Don't Forget About ERISA in Your Health Plan's Cybersecurity Efforts: Important Reminders for Plan Fiduciaries in the Wake of Healthcare Cyberattack

Insights
7.03.24

Earlier this year, a cyberattack on a leading healthcare claims processing provider had an unprecedented impact on patients and healthcare providers across the country. While group health plans were not directly targeted in the attack, the magnitude of the incident serves as an important reminder for plan sponsors and fiduciaries to ramp up their cybersecurity efforts. When you think about health data security, HIPAA might be the first law that comes to mind. However, ERISA can also come into play due its rules for plan fiduciaries. We'll give you an overview of the costly cyberattack and what you should know about your cybersecurity responsibilities as a plan sponsor or fiduciary under ERISA.

Change Healthcare Cyberattack

On February 21, cyber criminals accessed Change Healthcare's computer systems, encrypted vital IT data, and claimed to have stolen six terabytes of sensitive information, including personally identifiable information and medical records. In response to the attack, Change Healthcare disconnected its systems – paralyzing hospital and pharmacy systems, claims approvals, and billing and payment systems across the country. It was arguably the most significant cybersecurity disruption to healthcare in U.S. history.

UnitedHealth Group, Change Healthcare's parent company, paid a $22 million ransom to the cyber criminals to reduce the risk of the stolen medical data being publicly disclosed – and an additional $3.3 billion to affected providers. These losses don't include the forensic, incident, and legal costs needed to respond to the attack. In its 2024 first-quarter report, UnitedHealth Group reported a loss of $872 million in "unfavorable cyberattack effects."

The U.S. Department of Health and Human Services (HHS) Office of Civil Rights (OCR) announced on March 13 that it had opened an investigation into the Change Healthcare attack. OCR oversees and enforces the Health Insurance Portability and Accountability Act of 1996 (HIPAA) privacy, security, and breach notification rules that apply to "covered entities" – such as healthcare providers, clearinghouses, and health plans – and their business associates.

While OCR stated that its investigation does not prioritize the health plans or other covered entities impacted by the attack, the agency reminded covered entities of their "regulatory obligations and

impacted by the attack, the agency reminded covered entities of their "regulatory obligations and responsibilities, including ensuring that business associate agreements are in place and that timely breach notification to HHS and affected individuals occurs as required by the HIPAA Rules."

Beyond HIPAA: How ERISA Impacts Health Plan Fiduciaries' Cybersecurity Responsibilities

While the OCR investigation called on health plans and other covered entities to ensure compliance with HIPAA, most employer-sponsored group health plans are additionally subject to the Employee Retirement Income Security Act (ERISA). While this Insight will focus on the ERISA rules, both HIPAA and ERISA can be relevant to your plan's cybersecurity measures, as summarized below.

HIPAA

Under HIPAA, covered entities such as health plans must designate a privacy officer and a security officer to develop and enforce the plan's HIPAA compliance policies and procedures. HIPAA's Security Rule requires appropriate administrative, physical, and technical safeguards to secure electronic personal health information. As mentioned above, OCR (which is part of HHS) enforces the HIPAA rules. You can find OCR's cybersecurity guidance material here.

ERISA

Under ERISA, any person who exercises any discretionary authority or control under the plan is an ERISA fiduciary. Fiduciaries might include the employer sponsoring the plan (especially if the plan is fully or partially self-funded) or certain individuals, such as plan trustees or administrators. ERISA requires fiduciaries to administer the group health plan prudently while acting solely in the best interests of the plan participants and beneficiaries – which may include mitigating cybersecurity risks. ERISA is enforced by the U.S. Department of Labor's (DOL) Employee Benefits Security Administration (EBSA). We'll discuss the DOL's cybersecurity guidance below.

Potential Overlap

Note that a plan's HIPAA privacy or security officer could also be an ERISA fiduciary if they exercise sufficient discretionary authority as to the plan. However, under current guidance, status as a HIPAA privacy or security officer does not *automatically* create ERISA fiduciary status.

DOL Cybersecurity Guidance for Plan Sponsors and Fiduciaries

In 2021, the DOL issued cybersecurity guidance aimed at plan sponsors and fiduciaries regulated by ERISA, as well as plan participants and beneficiaries. Initially, this non-binding guidance was geared toward ERISA-governed retirement plans, but the DOL subsequently stated that it also applies to ERISA-governed group health plans.

Under the guidance, ERISA fiduciaries must take appropriate precautions to mitigate any cybersecurity risks. Therefore, ERISA fiduciaries, (including HIPAA privacy and security officers

who qualify as ERISA fiduciaries), have a legal responsibility to notify plan participants and their beneficiaries of any cybersecurity breach while mitigating any potential harm as soon as they become aware of the attack.

What Should You Do?

If your company sponsors an ERISA-governed health plan, you should strongly consider adopting the DOL's Cybersecurity Program Best Practicesto help mitigate cybersecurity risks and withstand any DOL scrutiny in the event of an attack. Since the DOL initially developed this guidance with retirement plans in mind, you may need to make adjustments to fit the specific needs of your health plan.

Work with your counsel to ensure that you satisfy any fiduciary duties that you (as the plan sponsor), your employees, or third-party service providers might have. Keep in mind that you could have additional cybersecurity obligations, including under HIPAA and other federal, state, or local laws.

Conclusion

If you have questions about group health plan compliance in light of the recent health industry cybersecurity attacks, feel free to reach out to your Fisher Phillips attorney, the author of this Insight, or any attorney in our Employee Benefits and Tax Practice Group or Privacy and Cyber Practice Group. We will continue to provide tips, guidance, and updates on employee benefits and other workplace law topics, so make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information directly to your inbox.

Related People

Jennifer S. Kiesewetter
Of Counsel
615.488.2905
Email

Service Focus

Employee Benefits and Tax

Privacy and Cyber