THE ERISA INDUSTRY COMMITTEE
Shaping benefit policies before they shape you.

JAMES GELFAND
President

Understanding Health Plans and Cybersecurity Activities

Testimony Before the Department of Labor
Employee Benefits Security Administration
ERISA Advisory Council on Employee Welfare and Pension Benefit Plans

Washington, DC

July 20, 2022

Introduction and About ERIC

Thank you for this opportunity to testify before The ERISA Advisory Council on group health plans and cybersecurity. I'm James Gelfand, President of The ERISA Industry Committee – ERIC for short. ERIC is a national nonprofit organization exclusively representing the largest employers in the United States in their capacity as sponsors of employee benefit plans for their nationwide workforces. With member companies that are leaders in every economic sector, ERIC is the voice of large employer plan sponsors on federal, state, and local public policies impacting their ability to sponsor benefit plans, and to lawfully operate under ERISA's protection from a patchwork of different and conflicting state and local laws, in addition to federal law.

Americans engage with an ERIC member company many times a day, such as when they drive a car or fill it with gas, use a cell phone or a computer, watch TV, dine out or at home, enjoy a beverage or snack, use cosmetics, fly on an airplane, visit a bank or hotel, benefit from our national defense, receive or send a package, or go shopping.

ERIC member companies provide comprehensive health care and retirement benefits to millions of active and retired workers and their families across the country. Our members offer these great benefits to attract and retain employees, be competitive for human capital, improve health – physical, mental, and financial health – and provide peace of mind.

On average, ERIC large employer members pay around 85 percent of health care costs on behalf of their beneficiaries – that would be a gold or platinum plan if bought on an Exchange. These plans are self-insured, meaning that ultimately it is the company that is on the hook for the vast majority of the costs of our patients' care. Self-insured employers abiding by the Employee Retirement Income Security Act of 1974 (ERISA) act as fiduciaries, ensuring that plan dollars are well spent, vendors are well managed, and patient data is protected, among many other responsibilities. Prior to COVID-19, there were an estimated 181 million Americans who got health care through their job, with about 110 million of them in self-insured plans like ours.

Employers like ERIC member companies roll up their sleeves to improve how health care is delivered in communities across the country. They do this by developing value-driven plan designs and coordinated care programs, implementing employee wellness programs, providing transparency tools, and adopting a myriad of other innovations that improve quality and value, while making health care more affordable for patients. Health plans, including self-insured plans, abide by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to protect sensitive patient health information.

It is our understanding that health data is the most valuable information that the most hackers are after, compared to other data sold on the dark web. For example, if hackers gain an individual's protected health information (PHI), it is a valuable commodity that can be used to enable improper access to other data, and potentially aid in accessing a beneficiary's financial information, eventually allowing hackers to access an individual's Social Security, retirement, and bank accounts. You can see why PHI is so valuable – it relates to past, present, or future physical or mental health conditions, payments for the provision of health care, demographic and financial information, and it can all be accessed virtually. This information is maintained by the group health plan and their vendors, and it identifies the individual directly.

Self-insured employers take an active role in contracting with major health plan carriers and are increasingly active in ensuring that their workers' health information is protected. That is why today ERIC recommends that the Council include in its final report to The Department of Labor (DOL) that the DOL should:

(1) Coordinate with the Department of Health and Human Services, including the Office for Civil Rights, as well as other relevant agencies – such as the IRS, the Equal Employment Opportunity Commission, and others – to harmonize rules that may be overlapping or conflicting;

(2) Ensure that the health care industry can adopt cyber security practices in real-time, evolving as standards and best practices arise and improve, rather than setting an overly-prescriptive government standard; and

(3) Rather than issue new cybersecurity guidance or standards, DOL should clarify whether the 2021 sub-regulatory cybersecurity guidance applies to all group health plans, and continue to provide useful information to plan sponsors looking for best practices.

