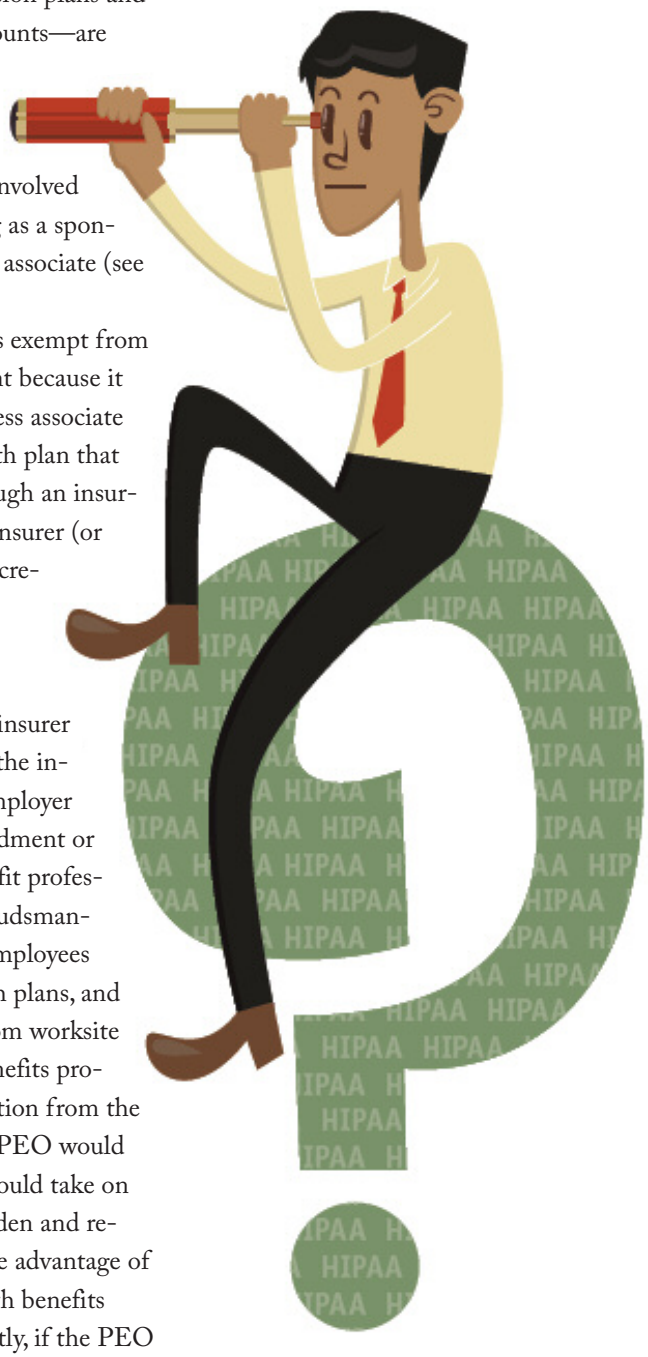
Long-Awaited Final Rule Affects Several HIPAA Provisions

Barry L. Salkin, Esq.

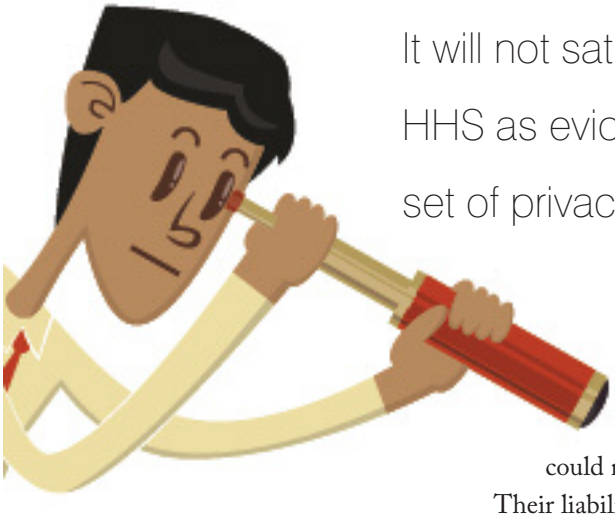
On January 25, 2013, the Department of Health and Human Services (HHS) issued its long-awaited final omnibus rule modifying numerous aspects of the regulations under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), including its privacy, security, and breach notification provisions. Many of the changes will primarily affect healthcare providers, but healthcare plans (and indirectly their plan sponsors) are also affected.

One of the reasons PEOs need to be concerned about the issuance of these final regulations is that the stakes are high: there is a tiered penalty structure, varying from $100 to $50,000 per occurrence, depending upon the culpability of the covered entity, with a maximum penalty of $1.5 million for all identical violations during a calendar year. Further, the final rule allows HHS to share information with other law enforcement entities, such as state attorneys general or the Federal Trade Commission (FTC), which may expand investigation and enforcement activities. The HHS has also recently completed a pilot program and appears to have stepped up enforcement activity.

