HEALTHCARE CYBER RECOVERY CASE STUDY · 2023

PROSPECT MEDICAL HOLDINGS

When the Technical Recovery Window Became the Business Crisis

- 16-hospital system · CT hospitals featured
- August 2023 · ransomware
- 40 days to restore

PROSPECT'S SYSTEMS CAME BACK ONLINE IN 40 DAYS. FINANCIAL AND COMPUTER NORMALIZATION TOOK MONTHS LONGER.

WHAT HAPPENED

Prospect Medical Holdings, which operates a 16-hospital system, identified unauthorized access to its network on August 1, 2023. A subsequent forensic investigation placed the intrusion window between July 31 and August 3, and found that patient files were accessed or acquired. Prospect took containment steps, notified law enforcement, and engaged a third-party forensic firm. [3][4] Across affected facilities, operations reverted to paper records, and emergency, outpatient, imaging, blood-draw, and procedure services were curtailed. In Connecticut, state records documented 29 diversion notifications over more than 40 days and a 17-day full diversion at Manchester Memorial Hospital; nearly half of elective procedures at the reviewed hospitals were postponed. Facilities were declared back online on September 12, about 40 days after the attack, though state officials said financial and computer normalization continued well beyond that date. [1][2]

40 days	29	17 days	~$7.5M
until facilities declared services back online	diversion notifications over 40+ days (Connecticut)	full diversion at Manchester Memorial Hospital	Connecticut Medicaid advance for unbillable claims

Sources: Becker's Hospital Review; Connecticut Mirror investigation. No consolidated enterprise-wide cost total was publicly disclosed.

RECOVERY TIMELINE

1. **July 31–Aug. 3 — Access Window**
   Intrusion window later established by forensic investigation.
2. **Aug. 3 — Disruption**
   Paper operations and service restrictions begin across affected facilities.
3. **August–Sept. 11 — Extended Recovery**
   Diversions, imaging, procedure, and billing effects continue at Connecticut hospitals.
4. **Sept. 12 — Major Milestone**
   Systems and services declared back online, about 40 days after the intrusion window.
5. **After Sept. 12 — Residual Recovery**
   Financial and computer normalization continues; executives cite paper vendor checks and a multi-month timeline.

THE COST OF RECOVERY

Prospect did not publish a consolidated, enterprise-wide incident-cost total. The strongest quantified financial evidence concerns three Connecticut hospitals, where the state stepped in to keep cash moving.

Medicaid billing interruption — ~$7.5M

Connecticut hospitals could not bill Medicaid, prompting the state Department of Social Services to advance interim payments.

Lost or deferred procedure revenue

Nearly half of elective procedures at the reviewed Connecticut hospitals were canceled during the outage.

Vendor-payment disruption

Executives reportedly continued using paper checks to pay vendors well after services were declared back online.

Prolonged financial normalization

Hospital leaders told state legislators that financial recovery and complete system restoration were continuing and could take additional months.

Source: Remparo Combined Financial Consequences and Recovery Costs, Prospect Medical Holdings brief. The $7.5M is a state advance, not a loss or grant.

WHAT THE RECORD SHOWS

Prospect's public notices establish outside forensic involvement and added safeguards. They do not include a public forensic report, attestation letter, payer acceptance decision, or documented ecosystem all-clear. The record supports the conclusion that technical recovery alone can consume weeks; it does not support attributing the full 40 days to a completed attestation process.

> ***"They continue to have to use paper checks to pay vendors, and it will likely take a few more months for everything to get fully sorted out."***
>
> **State Rep. Cristin McCarthy Vahey** (D-Fairfield) — quoted by the *Connecticut Mirror*

MEASURED AGAINST RECOGNIZED GUIDANCE

Prospect Medical Holdings' Connecticut hospitals followed several recognized elements of incident response even as the business impact ran far longer than the technical outage. The record below shows where that discipline is documented, and where the public standards simply stop describing what happened next.

NIST SP 800-61	Prospect engaged a third-party forensic firm and notified law enforcement promptly after detecting unauthorized access, matching the Detection & Analysis phase of NIST's incident-handling guide.
ISO 22301	Reverting to paper records and curtailing emergency, outpatient, imaging, and procedure services at affected facilities reflects the kind of degraded-mode operating plan a Business Continuity Management System is meant to define.
NIST SP 800-34	SP 800-34's recovery objectives are built around restoring a system by a target date. They say nothing about a state Medicaid agency having to advance $7.5 million in interim payments because a hospital still cannot bill, weeks after services were declared back online.
NO STANDARD ADDRESSES THIS	No public forensic report, attestation letter, or payer acceptance decision was identified in the record. The 40-day restoration milestone measures when systems came back. It does not measure when Prospect's counterparties, Medicaid included, treated the business as fully reconnected.

