

REVIEW

CYBER INCIDENT RESPONSE BREACH CASE: LAW FIRM BREACH, HIPAA

CLIENT'S CHALLENGE

A large regional law firm representing US-based and international clients across several practice groups, including financial services, healthcare, employment, and IP, experienced a data breach, exposing a dataset of 68,666 documents. Early on, the client believed the dataset contained only PII, but during the initial data assessment, we discovered the dataset also contained PHI, triggering additional notification requirements under HIPAA. Based on this new information, the project scope expanded the notification requirements across forty-four states.



CYTREX CYBERS' APPROACH

With the data assessment complete, we had a clear picture of the dataset's contents, including document counts, file types, false positives, true hits, file path information, and impacted geographies. With this granular level of detail, we segregated and removed like files, false positives, and data that were alike in every way except format from the relevant data population. We also excluded files containing repeating entities and information, such as excel files, from the downstream review and extraction. This lowered the total costs of the project and allowed us to deliver sooner than our originally anticipated deadline.

WHY CYTREX CYBER?

CyTrex was referred to the decision-maker on this breach review project by another client saying, "they are so easy to work with. They will do whatever they can to make you look good to your client."

**Trust your cyber incident
notification project to the experts
at CyTrex Cyber.**

Notify the right people on time

Contact us today for assistance with your
incident ir@cytrexcyber.com

+1 877.998.0949