

Is Your Finance Team Ready for a Cyber Event?

A pre-breach checklist for healthcare CFOs, revenue cycle leaders, and patient access teams.

01 Claims stop first

02 Cash stops second

03 Payroll stops third

Ransomware gets treated as an IT problem, but Finance and Revenue Cycle feel it first. When billing, eligibility, and registration systems go dark, these questions stop being hypothetical. They become the difference between a manageable disruption and a claims and cash crisis. Work through this checklist with your CFO, revenue cycle director, and patient access lead. **Any question you can't answer with confidence, and a location, is where a real event will hurt you.**

CLAIMS & BILLING PROCEDURES

- ☐ Can you find your claims processing and payer portal submission steps without access to your network or your work machine?
- ☐ Do you know which payers won't accept a paper or direct claim at all, and have you flagged that timely-filing risk in advance?
- ☐ If your clearinghouse goes dark, do you have a backup clearinghouse with EDI enrollment already complete, payer by payer, rather than started after the fact?
- ☐ Do you know your realistic manual claims capacity, in claims per person per day, and whether it covers your real volume?

PROVIDER & PAYER IDENTIFIERS

- ☐ How would you know which TINs belong to which department or entity without your RCM or EMR system in front of you?
- ☐ Do you have an offline copy of every NPI, PTAN, CCN, and CLIA number your organization bills under, with expiration dates tracked?
- ☐ Is your provider revalidation calendar (PECOS and Medicaid) kept somewhere your team can reach without corporate email?
- ☐ Do you have a current individual provider roster, including DEA numbers and license expirations, stored somewhere that doesn't depend on your credentialing system?

WHY THIS MATTERS

When the February 2024 Change Healthcare attack cut off electronic claims nationwide, many providers discovered that their manual submission steps, payer contacts, and provider identifiers existed only inside the systems that had just gone dark.

AUTHORIZATION & ELIGIBILITY

- ☐ How and where would you perform prior authorization during downtime? Is the process documented, or does it live in one person's head?
- ☐ Do you have a phone-verification reference, including IVR steps and numbers, for eligibility and authorization with your top payers?
- ☐ Do you know which services still require authorization during an outage, and who owns tracking them so care isn't denied after the fact?
- ☐ If your eligibility portal is down, do you have a tested fallback for capturing insurance information at the point of service?

PATIENT ACCESS & REGISTRATION

- ☐ Which staff are essential to keep eligibility and benefits (E&B) verification moving for the ER and patient intake during downtime, and do they know it's them?
- ☐ Have you reserved downtime identifier ranges (MRN, CSN, account) with IT in advance? They cannot be created once an incident is underway.
- ☐ Do your printed registration and consent forms mirror your system's field order closely enough to reconcile cleanly once you're back up?
- ☐ Who is authorized to declare registration downtime, including nights and weekends, and how does that declaration reach the front desk?

WHY THIS MATTERS

Roughly 40% of the information that determines whether a claim gets paid is captured at registration (HFMA). If patient access can't function on paper, every department downstream inherits the problem.

BANKING & PAYMENT CONTROLS

- ☐ Are your banking contacts, account details, and signer authority documented somewhere other than your own network?
- ☐ Do you have a plan for keeping lockbox deposits, patient payments, and payroll moving if your systems are offline?
- ☐ Have you decided in advance whether to freeze vendor bank-detail changes during an incident? They are a common fraud target after a public breach.
- ☐ Do you know your dual-control and wire authority limits for every account, and who can execute a transaction if your primary approver is unreachable?

CASH & EMERGENCY FUNDING

- ☐ Do you know, in days, how long your cash on hand covers a full billing and collections outage? Could your CFO defend that number to the board today?
- ☐ Have you called your bank and lender to ask how fast they can move money in an emergency, or are you assuming an answer you've never tested?
- ☐ Do you know the CMS Accelerated and Advance Payment process step by step, or would your team be learning it live during the event?
- ☐ Have you identified every emergency funding lever available to you, and how long each one takes to produce cash?

PAYROLL CONTINUITY

- ☐ Do you have a named, documented interim pay method that doesn't require Finance or HR to invent one on the spot?
- ☐ Have you reviewed your payroll vendor's own incident-response commitment, given that the largest recent healthcare payroll outage was vendor-side?
- ☐ Can your organization collect and reconcile hours by hand if timekeeping is down for weeks rather than days?
- ☐ Is your offline employee roster, with personal contact information, current enough to reach your workforce if email and paging are down?

INSURANCE, LEGAL & DOWNTIME PROCEDURES

- ☐ Has someone in Finance or Legal read your full cyber policy, not just the certificate, and can they name the business-interruption waiting period and sublimits?
- ☐ Do you have a pre-drafted litigation hold and "do not wipe" directive ready to issue to IT within the first two hours?
- ☐ Has your organization set a written position on ransom payment, including who has authority to approve it, before the day you need that answer?
- ☐ Do you have a documented downtime staffing plan with named people, not just roles, assigned to eligibility, prior auth, claims submission, and payer liaison duties?

WHY THIS MATTERS

The February 2024 Change Healthcare attack disrupted claims and cash flow for providers nationwide for weeks. It wasn't isolated. The 2021 Kronos/UKG ransomware incident affected roughly 8 million employees, and some hospitals ran payroll entirely by hand for over a month.

SCORE YOUR READINESS | COUNT YOUR CHECKED BOXES (32 TOTAL)

0 to 10

EXPOSED

A live event would be improvised in real time, department by department.

11 to 21

AT RISK

Some fundamentals exist, but critical gaps would surface under pressure.

22 to 32

READY

Documented, tested, and current. Confirm it with a tabletop exercise.



CLOSES THESE GAPS IN THREE STEPS

01

Map

We guide your team through every operational dependency that would break in an outage, department by department, not just IT.

02

Document

Your answers become a secure, offline-ready playbook stored in a HIPAA-compliant vault your team can reach even when your systems can't.

03

Test

We run the playbook against a real scenario so gaps surface in a tabletop exercise, not in your first live event.

This checklist shows you the gaps. **Remparo Continuity** closes them.

The process, workbook, and secure technology built for healthcare finance and revenue cycle teams, so a cyber event never becomes a cash event.

remparo.com
info@remparo.com