Sources: NIST SP 800-61 Rev. 2; NIST SP 800-34 Rev. 1; ISO 22301:2019.

Prospect's Connecticut hospitals show a response that met the basics of incident handling and business continuity. What the standards don't explain is why a state agency had to step in to keep three hospitals solvent, weeks after the attack began.

2 of 4 elements followed recognized guidance

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

2 of 4 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

Prospect's Connecticut facilities were declared back online on September 12, 2023, about 40 days after the intrusion window closed. State officials and Prospect's own executives described a very different picture for the months that followed: paper checks to vendors, an unresolved Medicaid billing gap, and financial normalization still described as ongoing.

> **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

The $7.5 million Connecticut advanced was not a grant or a recovery payment. It was an acknowledgment that Prospect's hospitals could not bill Medicaid on their own systems weeks after those systems were reported working, and that patients and providers could not wait for a private billing dispute to resolve itself. That is what an attestation gap costs when nobody is tracking it as its own recovery objective.

SERVICES DECLARED BACK ONLINE IN 40 DAYS. FINANCIAL NORMALIZATION WAS STILL ONGOING MONTHS AFTER THAT.

WHAT THIS MEANS FOR YOUR EXECUTIVE TEAM

- Test degraded operations that last weeks, not hours, in tabletop exercises.
- Track clinical, diagnostic, financial, and technology milestones on separate timelines, not one combined "systems restored" date.
- Confirm in advance how Medicaid and commercial-payer billing will continue if core systems stay down past a first restoration milestone.

Adapted from Remparo Recovery In Depth™ case research, Prospect Medical Holdings (2023).

THE SIX EXECUTIVE QUESTIONS, APPLIED TO PROSPECT MEDICAL HOLDINGS

Prospect's Connecticut 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?

A state Medicaid advance of roughly $7.5 million kept three hospitals solvent while their own billing systems could not process claims, a stopgap no hospital should have to depend on a state agency to provide.

PAPER 4

What must keep operating?

Nearly half of elective procedures were canceled and 29 diversion notifications were issued over more than 40 days, evidence that "systems restored" and "normal operations" were measuring two different things.

PAPER 3

What can we still trust?

No public forensic report, attestation letter, or payer-acceptance decision was identified for Prospect, leaving open exactly which counterparties treated the environment as trustworthy again, and when.

PAPER 2

How do we communicate?

Much of what the public knows about Prospect's Connecticut recovery comes from state legislative testimony, not from Prospect itself, evidence that transparent, ongoing communication is its own recovery deliverable, not just a compliance notice.

PAPER 1

RECOVERY IN DEPTH™ LESSON

Remparo Continuity is built for exactly that gap: running billing, scheduling, and eligibility on infrastructure that was never touched by the breach, so a health system isn't still cutting paper checks to vendors months after its systems are declared "back online."

40 days to declared restoration — months more before financial normalization was complete.

EVIDENCE-STRENGTH ASSESSMENT

CLAIM AREA	EVIDENCE STRENGTH	BASIS / LIMITATION
40-day restoration milestone	High	Prospect statement and Connecticut state records
Connecticut operational impacts	High	State records and diversion logs
~$7.5M Medicaid advance	High	State information in investigative reporting
Third-party forensic firm engaged	High	Prospect incident notices
Enterprise-wide (all 16 hospitals) detail	Moderate	Most public detail is Connecticut-specific
Partner/payer attestation evidence	Not established	No public documentation reviewed

REFERENCES

[1] Becker's Hospital Review, 40-day restoration report. https://www.beckershospitalreview.com/healthcare-information-technology/cybersecurity/prospect-medicals-16-hospitals-back-online-40-days-after-cyberattack/

[2] Connecticut Mirror, investigation. https://ctmirror.org/2023/10/01/ct-prospect-medical-holdings-hospitals-cyberattack-yale-sale/

[3] Prospect Medical, updated notice. https://www.healthcarefacilitiestoday.com/posts/Updated-Notice-from-Prospect-Medical-Regarding-Data-Breach--28978

[4] Crozer Health / Prospect Medical, substitute HIPAA notice. https://www.crozerhealth.org/globalassets/prospect-medical---updatedphase-2---hipaa-substitute-website-notice---updated-1.pdf

[5] BankInfoSecurity, legal and business fallout report. https://www.bankinfosecurity.com/prospect-medical-facing-more-legal-fallout-from-2023-hack-a-25975

[6] HIPAA Journal, lawsuit and breach report. https://www.hipaajournal.com/prospect-medical-holdings-data-breach-lawsuit-survives-motion-to-dismiss/

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

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 Prospect Medical Holdings.