MY BENEFIT ADVISOR

Anthem Cyber Attack

Issued date: 03/10/15

Frequently Asked Questions

On January 29, 2015, Anthem discovered that it had experienced a cyber attack where a hacker gained unauthorized access to Anthem's computer systems and obtained certain personal information regarding Anthem's consumers who were or are currently covered by Anthem or other independent Blue Cross and Blue Shield plans that work with Anthem. This includes, but is not limited to, employer-sponsored group health plans (both insured and self-insured). Anthem believes the suspicious activity occurred over the course of several weeks beginning in early December 2014. The below FAQs are intended to provide you with information regarding the recent cyber attack experienced by Anthem. Information on this situation is changing and should be closely monitored.

Whose Information Was Compromised?

Anthem's cyber attack resulted in an improper disclosure of nearly 80 million records and may affect participants who received services from an Anthem Blue Cross and Blue Shield contracted health provider from 2004 through the date of the cyber attack. Any health plan participant that was covered under a Blue Cross and Blue Shield Plan could have been impacted if they received services in a state serviced by the Anthem network of health care providers.

It may be prudent for any participant who had Blue Cross and Blue Shield coverage from 2004 on to review the www.anthemfacts.com website and request credit protection services. Plan sponsors may wish to include in any notice to employees that the breach relates to records created from 2004 on and may affect employees who had previously been covered under other employer sponsored health plans accessing Blue Cross and Blue Shield network providers. Anthem, formerly known as Wellpoint, runs health care plans under the Blue Cross Blue Shield, Empire Blue Cross, Amerigroup, Caremore, Unicare, Healthlink, DeCare, HealthKeepers and Golden West brands.

What Information Was Compromised In The Breach?

Anthem has indicated that to date, they believe certain personal information, including names, dates of birth, member ID numbers, social security numbers, street addresses, emails and employment and income information has been compromised. Anthem does not currently believe that credit card or detailed medical information (such as claims, test results or diagnostic codes) were compromised.

Is The Anthem Cyber Attack A Breach Under HIPAA?

According to a Town Hall conference call on February 11, 2015 and a letter provided to plan sponsors dated February 23, 2015 from Kenneth Goulet, President, Commercial and Specialty Business at Anthem, Anthem views the unauthorized access of information as a result of this cyber attack a breach under HIPAA and under certain state privacy laws. Anthem continues to investigate this issue and work with applicable regulators at the federal and state level.

Generally, self-insured group health plans that contract with Anthem as a TPA are subject to HIPAA breach rules, while Anthem is solely responsible for HIPAA breach issues for fully insured plans that do not receive PHI. Larger fully insured health plans that have access to or are provided with PHI will need to assure that they are compliant with HIPAA breach rules if their participants were affected.

What Are Plan Sponsor Obligations?

Because group health plans are subject to the HIPAA Privacy and Security Rules, the plan sponsor has obligations to determine whether a breach of protected health information (PHI) has occurred and, if so, provide notification to affected participants, cure the cause of the breach, and attempt to address any harm that may have occurred to a participant as a result of the breach.

What Do Plan Sponsors Need To Do?

Hopefully not much. Anthem has outlined, in the letter previously referenced, that they will be assisting clients in fulfilling obligations under HIPAA or state privacy laws. Their goal is to promote a consistent message to potentially impacted individuals. In that regard, Anthem intends to issue notices to affected participants and to appropriate state and federal regulators. Anthem has indicated that it believes these notices will satisfy the plan sponsor notice requirements, including notice obligations under the HIPAA breach notification regulations issued.

Specifically, according to the letter, Anthem has taken or intends to take the following actions:

- As a business associate with health plans, Anthem will provide to the plan sponsor written notice of the breach and provide information as required by HIPAA within sixty (60) days after Anthem discovered the breach;

- Anthem will provide, on behalf of the health plan, notice to potentially impacted individuals for whom Anthem has contact information within legally required timeframes;

- Anthem will deliver written notice to identified state regulators as required by state data breach notification laws and that notice will reference any affected health plan by name;

- Anthem will make substitute notice under HIPAA or state data breach notification laws on behalf of the affected health plan to potentially impacted individuals for whom Anthem has insufficient or out-of-date contact information or where otherwise permitted by law; and

- Anthem will notify federal regulators on behalf of the health plan, including the Department of Health and Human Services' Office for Civil Rights, and that notice will reference specifically affected health plans by name.

Anthem has indicated that while it does not provide legal advice, it believes that all notices already delivered, and those that will be delivered in the future, comply with the applicable laws that require those notices. It is Anthem's position that these notices will fulfill both Anthem and affected health plan's notice obligations relating to the breach of participant information. However, Anthem encourages affected health plans to seek advice from counsel to address specific questions or concerns.

What Is Anthem Doing To Help Affected Participants?

Anthem is notifying potentially impacted current and former members by U.S. Postal mail regarding the cyber attack and is including information on how individuals may protect themselves. One service Anthem is offering includes identity protection and repair services free of charge. Anthem is working with AllClear ID, an identity protection provider, to offer 24 months of identity theft repair and credit monitoring services to current or former members of an affected Anthem plan dating back to 2004.

Anthem established a website for ongoing information regarding this situation, www.anthemfacts.com.

What Steps Should Plan Sponsors Take Now?

Plan sponsors should do the following:

- Assess whether health plan participants may have been affected by the Anthem breach.

- For self-insured plans using Anthem as a TPA, determine what contracts the plan might have with Anthem (TPA service agreement, BAA agreements, etc.) and whether those contracts impact Anthem's obligations to the plan.

- For insured plans, Anthem is the Covered Entity so it is directly responsible for contacting affected participants.

- Notify affected participants of the opportunity to obtain identity protection by directing them to the www.anthemfacts.com website.

- Consult with counsel to assess whether Anthem's actions on behalf of your health plan satisfy any applicable HIPAA and state law privacy or notice obligations the plan may have.