

# Corporate Counsel

Monday, May 14, 2001

## HIPAA Privacy Rules Impact Employers

**P**RESIDENT BUSH has just sent the healthcare industry into a tailspin. What many employers outside the healthcare industry may not realize is that his action has consequences for them as well.

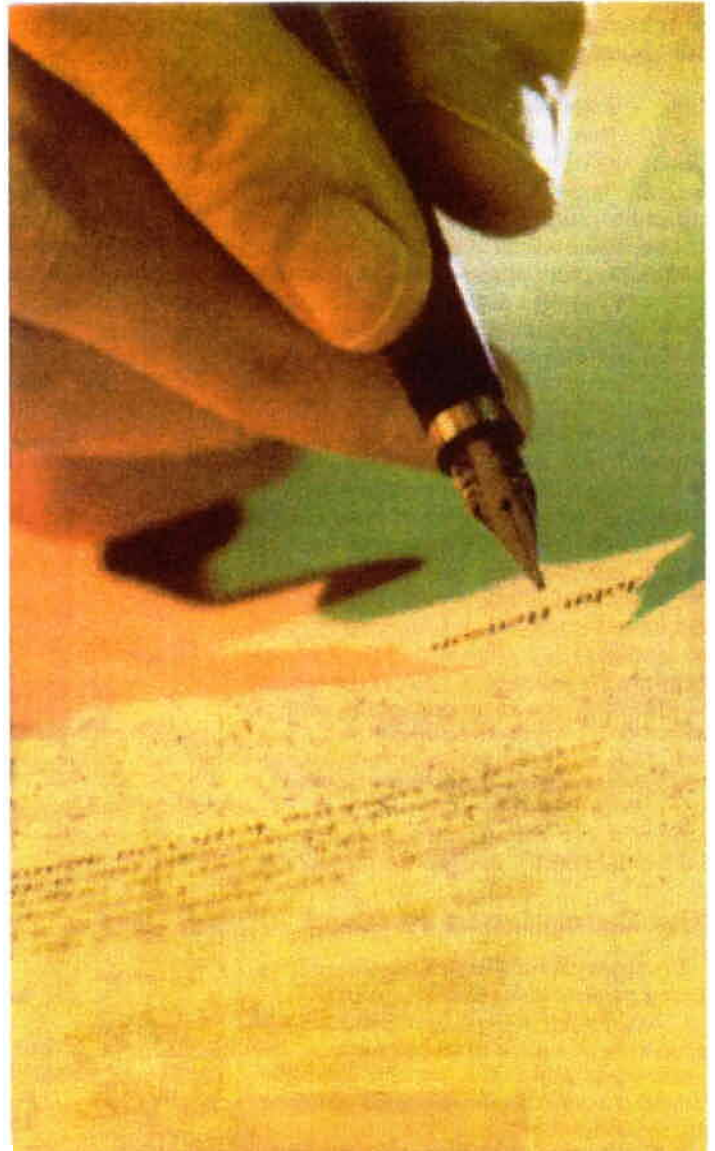
Contrary to expectations, the President allowed the privacy regulations promulgated under the Health Insurance Portability and Accountability Act (HIPAA) and issued in final form on Dec. 28, 2000 (Privacy Rule or Rule),<sup>1</sup> to go into effect as scheduled on April 14, 2001. The Secretary of the U.S. Department of Health and Human Services (HHS) indicated, in a press release dated April 12, 2001, that additional guidelines will be issued to the Privacy Rule, and possibly modifications as well, in order to address the more than 24,000 comments that were sent to HHS in the one-month comment period granted by the Secretary after the final Rule was issued.

It must be emphasized that although the impact of the Privacy Rule on employers has not been in the spotlight, it is nevertheless crucial for them to familiarize themselves with it because, although most employers do not consider themselves part of the healthcare industry, they will nevertheless be affected, in some cases dramatically, by the Rule.

### Covered Entities

Nearly all employers will be affected by the provisions of the final Rule if they provide healthcare coverage to their employees, whether through self-insured or fully insured arrangements. Specifically, the Privacy Rule does not cover employers directly, but rather indirectly, through the group health plans that they establish.

A group health plan is considered a "covered entity"<sup>2</sup> in the Rule and is defined consistent with the Employee Retirement Income Security Act of 1974 (ERISA) to mean, generally, an employee welfare benefit plan that, whether through insurance or via a self-insured arrangement, pro-



---

**Linda Abdel-Malek** is a senior associate in the healthcare group of Moses & Singer LLP.

vides healthcare to its employees and/or dependents. However, to be covered by the Rule, a group health plan must have 50 or more participants or be administered by an entity other than the employer that established and maintains the plan.<sup>3</sup> In other words, small, self-administered plans are not covered by the Privacy Rule.

