The Anthem Breach Does Not Have To Mean A Breach Is Inevitable For Everyone

February 9. 2015

By now you have probably heard about the data breach involving Anthem, Inc. It is widely believed that with the data of potentially 80 million people compromised, this will end up being the largest healthcare breach ever. One of the more chilling aspects of this event is the notion that if the second largest health insurer in the country cannot protect its data, how can a much smaller organization with far fewer resources. The reaction of many smaller healthcare organizations is to say "it cannot happen to me" or "I do not know what I can do," and wait for an eventual breach. However, this defeatist mentality is unnecessary. An analysis of what we know about Anthem's missteps demonstrates that appropriate safeguards are attainable even for smaller healthcare organizations.

Anthem lacked some of the basics in cybersecurity breach prevention.[1] First, their data was only encrypted when it was moving outside of their systems. Data that was within their systems was not encrypted. While this type of encryption is not required by HIPAA, it is widely accepted as a best practice for healthcare organizations. The lack of such a safeguard is indicative that Anthem chose not to implement security basics.

Secondly, according to early reports, Anthem did not appropriately classify and segregate sensitive data. The personal information that seems to have been compromised was comingled with non-sensitive or less sensitive data. If the personal information had been classified and segregated, it would have limited the damage in the event of inappropriate access. Not classifying and segregating the personal information showed Anthem chose a less costly approach to facilitate date access instead of implementing basic cybersecurity safeguards which could have mitigated or prevented this breach.

For healthcare organizations that lack Anthem's compliance resources, preventing a similar breach begins with creating a good security and privacy foundation; something Anthem clearly failed to do. Not just classifying, segmenting, and encrypting data, but also developing a risk based data management process. At first glance, it can seem overwhelming and can make an organization want to admit defeat. However, after a closer examination, safeguarding protected information can be accomplished by an organization of any size.

The first step, and the one that Anthem failed to complete, is implement a strong foundation of security and privacy safeguards. If there is not a strong foundation of enterprise safeguards, whatever is built on top is less effective. The good news is there is an array of easy-to-use and cost-effective tools that are suitable for organizations of any type and size to aid in the implementation of those basic safeguards. Once the basics are in place and the foundation is laid, safeguards implemented will have the ability to reduce exposure and have the potential of making an organization more successful.

Is this most recent breach a possible industry game-changer? Yes. Does it mean all healthcare organizations should just assume at some point they will face the same fate? No. Anthem lacked some important basic safeguards, which were exploited and allowed for this breach to be

[1] http://www.ihealthbeat.org/articles/2015/2/6/anthem-cyberattack-shows-health-care-organizations-vulnerability

so widespread. However, with attainable foundational safeguards in place, a similar outcome is avoidable regardless of an organization's size or amount of compliance resources.

For more information on how to establish the necessary foundation visit qipsolutions.com or contact us at 1.877.452.5303.