ACTFORE and Turning Complexity into Clarity After a Healthcare Data Breach

ACTFORE

SUMMARY

A nationwide healthcare support services provider operating across the United States and select international markets experienced a significant cybersecurity incident involving unauthorized access to internal systems. While the organization does not deliver direct clinical care, its operations support thousands of healthcare facilities—placing it in possession of sensitive personal and protected health information tied to employees, patients, and partners.

When suspicious activity was identified, leadership quickly recognized that the potential exposure extended beyond a single system or timeframe. Initial disclosures confirmed that data had been accessed and copied, triggering regulatory obligations and notification requirements. What remained unclear was the true scope of the exposure: which data elements were involved, how deeply sensitive information had propagated across systems, and how many individuals were truly impacted.

To answer those questions with defensibility, the organization engaged ACTFORE to conduct a comprehensive forensic data analysis capable of replacing uncertainty with evidence.

RESULTS

1.32TB
of Data Received

1.56M
Files processed

241M
sensitive data extractions

CUSTOMER DETAILS

Healthcare Support Services

35,000+ Employees

Headquarters: United States

3,000+ Facilities Serviced

COUNSEL

Am Law 200

PROPRIETARY PRODUCTS

BOXER

CLARITY

DISCOVER

THE INCIDENT & RISK LANDSCAPE

The organization's data environment reflected years of operational growth. Active systems existed alongside archives, backups, and legacy repositories that were no longer routinely accessed but still contained regulated data. Once the breach was confirmed, the challenge was not simply identifying recent activity, but understanding how sensitive information was distributed across this complex landscape.

The engagement involved 1.32 terabytes of data and more than 1.5 million files, spanning structured and unstructured formats. Many files were lengthy, inconsistently formatted, or poorly legible, complicating automated analysis. Early assumptions about scope risked either overstating exposure—leading to unnecessary notifications—or understating it, which could invite regulatory scrutiny under HIPAA and state privacy laws.

Compounding this complexity was the geographic reach of the organization's operations. Impacted individuals were ultimately found across all 50 U.S. states and multiple countries, requiring a response that could withstand legal, regulatory, and insurance review.

Complicating matters further, the data did not exist in clean, isolated systems. Sensitive identifiers appeared repeatedly across operational records, exports, reports, and historical datasets—often in formats that obscured their significance at first glance. Without disciplined analysis, it would have been easy to misinterpret isolated findings or miss how seemingly unrelated files linked back to the same individuals. In a healthcare context, those blind spots translate directly into regulatory and reputational risk.

> What mattered most was getting answers we could rely on. Once we had a clear, validated view of the data, every decision that followed became easier and far more defensible.

Client
Chambers | Crisis & Risk Management 2025

ACTFORE'S RESPONSE AND OUTCOMES

ACTFORE began by ingesting and indexing the full dataset, establishing a uniform analytical foundation across 1,560,000 files. Using a combination of AI-driven classification, OCR workflows, and structured extraction logic, the platform evaluated 42 regulated data elements, including both PII and PHI.

Over an 8-week span, ACTFORE isolated more than 800,000 responsive files and validated exposure through entity resolution, deduplication, and lineage tracing back to source systems. This process transformed more than 241 million rows of sensitive data extractions into an audit-ready dataset that tied sensitive identifiers directly to impacted individuals and originating systems.

Deduplicating the millions of sensitive data hits, the final analysis confirmed over 415,000 impacted individuals—supported by validated counts of Social Security numbers, dates of birth, medical record identifiers, and authentication credentials. Rather than relying on estimates or broad assumptions, leadership and counsel were able to proceed with notification and regulatory reporting grounded in confirmed facts.

By the conclusion of the engagement, the organization had moved from reactive response to informed control. Decisions were no longer driven by uncertainty, but by defensible evidence—allowing the organization to meet its obligations, communicate responsibly, and move forward with confidence. The engagement did more than satisfy immediate response requirements. It provided leadership with a durable understanding of their data environment—one that could inform remediation, future security planning, and ongoing compliance efforts long after the incident itself had passed.

DEFINING THE TRUE SCOPE OF EXPOSURE

Through meticulous indexing and classification, ACTFORE isolated the files most likely to contain sensitive content, enabling counsel to target review and notifications efficiently rather than treating all data as equally risky.

800,000
Responsive files identified

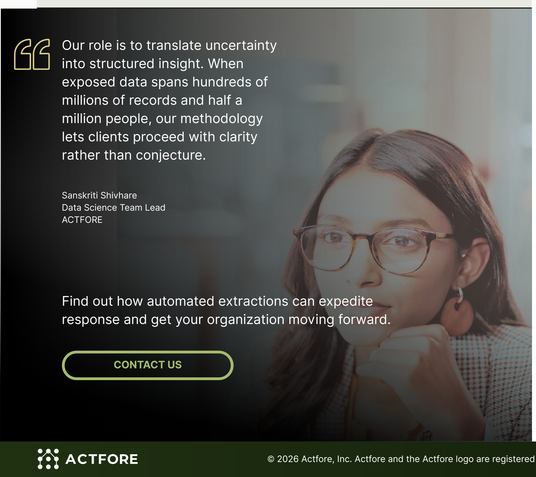
CLARITY THAT ENABLES CONFIDENT ACTION

Rather than relying on initial estimates, the final analysis identified more accurate individual impact metrics grounded in validated relationships between data elements and personal identities.

415,000
Impacted individuals

> Our role is to translate uncertainty into structured insight. When exposed data spans hundreds of millions of records and half a million people, our methodology lets clients proceed with clarity rather than conjecture.

Sanskriti Shivhare
Data Science Team Lead
ACTFORE



Find out how automated extractions can expedite response and get your organization moving forward.

CONTACT US