Published on *The National Law Review* https://www.natlawreview.com

New Notification Requirements in New York for Healthcare Providers Facing a Cybersecurity Incident

Article By:

Frank J. Fanshawe

Joseph J. Lazzarotti

Jason C. Gavejian

Maya Atrakchi

On August 12, Mahesh Nattanmai, New York's Chief Health Information Officer, issued a notice letter ("the notice") on behalf of the **New York State Department of Health** ("Department") requiring healthcare providers to use a new notification protocol for **informing the Department of a potential cybersecurity incident**. The updated protocol is considered effective immediately from a healthcare provider's receipt of the notice letter.

> "We recognize that providers must contact various other agencies in this type of event, such as local law enforcement. The Department, in collaboration with partner agencies, has been able to provide significant assistance to providers in recent cyber security events. Our timely awareness of this type of event enhances our ability to help mitigate the impact of the event and protect our healthcare system and the public health. The Department has designed a more efficient process to engage assistance for providers, as needed,"

the Department states in its notice letter.

Moreover, the Department provides the types of healthcare providers, which should be implementing this update notice protocol immediately:

- Hospitals, nursing homes, and diagnostic and treatment centers,
- Adult care facilities, and
- Home health agencies, hospices, licensed home care services agencies.

A cybersecurity incident is defined by the notice as “the attempted or successful unauthorized access, use, disclosure, modification, or destruction of data or interference with an information system operation”. Therefore, even if a healthcare provider is aware of an *unsuccessful* attempt of a breach (*e.g.* by a disgruntled employee), that incident should be reported to the Department.

The notice does not state the time period within which the Department should be notified upon a healthcare provider’s discovery of the cybersecurity incident. It is worth noting that the recently enacted New York SHIELD Act exempts HIPAA compliant covered entities from notification requirements following a data breach. Under HIPAA a covered entity is generally required to report a data breach of over 500 individuals to the U.S. Department of Health and Human Services (HHS) within 60 days of discovery of the breach, so it would not surprising if the length of time is similar, however we are currently confirming with the Department whether this is indeed the case. Contact information for the Department will vary depending on the healthcare provider’s location in New York. The notice provides contact information for each region: Capital District, Central New York, Metropolitan Area, Central Islip, New Rochelle and Western Area.

A recent study found that 70% of healthcare providers have experience a data breach. You can never be too prepared for a cybersecurity incident. Below are helpful resources from our blog on cybersecurity incident prevention and response for healthcare providers:

- A Trio of OCR HIPAA Breach Resolutions: Is Your Organization HIPAA Compliant?
- Cost – Benefit Analysis 101 for Healthcare Providers
- Lessons to be Learned from the Breach of Nearly 500,000 Individual Health Records Reported in September 2017
- Healthcare Providers and Business Associates: Don’t Ignore the Insider Threats
- Enhanced HHS HIPAA Breach Reporting Tool May Aid Health Care Industry Data Security Efforts

National Law Review, Volumess IX, Number 228