EDI Clearinghouse™

E-BOOK

How to Maintain Your Revenue Cycle in Crisis

Fifteen Steps You Can Take to Mitigate the Fallout of Industry Cyberattacks

Office Ally

Contents

Introduction

In February of 2024, the U.S. healthcare system was rocked by a cyberattack on one of the nation's largest healthcare claims clearinghouses. The attack effectively forced the clearinghouse to shut down essential parts of its electronic billing and payment system, keeping insurance providers from receiving claims and preventing hospitals and pharmacies from obtaining insurance approvals — effectively preventing providers from being paid for their services.

This disruption created a financial strain for medical providers large and small. According to American Medical Association member surveys, 80 percent of physician practices have lost revenue from unpaid claims, and even as of April 29, 2024 (more than two months after the attack), 90 percent of survey respondents were still losing revenue[1]. Many physicians were forced to use personal funds to cover practice expenses, delay procedures and severely limit pain management efforts, resulting in worse overall patient care and an increase in hospital mortality rates[2]. Many healthcare systems and practices affected by the cyberattack couldn't afford to stay open, and those that could did so at great financial expense — an expense that may not be feasible should such an attack occur twice.

According to American Medical Association member surveys, 80 percent of physician practices have lost revenue from unpaid claims as a result of the cyberattack in February 2024.

It's clear that, due to the interconnected nature of healthcare industry infrastructure and the dependency on large conglomerates for required services, an attack on a vendor or partner can impact the entire industry, making it especially vulnerable to cyberattacks. Furthermore, the immense value of patient information has led cybercriminals to view healthcare organizations as highly desirable targets.

These factors, when combined with outdated and fragmented federal regulation of health systems security, have led government officials and cybersecurity consultants to consistently identify healthcare as the sector of the U.S. economy most susceptible to attacks3. The question is no longer "will a cyberattack happen?" but rather "when?" Is your system resilient enough to weather such an eventuality? If you're unsure, then it's important that you fortify your processes now.

Thankfully, the steps to building and maintaining a healthcare system that is resilient to cyberattacks are clear, easy to follow and laid out within this guide. Whether recovering from a cyberattack or preparing for one, you can follow these steps to fortify your revenue cycle systems and processes to protect data and recover quickly when a cyberattack eventually occurs.

1 Change Healthcare cyberattack impact Key takeaways from informal AMA survey. (n.d.). https://www.ama-assn.org/system/files/change-healthcare-survey-results.pdf

2 McGlave, C. C., Neprash, H., & Nikpay, S. (2023, October 4). Hacked to Pieces? The Effects of Ransomware Attacks on Hospitals and Patients. Social Science Research Network. https://doi.org/10.2139/ssrn.4579292

3 Abelson, R., & Sanger-Katz, M. (2024, March 29). 4 Things You Need to Know About Health Care Cyberattacks. The New York Times. https://www.nytimes.com/2024/03/29/health/cyber-attack-unitedhealth-hospital-patients.html

First Steps

It's never too early to strengthen security and address the gaps in your revenue cycle; cyberattacks can happen at any time, and the cost of being unprepared is high.

How high? The average healthcare breach costs nearly $11 million[4]. Working proactively to prevent cyberattacks is worth the investment and is the easiest part of the process, as the following steps show.

Fortify Your System's Defenses

The best time to refine and improve your defenses is before an attack happens. There is never a convenient time to do so, but you must take time to pause and examine the current state of your revenue cycle systems and identify their weaknesses. Through the lens of hindsight, we understand the causes and fallout of the February 2024 cyberattack. Using lessons learned, you can proactively diagnose and fortify any potential weaknesses in your revenue cycle, thus mitigating risks and potential damage.

