HEALTHCARE CYBER RECOVERY CASE STUDY · 2023

ARDENT HEALTH SERVICES

A Faster Critical-Recovery Comparison

- Nashville, TN · multistate system
- November 2023 · ransomware
- 12–13 days to core restoration

ARDENT'S CORE CLINICAL SYSTEMS WERE BACK IN 13 DAYS. FULL PATIENT-PORTAL RECOVERY STILL TOOK SEVEN WEEKS.

WHAT HAPPENED

Ardent Health Services detected ransomware on November 23, 2023, and responded by disconnecting broad portions of its environment, including corporate servers, Epic, internet services, and clinical programs, shutting off, in the words of its own CTO, "the entire internet" as an initial containment measure. Ardent retained forensic and threat-intelligence advisors immediately. Some emergency patients were diverted and non-emergent procedures were rescheduled; by November 30, all 25 of Ardent's emergency departments were again accepting ambulances, though some specialty diversions remained. Epic and other core systems were restored December 6, about 12–13 days after detection. Non-emergent surgeries resumed by December 19, and every MyChart patient-portal feature was operational by January 9, 2024, seven weeks after the attack began. [1][2][3]

12–13 days
until Epic & core systems restored

25 of 25
emergency departments accepting ambulances within 7 days

7 weeks
until full MyChart portal recovery

~$74M
adverse pre-tax 2023 impact, net of insurance

Sources: Ardent official incident disclosure; Fierce Healthcare; Healthcare Dive; Ardent Form 10-Q.

RECOVERY TIMELINE

1. **Nov. 23 — Isolation**
   Network and applications taken offline; forensic and threat-intelligence advisors retained.
2. **By Nov. 30 — Stabilization**
   All 25 emergency departments accepting ambulances again; some specialty diversions remain.
3. **Dec. 6 — Critical Restoration**
   Epic and core systems restored, about 12–13 days after detection.
4. **Dec. 19 — Procedure Recovery**
   Non-emergent surgeries resume.
5. **Jan. 9, 2024 — Portal Recovery**
   Full MyChart functionality available, seven weeks after the attack.

THE COST OF RECOVERY

Ardent disclosed a specific pre-tax impact figure in its SEC filings, along with the operational volume effects that sat behind it.

Adverse pre-tax impact — ~$74M

For the year ended December 31, 2023: lost revenue from business interruption plus remediation costs, net of insurance proceeds.

Volume reductions, Q4 2023 vs. Q4 2022

Admissions down 2.5% (vs. a pre-incident estimate of +4.1% growth); surgeries down 2.1% (vs. +5.5% estimated); ER visits down 5.7% (vs. +3.3% estimated).

Billing & reimbursement delays

Claims billing, reimbursement, and payment delays continued through the first quarter of 2024.

Insurance & ultimate impact uncertain

As of its June 30, 2024 SEC filing, Ardent said the ultimate financial impact and degree of insurance offset had not yet been determined.

Source: Remparo Combined Financial Consequences and Recovery Costs, Ardent Health Services brief (Form 10-Q for the quarter ended June 30, 2024).

WHAT THE RECORD SHOWS

Later leadership accounts described a disciplined containment-restoration-recovery sequence: whole-network disconnection, account resets, identity controls, cross-functional workgroups, and continuous coordination, including the discovery of approximately 520 applications in the environment against an expected inventory of 390. The record strongly supports outside forensic and threat-intelligence involvement; no public partner-attestation record was identified.

> ***“There are vendors, and then there are partners. We quickly came to find out who were vendors and who were partners.”***
>
> **Lonnie Garrison**, Chief Technology Officer, Ardent Health Services — quoted by *HealthSystemCIO*

MEASURED AGAINST RECOGNIZED GUIDANCE

Ardent Health Services ran one of the more disciplined incident responses in this series, and its own leadership has spoken publicly about the process. The table below maps that discipline to recognized guidance, and shows where even a fast, well-run recovery still ran into the same structural gap.

NIST SP 800-61	Ardent's decision to disconnect its network entirely, in its CTO's words "the entire internet," is an aggressive but textbook execution of the Containment phase of NIST's incident-handling guide, prioritizing containment speed over short-term convenience.
NIST SP 800-34	Discovering roughly 520 applications in the environment against an expected inventory of 390 is exactly the kind of contingency-planning gap SP 800-34 exists to close in advance; Ardent closed it live, during the incident, instead.
CISA #STOPRANSOMWARE	Retaining outside forensic and threat-intelligence advisors immediately, before restoration began, matches CISA's guidance to bring in trusted third-party expertise as part of the response.
NIST SP 800-34	Epic and core systems were restored in 12–13 days, an unusually fast recovery-time result. SP 800-34 has nothing further to say once that milestone is hit. It does not track the additional five weeks Ardent needed before every MyChart patient-portal feature was working again.
NO STANDARD ADDRESSES THIS	No public record shows a formal attestation process for Ardent's vendors and partners. Ardent's own CTO described learning, in real time, which vendors were merely vendors and which functioned as recovery partners, a distinction no standard requires an organization to make in advance.

