# STEPPING UP CYBERSECURITY

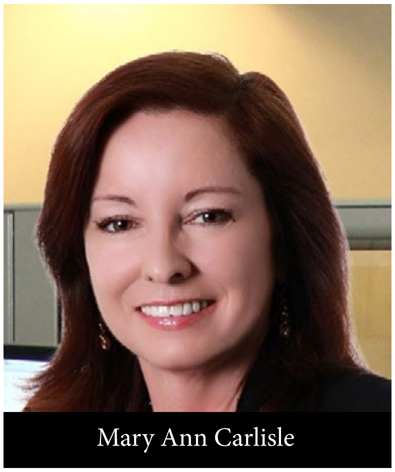
## FROM TREATING EMAILS WITH CAUTION TO ENGAGING OUTSIDE EXPERTISE, ERECTING GUARDRAILS HAS BECOME NECESSARY FOR SELF-INSURED PLANS

Written By Bruce Shutan

As the workplace deepens its digital footprint and electronic medical records become the norm, efforts to shore up cybersecurity protection have become a necessary cost of doing business across the self-insurance community.

Cybercriminals are increasingly mining health care data by making payers, providers and plans their top targets last year, according to a recently released report from Fortified Health Security. The number of medical record breaches increased to 51.4 million, which was up from 49.4 million the previous year, with more than 78% attributed to hacking and IT incidents. In addition, health care providers remain the overwhelming source of breaches, accounting for 70% of 2022 incidents.

Industry observers often say that these thieves are more sophisticated with their attacks, which is why cybersecurity protection is an area where expertise cannot be understated.


Mary Ann Carlisle

"My biggest recommendation would be to look for a very look for a good outside vendor who can support your company and meet with that entity once a month just to review their protocols," says Mary Ann Carlisle, chief operating officer of ELMCRx Solutions, LLC, which assists self-insured employers in managing their prescription drug benefits. "It's an investment in your company and a lot less expensive than trying to build all of that inside your own organization."

## LEGAL IMPLICATIONS

In keeping with ERISA's fiduciary standard to act in the best interest of plan participants, PlanTools, LLC CEO David Witz explains that advisers must obtain on behalf of the plan sponsors they serve an annual due diligence report on cybersecurity for two reasons. One is that documentation demonstrates a fiduciary process. Also, it helps the commercial insurance carrier supplement its policy with the appropriate terms and coverage to protect employers from cybersecurity claims.

Like all benefit plan sponsors and administrators, self-insured health plan administrators are obliged to monitor and ensure that the recordkeeper has state-of-the-art cybersecurity protections in place, says Susan Rees, an attorney with extensive ERISA experience with the Wagner Law Group. But plans and plan fiduciaries also must be prepared to have their own cyber insurance policy to help mitigate these risks, she adds.

David Witz

Liability for cybersecurity breaches may include civil or criminal penalties under the Health Insurance Portability and Accountability Act, as well as litigation expenses related to participant claims for ERISA fiduciary breach or state privacy and security violations, notes Sarah Bassler Millar, a partner at Faegre Drinker.

Sarah Basslar Millar

Given how technology has evolved since HIPAA took effect in 1996 and in light of remote work's increasing popularity, she advises plan sponsors to review their privacy and security policies and procedures. With so many working Americans logging into their laptops at home, local coffee shops or on the road, more personal data is now at risk for hacking than ever before.

There also are state and federal regulatory challenges to consider. "One of the problems is that the recordkeepers are subject to state law, and state privacy laws will give participants a cause of action against the recordkeeper where that same cause of action against the plan sponsor or plan fiduciaries is most likely preempted by ERISA," Rees explains. "So recordkeepers are on the line for sure."

Another obstacle is that there's limited case law and the most noteworthy litigation involves retirement plan assets rather than health plans. All lawsuits involving cybersecurity breaches of employee benefits plan participant data or assets have been settled at the district court level, she notes. "So we don't have any strong legal guidance on some of the issues," she explains.

This void has been partially filled by the Department of Labor (DOL), which in April 2021 issued a dozen best practices that plan sponsors, fiduciaries, recordkeepers and participants can follow to reduce the risk of sensitive employee medical information falling into the wrong hands.

Although, it seems like the courts, and DOL are inclined to take the position that "when a recordkeeper's computer system gets hacked, it's the responsibility of that service provider to have provided an adequate service to the plan to protect the plan assets and plan data," Rees says, describing the DOL guidance as good advice.

Among the noteworthy court cases, three involve lawsuits against Alight Solutions LLC, a cloud-based human capital and technology services provider. One of the first publicized cases of a cybersecurity breach in the employee benefits arena was filed in April 2020. A U.S. district court judge presiding over *Bartnett v. Abbott Laboratories* dismissed claims against the plan fiduciaries involving the theft of $245,000 from the plaintiff's retirement plan account, but allowed both ERISA and state law claims to proceed against Alight Solutions. The vendor was named as a defendant in a separate suit filed by a participant in Estee Lauder's 401(k) plan over $99,000 in missing assets, which was settled in March 2020, and also subject to a DOL successful subpoena enforcement action in the Seventh Circuit.

