Published on *The National Law Review* https://natlawreview.com

WellPoint, Inc. Pays Department of Health and Human Services (HHS) $1.7 Million to Settle Affiliated Covered Entity's Alleged Health Insurance Portability and Accountability Act (HIPAA) Violations

Article By:

Jennifer R. 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 HIPAA Privacy and Security Rules, which related to a 2009-2010 security breach of an Internet-based consumer application database.

WellPoint, on behalf of the health plans under its ownership or control, which were designated as a single "Affiliated Covered Entity" under the **Health Insurance Portability and Accountability Act of 1996** ("**HIPAA**") Privacy Rule, agreed on July 8, 2013, to pay HHS $1.7 million to settle the alleged violations. The Affiliated Covered Entity is composed of nearly 50 health plans, most of which operated in a single state.

HIPAA Breach

WellPoint initially reported the breach of electronic protected health information (ePHI) to HHS's Office for Civil Rights (OCR) in 2010. A subsequent investigation by 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, OCR determined that WellPoint failed to

(1) adequately implement policies and procedures for authorizing access to ePHI in the database, (2) perform an adequate risk analysis following a software upgrade that affected the database, and

(3) adequately implement technical safeguards to verify the identity of persons trying to access ePHI in the database.

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

Resolution Agreement

Interestingly, the Resolution was entered into between HHS and Wellpoint, an Indiana corporation that is not a traditional covered entity. Instead, WellPoint is a holding company that owns an interest in the health plans that form the Affiliated Covered Entity. HHS asserted that because WellPoint was the controlling entity around which its covered entity affiliates formed the Affiliated Covered Entity—and because protected health information (PHI) was shared between the Affiliated Covered Entity and WellPoint—WellPoint should be responsible for the alleged violation. Supporting this assertion were the facts that (1) certain WellPoint employees served as workforce members of the Affiliated Covered Entity, (2) WellPoint developed policies and procedures on behalf of the Affiliated Covered Entity, and (3) the server from which the breach occurred was located in WellPoint's offices.

While the Resolution Agreement is a voluntary settlement such that HHS did not have to prove jurisdiction, this should be of note—and potentially of some concern—to "parent" or other holding companies to which HIPAA does not apply directly, but applies instead to its controlled affiliates. Holding companies that have active participation in the affairs of a covered entity could be subject to the provisions of HIPAA, either as a business associate or a member of an Affiliated Covered Entity. Holding companies and their Affiliated Covered Entity components also should consider whether business associate or other agreements are necessary for the sharing of PHI outside their covered entity components. As of September 23, 2013, OCR has indicated that it intends to enforce HIPAA's Privacy Rule and Security Rule against entities that perform the function of a business associate, whether or not a business associate agreement is in place.

Notably, the Resolution Agreement does not contain a Corrective Action Plan (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 a formal CAP and with OCR's monitoring of such plan. The HHS action itself, as well as the significant settlement amount, serve 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, HHS noted that "[t]his 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 That Covered Entities Can Take to Protect Against Similar HIPAA Enforcement

- Review relationships and the documentation of such relationships among and between Affiliated Covered Entities and other related entities with which they share PHI
- 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

National Law Review, Volume III, Number 206