Insurance

Check yourself: A data security audit for insurers

Use this self-audit worksheet to learn and uphold best practices for safeguarding sensitive client information.

ShareFile™

Cybersecurity: A modern-day insurance imperative

It's not easy to stay on top of cybersecurity best practices in a high-stakes, fast-paced modern work environment. But for every type of organization—and especially for insurance companies dealing with hundreds of sensitive documents every day—cybercrime is a very real and potentially costly threat.

According to **Statista**, the average data breach in the United States in 2023 cost $9.48 million. Financial and reputational damage typically extend months or years beyond the initial breach, often resulting in costly legal issues, fines, and customer churn. The health insurance giant Anthem remains a cautionary tale years after a 2015 data breach resulted in the theft of personal information belonging to **8 million** current and former employees and customers. Mitigation ultimately cost the company over $100 million.

With so much on the line, insurers must proactively work to protect customers' personally identifiable information (PII) and protected health information (PHI) from cyberattacks. But why do data breaches still happen when companies have strong security solutions?

Smarter cyber criminals

Providing password protection and virus scanning software is not enough. Today's cyber criminals are more sophisticated than ever before. A 2022 study **found** that phishing campaigns attempting to trick professionals into downloading malware or giving away sensitive information increased 61% from the previous year.

In addition to becoming more common, these attacks are becoming more calculated. Cybercriminals may send emails or texts that appear to be from a trusted source or use **topical issues** to lure their victims, with subject lines that suggest shopping deals around the holidays or fake alerts about tax filing during tax season.

AI-created malware is especially good at avoiding detection by traditional antivirus software, leading to a sharp **increase in ransomware cases** in 2023. These mounting threats from cybercriminals increased the likelihood for insurance agents to fall into a well-conceived trap.

Preferring familiar tools and applications

With the rapid adoption of cloud-based services, professionals have become more comfortable downloading and using outside applications without informing their IT departments. While they don't mean to do any harm with this practice, known as Shadow IT, they end up bypassing security measures and putting PPI or PHI in jeopardy.

Despite some awareness of the risks, many insurance agents will continue using these unsanctioned applications because they feel familiar. It's human nature to prefer tools and applications we're already used to, and it can be difficult to adjust to working with different platforms even if they are more secure.

Working under pressure

Reluctance to adopt secure tech goes beyond the Shadow IT issue. People working in fields that deal with clients' personal data and information are often under pressure to get things done quickly without time-consuming protocols standing in their way. Adding an extra step or layer to their security processes can feel too overwhelming to consider.

Steps you can take to increase data security

We understand how difficult it can be to keep security top-of-mind while you're busy managing policies and keeping customers happy. The security audit worksheet on the following pages outlines simple steps to take and features to enable so you can keep working efficiently while feeling confident about your data security practices.

Consider returning to this audit worksheet once a quarter to make sure you're consistently following up with these recommendations. Better data security habits shouldn't feel out of reach. Even when you're pressed for time, it's important for insurance professionals to remember that simply changing a few settings can go a long way toward providing you with peace of mind that customer information is safe.

Audit worksheet: How can you protect customer data?

Read through the following sections and check the "Yes" or "No" boxes. At the end of this worksheet, you'll tally up the number of times you checked "yes." This score will help you understand how effective your current data security practices are.

PART 1:

Secure files and devices

There should be no gaps in security when insurance organizations are sending, receiving, and collaborating on files with PII or PHI. Email and file encryption scrambles text into an indecipherable format while in transit and offers protection from bad actors, but it's only the beginning of a comprehensive security strategy.

The following questions will help you understand what steps you can take to ensure files are completely secure. If you're unsure whether you have the right software to enable these recommended security features, consider checking with your IT department.

When receiving, storing, and sending files containing sensitive client information, are you:

Limiting information collection to necessary data?

☐ Yes
☐ No

Determining how much protection information needs and applying the right level of permissions?

☐ Yes
☐ No

Enabling email encryption for the body of the message and attachments?

☐ Yes
☐ No

Enabling file encryption to protect sensitive information in transit or at rest?

☐ Yes
☐ No

Utilizing custom permissions for folders and files to control who has access and for how long?

☐ Yes
☐ No

Enabling automated alerts that immediately flag security issues when they occur?

☐ Yes
☐ No

Looking at security dashboards where you can identify patterns in situations where threats are recurring?

☐ Yes
☐ No

OF YES ON THIS PAGE _____

PART 2:

Beyond files: Ensure all devices are secure

The following questions will help you understand what steps you can take to ensure all devices your team or agency uses are completely secure. If you're unsure whether your team is taking all the necessary steps to ensure all devices are safe, consider having them reference this checklist once a month.

In order to safeguard devices and proactively protect customer data, do you:

Enable multi-factor authentication for more secure log-ins?

☐ Yes
☐ No

Avoid the use of personal devices?

☐ Yes
☐ No

Create strong, unique passwords for your accounts and devices?