Sources: NIST SP 800-61 Rev. 2; NIST SP 800-34 Rev. 1; CISA #StopRansomware Guide.

Ardent's response is close to a best-case execution of current incident-handling guidance. Even so, the standards it followed have nothing to say about the seven weeks between Epic coming back and every patient-facing feature working again.

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

Ardent is the fastest documented critical-system recovery in this series. Epic was back in less than two weeks. That speed is real, and it matters. It also did not shorten the seven weeks patients had to wait for full portal functionality, because the standards Ardent was measuring itself against stop at the system, not at the patient or the partner on the other end of it.

> **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

Ardent's own account of the recovery draws a sharp line between vendors and partners, a distinction that only matters because some counterparties required more from Ardent than a restored system before they would resume full cooperation. Even the best-executed technical recovery in this series still had a second, slower clock running underneath it.

EPIC RESTORED IN 12–13 DAYS. FULL PATIENT-PORTAL RECOVERY STILL TOOK SEVEN WEEKS.

WHAT THIS MEANS FOR YOUR EXECUTIVE TEAM

- Define a minimum viable clinical capability in advance, so containment decisions don't have to be improvised under pressure.
- Track Epic, procedures, patient portals, finance, and ecosystem restoration on five separate timelines, not one.
- Keep a current, verified application inventory before an incident; discovering it during one costs time you don't have.

Adapted from Remparo Recovery In Depth™ case research, Ardent Health Services (2023).

THE SIX EXECUTIVE QUESTIONS, APPLIED TO ARDENT HEALTH SERVICES

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

What must keep operating?

All 25 emergency departments were accepting ambulances again within a week, even before Epic was restored, evidence of a real degraded-mode operating capability rather than a full stop.

PAPER 3

How do we rebuild the confidence of everyone we depend on?

Learning, mid-incident, which relationships were vendors and which were partners shows ecosystem trust functioning as a distinct recovery track, running well after core systems were already back.

PAPER 5

How do we keep revenue and cash moving?

A ~$74 million adverse pre-tax impact and Q4 volume declines across admissions, surgeries, and ER visits show the financial recovery track continuing well after Epic and core systems were already restored.

PAPER 4

What can we still trust?

Ardent discovered roughly 520 applications running in its environment against an expected inventory of 390, only after the attack forced a full accounting. An organization can't decide what to trust, or reconnect safely, faster than it can inventory what it actually has.

PAPER 2

RECOVERY IN DEPTH™ LESSON

That's the pattern Remparo Continuity and Vault are built around: keeping the slowest clocks, scheduling, eligibility, and billing, from being the ones that gate a hospital's full return to normal, even when the technical recovery itself goes about as well as it can.

12–13 days to core clinical restoration — 7 weeks to full portal recovery.

EVIDENCE-STRENGTH ASSESSMENT

CLAIM AREA	EVIDENCE STRENGTH	BASIS / LIMITATION
Broad, whole-network shutdown	High	Official Ardent disclosure and CTO statements
Forensic / threat-intelligence support	High	Official Ardent disclosure
Dec. 6 Epic restoration	High	Contemporary reporting
12–13 day characterization	Moderate to high	Retrospective leadership accounts, consistent with dated reporting
Jan. 9 full MyChart recovery	High	Dated contemporary reporting
Partner attestation process	Not established	No public acceptance evidence identified

REFERENCES

[1] Ardent Health Services, official incident disclosure. https://ardenthealth.com/our-stories/ardent-health-services-reports-information-technology-security-incident

[2] Fierce Healthcare, recovery report. https://www.fiercehealthcare.com/health-tech/ardent-health-struggles-get-systems-back-online-hospitals-reopen-emergency-rooms

[3] Healthcare Dive, patient-portal update. https://www.healthcaredive.com/news/ardent-health-services-ransomware-attack/700775/

[4] HealthSystemCIO, “Anatomy of a Ransomware Attack” retrospective. https://healthsystemcio.com/2024/11/13/anatomy-of-a-ransomware-attack-inside-ardent-health-services-response-recovery/

[5] Advisory Board, Radio Advisory leadership discussion. https://www.advisory.com/radio-advisory/252

[6] Ardent Health Partners, Form 10-Q for the quarter ended June 30, 2024 (SEC). https://www.sec.gov/Archives/edgar/data/1756655/000162828024037278/ardt-20240630.htm

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

[8] NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-34r1.pdf

[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 Ardent Health Services.