

Although by now the healthcare industry is all too familiar with the Privacy Rule contained in the Health Insurance Portability and Accountability Act, or HIPAA, many outside the industry are not necessarily aware of the fact that the Privacy Rule may have a significant impact on them as well.

Employers may not know that any employer that provides healthcare coverage to its employees, either through a fully insured or self-insured health plan, will be affected by the Privacy Rule and will be required to change its operations to comply with the Rule. Employers will need to evaluate their operations soon, since the deadline for compliance with the Privacy Rule is April, 2003 for the group health plans of most employers (the Privacy Rule allows "small health plans", i.e. those with \$5 million or less in annual receipts, an additional year for compliance). Still, the scope of necessary changes to operations could be quite burdensome for many.

Since the U.S. Department of Health and Human Services ("HHS") was not authorized to regulate employers directly, employers are regulated under the Privacy Rule indirectly, through the group health plans that they establish. Pursuant to the Privacy Rule, a group health plan is considered a "covered entity", and is therefore directly regulated unless it is a small, self-administered plan with less than 50 participants. Practically speaking, however, many group health plans are merely contractual entities with no independent assets. Although not directly covered by the Rule, employers acting as "plan sponsors" who must administer the group health plan will be responsible for ensuring that the mandate of the Privacy Rule is met.

For example, although a Business Associate Agreement is not required for disclosures of protected health information, or PHI, between a group health plan and the plan sponsor, the employer will have to voluntarily agree to use or disclose such PHI only as permitted or required by the Privacy Rule.

Subject to certain exceptions, below are the major steps that an employer will need to take in order to comply with the Privacy Rule with respect to use and disclosure of PHI between the group health plan and the plan sponsor:

1. Create privacy policies and procedures that ensure that all PHI relating to employees is adequately protected to comply with the Privacy Rule,
2. Amend group health plan documents to specify how the use of PHI will be restricted to the purposes permitted by the Privacy Rule,
3. Establish policies and procedures to ensure that consent is obtained from an employee prior to using PHI for purposes such as enrollment in a group health plan,
4. Establish "firewalls" between personnel (and workspace) associated with handling PHI for purposes of administering the group health plan and the rest of the employer's personnel and operations,
5. Implement a compliance program for employees which includes appointing a privacy officer, training employees likely to come into contact with PHI, and creating a process to sanction employees who violate the employer's privacy policies and procedures.

It is important to note that regarding the second point above, the Privacy Rule instructs entities as to the types of restrictions that must be included in plan documents prior to any disclosures of PHI being made by the group health plan to the plan sponsor. And the fourth point above is a very important issue for employers because it requires them to set up firewalls in order to ensure that PHI is used for purposes of plan administration only, and not for any other employment related purposes, such as decisions on employee hiring or termination. Additionally, although the Privacy Rule does not dictate how these firewalls must be established, it does describe the general issues that must be addressed by the employer in creating such firewalls. Specifically, these issues must be included 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.

In connection with implementing a compliance program (see point 5), group health plans are exempt from these 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 regarding the status of an individual's enrollment, or disenrollment from the HMO or health insurance issuer.

It is important to note that employers must consider their activities not only in the context of use and disclosure of PHI between the group health plan and the plan sponsor, but also in the context of any redisclosure of PHI to a third party. For example, a disclosure from the group health plan to a third party administrator would require adequate assurances of confidentiality, and would therefore appear to require a business associate agreement under the Privacy Rule before PHI could be disclosed.

Lastly, employers must be aware of the potential penalties for noncompliance with the requirements discussed above. The Secretary of HHS may investigate any complaints filed regarding group health plans that have allegedly violated the Privacy Rule. A finding of noncompliance can impose large burdens on the employer, 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 ten years imprisonment for a violation with intent to sell, transfer, or use PHI for commercial gain.



Linda A. Malek is a partner at Moses & Singer LLP
and chair of the healthcare practice group.
She can be reached at lmalek@mosessinger.com

MOSES & SINGER LLP

1301 AVENUE OF THE AMERICAS
NEW YORK, NY 10019-6076
212.554.7800 FAX: 212.554.7700
