Integrated Payor Solutions

# Safeguarding Self-Funded Plans in the Age of Cyber Threats

## The escalating importance of cybersecurity within healthcare.

As technology advances by the day, organizations increase their dependence on technology to accurately and efficiently perform certain tasks, organize and manage information, and ultimately help keep the business running smoothly. For the most part, the use and advancement of technology has been beneficial. This is especially true in the healthcare field, particularly in the self-funded sector. Technology allows for quicker, more accurate management of data, improved accessibility, and often safer communication.

Unfortunately, safety has become an increasingly harder thing to guarantee, due to the advancement of cyberattacks. As healthcare organizations increasingly rely on digital systems to manage sensitive patient data, the frequency of cyberattacks has risen dramatically. This is a growing concern for self-funded health plans, as they are directly responsible for member healthcare data, and breaches can lead to devastating consequences.

### *So, what are these consequences that make cybersecurity a must?*

For starters, healthcare insurance organizations as a whole face two significant threats. The first is financial risk—from ransom payments, remediation expenses, legal fees, and more, cyberattacks can lead to significant costs and potentially devastating financial consequences. Other costs include the losses from service disruption and increased operational expenses that are bound to crop up in the attempts to fix the damage.

The second threat is the break in trust, an equally vital part of the relationship between fiduciaries and their clients. The breaches from cyberattacks can severely damage that relationship and the trust and reputability of the entity, as patients and policyholders expect their sensitive health information to be protected. The loss of confidence in an insurance company to protect vital information can quickly lead to a loss of business from reputational harm. It's possible to rebuild trust, but not without significant effort, and a considerable investment in security improvements and transparent communication—which of course, means more financial loss.

As technology continues to evolve, cyberattacks will continue to grow in frequency. With that in mind, the intersection of cybersecurity and fiduciary responsibility is critical. As more and more systems move entirely to the digital world, the protection of sensitive patient data and personal health information is more pressing than ever. Under fiduciary duty, healthcare organizations, including self-funded health plan administrators, are obligated to act in the best interest of their members. First and foremost, this means implementing robust cybersecurity measures to safeguard against breaches and data theft.

The failure to protect patient data and other private information not only jeopardizes patient trust, but it can lead to significant legal repercussions and financial liabilities. A focus on cybersecurity is instrumental for self-funded health plans to succeed in today's world. As cyber threats continue to evolve, healthcare entities and plan sponsors must adopt comprehensive security strategies and stay compliant with regulations to fulfill their fiduciary responsibilities effectively.

## Current Overview of Healthcare Data Breaches and Cyberattacks

From October 21, 2009, to December 31, 2023, alone, there were 5,887 large healthcare data breaches reported to the Department of Health and Human Services (HHS) Office for Civil Rights (OCR).1 Trends show a continuous upward trend in these attacks over the past fourteen years, with 725 breaches reported for the year 2023. In those breaches, 133 million records were reported as having been exposed, putting the private information of millions of patients at risk.

There are a number of notable cyberattacks in recent history worth exploring, but there are a few recent breaches that stand out as particularly devastating. Let's take a closer look at the attacks launched on Change Healthcare, Ascension Health System, and Group Health Cooperative of South Central Wisconsin to see what went wrong and how it could have potentially been avoided.

## Change Healthcare

Perhaps one of the most devastating cybersecurity attacks in recent years was the attack on Change Healthcare. Regarded as one of the most "significant and consequential incident[s] of its kind against the U.S. healthcare system in history"[2], the attack has been compared to targeting the entire healthcare system, with the response costing over $2.3 billion.

On February 21, 2024, Change Healthcare, a major player in health technology and data analytics, experienced unauthorized access to sensitive information, which directly affected healthcare providers, payers, and patients. Following the incident, the company took steps to contain the breach, improve its cybersecurity measures, and notify affected parties. Unfortunately, the damage was already done.

A ransomware group named BlackCat claimed responsibility for the attack, supposedly having stolen four terabytes of data.[2] They demanded payment worth $22 million, while large health systems lost over $100 million a day due to Change Healthcare's failure to establish an adequate temporary funding program. Apart from highlighting the financial devastation that can occur from data breaches, the attack underscored the growing vulnerability of healthcare organizations to cyber threats and highlighted the need for robust security protocols to protect sensitive health information.

