# Anthem Breach Overview

February 2015

On February 4, 2015 health insurer Anthem, Inc., one of the largest health insurers in the US, announced that it had been the target of a sophisticated cyber attack. To date, the company acknowledges that the attack impacted:

- Anthem Blue Cross
- Anthem Blue Cross and Blue Shield
- Blue Cross and Blue Shield of Georgia
- Empire Blue Cross and Blue Shield
- Amerigroup
- Caremore
- Unicare
- Healthlink
- DeCare

Anthem has a significant presence in the country's most populous states, particularly California and New York. It also serves as a third-party claims administrator for many self-insured, employer-sponsored group health plans.

The breach is being investigated by the FBI, and reports have linked the attack to a foreign state. It is unknown if the hackers moved some or all of the data to other sites before the data was locked down by investigators.

The compromised data includes personal information of its insureds, such as:

- Names of enrollees
- Birthdays
- Medical IDs/Social Security numbers
- Street addresses
- Email addresses
- Employment information, including income data

Anthem has said that the breach does not include "credit card or medical information, such as claims, test results, or diagnostic codes."

LOCKTON®

## THOSE AFFECTED

Anthem has not stated how many individuals' records were affected; however, reports have stated that the breach may have affected as many as 80 million current and former Anthem members.

Anthem is making information about the breach available at www.AnthemFacts.com.

## NEXT STEPS

Anthem has taken the first steps in the response to the event and has already started the process of notifying affected individuals—by mail, and where possible, email—everyone whose personal information was stored on the compromised database.

However, every organization whose employees may have been affected should determine whether and how to communicate to their employees or other affected individuals.

The strategy for your response, if any, should be coordinated between your internal and external legal resources.

## FAQS RELATED TO ANTHEM'S DATA BREACH

### If an employer uses Anthem as the insurer of its health plan, does the employer have an obligation to notify employees about the breach?

The obligation to provide notice of a breach of "personally identifiable information" (PII), such as names, Social Security numbers, addresses, etc., and "protected health information" (PHI), such as certain enrollment information and individually identifiable health information related to past, present, or future medical care, is governed by both federal and state law.

Anthem has specific notice obligations and has publicly stated it intends to notify, by email or letter or both, individuals affected by the data breach. Whether an employer using Anthem as an insurer has a notice obligation to its affected employees depends on a variety of factors.

The federal Health Insurance Portability and Accountability Act (HIPAA), as amended by the federal Health Information Technology for Economic and Clinical Health (HITECH) law, imposes very specific notice and disclosure obligations on health plans in the wake of a breach of unsecured PHI. Where Anthem is acting as an *insurer,* and the employer is not "hands on" with the plan's PHI (i.e., it does not acquire, maintain, or transmit the plan's PHI), the notice and disclosure obligation is Anthem's. Anthem's affirmative notice efforts now underway appear to reflect Anthem's understanding that it has the obligation.

### If an employer uses Anthem as a third-party administrator of its health plan, does the employer have an obligation to notify employees of the breach?

The starting point for an employer would be to review its agreement with Anthem. Where the health plan is self-insured and Anthem is acting as a "business associate" of the plan, Anthem (as the plan's third-party claims payor) has a duty under HIPAA/HITECH to notify the employer health plan of the breach.

Generally, it is the *health plan's* responsibility to then supply notice to affected individuals and, in some cases, federal authorities and media outlets. *However*, health plans and their business associates may agree upon who will actually supply the notice. The federal Department of Health and Human Services, which oversees federal enforcement of HIPAA, encourages plans and their business associates to consider who is in the best position to provide notice to affected individuals.

In this case, it is worth noting that Anthem has pledged to supply notice to all affected individuals.

## Is an employer responsible for any financial consequences of the Anthem breach?

The loss resulting from the Anthem breach could be enormous. Estimates of the cost to respond to a breach like this run from $100 to $230 per individual affected. Based on Anthem's public statements, costs to notify affected individuals and provide identity theft protection and other services should be borne, initially or ultimately, by Anthem.

## If an employer incurs costs as a result of the breach affecting their employees will the employer's insurance policies pay them?

Whether any losses incurred will be covered by insurance depends on the nature of the loss and the terms of the relevant insurance policies.

If an employer incurs any direct costs related to the breach—such as notification, legal, public relations, call center, or credit/identity monitoring costs—its data security and privacy liability (cyber) insurance policy may cover those expenses, especially if it is determined that the employer is legally obligated to respond to the breach.

If a lawsuit or other claim is filed against the employer for damages related to the Anthem breach, the privacy liability insuring agreement in the employer's cyber policy may provide coverage for defense costs and damages associated with the claim.

Other policies, such as D&O and General Liability, may also provide some coverage, though many of these will have specific exclusions or other language that insurers frequently use to deny such coverage. In the event a claim is made against an employer, its broker and legal counsel can help determine which insurance policies might apply.

## Does an employer affected by this need to provide notice to its cyber liability insurers now?

The Anthem breach may include data for which your company has an obligation to notify affected individuals. Under HIPAA notice must be provided within 60 days after the breach is discovered. Some states require notice to be given even more quickly. Cyber policies are intended to cover the cost of legal advice needed to determine the existence and extent of any notice obligation as well as other expenses incurred as a result of a breach. Such policies are triggered by timely notice being given to the insurer. Lockton recommends that companies give formal notice of the breach to their cyber insurers now.

It is less clear whether immediate notice is needed under other policies that might cover claims arising from the Anthem breach. Each employer should discuss its unique circumstances with its broker to determine whether additional notices should be given now.

## Can an employer be held liable on account of the Anthem breach?

Class action lawsuits have already been filed against Anthem as a result of the breach and many more such suits are almost certain to follow.

Claims against employers that do business with Anthem are less certain, but still possible. An employer may be held responsible for data that it collects, even if that data are then transferred to a third party such as Anthem, where the breach occurs. While an employer's liability for such a breach may be tenuous, it is possible for a lawsuit or other claim to be made, and while such claims are likely to face significant obstacles, the defense costs can still be substantial.

Defense costs for such a claim could be covered by the privacy liability insurance agreement of an employer's cyber policy. Also, if the claim alleges that individuals breached their fiduciary responsibilities to employees, D&O and fiduciary liability policies might also respond.

## Are there resources available to me to help me determine how I should respond?

Your insurance broker, in conjunction with experienced privacy counsel, can help determine the appropriate response to this breach and advise you on any insurance coverage that might be available. They can, in turn, direct you to any other resources you may need, such as public relations and communication teams, to assist in the strategy for the overall response.




g\lbg\2015\anthem breach.indd

LOCKTON®

www.lockton.com