☐ Yes
☐ No

Store passwords in a secure place?

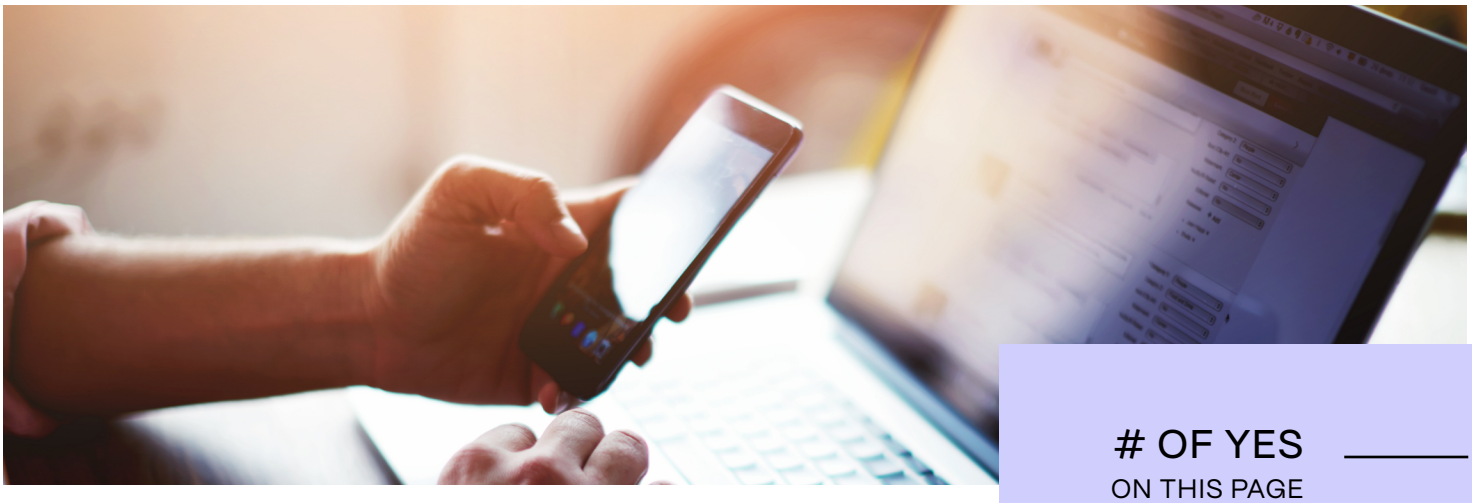
☐ Yes
☐ No

Stay on top of software updates that impact the effectiveness of your security features?

☐ Yes
☐ No

Take an occasional free security course or read about the latest phishing threats?

☐ Yes
☐ No



OF YES _____
ON THIS PAGE

PART 3:

Security and productivity can go hand-in-hand

The following questions will help you understand if your team has the technological capabilities to protect customer information while still working efficiently on their behalf.

If you're unsure whether your team has the tech they need to do their best work in a more secure way, consider adopting stronger, more comprehensive solutions that integrate into existing workflows.

When working across applications and collaborating with others, are you using:

Single sign-on capabilities to avoid repeated log-ins across apps?

☐ Yes
☐ No

Secure link sharing so your customers can access documents with one click (instead of having to download a file)?

☐ Yes
☐ No

A single, secure space such as a portal or dashboard where you can track and collaborate internally or directly with customers (as opposed to a platform that isn't secure)?

☐ Yes
☐ No

Built-in workflows for collaboration platforms that offer safe document requests and collection?

☐ Yes
☐ No

OF YES _____
ON THIS PAGE

Your score

In the space below, tally up the number of times you checked "Yes" and put your score.

Score: _____ / 17

Assess your score against the scoring key here to analyze the strength of your current data security strategy.

**Not the score you were hoping for? It's never too late to implement best practices and strategies to better protect sensitive data. Continue refining your approach to data security and revisit this worksheet to track your progress.*

Scoring Key:

0–5 = Just getting started*

6–11 = Making progress

12–15 = Almost there

16–17 = Expert-level

Security and productivity with collaborative technology

If you scored less than 10, it could be because of your security tools' limitations.

While rigorous security practices can interfere with productivity, **they don't have to**. There are solutions available that offer both productivity and protection by embedding greater security into existing workflows.

Considering both the pressure insurance agents are under to work efficiently and the costly consequences of a data breach, security solutions should ensure that neither are ever compromised. Software that protects data while allowing for streamlined workflows and end-to-end productivity is well worth the investment.

Peace of mind and seamless workflows: The ideal security solution

To guarantee customers' data is protected, insurance agencies must invest in airtight data security solutions—and professionals must be able to use those tools without limiting their ability to work productively. By referring back to the above checklists, you can quickly determine what steps to take to fit security best practices into your busy work week. Both your actions and the tools you use have a real impact on preventing data breaches from happening to your insurance organization.

Learn more about partnering with ShareFile to enhance data security through collaborative technology.