jackson|lewis

Employer FAQs: Responding to the Anthem Breach

By Joseph J. Lazzarotti, Esq., CIPP

The first massive data breach of 2015 hit one of the country's largest insurance issuers, Anthem, Inc., including Anthem Blue Cross and Blue Shield and other related entities (Anthem). The incident reportedly affected over 80 million persons who are or were covered under a policy or program insured or serviced by Anthem. The personal note from Anthem's CEO, Joseph R. Swedish, and the Anthem Facts (or FAQs) seek to provide helpful information to the millions of individuals affected. These communications address what is known about the incident, describe the kinds of information compromised, warn affected persons about potential email attacks, and advise that there is more information coming.

But there is not much information at this point for employers that are plan sponsors of group health plans and other welfare plans serviced by Anthem either as an insurance issuer or a third party claims administrator (TPA). Below are some FAQs about the Anthem breach for affected employers.

Isn't this really Anthem's problem?

From a legal compliance standpoint, the answer largely depends on whether the plan is insured or self-funded. For example, as discussed below, in the case of a self-funded group health plan, the HIPAA breach notification rules place the obligation to notify affected persons on the covered entity (i.e., the plan, and practically the plan sponsor) and not on the business associate (i.e., the TPA). However, contract obligations in the business associate agreement (or administrative services only agreement) have to be considered. Finally, as a practical matter, because employees and other persons covered under the plan(s) will be concerned and have questions, employers will need to have a strategy for addressing those concerns.

Is the information involved subject to HIPAA; the Anthem FAQs say Anthem does not believe diagnosis or treatment information was compromised?

According to the Anthem FAQs:

> ***the member data accessed included names, dates of birth, member ID/ social security numbers, addresses, phone numbers, email addresses and employment information…[but its] investigation to date indicates there was no diagnosis or treatment data exposed***.

Many maintain the mistaken belief that, in the case of a group health plan, a covered person's name and social security number, alone, is not "protected health information" (PHI) under the privacy regulations issued under the Health Insurance Portability and Accountability Act (HIPAA). The absence of diagnosis or treatment data does not make information any less PHI. This is because the regulatory definition includes not only information about a person's physical or mental health condition, *but also how care is paid for and provided*. Thus, data elements that relate to the payment or provision of health care, such as address and email address, could constitute PHI even if not as sensitive as a covered person's diagnosis information.

What about the state breach notification laws, do they apply?

The Anthem breach involves personal information of individuals, such as names, member ID/social security numbers and other data, the kind of information protected by state breach notification laws, which currently exist in 47 states. Given the massive scale of the breach, it is likely that there are affected individuals residing in all 50 states and beyond.

Some of those state laws have exceptions when HIPAA or other federal regulations apply. Some do not. According to the Anthem FAQs, all product lines have been affected, not just health insurance (medical, dental and vision). This includes life, disability, workers compensation and other policies and products which typically are not subject to HIPAA. Thus, regardless of the Anthem policy or product at issue, the applicable state laws will need to be considered to determine their application in this case.

Our plan is/was insured by Anthem, what should we be doing?

Under HIPAA, both the employer's group health plan under ERISA and the health insurance issuer that provides the insurance for that ERISA plan are covered entities under HIPAA. Covered entities have the primary breach notification obligations. Under state breach notification laws, the primary notification obligation generally falls on the entity that owns or licenses the data, not necessarily the entity that held the data at the time of the incident. However, in the case of a breach experienced by an insurer, and not the employer sponsoring the plan, the insurer generally is considered to be responsible for responding to the breach. Even if not entirely clear in the applicable statutes or regulations, this makes practical sense because the carrier is in control of the investigation and the facts, and usually is in the best position to work with law enforcement. Carriers can typically disseminate notifications more efficiently across the affected policies, as well as to federal and state agencies, and the media.

To date, Anthem appears to be taking the lead on the investigation and notifying affected persons. For example, its FAQs inform members that they can expect to "***receive notice via mail which will advise them of the protections being offered to them as well as any next steps***". Because this incident affects both HIPAA-covered and non-HIPAA plans, it is likely the notices will address the applicable HIPAA and state law requirements.

Still, there are some action items for affected employers to consider:

- **Stay informed.** Closely follow the developments reported by Anthem, including coordinating with your benefits broker who might have additional information.
- **Consult with counsel.** Experienced counsel can help employers properly identify their obligations and coordinate with Anthem as needed.
- **Communicate with employees.** Be prepared to respond to employee questions – consider providing a short summary of the incident to employees along with links to the Anthem materials and FAQs.