Another case filed in July 2022 involving Alight that Rees says serves as a cautionary tale is *Disberry v. Employee Relations Committee of the Colgate-Palmolive Co.* et al. The plaintiff, a retired Colgate-Palmolive marketing executive named Paula Disberry, alleged a breach of fiduciary duty under ERISA after a cyberthief emptied more than $750,000 from her 401(k) plan.

With regard to this ruling, she says the judge seemed to suggest that the parties needed to figure out a way to pay the plan participant her money and greenlit the case for trial. "It's almost like the judge was helping the participant to make her case, which is really not the job of a district judge," according to Rees, who assumes this case will be settled.

## SCHEMES OF DECEPTION

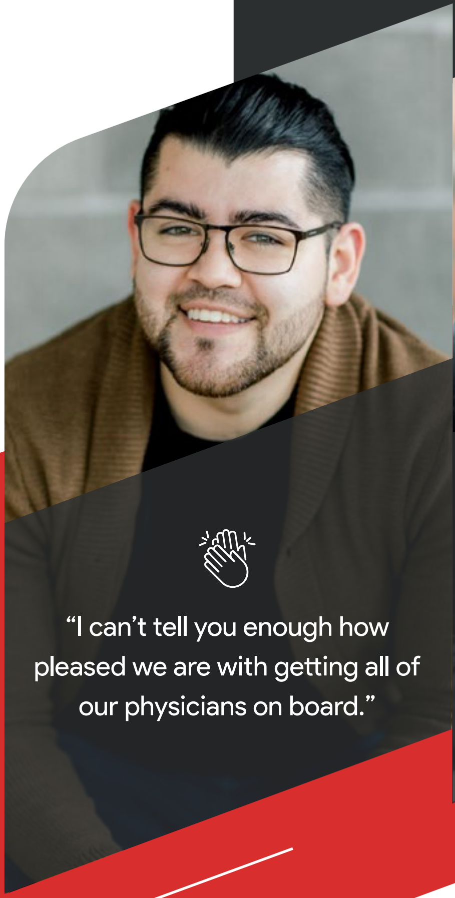
While cyber thieves continue to crack complicated codes, they also know all too well the value of simple schemes of deception. One of the most underrated areas of cybersecurity breaches involves email, observes Michael Carrara, CEO of Hi-Tech Health, whose claims management platform is used by third-party administrators, carriers and provider-sponsored plans.

Michael Carrara

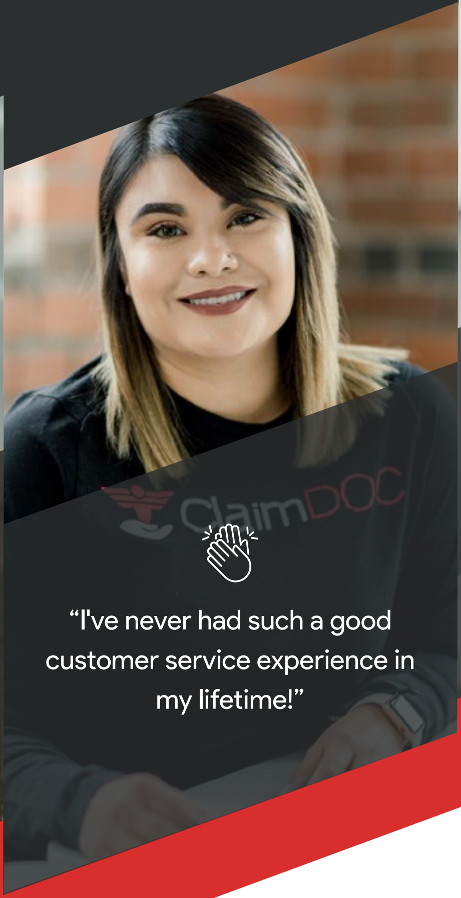
"People don't understand an email is not secure by nature," he says. "All it takes is a name associated with an address, date of birth and the first three of a Social Security number, and people can take out car loans, mortgages and credit cards. It's really scary."

# Nobody delivers like we do.

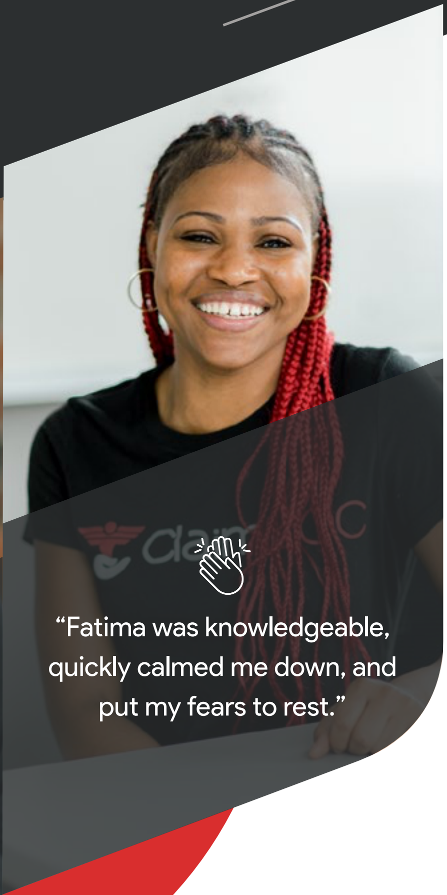
ClaimDOC's reference based pricing program is unlike any other.  Experience savings and a caring team who is always there to go above and beyond for members.