## Ascension Health System

Another significant cyberattack occurred on May 8th of 2024, on the Ascension Health System, one of the nation's leading non-profit, Catholic healthcare systems.[3] The attack caused widespread outages at Ascension hospitals across the nation, interrupting Hospital EHR access, pharmacy processing, and access to patient portals.[4] Ascension quickly began working with cybersecurity experts in order to get operations back up and running, but it took until May 27th for patients and clinicians to start seeing progress. By September 17, 2024, the financial consequences for Ascension had reached $1.8 billion in operating margin loss.[5]

## Group Health Cooperative of South Central Wisconsin

On January 25, 2024, a cyberattack occurred on Group Health Cooperative of South Central Wisconsin. The breach involved unauthorized access to its systems, as a third party managed to access the network and attempted to encrypt files through ransomware.6 While the file encryption was not successful, some systems were rendered temporarily unavailable while systems were secured. Cybersecurity experts later confirmed that the attacker had successfully copied files from the network, potentially exposing personal health data, including names, addresses, and medical records of members. The attacker later made contact with Group Health Cooperative of South Central Wisconsin, demanding payment in exchange for deleting the stolen data, though whether or not that ransom was paid was never confirmed. Ultimately, the attack put the information of 533,809 patients at risk.[6]

## The Ripple Effects of Cyberattacks

Self-funded plans are particularly vulnerable to cyberattacks since there are multiple integrations across vendors and systems, all having access to patient data. The lessons to take away from these security breaches are hard-earned and straightforward. The implications of cyberattacks on patient privacy and financial stability are only the tip of the iceberg, though certainly disastrous ones.

### To recap:

**Patient Privacy**

Breaches can expose sensitive personal health information, leading to identity theft, financial implications, delays in care, and even the potential for blackmail or discrimination. Patients may lose trust in their healthcare providers, deterring them from seeking necessary medical care. In addition to the erosion of trust, these breaches can also lead to emotional and psychological distress because of the uncertainty of how their health data might be used.

**Financial Stability**

Healthcare organizations face substantial costs associated with data breaches, including remediation expenses, legal fees, regulatory fines, credit monitoring services for those affected, losses of business due to reputational harm, and even costs associated with the loss of productivity while addressing the breach. These financial burdens can strain resources and affect the overall sustainability of the organization.

**Operational Disruption**

Cyber incidents can disrupt healthcare services, leading to delays in patient care and increased operational costs. It can also result in fraudulent use of identity for medical purposes leading to inaccurate medical histories and unexpected bills. This can affect patient outcomes and reduce the efficiency of healthcare delivery.

Cybercriminals continue to evolve their tactics to exploit vulnerabilities in healthcare systems. Increasingly sophisticated methods, such as ransomware attacks, phishing schemes, and advanced persistent threats (APTs), target sensitive patient data and disrupt operations. To make things worse, these tactics are easily tailored to the unique challenges of the healthcare sector, including the urgent need for access to data and the potential for high financial gains.

In order to combat these evolving threats, there is a vital need for heightened vigilance through comprehensive cybersecurity strategies, regular training for staff, and advanced threat detection systems. Proactive measures are essential to protect patient information and ensure the integrity of healthcare services in an increasingly complex cyber landscape.

## The Role of Fiduciary Responsibility in Health Benefits

There's no question that increased vigilance and preventive measures are vital to safeguard against cyber threats. But who does the responsibility of ensuring these needs are met fall upon?

> ***For most purposes, it falls on the fiduciary.***

When it comes to self-funded healthcare plans, a fiduciary is responsible for managing plan assets, ensuring plan operation, and looking out for the best interests of plan participants.[7] With this in mind, it is the fiduciary's responsibility to ensure the protection of those participants' sensitive health data, safeguarding the trust of patients and members in the plan.

There are a number of legal, ethical, and financial obligations a fiduciary is required to fulfill, many of which directly pertain to addressing cyber threats. These principal responsibilities are as follows[7]:

- To act in the best interest of plan participants.
- To manage plan assets while adhering to objectives and minimizing risk.
- To ensure that the plan complies with current laws and regulations.
- To monitor plan performance, including financial performance and benefits to participants.

Not only are plan fiduciaries responsible for looking out for plan members' best interests, but they are also responsible for protecting the sensitive information of those members. From risk assessments to ensuring compliance, regular audits, and incident planning, fiduciaries must be prepared to safeguard from these cybersecurity threats and respond quickly if an attack does occur. Failing to uphold this responsibility results in legal consequences, significant financial losses, and damaged or broken trust — the consequences of successful cyberattacks.

Ultimately, the main stakeholders responsible for ensuring robust security measures as protection against rising cybersecurity threats are plan sponsors and third party administrators (TPAs). These responsibilities extend to brokers and vendors as well, as we'll look at below.

