ECKERT SEAMANS
ATTORNEYS AT LAW

September 2024

Employee Benefits Update

DOL Expands Cybersecurity Guidance to Cover Health & Welfare Plans

By Lawrence Finnell and Samantha Walter

DOL Expands Cybersecurity Guidance to Cover Health & Welfare Plans[1]

On September 6, 2024, the US Department of Labor ("DOL") issued Compliance Assistance Release No. 2024-01 ("Announcement"), confirming that its cybersecurity guidance directed at retirement plans shall generally apply to all employee benefit plans – including health and welfare plans. In 2021, the DOL published guidance concerning best practices for plan sponsors, fiduciaries, record-keepers, participants, and beneficiaries pertaining to cybersecurity for retirements plans. Now directed at both retirement and health and welfare plans, the DOL's guidance focuses on three specific topics: hiring service providers, managing cybersecurity risks, and online security tips for participants to avoid risk of fraud and loss. The DOL also updated its prior guidance by endorsing the Department of Health and Human Services' ("HHS") publications for managing cyber threats and protecting patient information, as well as best practices for small, medium, and large healthcare organizations.

This Announcement sends a clear message that cybersecurity and the protection of plan data, personal information, and plan assets should be a key priority for plan fiduciaries, sponsors, and service providers, as well as participants and beneficiaries.

To follow, please find a summary of some of the key points raised in this Announcement, as well as some helpful insights to be considered in connection with the DOL's recommendations.

Tips for Hiring a Service Provider[2]

Under ERISA, plan fiduciaries must act prudently when selecting and retaining plan service providers. Since plan service providers are often relied upon to preserve and secure plan records and participant data, it is essential that fiduciaries ensure that service providers implement strong measures to defend this information against potential cyber threats. In light of the large volumes of plan records and participant data held by plan service providers, the DOL recommends that plan sponsors make certain that vendors have sufficient security systems in place to guard against attacks and prevent potential breaches. In its Announcement, the DOL offered suggested practices when contracting with service providers, including the following:

- Review the service provider's security standards, practices, policies, and the results of audits of security systems and compare this information with industry standards. Plan fiduciaries should look for vendors who follow a recognized information security standard that validates its compliance and utilize an independent auditor to verify information security, system/data availability, processing integrity and data confidentiality.

[1] https://www.dol.gov/agencies/ebsa/key-topics/retirement-benefits/cybersecurity/compliance-assistance-release-2024-01
[2] https://www.dol.gov/agencies/ebsa/key-topics/retirement-benefits/cybersecurity/tips-for-hiring-a-service-provider-with-strong-security-practices

- Verify that the service provider follows recognized information security standards and inquire as to how they validate those their cybersecurity practices and security standards. Ensure their audit results reflect compliance with those standards and are available for review.
- Evaluate the service provider's track record in the industry, including any public information regarding prior security incidents, litigation, and legal proceedings related to their services.
- Ask about any prior security breaches, including the cause of such breaches and the service provider's responses.
- Review the service provider's insurance policies to determine whether they would cover losses for cybersecurity and identity theft breaches. Evaluate whether their coverage would cover breaches caused by their own workforce, as well as external attacks.
- Ensure that contracts require service providers to continue to maintain their cybersecurity and information security standards originally agreed to by the parties. Consider requiring notice in the event of a deviation from these standards or a change in their systems which impacts their ability to meet these standards. Beware of contract provisions that limit the service provider's responsibility for IT security breaches.
- Include terms in the contract that would enhance cybersecurity protection for the plan and its participants, such as provisions that would:
    - Require annual third-party audits to determine compliance with information security policies and procedures and require access to the results of those reviews.
    - Specifically identify the service provider's obligation to preserve confidential information, prevent its use or disclosure without written permission, and protect against unauthorized access, loss, disclosure, modification, or misuse.
    - Require notification of cyber incidents or data breaches within a certain amount of time and ensure that the service provider will cooperate in investigating and addressing the cause of an incident or breach.
    - Specify their obligations to comply with all applicable federal, state, and local laws, rules, regulations, directives, and other governmental requirements pertaining to the privacy, confidentiality, or security of participants' personal information.
- Consider insisting on insurance coverage such as professional liability and errors and omissions liability insurance, cyber liability, and privacy breach insurance, and/or fidelity bond/blanket crime coverage, and ensure that the policy covers the plan against any cybersecurity breaches and incidents before depending on it to protect against losses.