HIPAA only applies to covered entities: healthcare clearing houses, healthcare providers, and health plans (technically not the sponsors or administrators of those plans). Keep in mind that for these purposes, arrangements that are exempted from other HIPAA requirements—such as stand-alone dental and vision plans and health flexible spending accounts—are subject to these HIPAA requirements. There are a number of possible scenarios in which a PEO can be involved with a health plan, including as a sponsor of a plan or as a business associate (see below).



A PEO may believe it is exempt from HIPAA's privacy requirement because it does not function as a business associate and it sponsors a group health plan that provides benefits solely through an insurance contract with a health insurer (or HMO). The PEO does not create, maintain, or receive protected health information (PHI). It receives summary health information from an insurer that it uses to contract with the insurer and perform certain employer functions such as plan amendment or modification. It retains benefit professionals who serve in an ombudsman-like role between worksite employees and insurers regarding health plans, and requires an authorization from worksite employees to allow these benefits professionals to receive information from the insurer. In this scenario, the PEO would be correct that the insurer would take on the HIPAA compliance burden and responsibility. However, to take advantage of the exclusion, all group health benefits must be insured. Consequently, if the PEO



It will not satisfy HHS if all that a PEO can provide to HHS as evidence of its compliance is an off-the-shelf set of privacy or security procedures.

sponsors a health flexible spending account (or, depending upon the manner in which it is structured, a wellness program) or engages in plan administrative functions under its group health plan, it must comply with the HIPAA privacy rules. Additionally, if it stores or transmits PHI electronically, it is also subject to HIPAA's security rules. While the security rules are scalable, they must all be addressed. That is, a PEO would not need to have as elaborate, sophisticated, or costly system as would a large hospital in a major metropolitan area, but it would still be required to satisfy these rules in a manner consistent with its risk assessment.

It will not satisfy HHS if all that a PEO can provide to HHS as evidence of its compliance is an off-the-shelf set of privacy or security procedures. HHS is requiring evidence that these policies and procedures have been implemented, that such implementation can be documented, and that those employees of the PEO dealing with PHI have been trained.

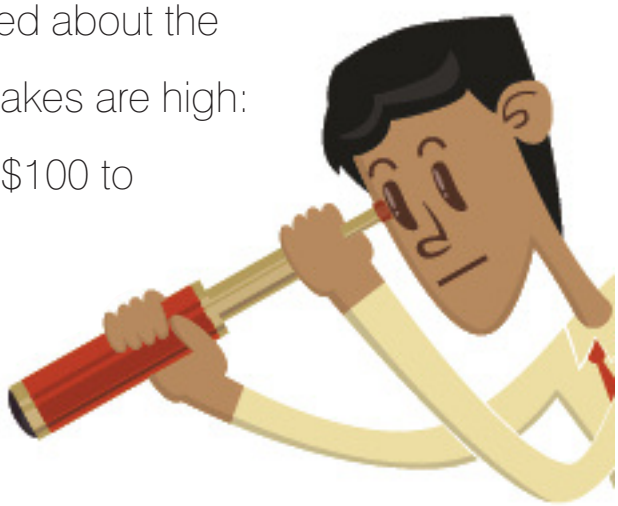
Business Associates

Certain PEOs will serve as business associates of their clients' group health plans. Before the enactment in 2009 of the Health Information Technology for Economic and Clinical Health Act (HITECH) and the recently issued regulations, business associates were not directly liable for HIPAA violations and could not be punished by the HHS. Their liability, if any, was to the client company as a contractual matter under a business associate agreement. Under HITECH, business associates are now directly liable and can be penalized for, among other things: impermissible uses and disclosures of PHI; failure to provide a breach notification to the client company; and failure to comply with the HIPAA security standards. Further, if the PEO, acting as a business associate, engages a subcontractor to perform some of its services with a group health plan, it must enter into a business associate agreement with that subcontractor.

For PEOs that use business associates to service their clients, the final regulations present a new challenge. Prior to HITECH, a covered entity such as a group health plan would only be liable for a business associate's activities if it knew of a pattern of activity or practice of the business associate that constituted a material breach or violation of the business associate's obligations. Under the new regime, a group health plan maintained by a PEO is liable for the activities of business associates who are its agents under the federal common law of agency when the business associate or its subcontractors are acting within the scope of the agency. This issue is not one that can be addressed by adding language to a business associate agreement. The HHS stated in the preamble to the final regulations that the label given to the relationship between the parties is not determinative: rather, the determination is fact-specific. For those readers who are not attorneys, or those attorneys who did not have any classes about the laws of agency (or those who did have such a class but whose recollections of the specifics have become hazy with the passage of time), the HHS indicated that the essential factor in an agency relationship is the "right or authority of the covered entity to control the business associate's conduct in the course of performing a service on behalf of the covered entity."

