HorizonBlue.com

Brief Notes

News for Brokers and Consultants

March 18, 2015

Applies to: All Markets

Premera Cyber Attack

Premera Blue Cross (Premera), which operates in Washington and Alaska, announced that cyber attackers had executed a sophisticated attack to gain unauthorized access to its Information Technology (IT) systems. Premera is working closely with Mandiant, one of the world's leading cyber security firms, and the FBI to investigate the attack.

To date, the investigation has determined that the attackers may have gained unauthorized access to members' information, which could include member name, date of birth, email address, address, phone number, Social Security Number, member identification number and claims information, including clinical information. The information involved in this attack dates back to 2002.

Premera has created a website, **premeraupdate.com** to keep customers informed. Premera is beginning to mail letters to the approximately 11 million affected individuals and is providing two years of free credit monitoring and identity theft protection services to impacted individuals. Individuals who believe they may be affected by this cyber attack but who have not received a letter by April 20, 2015, are encouraged to go to **premeraupdate.com** and to enroll in the free identity theft protection and credit monitoring services.

Horizon Blue Cross Blue Shield of New Jersey is a separate and distinct company from Premera. However, some Horizon BCBSNJ members who have accessed health care in Premera's service areas may have had their information stored in Premera's IT systems.

Thirty-seven independent companies operate in various locations across the United States and Puerto Rico to form the Blue Cross and Blue Shield network. This network enables members to receive the same health insurance benefits for any medical care they may need while living or traveling within the coverage areas of any other Blue Cross and/or Blue Shield company.

(Continues)

In those instances, the member's medical claim is sent, on their behalf, from the Blue Cross and/or Blue Shield company that received it to the local Blue Cross and/or Blue Shield company that maintains the member's health care plan. This process ensures that the member's claim is processed based on their personal benefit plan, while receiving the discounts agreed upon between the provider and the Blue Cross and/or Blue Shield company that received it while the member was living or traveling outside of the Blue Cross and/or Blue Shield company's service area.

Therefore, if a member received care in Premera's service areas since 2002, the member's information may have been retained in Premera's IT systems.

Information security is a top priority at Horizon BCBSNJ, and in the wake of the recent cyber attacks, Horizon BCBSNJ used the information provided by the National Healthcare and Public Health Information Sharing and Analysis Center (NH-ISAC) to conduct an extensive review of our systems. To date, Horizon BCBSNJ has detected nothing that indicates data theft from its systems. The Company diligently monitors for threats to its systems and sensitive information, and has deployed leading security measures to do so.

More specifically, Horizon BCBSNJ has deployed and continually monitors:

- Encryption software to all desktops and laptops
- Antivirus software deployed to all desktops and laptops
- Forensics capability deployed to all desktops and laptops
- Endpoint device protection to geo-locate devices and render such devices unusable, if necessary
- Data Loss Prevention (DLP) tools deployed to all desktops/laptops and at chokepoints in its network
- Advanced firewall and intrusion detection/prevention solutions throughout its network
- Security Incident and Event Monitoring capabilities which are actively monitored and mined

Additionally, Horizon BCBSNJ is an active and vocal participant in the security threat intelligence community, and collaborates with national health care payers, providers, pharmacy companies and others to continually detect and respond to cyber threats.

Horizon BCBSNJ continuously revises and improves its security program based on lessons learned from its proactive penetration testing and tabletop incident management exercises.

If you have questions, please contact your Horizon BCBSNJ sales executive or account manager.