Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

WellPoint Settlement: A Warning For HIPAA-Covered Entities

(August 7, 2013, 12:52 PM EDT)


Jennifer Breuer

Managed care company WellPoint Inc. recently entered a resolution agreement with the U.S. Department of Health and Human Services to settle alleged violations of the Health Insurance Portability and Accountability Act privacy and security rules, which related to a 2009-2010 security breach of an Internet-based consumer application database.

WellPoint entered into the resolution agreement on behalf of the health plans under its ownership or control and agreed on July 8, 2013, to pay the HHS $1.7 million to settle the alleged violations. Its affiliated health plans were designated as a single "Affiliated Covered Entity" (ACE) under the HIPAA privacy rule. Specifically, WellPoint's ACE is comprised of 45 individual plans, most of which operate under the names Anthem, Blue Cross and/or Blue Shield and UNICARE.

Affiliated Covered Entities

The HIPAA privacy rule permits legally separate covered entities under common ownership or control to designate themselves as an ACE, which then permits sharing of protected health information among all components of the ACE as if they were a single covered entity.[1]

Covered entities are deemed to be under "common ownership" if they share an ownership or equity interest of 5 percent or more. "Common control" exists if an entity has the power, directly or indirectly, significantly to influence or direct the actions or policies of another entity.[2]

To be considered an ACE, the participating covered entities must document their participation in the affiliation and each covered entity must maintain a written or electronic record of the designation.[3] Practically speaking, compliance with this documentation requirement may most easily be accomplished by including language so stating in each covered entity's notice of privacy practices.

HIPAA Breach

WellPoint initially reported the breach of electronic protected health information (ePHI) to the HHS's Office for Civil Rights (OCR) in 2010. A subsequent investigation by the OCR revealed that WellPoint had not maintained adequate administrative and technical safeguards to protect its customers' data as required by the HIPAA security rule.

Specifically, the OCR determined that WellPoint failed to adequately implement policies and procedures for authorizing access to ePHI in the database, perform an adequate risk analysis following a software upgrade that affected the database and adequately implement technical safeguards to verify the identity of persons trying to access ePHI in the database.

As a result of these inadequate security measures, WellPoint impermissibly disclosed ePHI of 612,402 health insurance applicants. The unsecured data included customer names, dates of birth, addresses, Social Security numbers, telephone numbers and health information.

Resolution Agreement

Interestingly, the resolution agreement was entered into between the HHS and WellPoint, an Indiana corporation that is not a covered entity. Instead, WellPoint is a holding company that owns an interest in the health plans that form the ACE.

The HHS asserted that because WellPoint was the controlling entity around which its covered entity affiliates formed the ACE — and because PHI was shared between the ACE and WellPoint — WellPoint should be held responsible for the alleged violation. Supporting this assertion were the facts that certain WellPoint employees served as workforce members of the ACE, WellPoint developed policies and procedures on behalf of the ACE, and the server from which the breach occurred was located in WellPoint's offices.

The HHS's approach with WellPoint can be contrasted with its approach to its resolution agreement in June 2013 with Shasta Regional Medical Center (SRMC) and the 15 other covered entities that designated themselves a single ACE under common ownership of or control by Prime Healthcare of California. Pursuant to the SRMC resolution agreement, each of the individual covered entities that comprised the ACE — but not Prime Healthcare — collectively were required to pay $275,000 as a settlement amount and to comply with the terms of a corrective action plan (CAP).

The SRMC settlement arose out of allegations that the SRMC provided PHI to several media outlets without proper authorization of the subject of the PHI. In this instance, the alleged violations of the SRMC were imputed to the other legally separate covered entities that comprised the ACE. Thus, the SRMC's designation with the others as an ACE led the HHS to find all of the ACE components jointly and severally liable for the disclosures made by the SRMC.

Although the Prime Healthcare and WellPoint ACE settlements are based on very different underlying facts resulting in violation of HIPAA, both involve ACEs that could have been found to be jointly and severally liable for the violation of one of its component parts. However, the OCR took very different approaches to enforcement in these two cases.

As described above, in the Prime Healthcare matter, the SRMC and the other covered entities that comprised the ACE were determined to be jointly and severally liable for the violation by the SRMC. In contrast, the OCR likely determined that WellPoint itself was not a covered entity but instead acting as a business associate of the covered entities that comprised its related ACE. As the responsibility for the violation could be traced to WellPoint itself, the OCR sought and obtained a settlement with WellPoint — even though the OCR did not have jurisdiction over business associates at the time of the violation.

While a resolution agreement is a voluntary settlement such that the HHS did not have to prove jurisdiction, the HHS' approach in the WellPoint settlement should be of note — and potentially of some concern — to "parent" or other holding companies, especially after the Sept. 23, 2013, enforcement date of the HIPAA omnibus final rule.

Holding companies and their ACE components should consider whether business associate (BA) or other agreements are necessary for the sharing of PHI outside their covered entity components. If the parent or holding company is itself a health care provider or covered entity participating in the ACE, then no BA agreement is required where it performs a service on behalf of the ACE or any covered entity participating in the ACE.[4] However, if the parent or holding company is not a health care provider or covered entity participating in the ACE, then a BA agreement would be required for any disclosure of PHI from ACE to the parent or holding company.

Notably, the WellPoint resolution agreement does not contain a CAP. The lack of CAP seems to indicate that WellPoint took sufficient mitigating action and adopted adequate security measures following its discovery of the breach in 2010. Such action may have saved WellPoint millions of dollars associated with maintaining compliance with legally required corrective action measures and with the OCR's monitoring of the CAP.

The HHS action itself, as well as the significant settlement amount, serves as a warning to HIPAA-covered entities and business associates that all Internet-based applications, portals and information systems containing ePHI must comply with the HIPAA security rule, both when originally

implemented and with each subsequent upgrade.

In a press release announcing the resolution agreement, the HHS noted, "This case sends an important message to HIPAA-covered entities to take caution when implementing changes to their information systems, especially when those changes involve updates to Web-based applications or portals that are used to provide access to consumers' health data using the Internet."

Steps to Protect Against Similar HIPAA Enforcement

We recommend that covered entities that comprise an ACE, as well as the parent or holding companies through which such covered entity components of an ACE are related, take the following steps to avoid liability from a HIPAA violation — whether under the joint and several liability theory or business associate theory:

- Review relationships and the documentation of such relationships among and between ACEs and other related entities with which they share PHI.
- Consider whether intercompany contribution agreements may be beneficial to restore financial responsibility for any HIPAA violations to the party responsible for the violation.
- Revisit risk analyses, especially following any changes to the underlying technology.
- Update policies and procedures as necessary to account for changes in technology or practices.
- Continue workforce training.
- Audit ongoing programs.
- Monitor security intrusions.
- Implement a breach response plan.

--By Jennifer R. Breuer, Sara H. Shanti, David A. Mayer and Fatema Zanzi, Drinker Biddle & Reath LLP

Jennifer Breuer is a partner, Sara Shanti and Fatema Zanzi are associate, and David Mayer is a senior adviser in the firm's Chicago office.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] 45 C.F.R. 164.105(b).

[2] 45 C.F.R. 164.103.

[3] 45 C.F.R. 164.105(c).

[4] We also note that based on the commentary to the Omnibus Final Rule, a well-drafted BA agreement may negate an agency relationship between a covered entity and its business associate, and may further limit a covered entity's liability for the actions of its business associate.