Heed Warning Signs

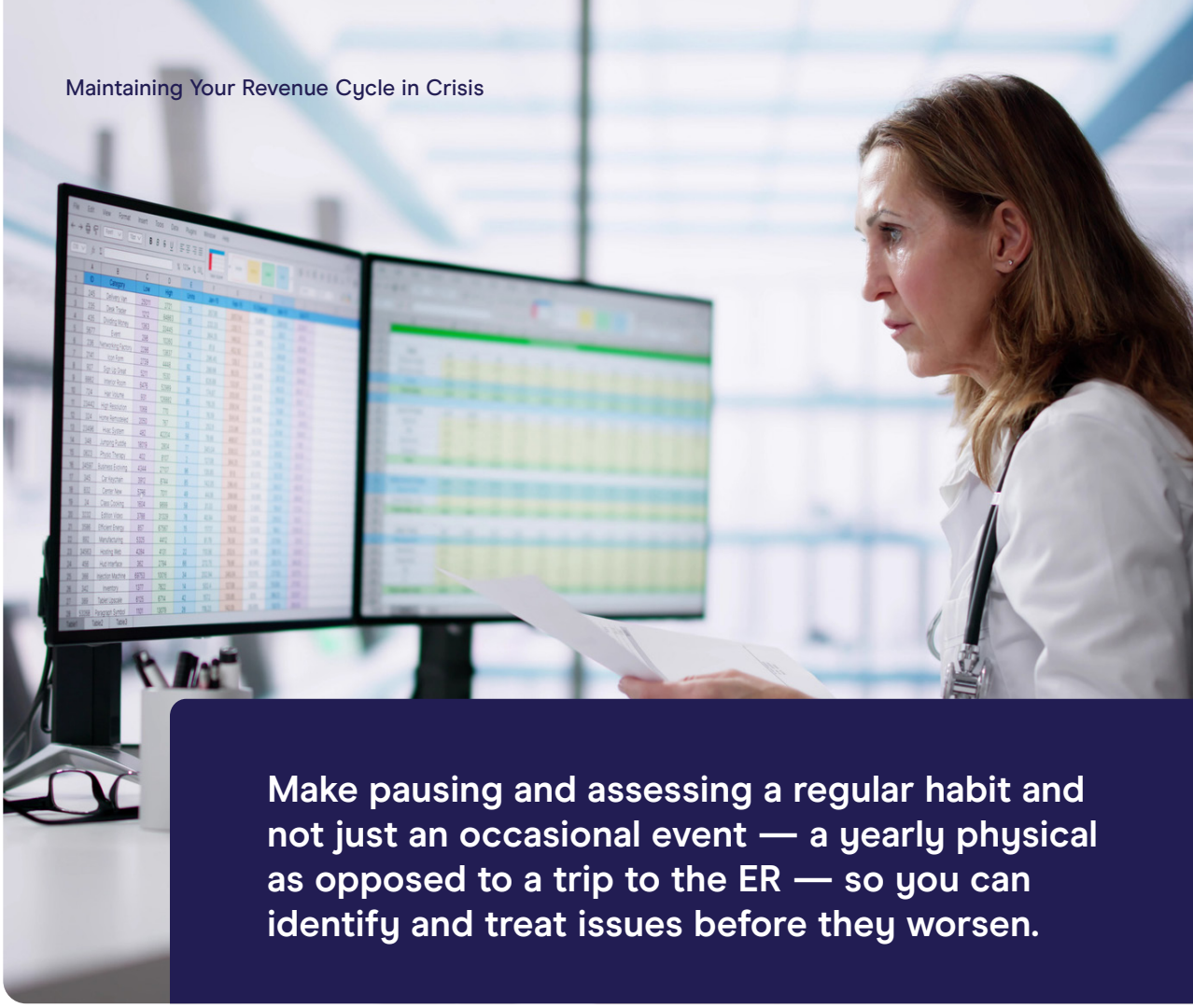
Cyberattacks generally don't occur out of the blue. More often than not, there are warning signs to watch for. These could take the form of lacking or outdated regulations, the use of improperly vetted systems or even reports of smaller businesses becoming victims of cyberattacks. Cyber criminals are perpetually searching for targets and opportunities; it's paramount that leaders and administrators of revenue cycle management make note of cyberattacks and ransomware attacks to stay ahead of the curve.