ERIC commends the Council for holding today's hearing to explore this topic, and in addition to the recommendations above, we will also discuss:

(1) The current laws in place governing health data, and employer efforts to abide by those laws;

(2) The current activities by cyber thieves attempting to penetrate group health plans and our carriers in order to gain PHI and personal identifiable information (PII); and

(3) The current activities plan sponsors have charged insurers with carrying out, to protect plan beneficiaries from these cyberattacks.

With that, let's first turn to the current regulatory landscape for group health plans on cyber security.

Health Plans and Cyber Security Laws

The DOL has a longstanding interest in cybersecurity issues specifically for retirement plans. It made retirement plan cybersecurity a subject of ERISA Advisory Council reports in 2011, 2015, and 2016. Starting a few years ago, it began to include questions about cybersecurity policies, attacks, and responses in audit requests for retirement plan documents. Through the years, however, the DOL had not provided formal guidance for plans sponsors and fiduciaries on the question of whether they were responsible for taking action with regard to their plans' cybersecurity risks.

At the request of Congress, in February 2021, the Government Accountability Office (GAO) issued a report on cybersecurity risks in defined contribution plans. The GAO recommended that the DOL formally state whether it is a fiduciary's responsibility to mitigate cybersecurity risks in 401(k) plans and other retirement plans. The GAO also recommended the DOL publish minimum expectations for addressing such risks.

A few months later on April 14, 2021, the DOL issued three pieces of sub-regulatory guidance addressing the cybersecurity practices of plan sponsors, their service providers, and plan participants, respectively. This guidance provides insight into DOL's expectations for a "prudent" plan fiduciary's cybersecurity practices. For example, each of the three pieces of guidance addresses a different audience: service providers, recordkeepers, and plan participants. While the DOL characterizes the guidance for fiduciaries and service providers as "tips" and "best practices", the documents use strong language and provide thorough steps a plan sponsor should take, including significant processes that should be in place to vet vendors and performance.

No matter the policy or issue area in question, ERIC is always concerned about agency "best practices," sub-regulatory guidance, or other publications created without notice and comment, becoming unofficial requirements. Although the guidance does not specify any minimum requirements for the plan sponsors and fiduciaries to follow, it advises them of best practices, and leaves it to the plan sponsor to decide which steps to take and procedures to apply in accordance with the facts and circumstances of their plans. The guidance also leaves many open questions. For example, how should plan fiduciaries and service providers address existing arrangements that do not comport with the guidance? Does the DOL believe that ERISA preempts state data privacy laws as they relate to ERISA benefit plans? Does the DOL expect fiduciaries to communicate the Online Security Tips to participants and beneficiaries, and, if so, how often?

DOL is currently auditing cybersecurity programs of ERISA plan sponsors and fiduciaries relating to retirement plans. DOL has issued information and documentation requests to ERISA plan sponsors and fiduciaries that are extremely detailed, requesting the production of all documentation relating to cybersecurity or information security programs relating to the data of employer's ERISA-governed retirement plan, including security programs maintained by each service provider to the plan, as well as cybersecurity training and report of incidents of past breaches. Specific document requests include all policies, procedures, guidelines, and communications such as:

- *Implementation of access controls and identity management, including any use of multi-factor authentication;*

- *Processes for business continuity, disaster recovery, and incident response;*

  Management of vendors and third-party service providers, including notification protocols for cybersecurity events and the use of data for any purpose other than the direct performance of their duties;

- *Cybersecurity awareness training;*

- *Encryption to protect all sensitive information transmitted, stored, or in transit;*

- *Past cybersecurity incidents;*

- *Security reviews and independent security assessments of the assets or data of the retirement plan stored in a cloud or managed by service providers;*

- *Security technical controls, including firewalls, antivirus software, and data backup;*

- *All cybersecurity capabilities and procedures;*

- *Policies and procedures of service providers for collecting, storing, archiving, deleting, anonymizing, warehousing, and sharing data; and*

- *Permitted uses of data by the sponsor of the plan or by any service providers of the plan, including, but not limited to, all uses of data for the direct or indirect purpose of cross-selling or marketing products and services.*

It is our understanding that plan sponsors are eager to meet DOL's expectations, and to avoid unnecessary audits or reprimands. As such, they think carefully about their current cybersecurity practices, contracts with service providers, and how best to improve their protocols.

