is so even where these records include individually identifiable health information. As an important, practical matter, this means that medical information that an employer needs to carry out its obligations under FMLA, ADA, and similar laws, as well as files or records related to occupational injury, disability insurance eligibility, sick leave requests and justifications, drug screening results, workplace medical surveillance, and fitness-for-duty tests of employees are generally treated as employment records that are beyond the scope of the rule.

> **Example:** Employee A has worked for Company X full time for more than 12 months and now finds himself in need of FMLA leave to care for a recently diagnosed medical condition. Company X's HR director provides A with the prescribed DOL form. A makes an appointment to see his physician, and asks the physician to complete the form and deliver it to Company X. Assuming that A's physician conducts covered transactions electronically (and is therefore subject to the rule), she will need to get A's authorization to release her report. This is so because her report is not being used for her treatment, payment and operations purposes. It is not Company X's responsibly to see to it that A's physician obtain his consent. Once the report gets to Company X, it is an employment record, which is not subject to the rule.

(e) *The HITECH Act*

Congress subsequently modified and expanded the HIPAA administrative simplification rules in the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009. In January 2013, the U.S. Department of Health and Human Services (HHS) issued a comprehensive omnibus rule implementing the HITECH Act. The omnibus rule includes a series of substantive and procedural changes including the addition of breach-notice rules. As required by HITECH, the final omnibus rule also provides a robust template for compliance along with a penalty scheme and enforcement profile that strongly encourage compliance. In particular, the omnibus rule imposes severe penalties where an employer fails to comply out of willful neglect. While willful neglect can take many forms, the most obvious is for an employee to simply do nothing.

II. Selected Issues

Set out below are issues that have, in the author's experience, posed particular problems for employers either in understanding or complying with HIPAA administrative simplification rules. Perhaps the single biggest compliance challenge is for employers that sponsor group health plans that they might need to do *something* to comply. While this notion was perhaps "quaint"

when these rules went into effect, it is no longer that way. The HITECH Act added new breach notice requirements, modified the basic compliance standards in certain important respects, and increased fines associated with non-compliance. The bar is now higher for all HIPAA covered entities, group health plan sponsors included. The cost of failing to "get the HIPAA memo" is now prohibitive.

(a) *What is a "group health plan" covered entity, exactly*?

The HIPAA administrative simplification rules apply to "covered entities," i.e., health care providers, health plans, and health care data clearing houses. Confusingly, the term "health plan" includes both group health insurance sponsored and sold by state-licensed insurance carriers and employer-sponsored group health plans. Once HHS began issuing regulations, it became apparent that this law was directed principally at health care providers and health insurance issuers or carriers. The problem for this latter group of covered entities is determining what, exactly, is being regulated. The regulatory scheme treats an employer's group health plan as a legally distinct entity, separate and apart from the employer/plan sponsor. This approach is, of course, at odds with the experience of most human resource managers, employees and others, who view a company's group health plan as a product or service that is "outsourced" to a vendor. In the case of an insured plan, the vendor is the carrier; in the case of a self-funded plan, the vendor is a third-party administrator.

The idea that a group health plan may be treated as a separate legal entity is not new. The civil enforcement provisions of the Employee Retirement Income Security Act of 1974 (ERISA) permit an "employee benefit plan" (which includes most group health plans) to be sued in its own name. (ERISA § 502(d) is captioned, "Status of employee benefit plan as entity.") The approach taken under HIPAA merely extends this concept. But what exactly, is an "employee benefit plan"? In a case decided in 2000, the Supreme Court gave us an answer, saying:

> "One is thus left to the common understanding of the word 'plan' as referring to a scheme decided upon in advance . . . . Here the scheme comprises a set of rules that define the rights of a beneficiary and provide for their enforcement. Rules governing collection of premiums, definition of benefits, submission of claims, and resolution of disagreements over entitlement to services are the sorts of provisions that constitute a plan." (*Pegram v. Herdrich*, 530 U.S. 211, 213 (2000).)

Thus, what HHS has done in the regulations implementing the various HIPAA administrative simplification provisions is to impose rules on a set of promises and an accompanying administrative scheme. (Is there any wonder that these rules have proved difficult to administer?) It's one thing to regulate a covered entity that is a large, integrated health care system; it's quite another to regulate an amorphous blob.