Multi-employer plans are also covered under the Privacy Rule's definition of "covered entity" and are generally defined within the category of "health plan" as "an employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers."<sup>4</sup> An additional type of entity which is considered a covered entity may have an impact on large employers that provide health care onsite through, for example, onsite clinics which provide health care for employees on the premises of the employer.

This type of covered entity is called a "hybrid entity" by the Privacy Rule, and is intended to cover organizations whose "covered function," or healthcare function, is not its primary function, but which nevertheless is a single legal entity and, therefore, the entire organization is deemed by the Privacy Rule to be a covered entity.<sup>5</sup> All of these covered entities are given two years from the effective date of the final Privacy Rule to comply, with the exception of small health plans,<sup>6</sup> which are given three years to comply.<sup>7</sup>

## Preemption

The Privacy Rule does not preempt state law that is considered to be "more stringent." As a rule of thumb, this term is generally defined in the Rule as a state law that provides greater privacy protection to the individual or that provides greater penalties for noncompliance than the Privacy Rule. In the context of ERISA, which preempts state laws that "relate to" employee benefit plans, the Privacy Rule states that its preemption clause does not affect ERISA preemption, but rather, the Rule's effect is to leave in place only those state laws whose privacy protections would otherwise

apply in the context of ERISA and that are "more stringent" than the Privacy Rule.<sup>8</sup>

## Treatment of Employers

Although employers are not directly covered under any particular category of covered entity, employers acting as "plan sponsors"<sup>9</sup> who administer the plan<sup>10</sup> are discussed throughout the Rule, and requirements are placed on them in the context of their dealings with the group health plans that they administer. However, the burden of compliance with the Privacy Rule and the liability for failure to comply rests with the group health plan, and not the plan sponsor.

This distinction creates a somewhat fictional situation, because practically speaking, most employers that establish a group health plan or a multi-employer plan are merely establishing a contractual entity that has no independent assets or employees. Rather, such assets and the employees involved in carrying out the necessary functions of the plan remain with the employer, acting as the plan sponsor. However, because Congress did not grant HHS the authority to regulate employers directly, this conundrum remains in the final Rule, and employers will need to determine methods with which to bring their operations into compliance with the Privacy Rule's requirements, which are discussed in more detail below.

## Disclosures of Information

Generally speaking, the disclosure of "protected health information"<sup>11</sup> (PHI) is addressed in the Privacy Rule when such PHI is disclosed from the group health plan to the plan sponsor. In the majority of cases involving disclosure of PHI from a health plan to a third party, the Privacy Rule requires that a "business associate"<sup>12</sup> agreement be established between the parties in order to assure that the third party maintains the confidentiality of PHI.<sup>13</sup> An exception to the business associate agreement requirement is made in the Rule for disclosures from group health plans (or health insurance issuers or an HMO with respect to a group health plan) to plan sponsors.

The group health plan may disclose PHI to the plan sponsor only for purposes of plan administration, and must ensure that the plan documents restrict uses and disclosures of PHI by the plan sponsor.<sup>14</sup> The restrictions that must be contained in the plan documents are similar to those required in business associate agreements and are such that the majority of employers will likely need to amend their plan documents to include them.

---

***Generally speaking, the disclosure of 'protected health information' ... is addressed in the Privacy Rule when such PHI is disclosed from the group health plan to the plan sponsor.***

---

## Know Effects of Privacy Rules

Patient consent or authorization prior to such disclosures would generally not be required for purposes of disclosures relating to plan administration, as plan administration activities are limited to activities that meet the definitions of payment or health-care operations<sup>15</sup> under the Rule.<sup>16</sup> However, disclosures made by the group health plan to the plan sponsor for purposes not considered to be plan administration functions, such as enrollment functions, would require individual authorization.<sup>17</sup>

The plan documents must contain provisions to do the following:

- Establish the permitted and required uses and disclosures of PHI by the plan sponsor.
- Provide that the group health plan will disclose PHI to the plan sponsor only upon receipt of a certification from the plan sponsor that the plan documents have been amended to incorporate the provisions contained in this list and that the plan sponsor agrees to, among other things:
  - not use or further disclose PHI other than as permitted or required by the plan documents or as required by law;
  - ensure that any agents (such as a subcontractor) to which the plan sponsor provides PHI also agree to the same restrictions and conditions that apply to the plan sponsor;
  - not use or disclose the PHI for employment-related purposes or in connection with any other employee benefit plan;
  - report to the group health plan any impermissible use or disclosure of PHI of which it becomes aware;
  - permit beneficiaries of the group health plan access to their PHI, the opportunity to amend such PHI, and an accounting of the disclosures of such PHI;
  - make all internal books and records related to PHI available to HHS for audit and inspection;
  - return or destroy PHI when copies are no longer needed for the purposes for which such PHI was disclosed; and
  - establish adequate separation between the group health plan and the plan sponsor.<sup>18</sup>

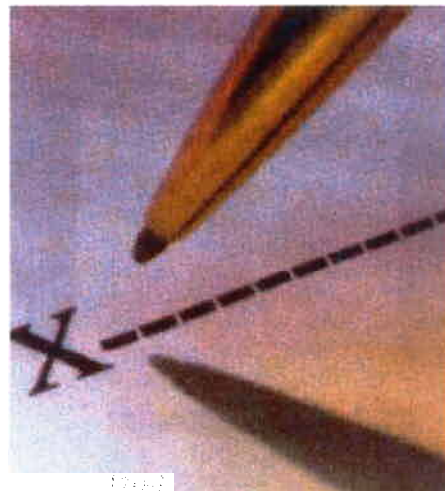
The last point in this list is critical in that it requires the employer to set up "firewalls" in order to ensure that PHI is used only for purposes of plan administration and not for any other employment-related decisions, and also to broadly protect such information from being viewed by persons other than those employees carrying out plan administration functions. The Privacy Rule, without prescribing the means by which plan sponsors must establish such firewalls,

sets forth the general measures that a plan sponsor must take in establishing such firewalls. These provisions must be contained in the plan documents and include the following:

- a description of the employees or classes of employees or other persons under the control of the plan sponsor who are to be given access to PHI;
- restrictions on the access to and use by such employees and other persons to permit only plan administration functions; and
- an effective mechanism for resolving issues of noncompliance by such employees or persons with the provisions set forth in the plan documents.<sup>19</sup>

In contrast to the requirements set forth above relating to disclosures made by a group health plan to the plan sponsor, disclosures of PHI from a group health plan to another entity, such as a third-party administrator, would likely require a business associate agreement, since the third-party administrator would most likely be considered a business associate of the group health plan under the Privacy Rule.

If the disclosure of PHI is to be made from the plan sponsor to the third-party administrator, a business associate agreement is most likely not required. Rather, the plan sponsor must only comply with the provisions of the plan document that require any subcontractors or agents to agree to the same restrictions that apply to the plan sponsor. Practically speaking, these requirements, as stated earlier, are similar to those of a business associate agreement, so that the result is that HHS remains within the confines of its authority to regulate group health plans and not plan sponsors, but achieves its goal of ensuring that the confidentiality of PHI is maintained to the greatest extent possible.



The major exception to the plan document requirements described above relates to disclosure by the group health plan of "summary health information" to the plan sponsor. "Summary health information" is information that summarizes claims history, claims expenses, or the type of claims experienced by individuals for whom a plan sponsor has provided health benefits under a group health plan and from which items tending to identify the individual have been removed.<sup>20</sup> Summary health information may be disclosed to the plan sponsor without compliance with the plan document requirements described above only for the purpose of obtaining premium bids from insurers or for the purpose of modifying, amending, or terminating the group health plan.<sup>21</sup>

## A Compliance Plan

In order to assure that all covered entities create a culture of compliance within their organizations, the Privacy Rule mandates that such covered entities comply with certain administrative requirements which essentially comprise a compliance plan for the organization. These requirements may prove to be quite burdensome for the entity and include the following:

- appointing a privacy officer for the organization;
- training all employees likely to come into contact with PHI;
- establishing appropriate administrative, technical and physical safeguards to protect PHI;
- creating a process by which individuals and employees can file complaints to the covered entity regarding alleged violations of the Privacy Rule (complaints may also be filed directly with the Secretary of HHS and the covered entity may not interfere with or retaliate against any employee filing such a complaint);
- forming a process to sanction employees for violations of the covered entity's privacy policies and procedures or for violations of the Privacy Rule;
- implementing policies and procedures to mitigate any violations of the privacy rule by the covered entity's workforce or by a business associate of the covered entity to the extent practicable and where the covered entity has actual knowledge of a violation; and
- documenting privacy procedures and activities.