### Third Party Administrators

TPAs are responsible for day-to-day administrative functions of the health plan including claims management, eligibility, customer service, vendor management, and protecting sensitive member data. With the added complexity of multiple vendors with access to protected health information, it's vital that TPAs take extra precautions to ensure compliance and invest in strong security measures. TPAs should have systems and plans in place for responding to potential data breaches in the event that a cyberattack does occur—though the hope is that such measures are never necessary.

### Brokers

Brokers take the role of advisors, helping clients select health plans and vendors. This includes evaluating the protective measures of their selected plan or vendor in order to ensure their clients are protected. Their primary role in combatting cyber threats is to assess vendors for low or high risk and facilitate clear communication between the health plan and vendor to ensure security expectations are upheld.

### Vendors

As health plan vendors provide a number of digital services including data storage, software, telehealth, and more, they have a direct responsibility to ensure robust cybersecurity measures are taken to protect that health data. Adhering to security standards, conducting regular security audits, and collaborating with TPAs to successfully implement cybersecurity measures across all platforms are all crucial aspects of a vendor's duties.

## Empowering TPAs: A Blueprint for Security

The stakes are only growing higher for TPAs—and so is the need for partnering with a trusted vendor. While some entities play a larger role than others, the responsibility for these attacks and preventing them falls on everyone involved within the plan, regardless of their position. The reality is that even if you are not the party directly responsible for security measures, such as the consultant or TPA, the client is still likely to hold you responsible for recommending a vendor whose systems were not up to current standards if an attack does occur.

Protection is paramount—which is why it's important for TPAs to keep in mind the best practices for enhancing cybersecurity posture and partnering with a trusted vendor. At a basic level, these include the following:

- Assess vendor security measures and regulation compliance.
- Consider the vendor's reputation and track record.
- Ensure the vendor clears specific cybersecurity requirements.
- Outline procedures for any breaches, including communication plans and a timeline.
- Regularly conduct security audits to ensure standards are up to date.
- Perform risk assessments to identify any vulnerabilities and mitigate them.
- Ensure the utilization of strong encryption methods for sensitive data.
- Provide regular training for employees to effectively enforce cybersecurity best practices.
- Continuously monitor any emerging threats, while reviewing and updating security practices as needed.

At IPS, we have our own checklist for vetting potential vendors. From our experience, there are a few key points to check right off the bat, determining whether the vendor is:

- ☑ HIPAA compliant
- ☑ SOC2-Certified
- ☑ Stable with a history of longevity
- ☑ Equipped with a reliable IT team

## Encompass+: A Holistic Solution for Managing Cybersecurity and Fiduciary Duties

### Built on Salesforce

Encompass+ is built on Salesforce, a cutting-edge solution with the power, scalability, and reliability to back businesses. Compared to the constant change and turmoil in the healthcare industry, Salesforce provides a refreshing stability. Plus, with Salesforce's platform designed for the healthcare industry, Health Cloud, fiduciaries can be assured that their member information is expertly secured.

### Compliant and Secure

Encompass+ is both HIPAA and SOC2-certified, meaning medical claims processing remains compliant and user data stays secure, avoiding any legal trouble.

### Ease of Use

Despite its solution's power, stability, and security, Encompass+ is easy to use. Employers and providers access the solution through user-friendly portals, and detailed and customizable reporting allows for quick comprehension of that data. Other features like automated processing, configurable alerts, automatic audits, and risk assessments add to the ease of use.

## IPS and the Future of Cybersecurity

As we've seen, the effects of cyberattacks can be detrimental to patients and fiduciaries alike, causing financial and emotional hardships for years to come. However, technology has also vastly improved how we conduct day-to-day processes with efficiency and precision. With these significant advantages and potentially disastrous disadvantages in mind, it stands to question—how do we coexist with both realities as we move forward?