To determine whether a business associate is an agent, the HHS will examine the business associate agreement and evaluate whether the plan sponsor: retains authority to give the business associate interim instructions; can direct how the business associate performs a service after the agreement is signed; and delegates HIPAA obligations to the business associate . However, the HHS indicated that a business associate is not an agent if the only way that the plan sponsor can control the business associate is through the business associate agreement, for example, by amending the business associate agreement or suing the business associate for breach of the agreement. This is an analysis that should probably be conducted by an attorney, and, in any event, for what it is worth, PEOs should consider asking their business associates to indemnify them if they are found to be liable for significant HIPAA penalties because of a HIPAA violation by the business associate. Of

One of the reasons PEOs need to be concerned about the issuance of these final regulations is that the stakes are high: there is a tiered penalty structure, varying from $100 to $50,000 per occurrence, depending upon the culpability of the covered entity, with a maximum penalty of $1.5 million for all identical violations during a calendar year.

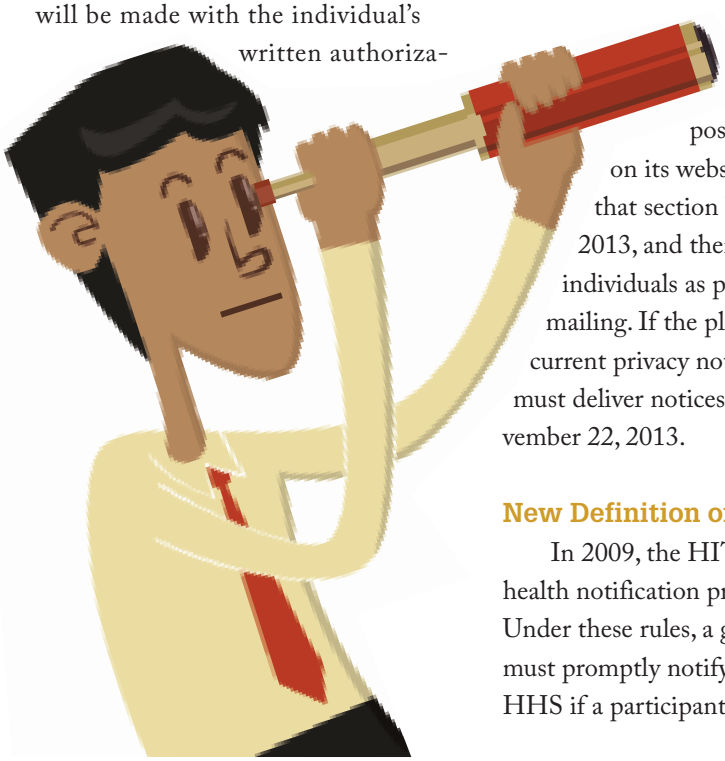


course, a business associate's indemnity is only valuable to the extent the business associate can satisfy any such obligation.

Updated HIPAA Privacy Notice

The new rules require the HIPAA privacy section to be updated to include the following:

- A description of the types of uses and disclosures that require an authorization, including, when needed, psychotherapy notes (if applicable), for marketing purposes, or related to the sale of PHI;
- A statement that other uses and disclosures not described in the section will be made with the individual's written authorization, which the individual may revoke;
- When a covered entity intends to engage in fundraising activities, that the worksite employee has the right to opt out of receiving such communication;
- When a covered entity intends to use disclosed PHI for underwriting purposes, a statement that the covered entity is prohibited from using or disclosing genetic information for such purposes; and
- A statement that a covered entity will notify affected individuals of a breach of unsecured protected health information.



If the PEO's group health plan posts its privacy notice on its website, it must update that section by September 23, 2013, and then deliver notices to individuals as part of its next annual mailing. If the plan does not post its current privacy notice on its website, it must deliver notices to individuals by November 22, 2013.

New Definition of Breach

In 2009, the HITECH Act added a health notification provision to HIPAA. Under these rules, a group health plan must promptly notify participants and HHS if a participant's unsecured PHI is disclosed due to a "breach." HHS initially defined "breach" as the unauthorized acquisition, access, use, or disclosure of PHI that posed a significant risk of financial, reputational, or other harm to the individual. Under the recently issued final rules, a group health plan must presume that its disclosure of unsecured PHI caused a breach unless it can demonstrate that there is a low probability that the PHI has been "compromised," an undefined term. The group health plan has the burden of proving that there was a low probability of breach or, if it cannot satisfy that burden, that all notices of the breach were provided. As a result, group health plans will be required to report breaches of unsecured PHI more frequently than under the prior definition of breach.

While these are only some of the changes to the final omnibus rules, these are the ones that are likely to have the greatest impact upon PEOs.•

Barry L. Salkin, Esq. is of counsel at Olshan Frome Wolosky LLP, based in New York, New York.