Health Care

February 9, 2015

Time for Self-Funded Employer Health Plans, TPAs to Take Data Breach Issues Seriously

By Allen Briskin and Gerry Hinkley

Recent data breaches have brought to the attention of employers who sponsor self-insured health benefit plans ("Plans"), many of which are administered by third party administrators ("TPAs") that are affiliates of national health insurance companies, the need to evaluate their contractual rights to ensure that they can properly respond if their TPA suffers a data breach. Similarly, these events remind TPAs to re-examine their obligations to Plans under applicable laws and their business associate agreements.

TPAs typically perform a variety of administrative services for or on behalf of Plans that require the TPA to create, receive, maintain, and/or transmit protected health information of the Plan's beneficiaries ("PHI"), and thus are "business associates" subject to the HIPAA regulations concerning the privacy and security of health information ("HIPAA"). As business associates, TPAs must comply with HIPAA's Security Rule and certain provisions of HIPAA's Privacy Rule and Data Breach Notification Rule. Business associates that fail to comply are subject to regulatory action under HIPAA's Enforcement Rule. In addition, HIPAA requires these TPAs to enter into business associate agreements ("BAAs") with Plans, which create contractual obligations TPAs owe to Plans in connection with the privacy and security of PHI.

HIPAA dictates some of the BAA's terms, but leaves the parties significant flexibility in establishing the business associate's obligations. At a minimum, the BAA must require that the TPA comply with those aspects of HIPAA that apply to it, including particularly that the TPA must comply with the Security Rule with respect to PHI in electronic form, and that the TPA report security incidents, data breaches, and other unauthorized uses or disclosures of PHI to the Plan promptly.

When the TPA is a national insurance company or its affiliate, PHI of the self-funded Plan's beneficiaries is commonly stored in the same systems that the insurer uses to store the information of its insureds. Under HIPAA, both the insurers and the Plans are "covered entities" with respect to their insureds and their beneficiaries, respectively. However, insofar as the insurer is acting as a TPA for a Plan, the insurer's responsibilities following a data breach of Plan beneficiaries' PHI are those of a business associate. Therefore, the TPA will have different responsibilities with respect to the PHI of individuals who are insured by the TPA or its affiliate, on the one hand, and the PHI of individuals who are covered by an employer-funded Plan, on the other

hand. The response to certain recent data breaches has demonstrated confusion about the parties' respective legal roles, and this confusion may lead to failures of compliance by both TPAs and Plans.

The breaches of health information most commonly reported publicly are breaches of "unsecured PHI" (*i.e.*, PHI that is not encrypted in accordance with standards established by the U.S. Department of Health & Human Services). HIPAA requires that the business associate report such breaches to the covered entity, as well as other security incidents and unauthorized uses and disclosures of PHI, within specified timeframes. The covered entity in turn must report the breach to affected individuals, the Department of Health & Human Services ("HHS"), and, if the breach involves more than 500 residents of a state or other jurisdiction, the prominent media outlets. A Plan should not assume that a TPA's response to a data breach appropriate to the TPA's or its affiliates' insureds is sufficient to address the Plan's independent obligations as a covered entity to respond to the data breach.

Moreover, HIPAA requires that the covered entity make those reports of a data breach without unreasonable delay and in no event later than 60 days after the covered entity discovers the breach or would have discovered the breach with the exercise of reasonable diligence. Often, the covered entity first learns of a data breach when the TPA announces it. Receipt of this announcement almost certainly qualifies as "discovery" of the breach, but the announcement may not be a legally sufficient report of the breach under HIPAA or the business associate contract. Thus, while the TPA's announcement that a breach has occurred marks the beginning of the Plan's legal responsibilities to respond, the TPA may not for quite some time provide the Plan with the information necessary for the Plan to begin its response.

In addition, certain state laws may impose similar breach reporting responsibilities upon either or both the Plan and the TPA, particularly if the breach involves categories of information beyond PHI, such as personal financial information.