A few issues are important to emphasize in this context. The first is that with respect to the sanction requirement above, the Privacy Rule is unclear regarding how much internal process is due an employee who is to be subject to such sanctions. Employers with unionized employees should anticipate that this issue would be addressed in the collective bargaining process.

Second, group health plans do not need to comply with the requirements listed in the bullet points above (except for the non-retaliation and documentation requirements) if they provide health benefits solely through an insurance contract with a health insurance issuer or an HMO and they do not create or receive PHI except for summary health information or information as to the status of an individual's enrollment or disenrollment with respect to a health insurance issuer or HMO offered by the group health plan.

Third, because group health plans which contain more than 50 members and are self-insured are likely to utilize health information which does not fall within the exception to the Rule's administrative requirements, those requirements may provide a disincentive for mid-size or large employers to be self-insured in order to avoid considerable additional expense and operational burdens.

## Enforcement

The Secretary of HHS may, within his discretion, investigate any complaints filed regarding group health plans that have allegedly violated the Privacy Rule. The Rule itself does not provide a private right of action.

A finding of noncompliance can cost the employer greatly, with civil penalties ranging from \$100 per violation to \$25,000 per person per violation in a single calendar year. Criminal penalties range from \$50,000 and/or one year imprisonment for a knowing violation up to \$250,000 and/or 10 years' imprisonment for a violation with intent to sell, transfer or use PHI for commercial gain.<sup>22</sup>

## Conclusion

Clearly, the Privacy Rule will require employers to evaluate their operations and face difficult decisions regarding, for example, whether to self-insure, how to protect themselves from increased liabilities, and the extent of their need for PHI in order to perform their healthcare administrative functions. Corporate counsel must review plan documents carefully, assess potential vulnerabilities and begin to prepare for the challenging ramifications posed by the Rule.

.....●●●.....  
(1) See 65 Fed. Reg. 82462 (Dec. 28, 2000), promulgating 45 CFR Parts 160 and 164.

(2) The Privacy Rule contains three general categories of "covered entities": providers, health plans, and health-care clearinghouses. Group health plans fall under the category of health plans and therefore must comply with all requirements in the Rule applicable to health plans except where specific exceptions are made for group health plans. See 45 CFR §160.102.

(3) *Id.*

(4) *Id.*

(5) 45 CFR §164.504(a).

(6) A "small health plan" is defined in the Privacy Rule as "a health plan with annual receipts of \$5 million or less." 45 CFR §160.102.

(7) 45 CFR §164.534.

(8) For further discussion on this issue, see 65 Fed. Reg. at 82483.

(9) A "plan sponsor" is defined in the Rule "as defined at section 3(16)(B) of ERISA, 29 U.S.C. 1002(16)(B)." 45 CFR §164.501.

(10) "Plan administration functions" is defined as administration functions performed by the plan sponsor of a group health plan on behalf of the group health plan, including quality assurance, claims processing and

auditing. Any other function performed by the plan sponsor in connection with any other benefit plan of the plan sponsor is excluded from this definition. 45 CFR §164.504(a); 65 Fed. Reg. at 82508.

(11) "Protected health information" is defined as individually identifiable health information that is transmitted or maintained by electronic media or in any other form or medium, with exceptions for information covered by the Family Educational Rights and Privacy Act (FERPA). 45 CFR §164.501.

(12) A "business associate" is defined generally as a person who is not a member of a covered entity's workforce and who, on behalf of a covered entity, performs, or assists in performing a function involving the use or disclosure of PHI or provides (other than as a member of the covered entity's workforce), legal, consulting, or financial services where PHI is disclosed to the person from the covered entity or another business associate of the covered entity. See 45 CFR §160.102.

(13) See 45 CFR §164.502(e)(1).

(14) 45 CFR §164.504(f)(3).

(15) 45 CFR §164.501.

(16) 65 Fed. Reg. at 82508. Consent requirements regarding payment and healthcare operations are set forth in 45 CFR §164.506 and are not mandatory when disclosure for such purposes is made by health plans.

(17) 65 Fed. Reg. at 82508.

(18) 45 CFR §164.504(f)(2)(i), (ii).

(19) 45 CFR §164.504(f)(2)(iii).

(20) 45 CFR §164.504(a).

(21) 45 CFR §164.504(f)(1)(ii).

(22) Section 262, Subtitle F of HIPAA gives the Secretary authority to impose civil and criminal penalties. Applicable civil penalties are found in 42 USC §1320d-5; criminal penalties are found in 42 USC §1320d-6. HHS plans to issue a separate Enforcement Rule to specifically address the issue of penalties.