The cyberattack in February 2024 can now be labeled as one such warning sign: the inadequate security standard, outdated regulatory framework and severe lack of resources in the American healthcare sector created an environment appealing to cyber criminals. This provided an opportunity for a crippling cyberattack on one of the industry's largest healthcare vendors, causing disruptions across the industry. Administrators and government officials now recognize that this attack could have been mitigated if they heeded the warning signs and acted proactively.

The global healthcare sector experienced a staggering 1,613 cyberattacks per week in the first three quarters of 2023, nearly four times the global average, and a significant increase from the same period the previous year. ... This surge has contributed to a steep rise in cyberattack costs for healthcare organizations, with the average breach cost nearing $11 million — more than three times the global average — making healthcare the costliest sector for cyberattacks.

– Nathan Eddy, Healthcare Finance (2024)

4 Healthcare cyberattacks are costing an average of $11 million per breach. (n.d.). Healthcare Finance News. Retrieved July 25, 2024, from https://www.healthcarefinancenews.com/news/healthcare-cyberattacks-are-costing-average-11-million-breach



Make pausing and assessing a regular habit and not just an occasional event — a yearly physical as opposed to a trip to the ER — so you can identify and treat issues before they worsen.

Honestly Assess Vulnerabilities

To simply be aware of warning signs is not enough; you need to learn from them and act accordingly. Start by assessing the systems and plans you have in place for cybersecurity emergencies — including cyberattacks on outside parties affecting your operations — and judge their effectiveness thoroughly. Do you use any outdated programs or hardware? Is there a security weakness that could be exploited? Identify, assess and rectify every vulnerability you discover.

Be both critical and transparent during these system assessments. If you notice that a process relies heavily on one vendor, clearinghouse or system, install backups and/or redundancies to maintain business continuity in the event of that system becoming compromised. To continue to rely on a single crucial system, vendor or clearinghouse is to limit the effectiveness of your response plans and allow unnecessary risk to exist within your operation. Understand your organization's vulnerabilities and use them to guide your defensive preparations.

Have the Right Emergency Management Plans

A lack of adequate planning can make an already bad situation worse. All businesses — especially those in healthcare — must create comprehensive emergency management plans and prepare for worst-case scenarios, including contingencies for backup procedures, redundancies for affected systems and financing for emergency responses.

Just as a fire extinguisher isn't the best response to a flood, each possible emergency must have the right response plan. Tailor emergency plans around your vulnerabilities and how specific contingencies can affect your business continuity. For example, a response tailored to resolve an outage with your ISP should detail the steps required to switch to a backup provider and maintain user accessibility, just as a data breach response would address the containment of compromised hardware and how to mitigate potential disruption.

Risks and threats are constantly evolving, and so should your responses to them. With every evaluation, update your emergency response plans and adapt them to address new threats that have emerged. This, just like every step in this guide, should be performed regularly to ensure full preparedness.

A commonly used reserve goal is three to six months' expenses. At the high end, reserves should not exceed the amount of two years' budget. At the low end, reserves should be enough to cover at least one full payroll, including taxes.

— Propel Nonprofits (2024)

5 Operating Reserves With Nonprofit Policy Examples. (n.d.). Propel. Retrieved July 26, 2024, from https://propelnonprofits.org/resources/operating-reserves-with-nonprofit-policy-examples/

Prepare a Proactive Cash Flow Response Plan

The worst-case scenario for any health system or hospital is to go out of business; this increases patient mortality rates, reduces their level of care and threatens the financial health of health systems. The key to ensuring that a hospital or health system maintains business continuity is to maintain cash flow and to prepare a proactive response, ensuring that the flow of claims is uninterrupted and that providers are paid for their services.

A comprehensive cash flow plan includes three components: cash reserves, lines of credit and alternative sources for claims submission. Cash reserves, obviously, cover expenses and payroll in the event of a halt in cash flow. Experts recommend a reserve large enough to cover three to six months of expenses . A line of credit with a bank can also keep cash flowing in case of an emergency, as they allow health systems to withdraw funds as needed.

Lastly, many healthcare organizations use multiple clearinghouses to diversify claim management processes. In the event one clearinghouse becomes compromised, the others can continue processing claims and keep cash moving. Many companies, including Office Ally, offer fast, capable clearinghouse solutions with robust security to ensure continuing cash flow and avoid a drain on reserves.