Cybersecurity Program Best Practices[3]

Like retirement plans, health and welfare plans house a treasure trove of dollars and data, making them attractive targets for cyberattacks. Identifying that plan fiduciaries have an obligation to properly mitigate cybersecurity risks, the DOL prepared best practices for use by recordkeepers and other plan service providers responsible for defending data and assets against such attacks and for plan fiduciaries responsible for prudently selecting those vendors. In its Announcement, the DOL offered certain best practices, which include the following:

[3] https://www.dol.gov/agencies/ebsa/key-topics/retirement-benefits/cybersecurity/best-practices

- Having a formal, well documented cybersecurity program.
- Conducting prudent annual risk assessments.
- Having a reliable annual third-party audit of security controls.
- Clearly defining and assigning information security roles and responsibilities.
- Having strong access control procedures.
- Ensuring that any assets or data stored in a cloud or managed by a third-party service provider are subject to appropriate security reviews and independent security assessments.
- Conducting periodic cybersecurity awareness training.
- Implementing and managing a secure system development life cycle program.
- Having an effective business resiliency program addressing business continuity, disaster recovery, and incident response.
- Encrypting sensitive data, both stored and in transit.
- Implementing strong technical controls in accordance with best security practices.
- Appropriately responding to any past cybersecurity incidents.

Online Security Tips[4]

The Announcement offered certain basic rules to reduce the risk plan data and asset loss and prevent fraud, including the following:

- Take ownership by registering, setting up, and routinely monitoring your online plan account, allowing account holders to protect and manage their investments. Regularly check accounts to reduce the risk of fraudulent access.
- Use strong and unique passwords, securely keep track of passwords, and change them annually or when there is a security breach.
- Use multi-factor authentication.
- Keep personal contact information current.
- Close or delete unused accounts and sign up for account activity notifications.
- Use only secure Wi-Fi and beware of free Wi-Fi networks.
- Beware of phishing attacks.
- Use antivirus software and keep apps and software current.
- Know how to report identity theft and cybersecurity incidents. The U.S. government has published valuable information on how to report cyber incidents.

[4] https://www.dol.gov/agencies/ebsa/key-topics/retirement-benefits/cybersecurity/online-security-tips

HHS Guidance for Managing Threats and Protecting Patients[5]

As mentioned above, the DOL endorsed various publications by HHS, which may help health plans and service providers maintain good cybersecurity practices. The HHS notes that organizations must be proactive, rather than reactive, and constantly prepare to defend against a future cyber-attack. Cybersecurity strategies should be constantly adapting to the current threat landscape and an organization's own structure.

This HHS guidance discusses the top five threats facing the health industry and offers ten best practices to combat those threats. The guidance is broken into two volumes – one for small healthcare organizations[6] and a second for medium and large healthcare organizations[7].

The HHS names the following as the top five threats facing the health industry:

1. **Social Engineering**. Social engineering is an attempt to trick you into giving out personal information or infecting your device by clicking on a link to give hackers access to patient data (i.e., phishing). These attacks can come in the form of an e-mail, text message, or other communication, posing to be from a colleague or familiar contact in an effort to gain access to your computer system.
2. **Ransomware**. Ransomware is a type of malware (malicious software) distinct from other malware; its defining characteristic is that it attempts to deny access to a user's data, usually by encrypting the data with a key known only to the attacker who deployed the malware, until a ransom is paid. After the user's data is encrypted, the ransomware directs the user to pay the ransom to the attacker (usually in a cryptocurrency, such as Bitcoin) in order to receive a decryption key.
3. **Lost or Theft of Equipment or Data.** Your devices, such as laptops, phones, and USB/thumb drives hold sensitive data and, if lost or stolen, can end up in the hands of hackers, resulting in unauthorized or illegal access, dissemination, and use of such sensitive data.
4. **Insider, Accidental, or Malicious Data Loss.** All organizations potentially face insider threats, where their employees, contractors, or other users have access to their technology infrastructure, network, or databases. Accidental insider threats are not malicious and can be caused by honest mistakes, such as being tricked, procedural errors, or a degree of negligence. Malicious insider threats pertain to those situations where employees, contractors, other users act with the objective of personal gain, extortion, or inflicting harm to the organization or another individual.
5. **Attacks Against Networks Connected to Medical Devices.** Attackers may target attacks on network connected devices, gaining access to computer networks and taking command of medical devices, putting patients at risk.

To combat the above threats, HHS recommends ten mitigating practices:

1. **Email Protection Systems.** E-mail systems should be the focus for additional security controls. These security controls should address the two most common phishing methods, which both occur by email access: credential theft and malware dropper attacks.
2. **Endpoint Protection Systems.** Access to endpoints, including desktops, laptops, mobile devices, and other network connected hardware devices, should be controlled, and endpoints should be protected from viruses and other risks.