"I can't tell you enough how pleased we are with getting all of our physicians on board."



"I've never had such a good customer service experience in my lifetime!"



"Fatima was knowledgeable, quickly calmed me down, and put my fears to rest."

ClaimDOC®

Fair Payment Solutions for Health Plans

With ClaimDOC you're in the driver's seat to create a rich and sustainable healthcare plan using RBP principles. Our approach to elevate the member experience, while diligently managing risk is what sets us apart.

**Learn more at Claim-doc.com or call (888) 330-7295**

The explosion of artificial intelligence is expected to further complicate cybersecurity protection. Carrara has little doubt that AI is becoming involved with "phishing" attacks that send fake emails or other messages that look like they're from reputable companies. The purpose of this fraudulent activity is to induce individuals to reveal personal information such as passwords and credit card numbers. "I get bills from FedEx with the company's logo and everything," he reveals. "Sometimes the attacks are hard to decipher whether they're real."

One of the most recent hacking attempts Carrara has noticed involves what he describes as "brute force threats from these bad actors who are constantly trying to infiltrate through different holes in your firewall."

Apart from having a dedicated department whose sole concern is cybersecurity, Hi-Tech Health relies heavily on its partners and tries to stay at the forefront of this topic through seminars and blogs. Other steps include moving all systems to a tier-one data center's managed hardware platform whose firewalls are safely maintained and the company is constantly apprised of threats. Different layers of protection also allow Hi-Tech Health to take advantage of everything from Center for Internet Security protocols to expertise from in-house network engineers.

Carrara's employees also undergo monthly online training with different scenarios and an annual penetration test from different third-party companies that supplements weekly penetration tests from Carson & Saint, a security and management consulting firm. In addition, Soc 1 and Soc 2 audits, which stand for service organizational control, are done to protect financial controls as well as security, processing integrity, confidentiality and privacy.

Cybersecurity compliance is difficult enough in the U.S., but those efforts expand even further when it involves overseas business. Since Hi-Tech Health's client base is worldwide, for example, the company is subject to general data protection regulation rules in Europe, as well as HIPAA in the U.S.

Another protective layer that has become a table stake for self-insured employers and their partners is cybersecurity insurance, which Carrara says is mandatory in this climate, noting that his firm has $2 million in coverage for each incident. “It’s not only government that’s being attacked,” he explains. “It’s health insurance. It’s banking. It’s retail. Attacks are doubling.”

While perfect protection against cybersecurity breaches is always the goal, and the vast number of attacks are thwarted, the reality that some health plan sponsors and participants face can be harsh. Adds Rees: “Some of the human errors that have enabled hacking up to this point are fairly low level. There are hundreds, if not thousands, of attempts to hack into plans and service providers, and 99% of them are unsuccessful. All it takes is that 1%.” ■

*Bruce Shutan is a Portland, Oregon-based freelance writer who has closely covered the employee benefits industry for more than 30 years.*

## SIMPLE STEPS TO SECURE SENSITIVE MEDICAL DATA

Self-insured health plans and their vendor partners should be following these five steps to stay ahead of cyber thieves and protect highly sensitive personal information, suggests Mary Ann Carlisle, chief operating officer of ELMCRx Solutions, LLC. They include:

1. **TFA or MFA:** Two factor authentication, or TFA for short, will send a code to one's smartphone whenever a password is changed, which must be entered in order to access an online account. When two or more steps are required every time someone logs into a system, it's called multi factor authentication, MFA for short.

2. **VPN or VDI:** Securing work conducted in a virtual personal network known as a VPN or virtual desktop interface known as VDI will keep information private and secure. Working through a cloud or server-based system that requires entering an email address and password that generates an authentication code is safer than logging into a computer's local drive, which creates a risk if the computer is lost or misplaced.

3. **Public facing:** Information that is stored on a company website is considered "public facing" content made available to the general public. It can be easily obtained by cyber thieves who break into the back end of a website. Medical information stored in the VDI is more safely contained in that ecosystem and is not public facing.

4. **Scanned attachments:** One of the most basic cybersecurity efforts involves scanning attachments for malware and viruses before making them available to recipients to be safely opened. Advanced threat protection scans attachments for these threats and ensures that any Word, Excel, PowerPoint, etc. documents are legitimate.

5. **Phishing tests:** Monthly phishing tests, along with mandatory training on this issue, will help walk users opening attachments or clicking on embedded links and how to spot red flags. One such example is when the sender's email address doesn't match up with the organization that is being impersonated to poach personal information. Any cyber threats should be documented and included in a monthly report to the cybersecurity carrier.■