All too often, employers get the notion that they "outsource" their HIPAA compliance to an insurance carrier, in the case of a fully-insured plan, and a third-party administrator, in the case of a self-funded plan. In the case of fully-insured "small group" plans, this is the case, since the employer does not see any PHI. In the case of a fully-insured large group plan, there is an exception allowing employers to have access to PHI for limited purposes, but employers are often unaware of how this exception works, and where they do avail themselves of it they often

find that the exception is too narrow to be of much use. In this latter case, the large, fully insured health plans routinely receive information from the insurance carrier that rises to the level of PHI, implicating the privacy and security rules. But even when these plans get help from their TPAs with HIPAA compliance, it is rarely integrated into a systematic compliance effort. Moreover, fully-insured plans are often paired with Health Reimbursement Accounts, or medical flexible spending arrangements, which are themselves self-funded arrangements that are in most instances separately subject to HIPAA.

HHS has permitted exceptions in cases of fully-insured plans because the health insurance carriers are themselves covered entities. Self-funded group health plans generally rely on an outside vendor referred to as a third-party administrator (or "TPA") to handle day-to-day plan maintenance and operation. The TPA is not a covered entity, *even in instances in which the TPA is itself a licensed carrier*. The TPA in these instances is, rather, a business associate—i.e., a person who "on behalf of such covered entity . . . creates, receives, maintains, or transmits protected health information for a [covered] function." Covered functions in this context include claims processing, data analysis, utilization review, and billing. Employers that sponsor self-funded plans sometimes say things like, "but we don't ever see any PHI, our TPA does it all." What they miss is that the TPA is the employer's agent. What the TPA sees, the employer is deemed to see. If this was not the case, then the plan could forgo HIPAA compliance with impunity.

The HIPAA privacy rule's substantive and procedural requirements also include a requirement that a covered entity train its "workforce." The omnibus rule defines the term "workforce" to mean and include:

> "[E]mployees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate."

Thus, members of a covered entity's workforce need not be employees of the covered entity. In addition, by reason of express terms of the definition of "business associate" set out above, business associates and workforce members are mutually exclusive—that is, if a person of entity is a business associate, that same person or entity cannot be a workforce member.

The omnibus rule clarified that, while business associates are not subject to each and every requirement of the Privacy Rule listed above, they must comply with the terms of a business associate agreement related to the use and disclosure of PHI; provide PHI to the Secretary upon demand; provide an electronic copy of PHI to an individual (or covered entity) related to an individual's request for an electronic copy of PHI; make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request; and enter into business associate agreements with subcontractors that create or receive PHI on their behalf.

(b) *The HITECH breach notice rule: Anthem Blue Cross/Blue Shield case study*

The HIPAA/HITECH breach-notice rules require a covered entity or business associate to report a breach in the case of an acquisition, access, use, or disclosure of PHI in a manner not permitted by HIPAA's privacy and security rules that has compromised the security or privacy of such PHI. Covered entities must report the breach to affected individuals, HHS and the media, in certain cases, *unless* the covered entity can demonstrate that there is a low probability that PHI has been compromised. Business associates report to the covered entity. In making this call HIPAA requires that covered entity or business associate, as the case may be, take into consideration, and to document (i) the nature and extent of PHI involved, (ii) the unauthorized person who used the PHI or to whom disclosure was made, (iii) whether PHI was actually acquired or viewed, and (vi) the extent, if any, to which risk has been mitigated.

On January 29, 2015, Anthem Blue Cross/Blue Shield first detected a breach of a database containing records for 80 million customers and employees. On February 4, less than a week later, Anthem disclosed the existence of the breach and began providing notice to affected individuals. It is not yet known whether this breach involved medical/clinical data but that does not mean it is not a HIPAA breach, since PHI includes personal identifying information, which was accessed in the breach. This breach implicated not only the HIPAA breach-notice rules, but also any number of state data breach notification laws (many states require reasonably prompt notice to affected persons when a breach occurs).

Members of the affected health insurance plans are not the only ones to be concerned about the Anthem breach. In the case of fully-insured group health plans that insured with Anthem, Anthem will have the obligation to report the breach and otherwise comply with the HIPAA and state data privacy rules. Self-funded arrangements for whom Anthem performs TPA services are affected, however. These latter plans are subject to the HIPAA breach notice rules. It is possible, of course, that the business associate agreement between the self-funded plan and Anthem puts the compliance obligations back on Anthem, but where that is not the case, then the plan administrator bears the compliance burden. Plan sponsors of self-funded plans should be able to consult their breach-notice policies and procedures to determine how to respond.

(c) *The basic HIPAA privacy obligations*

The Privacy Rule imposes on covered entities a series of requirements designed to safeguard PHI. These include the following:

(i) Privacy Policies and Procedures.

A covered entity must adopt written privacy policies and procedures that are consistent with the privacy rule.

(ii) Privacy Personnel.

A covered entity must designate a privacy official responsible for developing and implementing its privacy policies and procedures, and a contact person or contact office responsible for receiving complaints and providing individuals with information on the covered entity's privacy practices.

