HEALTHCARE CYBER RECOVERY CASE STUDY · 2022

COMMONSPIRIT HEALTH

When Investigation and Restoration Had to Proceed Together

- Chicago, IL · national system
- October 2022 · ransomware
- ~$160M adverse impact

COMMONSPIRIT'S CLINICAL SYSTEMS CAME BACK IN WEEKS. THE FINANCIAL AND FORENSIC TAIL RAN FOR MONTHS.

WHAT HAPPENED

CommonSpirit Health, one of the nation's largest nonprofit health systems, detected a ransomware attack on October 2, 2022. The system contained the incident, opened an investigation, engaged outside cybersecurity specialists, and notified law enforcement and HHS. Affected facilities took EHR systems and patient portals offline, disrupting appointments, procedures, scheduling, and prescription workflows in the affected markets. By November 9, most markets had regained EHR access, while portal scheduling remained under restoration in some locations. A subsequent external-forensics investigation determined the unauthorized-access window ran from September 16 to October 3 and found that data had been copied from two file-share servers rather than directly from the EHR. Detailed file-by-file review continued into February 2023, and CommonSpirit completed notifications to potentially affected individuals in April 2023. [1][2][3]

~$160M	$842M	~5 weeks	Feb.–Apr. 2023
estimated adverse financial impact (May 2023)	increase in accounts receivable, H1 FY2023	until most markets regained EHR access (by Nov. 9)	forensic file review & notification completed

Sources: CommonSpirit unaudited quarterly & annual reports; BankInfoSecurity. Estimate excludes potential insurance recoveries.

RECOVERY TIMELINE

1. **Sept. 16–Oct. 3 — Access Window**
   Unauthorized-access period later established by external forensic investigation.
2. **Oct. 2 — Containment**
   Ransomware detected; systems secured and some taken offline.
3. **Nov. 9 — Phased Restoration**
   Most markets regain EHR access; portal scheduling recovery continues in some locations.
4. **Feb. 21, 2023 — Data Review**
   Initial detailed file-by-file review phase completed.
5. **April 2023 — Notification**
   Potentially affected individuals notified.

THE COST OF RECOVERY

CommonSpirit's adverse-impact estimate rose as the financial picture came into focus, and the accounts-receivable effect outlasted the clinical outage by months.

Adverse financial impact — ~$160M

Estimated as of May 2023 (up from ~$150M in February), including lost revenue from business interruption, remediation costs, and related expenses. Excludes potential insurance recoveries.

Accounts-receivable accumulation — $842M

Increase during the first six months of fiscal 2023, primarily due to the incident. Reflects delayed cash conversion, not a permanent loss.

Working-capital pressure

Credit-line draws in November and December 2022 addressed collection shortfalls connected in part to the incident.

Insurance recovery delay

As of September 2023, the amount and timing of insurance recoveries remained undetermined.

Source: Remparo Combined Financial Consequences and Recovery Costs, CommonSpirit Health brief. Do not attribute the full FY2023 operating loss to the incident; multiple factors contributed.

WHAT THE RECORD SHOWS

An external forensics vendor identified the unauthorized-access period and determined that data had been copied from two file-share servers rather than directly from the EHR, a materially different, and more precisely scoped, finding than early outage reporting suggested. CommonSpirit said systems returned with added security and monitoring tools. This is strong independent-investigation evidence; no public assurance-letter or partner-acceptance evidence was identified.

> ***"…we expect it to take some time."***
>
> **Benjie Loanzon**, Senior Vice President, CommonSpirit Health, on the timeline for recovering costs through insurance — quoted by *BankInfoSecurity*

MEASURED AGAINST RECOGNIZED GUIDANCE

CommonSpirit Health's response combined disciplined forensics with a financial recovery that ran for the better part of a year. The table below shows where the response aligns with recognized guidance, and where that guidance runs out before the recovery actually did.

NIST SP 800-61	CommonSpirit contained the incident, engaged outside cybersecurity specialists, and notified law enforcement and HHS promptly, tracking the Containment and Post-Incident Activity phases of NIST's incident-handling guide.
CISA #STOPRANSOMWARE	An external forensics vendor precisely scoped the access period and determined that data was copied from two file-share servers rather than the EHR directly, a materially more rigorous finding than early outage reporting suggested, and a direct product of the kind of independent forensic engagement CISA recommends.
ISO 22301	Phased EHR restoration by market, with most markets back online by November 9, reflects a Business Continuity Management System prioritizing critical clinical functions first.
ISO 22301 (BIA)	Standard Business Impact Analysis practice treats financial impact mainly as a planning input, priced out in advance and handed to insurance and finance to tally retrospectively once incident response formally closes. CommonSpirit's $842 million accounts-receivable increase shows why that habit understates the real cost: the financial tail ran for months after the clinical systems were already back.
NO STANDARD ADDRESSES THIS	No public assurance-letter or partner-acceptance record was identified. Claims processing and collections were described as significantly disrupted well after EHR access was restored, evidence that payers were running their own recovery clock, on their own schedule.

Sources: NIST SP 800-61 Rev. 2; ISO 22301:2019; CISA #StopRansomware Guide.

CommonSpirit's forensics were unusually precise for this series, scoping the breach to two file-share servers rather than the EHR itself. Precision on the investigation side didn't shorten the financial recovery, because no standard treats accounts-receivable normalization as a tracked recovery objective.