[5] https://405d.hhs.gov/Documents/HICP-Main-508.pdf
[6] https://405d.hhs.gov/Documents/tech-vol1-508.pdf
[7] https://405d.hhs.gov/Documents/tech-vol2-508.pdf

3. **Identity and Access Management.** All users of data, applications, systems, and endpoints should be clearly identified, and their access should be monitored. Identity and access security controls, such as multi-factor authentication or condition-based access, can be used to control access to infrastructure and enable proper change control management.
4. **Data Protection and Loss Prevention.** A data security breach is the compromise, loss, or disclosure of sensitive data, including information relevant to your organization's business and protected health information. Data should be protected from being corrupted, lost, or stolen. Implementing data protection and loss prevention practices and educating employees on them is essential.
5. **IT Asset Management ("ITAM").** Effective ITAM, including by keeping an accurate inventory of all IT assets and securely storing them, is critical to ensuring that your cybersecurity controls are implemented and maintained across all assets.
6. **Network Management.** Networks much be securely established to limit communication between resources. Implementing network segmentation and network access controls can help limit exposure to cyber attacks.
7. **Vulnerability Management.** Organizations should implement proper vulnerability management practices to identify technology flaws and other vulnerabilities that cyber attackers could exploit. This process uses a scanning capability to proactively scan devices and systems in your organization.
8. **Security Operations Center & Incident Response.** Incident response programs, often referred to as "blocking and tackling," help organizations identify and mitigate security incidents, such as the installation and detection of malware and social engineering attacks that include malicious payloads (via attachments and links).
9. **Network Connected Medical Device Security.** Organizations should extend their cybersecurity practices to medical devices connected to a network or computer to process required updates. Organizations are encouraged to extend and implement the other cybersecurity practices mentioned above to medical devices.
10. **Cybersecurity Oversight and Governance.** Establishing and implementing cybersecurity policies, procedures, and processes is one of the most effective ways to prevent cyber attacks. Your employees, contractors, and vendors should know which data, applications, systems, and devices they are authorized to access and use, as well as the risks associated with going outside their authorization.

HHS's guidance varies by the size of the healthcare organization. For example, HHS encourages small organizations to do the following to implement effective e-mail protection systems:

- Install basic e-mail protection controls such as standard antispam and antivirus filtering controls, which should be implemented in any e-mail system.
- Acquire Multifactor Authentication for remote e-mail access, which is the process of verifying a user's identity using more than one credential, thus adding an extra layer of defense against e-mail attacks.
- Implement education and awareness activities, such as trainings, phishing simulations, and awareness campaigns, to assist employees and partners in protecting your organization against phishing attacks.

The HHS encourages medium and large healthcare organizations to follow the above tips for small healthcare organizations, as well as several more practices:

- Institute basic email controls including real-time "black hole" lists (i.e., IP addresses or domains that are known to be used for sending spam), distributed checksum clearinghouses (i.e., an anti-spam content filter used to detect and reject or filter spam or unsolicited bulk e-mail), and spam/virus checks on outbound messages.

- Utilize advanced and next generation tooling to combat phishing and malware. These tools use threat analytics and real-time response capabilities to provide protection against phishing attacks and malware.
- Perform analytical education by reviewing who in your organization is being targeted most and create cyber security education specifically for that group.

* * * * * * *

Given the massive amount of sensitive data held by employee benefit plans (i.e., social security numbers, dates of birth, banking information, and health information), plan fiduciaries must take cybersecurity seriously. Since issuance of its retirement plan guidance, the DOL has prioritized reviewing plan cybersecurity measures in its enforcement efforts. With the expansion of this guidance into the health and welfare plan space, it is clear that the DOL's focus on cybersecurity is here to stay!

Since the issuance of its cybersecurity best practices for retirement plans, we have seen the DOL pay increased attention to information and data security, privacy, and defenses against attacks during plan audits and investigations. We anticipate the DOL will similarly expand the scope of its review of health and welfare plans to address plan cybersecurity considerations.

Plan fiduciaries should consider the DOL's tips and insights when hiring new service providers and require compliance with the DOL cybersecurity guidance. Plans should also ensure that current contracts include cyber insurance that will cover losses in the event of a breach, as well as indemnification provisions to protect plans against liability. Once confirmed, plans should ensure continued compliance with these standards through periodical review of their vendors' contracts and operation – reviewing third-party audit results are satisfactory.

Plans should also ensure their own internal practices comply with the standards set forth in the Announcement, including offering regular cybersecurity training to its employees and staff, as well as maintain internal compliant cybersecurity policies and programs.

ECKERT SEAMANS ATTORNEYS AT LAW

This Employee Benefits Alert is intended to keep readers current on developments in the law. It is not intended to be legal advice. If you have any questions, please contact Lawrence Finnell at 609.989.5015 or lfinnell@eckertseamans.com, Samantha Walter at 412.566.1920 or swalter@eckertseamans.com, or any other attorney at Eckert Seamans with whom you have been working.