As you can see, DOL has had a significant focus on cybersecurity in retirement plans in recent years. This has led many plan sponsors and outside experts to conclude that the DOL's 2021 guidance was meant to apply exclusively to retirement plans. In fact, ERIC conducted a canvass of experts, which showed significant confusion about this guidance, particularly whether the guidance is meant to focus only on retirement plans, or also on group health plans. While ERIC does not take a position on this, we do believe that many plan sponsors, as well as their consultants and lawyers, are currently under the impression that this guidance does not apply to group health plans.

Even without the DOL guidance, there are multiple frameworks and standards that health plan sponsors and ERISA fiduciaries already comply with and use to protect sensitive plan and participant data. This includes HIPAA, which is by far the strongest federal law protecting patients' health information, but also ERISA, the Genetic Information Nondiscrimination Act of 2008 (GINA), and the Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009. HITECH strengthened HIPAA in a number of ways, including ensuring that health care organizations and business associates were implementing HIPAA and its safeguards correctly to keep health information private and confidential during the transition of paper records to electronic medical records.

HITECH re-enforced HIPAA during this change while implementing a robust new requirement for covered entities and business associates to report data breaches. HITECH gave the HHS Office of Civil Rights more power to enforce the law against non-compliant organizations that do not protect patient data appropriately. While the Office of the National Coordinator for Health Information Technology (ONCHIT) primarily governs HITECH, the Office continues to produce various guidance and rules to promote a nationwide, standards-based health information exchange while protecting patient data. HIPAA and HITECH are bonded, and require group health plans to take active measures to protect the privacy and security of PHI. The Department of Health and Human Services (HHS) published myriad regulations under both laws. Of particular note here, plan sponsors are keenly aware of two of these HIPAA rules that were updated when HITECH became law:

First, the privacy rule, also known as the *Standards for Privacy of Individually Identifiable Health Information,* enforced by the HHS Office for Civil Rights. The 2002 rule sets national standards to limit how PHI is used and disclosed, and to provide individuals with certain rights related to their PHI. It ensures that individuals' health information is properly protected by covered entities while allowing the flow of health information needed to provide and promote high-quality health care. It specifically outlines that a covered entity may use or disclose PHI to individuals or their personal representatives when they request access, or directly to HHS when it is conducting a compliance investigation, review, or enforcement action. The rule does discuss when covered entities are permitted to use and disclose PHI without a patient's authorization. This includes:

- Disclosing information directly to the individual;
- Information related to treatment, payment, and health care operations;
- Informal permission by the individual with the opportunity to agree or disagree within the setting;
- Incidents that require disclosure;
- Public interest and benefit activities such as workers' compensation; and
- Research and public health purposes.

Because the health care market is complex, the rule was designed to be flexible and comprehensive to cover the variety of uses and disclosures that need to be addressed.

Second, the security rule, also known as the *Security Standards for the Protection of Electronic Protected Health Information,* which is also enforced by the HHS Office for Civil Rights, defines administrative, physical, and technical safeguards necessary to protect confidentiality, integrity, and availability of electronic PHI. The 2003 rule establishes national security standards for technical and non-technical safeguards for covered entities. Prior to HIPAA, there were no generally accepted security standards or general requirements for protecting PHI, so the rule ensured that covered entities would include administrative safeguards such as:

- Established security management processes;

- Expert security personnel;
- Workforce training and and management;
- Appropriate information access protocols, and
- Continuous evaluation to ensure PHI was strongly protected.

The rule also includes physical safeguards, such as facility access and control, and technical safeguards like audits of technology hardware and software, and data transmission security. Because the rule held national standards to ensure covered entities implemented uniform standards, the rule outlined preemption of state laws that may be contrary to HIPAA regulations.

ERIC is aware that group health plans are under DOL jurisdiction, but based on our conversations with plan sponsors, carriers, and expert advisors to both, the rules published by the Office of Civil Rights at HHS, as well as other government agencies that do not generally directly regulate group health plan sponsors, are followed regardless. Because of this, DOL cybersecurity guidance could be an added layer of compliance beyond HIPAA and the HITECH requirements, unless it is carefully crafted to align with all other existing rules.