There are unfortunate instances, like the February 2024 cyberattack, where cash flow is halted entirely. In such circumstances, it's crucial that your cash flow recovery plan contains steps to quickly resume cash flow and maintain it.

Resuming Halted Cash Flow

If a cyberattack occurs and impacts your ability to connect with payers and receive claims, you should prioritize the following three operations to remain solvent and keep revenue flowing.

1. Resume Claims Submissions

In the event of an emergency, prioritize resuming claims submission as quickly as possible. There are many clearinghouse options on the market that can act proactively on your behalf and prioritize implementing migration plans to get you up and running as fast as possible.

Choose a clearinghouse that proactively works on your behalf and knows where to send your claims. The type of clearinghouse you partner with should be one that can work with you to meet your unique needs.

2. Address Unallocated Funds

After you've found a clearinghouse and resumed receiving claims payments, you need to figure out where they all go. Normally, your 835 forms would help sort your patients and procedures and match them with the funds allocated, but since the vast majority of 835s cannot be accessed without EDI enrollment (which can take two to six weeks for processing), it will take some time to get everything squared away. A good clearinghouse can help expedite the process, but there will still be downtime during the EDI enrollment process where you're receiving payments but can't yet match the funds with their respective patients and procedures.

During this downtime, you should go to each payer portal and manually download the 835 forms yourself to give to your new clearinghouse. This is necessary because until your new clearinghouse is authorized to receive incoming 835s, they will be sent to your former clearinghouse, and if your old clearinghouse is down or compromised, it can't do anything with the 835s it receives. This step is outside the normal purview for most revenue cycle teams, but it's a necessary step to reconcile your accounts and get paid.

3. Verify Eligibility and Benefits

Be proactive in verifying the eligibility and benefits of your patients. During the February cyberattack, many of the health systems and hospitals that used automatic verifications systems could no longer verify the eligibility and benefits of patients. Pharmacies could not refill or process insurance claims for medications, and insurance companies were unable to reimburse patients for paying out-of-pocket in a timely manner, thus restricting what services patients could afford.

In the event of a cyberattack, working with a good clearinghouse partner can help ensure you can continue to verify patient eligibility and benefits. To keep your revenue cycle running as smoothly as possible, continuing the eligibility and benefits verification process is critical.

A Running Start

At this point, you've taken the initial steps towards having a robust, resilient revenue cycle: you've prioritized business continuity, maintained cash flow, assessed and addressed your vulnerabilities, drafted comprehensive response plans and strategically allocated resources. It's a great start, but your work is not over. As the healthcare climate shifts and cyber criminals evolve, so too should your systems adapt. The next steps are everyday habits to practice and maintain to ensure you stay resilient.

Next Steps

Preparedness is complex, multifaceted and constantly shifting under the influence of technological advancements and the economic climate. Even though each hospital or health system's path is relatively unique, the following list of general steps can address the most fundamental requisites to maintain revenue cycle operations when faced with a crisis.

Ensure Data Accessibility

With your weaknesses and risks understood, edit or create new plans for maintaining cash flow and protecting your data. These two plans affect one another significantly as delayed access to your most important data prolongs medical claims processing, and impeded cash flow can delay data recovery services, costing millions of dollars. Thankfully, two simple preventative measures can ensure easy access to data should a disaster arise.

Use Standard Data Formats

In the event of compromised systems or vendors, you may need to transition to an alternative to maintain business continuity. This transition can be greatly hampered if your data is in a non-standard format and your alternate system(s) cannot easily process your files. To prevent this, use industry-standard data formats (e.g., X12 and HL7) for claims, records and all other necessary data.

During your regular system audits, take note of your systems' file formats. If they are not in a standard format or have become outdated, update your files and format them to industry standards to maintain compatibility with the vendors and systems you may use. The inability to seamlessly transition files from one system to another can quickly lead to a stall in operations and diminished cash flow.

Keep Mission-critical Information on Hand

In a cyberattack, you will need to have immediate access to vital information. Keep hard copies of your emergency response plans, contracts, licenses, tax records, insurance documents and key information for enrolling in backup systems, clearinghouses and vendors. These documents should also be kept in data file formats usable across all platforms, and in highly secured locations only administrators and response leaders can access.

