CLIENT ALERTS & INSIGHTS

Recent Dental Benefit Provider Data Breach Highlights Legal Risks and Need for Proactive Mitigation

JUNE 7, 2023

Authors: Christina Hultsch, Vince Nardone

Data Breaches risk legal consequences—both from state and federal governments and consumers, as well as reputational harm.

Last month, MCNA-a dental benefit provider-provided notice of a data breach that exposed the personal information of nearly nine million individuals. Everything from full names, contact information, social security numbers, and dental insurance information was exposed. In the breach notification published on its website, MCNA disclosed that hackers had access to its systems for almost two weeks before the incident was discovered. MCNA is offering twelve months' of credit monitoring and identity theft protection services to all affected individuals.

With the exponential increase in the volume and size of security incidents involving health-related data and other personal information, along with the ever-growing number of threats resulting from the use of modern technology, all businesses must take notice and be prepared to contend with a web of legal obligations that is woven by each of the U.S. state's data breach notification laws.

In addition to state law obligations, dental benefit providers and dental professionals, as well as any other entity falling within the "Covered Entity" definition of the Health Insurance Portability and Accountability Act and its regulations ("HIPAA"), must comply with the HIPAA breach notification rule. HIPAA also requires that business associates report a breach of PHI to the Covered Entity for which they provide services unless the Covered Entity contractually requires the business associate to report the breach directly to the U.S. Department of Health and Human Services ("HHS"). Business associates include those service providers performing functions or activities on behalf of, or certain services for, a Covered Entity that involve the use or disclosure of PHI, such as DSOs or billing companies.

But the risks faced by Covered Entities and their business associates in the context of a data breach extend well beyond the legal ramifications. There are business-to-consumer risks that arise from a broken sense of trust between the Covered Entity and its patients. There are also business-to-business risks, as a breach, and especially the mishandling of post-breach mitigation efforts, will likely tarnish any hard-earned reputation.

In today's digital world, with more and more data held in electronic form, it is a matter of when, not if, a bad actor will succeed in penetrating the cyber security defenses of any business, and, particularly, those of a Covered Entity. Therefore, the importance for dental benefit and care providers in taking proactive steps to plan for the inevitable cannot be overstated.

Please see below for a summary and review of potential consequences that may follow a data breach.

Risks of a Data Breach

1. Government Fines and Penalties

Covered Entities that fail to meet HIPAA's requirements including the HIPAA breach notification requirements may face civil and criminal penalties.

HHS has discretion to impose civil money penalties if the violations are not cured within 30 days. In cases of willful neglect, HHS can apply civil money penalties immediately. Depending on the egregiousness of the offense, the penalties can range anywhere from $100 to $50,000 per violation, with the highest annual maximum penalty set to $1.5 million.

Criminal violations of HIPAA are enforced by the U.S. Department of Justice. In addition to HIPAA penalties, Covered Entities also need to comply with any and all additional U.S. state data breach notification laws that might be applicable.

However, the consequences and risks that stem from a data breach go far beyond potential government fines and penalties.

1. Administrative Costs and Expenses

In the wake of a data breach subject to HIPAA reporting obligations, the Covered Entity and any business associate involved in the incident will face certain mandatory costs regardless of whether the Covered Entity or business associate were at fault.

Costs reaching into the hundreds of thousands of dollars are typically incurred just in administrative expenses (such as mailing out notices for nine million affected individuals) due to the fact that these notices will typically need to be sent out to every single affected individual. Accordingly, the larger a data breach, the higher the administrative expenses will be.

In addition, there will be significant legal fees incurred when a Covered Entity, and/or its business associate, engages legal counsel to investigate the incident and any resulting reporting obligations, both under HIPAA and state breach reporting laws.

Additionally, the Covered Entity, or any business associate, that suffered a data breach will undoubtedly incur additional costs related to: (1) investigating and auditing the existing information security program; and (2) either implementing or upgrading the information security program designed to ensure the same type of data breach does not occur again.

1. Reputational Harm

From a patient perspective, Covered Entities and their business associates are often trusted with an individual's most sensitive information, both in terms of health data related to a current or past medical/dental condition, or in terms of financial data related to their insurance coverage. If a patient

or individual no longer feels they can trust their dental benefit or care provider, they are less likely to return in the wake of a data breach.

There are also potential adverse consequences impacting the existing and prospective business relationships.

For example, if a business associate providing critical administrative services to a Covered Entity suffers a large data breach, it will become more challenging to continue with the same business-to-business model and sell the business associate's services to other health care providers going forward. Even if the business opportunity is not being lost altogether in the aftermath of the breach, the business associate will have surrendered all leverage in garnering the trust that equates to more favorable contract terms when establishing relationships with new customers.

1. Unknown Costs

There is also an element of the unknown in the wake of a data breach which increases the overall risk profile.

With larger data breaches, there is always a risk of a class action. Even if the Covered Entity or its business associate, finds success in fighting back against a class action, thus avoiding a settlement or an adverse court decision, the costs of defending against a class action will be significant.

There are also ancillary concerns such as cyber liability insurance. At first blush, a business with cyber liability insurance coverage will likely think it is well positioned if a data breach occurs. However, cyber liability insurance coverage-like any insurance policy-has conditions and exceptions. If the data breach is due to a failure of a business to maintain an adequate information security program, there is a heightened possibility a cyber liability insurance policy will not apply.

And even where the policy will provide coverage, depending on the terms of the policy, there is likely a substantial deductible to be met and the applicable premiums going forward may increase.

For additional information, please contact:

Christina Hultsch at chultsch@beneschlaw.com or 614.223.9381.

Vince Nardone at vnardone@beneschlaw.com or 614.223.9326.

Luke Schaetzel at lschaetzel@beneschlaw.com or 312.212.4977.