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

Breaches Within Breaches: Contractual Obligations After a Security Incident

Article By:

Roma Patel

We often cover consumer class action complaints against companies regarding the privacy and security of personal information. However, litigation can also arise from alleged breach of contract between two companies. This week, we will analyze a medical diagnostic testing laboratory's April 2025 complaint against its managed services provider for its alleged failure to satisfy its HIPAA Security Rule and indemnification obligations under the HIPAA Business Associate Agreement (BAA) between the parties.

Complaint Background

According to the complaint, the laboratory – Molecular Testing Labs (MTL) – is a Covered Entity under HIPAA, and Ntirety is its Business Associate. Reportedly, the parties entered into a BAA in September 2018. The BAA's intent was to "ensure that [Ntirety] will establish and implement appropriate safeguards" for protected health information (PHI) it handles in connection to the functions it performs on behalf of MTL. The complaint points to various provisions of the BAA related to Ntirety's obligations, including complying with the HIPAA Security Rule. According to MTL, the BAA also includes an indemnification provision that requires Ntirety to indemnify, defend, and hold harmless MTL against losses and expenses due to a breach caused by Ntirety's negligence.

Alleged HIPAA Violations

MTL asserts that around March 12, 2025, it received information about a material data breach involving data "that was required to have been secured by Ntirety under the BAA." The complaint is unclear about how or from whom MTL received that information.

The complaint asserts that MTL's forensic investigation determined that Ntirety had faced a ransomware attack, potentially from Russian threat actors. MTL's forensic investigation determined that Ntirety had "significant deficiencies, shortcomings, and omissions" in its procedures and practices that enabled the threat actors to access Ntirety's computer systems and MTL's confidential information.

In addition, MTL alleges that "Ntirety failed to provide material support to MTL for weeks" and that the support offered was conducted "slowly and incompetently." Allegedly, Ntirety informed MTL that

it would charge MTL for such efforts. MTL argues that under its BAA obligations, Ntirety was required to support MTL in its efforts to respond to and mitigate the security incident's harmful effects.

Alleged Breach of Contract – Indemnification Demand

MTL also asserts that it has incurred or expects to incur various damages related to "remediation efforts, HIPAA notification requirements, possible legal and regulatory actions, and direct and indirect harm to MTL's business." Specifically, MTL claims it has already incurred damages related to the forensic investigation and anticipates further damages associated with fulfilling HIPAA PHI breach notifications and providing credit monitoring services. MTL also expects to suffer harm to its business as a result of the breach and to be subject to lawsuits and regulatory action.

Reportedly, on March 25, 2025, and April 3, 2025, MTL sent formal demands to Ntirety for indemnification under the BAA for losses incurred as a result of the breach, but Ntirety "has provided no substantive response to MTL's indemnification demands."

Lessons Learned

After discovering a breach, companies have numerous obligations, such as determining whether data has been corrupted, containing the incident, conducting a forensic investigation, and identifying individuals whose data may have been involved. It can often take weeks or even months to understand the scope and extent of a breach, but companies should also promptly assess their contractual obligations post-breach. Whether in a BAA or another service agreement, companies may be required to let their vendors and other partners know about an incident.

In addition, companies should consider whether to communicate about the incident at a high level to their vendors and partners, even absent contractual requirements, particularly if news about the incident has already leaked. The risk of such communications includes potentially providing premature information that is likely to change as the forensic investigation unfolds. On the flip side, partners might appreciate the transparency and direct acknowledgment. There can be many legal and regulatory consequences of a data breach, but with adherence to contractual obligations and appropriate communication, a breach of contract claim doesn't have to be one of them.

National Law Review, Volume XV, Number 107