LAW ALERT

May 19, 2020

By: Leora F. Ardizzone, Esq.

RMF
RuskinMoscouFaltischek P.C.
Smart Counsel. Straight Talk.

Important First Steps After Data Privacy Breach

Throughout the COVID 19 crisis, government agencies have warned of increasing cyber-attacks. Ever more threat actors are taking advantage of reduced staff, work from home with reduced cyber-security and the general state of crisis. Phishing and ransomware attacks have found easy prey by simply including the words COVID-19 or coronavirus in their message. In such an environment, it is more important than ever to ensure that if your company has been breached, that you are aware of your obligations with respect to notifying affected parties and government agencies.

The healthcare industry is particularly vulnerable as providers, carriers and their business associates maintain sensitive data including protected health information (PHI) which is subject to the Health Insurance Portability and Accountability Act ("HIPAA"). Providers and carriers often also maintain payment card information (PCI) and like all other employers, will maintain employees' personally identifiable information (PII) such as social security numbers. Moreover, healthcare providers are most interested in news about testing, diagnosing and treating the novel virus. Health care organizations are subject to a variety of regulations and could have a number of different reporting obligations depending on the states where its patients reside, as well as pursuant to contract, which could impose shorter notice of breach obligations.

It is vital to remember that the time for notifying affected persons and government regulators has not been relaxed during the current crisis. Under HIPAAA, the time to notify or report begins on the date the breach has been detected or notice of breach has been received. While not all breaches are reportable, the time to determine whether any breach is reportable commences on that date of detection or notice of breach, ad under HIPAA, the time to notify and report remains the date that is not later than 60 days from the date you detected or were notified of a breach. For this reason, it is more important than ever that if you have detected or received notice of any breach, whether in your own environment or in that of a contracted service provider, that you carefully record the date of detection or notice of breach, follow your incident response policy and commence investigation of the breach immediately to determine:

a. The nature of the breach;
b. The nature of the data that may have been compromised; and
c. The universe of affected people including their state of residence.

Any delay in taking these basic first steps may result in delays in providing statutorily mandated notifications to affected persons, reports to appropriate government agencies, filing claims with cyber insurance carriers and determining appropriate remediation. Delays in notifications to affected persons can lead to fines and penalties, as well as making you vulnerable to suits by affected persons, including class action suits. Further, delays can result in reputational damage as your patients, clients, customers, employees, etc. may determine that you don't care about the privacy of their data or ensuring that they can timely take steps to protect their privacy.

If you have experienced a breach, we are here to help.

Leora F. Ardizzone, Esq.
(516) 663-6538
lardizzone@rmfpc.com