Plans should review their BAAs with TPAs and other business associates and determine the following:

- *The period of time within which the TPA must report a breach, security incident, or other unauthorized use or disclosure.* HIPAA requires that the business associate report breaches of unsecured PHI to the covered entity without unreasonable delay and in no event later than 60 days following discovery of the breach. In practice, BAAs typically require that report within a much shorter timeframe, often within a week or two following the time the business associate discovered the breach or would have discovered it if the business associate had used reasonable diligence.

- *The contents of the report of the breach.* HIPAA describes the minimum contents of the business associate's report of the breach, and the BAA may impose additional requirements. A legally complete report will identify the individuals whose information was or was reasonably believed to have been included in the breach, as well as several other elements of information that will permit the covered entity to make its required reports of the breach.

- *The TPA's other responsibilities in connection with the breach.* The BAA typically will require at a minimum that the business associate mitigate the potential harm that could result from the breach. Many BAAs describe the business associate's obligations, and the extent of its liability to the covered entity and/or affected individuals arising from the breach, in more detail. Sometimes, the BAA will require the business associate to perform some of the covered entity's responsibilities arising as a result of the breach, either independently or under the supervision of the covered entity.

- *The TPA's obligations, if any, to pay for the costs of responding to the breach and/or for indemnifying the Plan for losses suffered as a result of the breach.* HIPAA does not require that the BAA discuss financial

responsibility for data breaches or indemnification, but these subjects are commonly addressed either in the BAA or in the associated services agreement under which the business associate performs its services for the covered entity. Sometimes the two contracts contain overlapping or even contradictory terms addressing these concerns. Often, the contracts provide for the business associate to indemnify the covered entity for losses arising either from a breach of the contract and/or a violation of HIPAA. However, in some circumstances, the business associate may suffer a data breach without committing breach of contract or HIPAA violation. The specific terms in which the contracts describe the business associate's obligations to protect PHI and to indemnify for losses may differ greatly from one arrangement to the next, and the Plan should make itself familiar with the specific promises it has received from its business associate.

- *The TPA's obligations to maintain insurance.* HIPAA does not require that the BAA address whether the business associate will maintain cyber insurance to help fund the response to a data breach, but many BAAs or associated services agreements address this subject.

In addition, Plans should review their own HIPAA compliance programs to confirm that they are prepared to perform their responsibilities following a data breach suffered by their TPA, including the making of required reports to individuals, HHS, other agencies and the media. A Plan should also be prepared to investigate and evaluate the circumstances in which the data breach occurred, in order to determine whether to require corrective or other action by the TPA or to terminate its relationship with the TPA. Under HIPAA, when a covered entity determines that a business associate is not acting in compliance with its business associate contract, the covered entity is called upon to take reasonable steps to cure the problem or terminate its relationship with the business associate if it is feasible to do so. Plans should also review their own insurance coverage to determine whether they are sufficiently covered against the risk of data breaches.

Similarly, TPAs should review their HIPAA compliance programs and contractual obligations to confirm that they are prepared to perform their responsibilities, to investigate data breaches and identify and correct deficiencies that may have contributed to the data breach, and to demonstrate to Plans that the TPA has implemented all required corrective action to gain control of the breach and to prevent breaches from occurring in the future.

If you have any questions about the content of this alert, please contact the Pillsbury attorney with whom you regularly work, or the authors below.

Allen Briskin (bio)
San Francisco
+1.415.983.1134
allen.briskin@pillsburylaw.com

Gerry Hinkley (bio)
Los Angeles
+1.213.488.7188
gerry.hinkley@pillsburylaw.com

About Pillsbury Winthrop Shaw Pittman LLP
Pillsbury is a full-service law firm with an industry focus on energy & natural resources, financial services including financial institutions, real estate & construction, and technology. Based in the world's major financial, technology and energy centers, Pillsbury counsels clients on global business, regulatory and litigation matters. We work in multidisciplinary teams that allow us to understand our clients' objectives, anticipate trends, and bring a 360-degree perspective to complex business and legal issues—helping clients to take greater advantage of new opportunities, meet and exceed their objectives, and better mitigate risk. This collaborative work style helps produce the results our clients seek.