Keeping this data ready and in universally accepted file formats allows organizations to easily switch to alternate vendors, clearinghouses and programs during emergencies. This promotes interoperability and minimizes the impact on cash flow and patient care. Furthermore, you should keep physical, paper copies of your most important business documents, as they can be more easily converted to future file types than many complex digital formats and are far more difficult to steal than digital files.

Commit to a Robust Backup Plan

You have identified and addressed your weaknesses, made your data accessible and allocated resources strategically to maintain business continuity in the event of a cyberattack. The next step is to create a comprehensive response plan that utilizes your preparations efficiently and anticipates any contingencies and lingering vulnerabilities that may arise.

Create a Failover System for Data Backup and Recovery

In the event of primary system failure or compromise, incoming claims will come to a halt and your business will stop. Having a failover system on standby will allow you to quickly get your operations up and running again. Failover solutions automatically switch operations to a backup system if the primary system fails in some way. The switch minimizes downtime, enhances reliability and maintains seamless interactions for users by preventing service disruptions.

Failover systems also protect and provide uninterrupted access to data. By continuously replicating and synchronizing data between primary and backup systems, failover systems effectively prevent data from being lost or stolen.

Implement Redundant ISPs

In the event of an internet service provider (ISP) outage, a backup ISP ensures that your systems can operate without interruption and that all essential services remain available. This strategy minimizes downtime and data loss, allows for quick responses to network issues and prevents network outages. Moreover, redundant ISPs increase bandwidth and improve performance through increased capacity.

When deciding on redundant services, cost is always a consideration — a redundant ISP service should never cost more than your primary provider but will nonetheless be an expense. However, choosing not to implement a redundant ISP can cost even more when looking at lost revenue. The estimated median cost in lost revenue for a company experiencing an unplanned internet outage is approximately $11,000 per minute , with that number almost certainly increasing every year. Considering the threat of cybercrime, the risk of not implementing a redundant ISP is too costly to ignore.

In 2013, the median cost for an unplanned internet outage was $7,908 per minute. In 2016, this median rose to $8,851 per minute. By following this trend, it can be estimated that the median cost of an internet outage in 2025 will be over $11,000 per minute.

– Ponemon Institute (2016)

Enroll with Multiple Clearinghouses

Like having a backup ISP, redundant clearinghouses allow you to transition from one service to another in the event of an outage or cyberattack, thus mitigating disruption and maintaining cash flow. Consider using multiple clearinghouses in day-to-day operations and in emergency response plans so claims can be submitted through one or another should a primary option fail.

Note that many clearinghouse alternatives, such as Office Ally's Service Center, can mitigate risks without adding overhead costs. These services help ensure the uninterrupted flow of medical claims and revenue, even during emergencies, and are practical options for healthcare companies who want to mitigate risk without adding to their employee headcount.

Strengthen Procedures

Having the perfect network of redundancies will matter little if they can't be effectively used in an emergency. Prepare policies and procedures for your staff so that redundancies are utilized effectively and disruption is mitigated. Remember that these procedures should detail how and when to transition to backup systems and, importantly, when and how to switch back.

Effective communication is key in this step, as all employees should know their assigned task, know each role and who is responsible for it and know how to receive answers to questions. This ensures that everyone is on the same page and minimizes confusion, which can easily prolong business disruptions.

Commit to Continuous Improvement

By completing the previous steps, your emergency response plan is in good shape. You have fortified your defenses, prepared redundancies and failover systems and created effective policies and procedures for your teams to follow. Unfortunately, this alone is not enough, as emergency preparedness needs to be constantly reacting and adapting to changes within healthcare and the prevalence of cyberthreats. This last section will guide the evolution of your response plan to ensure resilience and readiness for whatever emergency you face.

Learn from Others

We've discussed the importance of watching the industry and heeding cyberattack warning signs, but you should also watch how other organizations are defending against cyberattacks and what steps they take to stay protected. Pay attention to industry leaders, incorporate advanced and updated technologies into your systems and continue to review real-world incidents to learn what has worked for others and what can and should be avoided.