3 of 5 elements followed recognized guidance

Containment, forensics, and business-continuity practice tracked NIST, ISO, and CISA guidance directly.

2 of 5 mark a gap no framework currently closes

Not a shortfall specific to this organization — a marker of where today's most-cited recovery standards stop measuring the business.

RESTORED IS NOT THE SAME AS TRUSTED

Most of CommonSpirit's markets had EHR access back by November 9, 2022, roughly five weeks after detection. Its accounts receivable did not follow the same timeline: it grew by $842 million over the following six months, primarily because of the incident, while forensic file review continued into February 2023 and notifications ran until April.

> **Disaster recovery does not equal recovered. When counterparties, payers, vendors, banks, also require their own attestation before reconnecting, the business and its operations can remain down while the incident response process is still formally underway, even after every system on the recovery time objective has been restored.**
>
> Remparo Recovery In Depth™ analysis

CommonSpirit's own SVP said most of the roughly $160 million in costs were expected to be recoverable, "but we expect it to take some time." That sentence describes a business that was still working through the consequences of the attack long after its systems were declared restored, exactly the gap between technical recovery and full operating recovery that a Recovery Time Objective was never built to measure.

MOST MARKETS REGAINED EHR ACCESS IN ABOUT FIVE WEEKS. ACCOUNTS RECEIVABLE DID NOT NORMALIZE FOR MONTHS LONGER.

WHAT THIS MEANS FOR YOUR EXECUTIVE TEAM

- Assign a single evidence-and-restoration lead who can authorize both forensic preservation steps and system bring-up decisions, without waiting on the other.
- Treat claims and collections as a distinct recovery track with its own milestones, not a byproduct of clinical restoration.
- Plan working-capital contingencies before an incident, not as an emergency draw once accounts receivable has already built up.

Adapted from Remparo Recovery In Depth™ case research, CommonSpirit Health (2022).

THE SIX EXECUTIVE QUESTIONS, APPLIED TO COMMONSPIRIT HEALTH

CommonSpirit's public record speaks most directly to four of the six questions Recovery In Depth™ asks every executive team to answer.

How do we keep revenue and cash moving?

An $842 million accounts-receivable increase and working-capital credit-line draws show claims and collections functioning as a separate, slower recovery track from clinical restoration, exactly the distinction standard BIA practice tends to miss.

PAPER 4

What can we still trust?

External forensics had to establish precisely what was accessed, two file-share servers, not the EHR directly, before CommonSpirit or anyone downstream of it could know what "contained" actually meant.

PAPER 2

How do we protect the people affected?

Detailed file-by-file review continued into February 2023, and notifications to potentially affected individuals were not complete until April 2023, six months after detection, a separate recovery track for the people whose data was involved.

PAPER 5

What must keep operating?

CommonSpirit restored EHR access market by market, bringing appointments, procedures, and prescription workflows back online in the hardest-hit locations first rather than waiting for a single, all-at-once restoration date.

PAPER 3

RECOVERY IN DEPTH™ LESSON

Remparo Continuity is designed to keep billing and claims moving on a separate, trustworthy track from day one, so the receivable pileup this case shows doesn't have to be the default outcome of a breach.

$842M accounts-receivable increase, primarily attributed to the incident, in six months.

EVIDENCE-STRENGTH ASSESSMENT

CLAIM AREA	EVIDENCE STRENGTH	BASIS / LIMITATION
Ransomware detection & containment	High	Official CommonSpirit sources
External forensic investigation	High	Filed regulatory notice
Phased EHR recovery by Nov. 9	High	Dated official update
~$160M financial impact	High	CommonSpirit annual report
Single, uniform “full recovery” date	Moderate	Public record shows staged milestones, not one date
Partner/payer attestation evidence	Not established	No public evidence reviewed

REFERENCES

[1] CommonSpirit Health, official update. https://www.commonspirit.org/news-articles/commonspirit-update

[2] Massachusetts, filed Notice of Data Event. https://www.mass.gov/doc/assigned-data-breach-number-29358-commonspirit-health/download

[3] CommonSpirit Health, 2023 Annual Report. https://www.commonspirit.org/content/dam/shared/en/pdfs/investor-resources/2023-CommonSpirit-Health-Annual-Report-SECURED.pdf

[4] HIPAA Journal, outage report. https://www.hipaajournal.com/commonspirit-health-confirms-system-outages-caused-by-ransomware-attack/

[5] CommonSpirit Health, Unaudited Quarterly Report, Feb. 15, 2023. https://emma.msrb.org/P21661663-P21278769-P21707024.pdf

[6] BankInfoSecurity, May 24, 2023. https://www.bankinfosecurity.com/commonspirit-ups-cost-estimate-on-its-2022-ransomware-breach-a-22155

[7] NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

[8] ISO 22301:2019, Security and resilience — Business continuity management systems. https://www.iso.org/standard/75106.html

[9] CISA, #StopRansomware Guide. https://www.cisa.gov/stopransomware/ransomware-guide

Claims in this case study are limited to the cited public record and Remparo’s source-verified Recovery in Depth™ research briefs. Analytical statements are labeled as Recovery in Depth™ analysis and are not statements made by CommonSpirit Health.