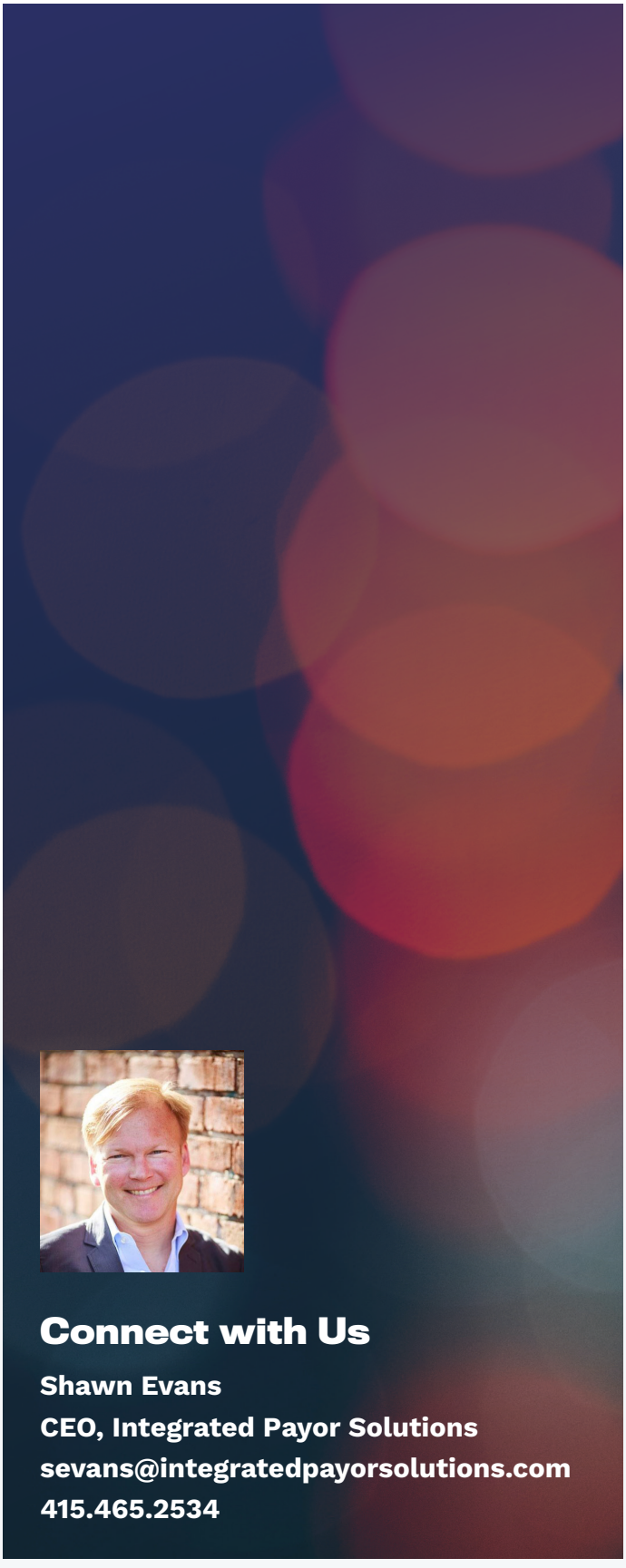
The answer lies in security. Modern TPAs looking to compete in a technology-driven landscape will need to adapt in order to survive and thrive. That includes heavily vetting and securing the right data technology and compliance vendor partner who can provide peace of mind in the midst of cyber threats.

At IPS, we work to create efficiency and security in one consolidated solution built on a singular platform, Salesforce. This cuts down on cyberattack points of entry, leading to robust security that safeguards protected health information and client trust. Not only does Salesforce conduct a full security review of our platforms annually, but they perform additional audits at regular intervals throughout the year. If any issues are found, IPS' platforms are briefly removed until the issues are rectified to Salesforce's satisfaction.

With this level of protection, Encompass+ is able to harness the power, scalability, and reliability of Salesforce, so you can rest easy from cyber threats.

Encompass+ provides the key for managing cybersecurity and fiduciary duties in healthcare.

***What will your future hold?***





## Connect with Us

**Shawn Evans**
**CEO, Integrated Payor Solutions**
**sevans@integratedpayorsolutions.com**
**415.465.2534**

## Sources

1. https://www.hipaajournal.com/healthcare-data-breach-statistics/
2. https://hyperproof.io/resource/understanding-the-change-healthcare-breach/#:~:text=In%20late%20February%2C%20the%20ALPHV,records%2C%20and%20other%20sensitive%20information
3. https://about.ascension.org/about-us
4. https://www.tebra.com/theintake/practice-operations/medical-news/the-major-cyberattacks-that-have-affected-healthcare-systems-in-2024#:~:text=Group%20Health%20Coop%20of%20South,security%20numbers%2C%20of%20533%2C809%20individuals
5. https://www.hipaajournal.com/ascension-cyberattack-2024/
6. https://www.hipaajournal.com/group-health-cooperative-south-central-wisconsin-ransomware/
7. https://www.linkedin.com/pulse/what-all-fiduciaries-self-funded-health-care-plans-reagan-cbpa/