Does the victim of a recent disaster use the same failover system that you use? Are your system's vulnerabilities similar to the weaknesses exploited in a competitor's cyberattack? Is your vendor planning to roll out an update, and does that raise concerns? If the risk is there, be proactive and update your plans to address these developments.

Regularly Review, Test and Update Plans

As you refine and update your systems and protocols, regularly test your systems for efficiency and functionality. Conduct simulations and drills and convene meetings to review and test procedures. A plan may look solid on paper, but a system could unexpectedly crash under a stress test or produce an unaccounted-for contingency, heavily disrupting your operations.

Reviews allow you to refine your response plans and invite feedback for systems that could be improved. For example, an employee who was not involved in a protocol's creation may notice an inefficiency during a drill and provide valuable feedback. Ensure employees know their roles and duties within response plans as well and can perform them effectively. If your contingency systems all function properly but your employees struggle to follow the plan, then the protocol needs to be fixed.

Foster a Culture of Preparedness and Resilience

A leader's attitude and actions set the tone and standard for how resilience and preparedness is valued in their organization. Part of your job as a leader is to promote and foster a culture that prioritizes disaster preparedness. To ensure that employees and the organization value emergency preparedness, a leader must advocate for their response plans.

When a team understands the value of emergency preparedness, they develop a vested interest in bolstering their organization's resilience and strive to contribute to its success. Furthermore, under the guidance and advocacy of their leader, a team can successfully anticipate and navigate emergencies when they arise.

If your contingency systems all function properly but your employees struggle to follow the plan, then the protocol needs to be fixed.

Reaching a Prepared and Resilient System

If you've followed this path to its conclusion and implemented the requisite steps throughout, your emergency response plan is now comprehensive, robust and prepared for whatever disaster may strike. At this point, your focus should now be on maintaining this response plan by keeping it current and making a habit of reviewing its effectiveness. To guide you in these reviews, please refer to the checklist below.

Checklist of Crucial Elements

- ☐ Heed warning signs and developments in the industry; stay current with updates and programs that have prevented or mitigated disasters for others.
- ☐ Honestly assess your vulnerabilities and identify how to fix them.
- ☐ Consider and prepare for all contingencies and any emergency scenario.
- ☐ Budget and allocate your resources strategically.
- ☐ Save your data in standard formats and file types for easy transference to new operating systems.
- ☐ Keep important business documents in both universally compatible file formats and as physical copies for easy access during an emergency.
- ☐ Create and implement a failover system in the event your main system fails or is compromised.
- ☐ Utilize redundant ISPs and clearinghouses to maintain business continuity and minimize downtime.
- ☐ Continuously review and strengthen procedures; ensure that your plans are the best fit for your organization.
- ☐ Regularly stress-test your plans, responses and systems.
- ☐ Promote a culture of preparedness and resilience among employees.

Remember that resilience requires constant awareness and review of internal and external factors. The cybersecurity landscape is constantly changing and adapting in response to new technologies and vulnerabilities. What is secure this year may become vulnerable the next. Luckily, numerous vendors and resources currently on the market have your best interest at heart. Office Ally is one such resource that offers a variety of toolkits to suit the needs of your revenue cycle management.

The cybersecurity landscape is constantly changing and adapting in response to new technologies and vulnerabilities. What is secure this year may become vulnerable the next.

How Office Ally Can Help

Office Ally is a leading provider of healthcare technology solutions, offering a comprehensive suite of products and services designed to streamline administrative workflows and improve revenue cycle management for healthcare providers. Office Ally's clearinghouse ensures that the flow of medical claims and revenue remains uninterrupted so that you can care for your patients and pay your providers, even during emergencies.

Office Ally's robust clearinghouse is an alternative that you can trust, with established connections to more than 3,000 payers and specialized implementation plans for large-volume submitters. Office Ally accepts multiple claim types and submissions from every practice management system and allows claim status checks in real time. Some claims can even be submitted the same day you sign up, and getting started is easy. Contact us today and let us help you get started.