# Responding to a Data Breach in Your Health Plan

**ATTORNEYS**

Jodi H. Epstein

Laurie E. Keenan

Kevin P. O'Brien

Kevin P. O'Brien

Spencer F. Walters

**PRACTICE AREAS**

Benefits & Compensation

Health & Welfare

*Employee Benefits Insider*

February 12, 2015

The recent data breach at Anthem, Inc. (formerly WellPoint), the second largest U.S. health insurer, reveals an unwelcome trend: Health care companies are increasingly becoming a target for hackers. These companies are repositories of vulnerable personal health information ("PHI"), such as Social Security numbers, names, birth dates, emails, and addresses.

Anthem has pledged to notify affected customers and to provide credit and identity-theft monitoring services for free. But if Anthem administers your self-insured health plan, you may need to take immediate action to avoid a violation of the privacy or security provisions of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health Act of 2009 ("HITECH"), as well as violations of various state and foreign privacy laws. Some of these steps are outlined below. (In a fully-insured health plan, the burden of notification, investigation, and mitigation would fall on Anthem instead.)

The starting point for analysis is the service agreement between Anthem and the plan. Where a plan is self-insured and Anthem serves as its third-party administrator, HIPAA only requires that Anthem notify the plan of a breach. **Under HIPAA, the plan would then bear the burden (i) to assess the damage, (ii) to notify all relevant parties, and (iii) to mitigate any harm.** The plan may have additional fiduciary obligations under ERISA as well.

***This burden can be shifted through the plan's service agreement, however.*** The Department of Health and Human Services ("HHS"), which oversees HIPAA enforcement, encourages plans and their business associates to reallocate these obligations contractually, to the party who is best positioned to carry them out. The Anthem data

breach serves as a reminder to take a hard look at the plan's service agreements. These contracts should be drafted to ensure that the costs of investigating, disclosing and correcting a vendor's privacy breach are borne by the vendor, rather than the plan or plan sponsor.

Below are the steps needed to remedy a HIPAA privacy breach. By negotiating a robust service agreement, you can protect your plan by shifting these added costs to the responsible third-party administrator:

- *Breach Procedures*. The plan should have (and follow) its breach policies and procedures. These should include notification (further described below), mitigation steps, updated risk analyses, and review of existing policies and procedures.
- *Notice to Plan*. Upon discovery of a breach, a business associate has the obligation to notify the plan of the breach and, to the extent possible, identify the individuals whose PHI was breached.
- *Notice to Media*. If a breach involves 500 or more residents of a state or jurisdiction, the plan must notify prominent media outlets serving the State or jurisdiction. This notification must occur without unreasonable delay and in no case later than 60 days after discovery of the breach.
- *Notice to HHS*. The plan must notify HHS of any breach, either at the same time as the media if applicable, or else it must log or document any breach involving fewer than 500 residents and report it to HHS within 60 days.
- *Notice to States*. Forty-seven states (as well as the District of Columbia and Puerto Rico) have enacted their own notification requirements that are not preempted by HIPAA unless "contrary" to the federal law. (ERISA preemption arguably could still apply.)
- *Notice to Insurers*. If the plan has purchased cyber-security insurance, the plan may need to notify the insurer in a timely manner.
- *Disclosure to Participants*. Without unreasonable delay, and in no case later than 60 days after discovery of the breach, the plan is required to notify via a plain-English disclosure each individual whose unsecured (i.e., unencrypted) PHI was, or is reasonably believed to have been, accessed or acquired as a result of the breach. Notice is generally required by first class mail or email; in some cases additional disclosures will be required on the employer's web page.
- *Duty to Mitigate*. The HITECH Act requires that the plan disclose the steps taken to mitigate the harm caused by a privacy breach. Below are several "best practices" that have emerged in this regard.

- *Call Center for Participants*. The HITECH Act requires, at a minimum, that the plan provide a toll-free number where affected participants can gain additional information. Although not legally mandated, it is routinely expected that the plan will establish a dedicated call center to respond to inquiries from participants. Establishment of a central website may emerge as a best practice as well.
- *Identity-Theft Monitoring Services*. It has become customary for the plan to provide identity-theft protection insurance and credit report monitoring services for affected participants. Robust protection in this area would include regular credit reports, identity theft assistance, and fraud monitoring (i.e., monitoring applications for new credit cards and bank accounts, for address changes, and for any data shared on the Internet black market) for all affected participants and their family members (including children).
- *Public Relations Consultants*. Although optional, hiring a public relations firm can help avoid long-term reputational damage.

- *Internal Investigation*. The plan sponsor should be prepared to cooperate with any internal investigation (by the third party administrator) into the source of the privacy breach. It also should be prepared for a potential internal audit of its existing policies and procedures.
- *Prepare for HHS and/or State Investigation*. HHS opens investigations into all large breaches (affecting 500 or more individuals), as well as some smaller breaches. Under HITECH, state attorneys general also may bring civil suits against the plan on behalf of state residents for HIPAA privacy and security violations. Additional investigations may be initiated by the plan sponsor's industry-specific regulators, or by other government authorities or law-enforcement agencies.

A HIPAA privacy violation can be costly for the plan. The HITECH Act heightened enforcement of the HIPAA privacy and security rules, by requiring proactive HHS audits and by imposing mandatory breach notification. These rules apply to both health plans and providers. The HITECH Act also introduced a new tiered civil penalty structure, increasing the maximum fine to $50,000 per violation (subject to a cap of $1.5 million per calendar year). Such violations have become a priority for the HHS Office for Civil Rights, as reflected in recent settlement agreements imposing fines well over $1 million on the responsible parties (and in at least one recent case, over $3 million for an entity that refused to cooperate in an OCR investigation). We expect to see an increase in such settlements in light of the new HIPAA Audit Program rolled out by OCR in 2014 (based on its 2011 pilot audit program).
http://www.hhs.gov/ocr/privacy/hipaa/enforcement/index.html

In addition to these civil penalties, the practical costs of remedying a privacy breach can be substantial. Among experts that we have canvassed, the general consensus is that the cost of investigation, notice, credit monitoring, call center, other remedial services and associated losses can be approximately $100 to $300 per affected record. In Anthem's

case, where 80 million individuals are affected, the total expected cost may be billions of dollars.

***FOR MORE INFORMATION***

*Contact the Ivins,*

*Phillips & Barker*

*Employee Benefits Practice*