- **Evaluate vendors.** Use this incident as a reason to examine more closely the data privacy and security practices of all third party vendors that handle the personal information of your employees and customers, including insurance companies. Of course, a data breach is generally not a reason, by itself, to switch vendors. With breaches of all sizes affecting many companies, there is no telling whether the grass will be greener. But making inquiries and pressing vendors to do more, including by contract, is a prudent course of action, and even required in some states.
- **Revisit your own data security compliance measures**. Employers should take this as an opportunity to assess or reassess their own data security compliance measures. As many have noted, it is not just large companies that are vulnerable to these kinds of attacks.

Our plan is/was self-insured and Anthem was our TPA, what should we be doing?

In this case, whether the plan is a health plan covered by HIPAA or another employee welfare benefit, as TPA, Anthem maintains the personal information of covered persons *on behalf of the employer*. In that case, Anthem's legal obligations under HIPAA and state law, as applicable, generally require only that it notify the employer concerning the circumstances of the breach – how it happened, the kind of information breach, who was affected, etc. Then it is up to the employer/covered entity to carry out an appropriate investigation, provide notice to affected persons and otherwise comply with the applicable federal and state laws. However, administrative service agreements and in the case of health plans, business associate agreements, may delegate some of these responsibilities to the TPA, as well as indemnification obligations. So, in addition to some of the steps listed above, employers have a number of things to consider and steps to take:

- **Determine if plans have been affected.** Employers might soon be receiving communications from Anthem concerning whether their plans have been affected. They also may want to reach out to Anthem and inquire.
- **Act quickly**. HIPAA and state breach notification laws generally require that notices be provided *without unreasonable delay*, as well as place outside limits on when such notices can be provided – e.g., 60 days following discovery under HIPAA, and 30 days in Florida.
- **Examine the administrative services agreement and/or business associate agreement.** For plans have been affected, employers need to review the related agreements as they could place certain obligations either on the employer or Anthem. The agreements also could be silent, in which case the plan/employer likely has the obligations to notify participants, agencies and media.

  If Anthem is responsible for responding, employers should consider taking certain steps to ensure Anthem's reaction is compliant – e.g., has it protected data from further attacks, completed the investigation, identified all affected persons, crafted content-compliant notifications (HIPAA and some state laws have specific content requirements), and notified the applicable federal and state agencies.

  If the employer retained the responsibility to respond, it should be taking steps immediately to determine what happened and coordinate with Anthem concerning the response. This includes some of the steps listed above. For instance, in the case of group health plans under HIPAA, employers will

need to confirm with Anthem whether Anthem or the employer/group health plan will be notifying the Department of Health and Human Services. Also, employers that have developed a data breach response plan (a good idea for all employers) should review that plan and follow it.

However, as a practical matter and regardless of what is in the services agreement, Anthem may decide to take the lead on the response, and not give employers much choice in shaping the communications made to persons covered under the plans.

- **Communicate with covered persons.** If it turns out that the employer will be notifying plan participants, in addition to the notification letters referred to above, employers also need to be prepared to address participant questions about the incident. Designating certain individuals or outside vendors to handle these questions and creating a script of anticipated questions and answers would facilitate a consistent and controlled response.
- **Evaluate insurance protections**. Some employers may have purchased "cyber" or "breach response" insurance which could cover some of the costs related to responding to the breach or defending litigation that may follow. Employers should review their policy(ies) with their brokers to understand the potential coverage and what steps, if any, they need to take to confirm coverage.
- **Document steps taken.** Employers should document the steps they take to investigate and respond to the incident, particularly if it affects one of their group health plans covered by HIPAA.

Some employees have complained about our data security practices, how should we respond?

Take them seriously! Data security has been recognized at the federal, state and local levels as an important public policy concern, most recently by President Obama at the recent State of Union Address. Disciplining or taking adverse action against an employee who has raised these concerns could expose the employer to retaliation claims or violations of employee whistleblower protections.

* * *

For employers large and small, incidents like this can be a significant disruption to the workforce. To minimize that disruption, employers may want and need to communicate with their employees, and should do so confidently, but carefully. More information can be very helpful, but too much information and information that is repetitive can be confusing and frustrating for employees. Employers should involve key persons inside their organizations and possibly seek outside expertise and counsel to reach an appropriate balance in their response strategy and communications.

For more information, contact Joe Lazzarotti at 973-451-6363, Nicky Jatana at 213-630-8233, a member of our Privacy, e-Communication and Data Security Practice Group, or the Jackson Lewis attorney with whom you normally work.

4852-1346-6657, v. 1