(iii) Workforce Training and Management.

Workforce members include employees, volunteers, and trainees, and may also include other persons whose conduct is under the direct control of the covered entity (whether or not they are paid by the entity). A covered entity must train all workforce members on its privacy policies and procedures, as necessary and appropriate for them to carry out their functions. A covered entity must also have and apply appropriate sanctions against workforce members who violate its privacy policies and procedures or the Privacy Rule.

(iv) Mitigation.

A covered entity must mitigate, to the extent practicable, any harmful effect it learns was caused by use or disclosure of protected health information by its workforce or its business associates in violation of its privacy policies and procedures or the Privacy Rule.

(v) Data Safeguards.

A covered entity must maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional use or disclosure of protected health information in violation of the Privacy Rule and to limit its incidental use and disclosure pursuant to otherwise permitted or required use or disclosure.

(vi) Complaints.

A covered entity must have procedures for individuals to complain about its compliance with its privacy policies and procedures and the Privacy Rule. The covered entity must explain those procedures in its privacy practices notice. Among other things, the covered entity must identify to whom individuals at the covered entity may submit complaints and advise that complaints also may be submitted to the Secretary of HHS.

(vii) Retaliation and Waiver.

A covered entity may not retaliate against a person for exercising rights provided by the Privacy Rule, for assisting in an investigation by HHS or another appropriate authority, or for opposing an act or practice that the person believes in good faith violates the Privacy Rule. A covered entity may not require an individual to waive any right under the Privacy Rule as a condition for obtaining treatment, payment, and enrollment or benefits eligibility.

(viii) Documentation and Record Retention.

A covered entity must maintain, until six years after the later of the date of their creation or last effective date, its privacy policies and procedures, its privacy practices notices, disposition of complaints, and other actions, activities, and designations that the Privacy Rule requires to be documented.

A simple thought experiment can provide a sense of how these requirements might affect employer-sponsored plans that don't qualify for a compliance exception: A HHS investigator contacts an employer and asks, can I please see your HIPAA policies and procedures? And can you introduce me to your privacy officer and tell me a little about his or her qualifications and training? Can you also show me your workforce training materials? At this point, the employer might panic and call the carrier or TPA, who in all likelihood respond by saying something like, "this is on you, and we are not your lawyers."

(c) *The Security Rule*

The Security Rule remains a mystery for most group health plan sponsors. While the rule requires written policies and procedures for some two dozen standards, this requirement is rarely followed. The regulators routinely refer to the security rules as "scalable"— i.e., small entities can comply by adopting approaches that are less complicated and costly. In practice, however, there is little truth to this claim. At a minimum, the rule requires covered entities to conduct a risk assessment. For group health plans, threats can come from two sources: internal (from the workforce) or external (communications on behalf of the health plan and brokers, consultants, and vendors). Accordingly, group health plans should, at least in theory, be able to easily identify potential risks and solutions to those risks. But even base-line risk assessments and policies and procedures quickly get to a point below which they simply cannot be further simplified. Compliance with the security rules if done right is time consuming and, particularly to smaller entities, costly.

(d) *Dealing with business associates*

Group health plans should request copies of privacy policies and procedures, risk assessments, and security policies and procedures from their business associates. (Although business associates are not required to have written policies and procedures, having policies and procedures is highly recommended and probably rises to the level of a "best practice.") Group health plans should also ensure that their business associate agreements have been updated to comply with the omnibus rule. Each business associate and downstream entity also must have a business associate agreement in place.

Conclusion

The substantial savings and administrative efficiencies of HIPAA transactions and code sets rules are compelling. With the benefit of hindsight, these rules have the aura of the inevitable. The privacy and security aspects of administrative simplification are, too, predictable if not inevitable. Both are manifestations of larger, global trends that flow from the rapid growth and deployment of information technology. But to be clear, group health plans and their sponsors sit at the periphery. These rules are, at their core, provider- and carrier-centric. Group health plans are a regulatory afterthought.

HIPAA's administrative simplification rules are qualitatively different from the vast majority of laws that alter the mechanics of the rules that govern employee benefits and executive compensation. This is not tinkering at the edges. It is rather something entirely new, and it's not going away. With HIPAA providing a regulatory floor, the fight for expanded

privacy rights will likely move to the state legislatures. This is happening at a time when the traditional ERISA preemption shield against state regulation of employer-sponsored health plans is eroding. As a result, employers are faced with vastly increased regulatory burdens while health care costs are skyrocketing. So employers, their advisors, and their vendors, are faced with the prospect of complying despite the many burdens that compliance might involve.

39692762v.3