Additionally, the Federal Trade Commission (FTC), as well as the Equal Employment Opportunity Commission (EEOC), have their own regulations on employee privacy rights. These rules can often complicate compliance with HIPAA and ERISA, requiring third parties to handle the data, and introducing other elements and standards. And of course the IRS has their own rules covering specific pieces of PII, such as Social Security numbers, which must also be followed.

Also, states have their own cybersecurity laws with enforcement by state attorney generals. It is our understanding that often these laws are not consistent across states, and create extreme challenges particularly for carriers, who often work across just as many states as ERIC's multi-state member companies.

Despite all of these many different rules, ERIC member companies routinely go above and beyond what may be required. Many plan sponsors voluntarily comply with the National Institute of Standards and Technology (NIST) guidelines. While NIST's cybersecurity framework is specifically recommended as security controls for information systems at the federal agencies, plan sponsors and a number of major carriers have found that these guidelines provide an enhanced level of security and protection, and therefore choose to voluntarily implement them. NIST compliance not only helps to ensure an organization's infrastructure is secure, but lays a strong foundation upon which companies can build as they implement protocols to comply with regulations such as HIPAA and HITECH. While plan sponsors do have discretion to design their own security regimen, and to implement best practices as they see fit in complying with federal rules and regulations, better coordination is needed between the agencies to confirm rules are cohesive. And care should be taken not to disincentivize plan sponsors from continuing to voluntarily comply with enhanced security standards like those of NIST.

Therefore, ERIC urges the Council to include in its recommendations that DOL coordinate with all relevant agencies, including HHS' Office for Civil Rights, the IRS, EEOC, FTC, ONCHIT, and others, to ensure that guidance harmonizes all existing federal rules that already apply to group health plan sponsors. It is our belief that ERIC member companies, and all group health plan sponsors, are eager to protect their beneficiaries – but they need one set of clear, consistent, workable rules.

Cyber Thieves, Hackers, and Bots: Concerning Activities

The health care industry is a prime target for attackers to monetize PHI. Hackers usually gain access to restricted information through ransomware, credential harvesting, keylogging, phishing, and many other tactics. These common hacking techniques are often used to either sell PHI on the dark web, or to hold an entity ransom until payments are made. Major cybersecurity breaches related to health plans have increasingly occurred since 2018, with the most recent being in 2021 and impacting nearly 45 million individuals.[1] However, health plans are not the only ones under attack. Hospitals and health care providers[2] have also been victimized and even individuals working from home[3].

No matter the information, whether it be PHI or PII, hackers have ways of monetizing it. And even as employers put into practice new safety measures, hackers are constantly creating new methods and strategies to get the information that they need.

It is worth mentioning that direct breaches of group health plans, or fully insured carriers, are uncommon. Plan sponsors have strong security features in place, and a July 2022 poll of ERIC member companies found that password-protected messages, mandatory account password updates, firewall protections, and secure portals are uniformly used cybersecurity measures group health plans have in place. While no system will ever be fully "hacker proof," employer plan sponsors feel that they are keeping up with best practices, and have security measures in place that would rival other systems with comparably sensitive information.

Far more often than directly accessing a group health plan's back-end systems, hackers gain access by posing as beneficiaries, and either guessing or illegitimately obtaining the user's credentials. Plan sponsors continue to work to improve verification efforts, but ultimately it is deeply challenging for an employer to protect an individual's PHI and PII, if that individual chooses an easily-guessed password, or writes their credentials on a piece of paper and leaves it in a public place.

[1] Critical Insight. Healthcare Breach Report. July-December 2021. https://cybersecurity.criticalinsight.com/2021_H2_HealthcareDataBreachReport
[2] U.S. Department of Health and Human Services Office for Civil Rights. Breach Portal https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
[3] Interpol. Report Show Alarming Rate of Cyberattacks during COVID-19. https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

ERIC recommends that DOL rely on the health care and technology industries to continue to evolve and update best practices in real time, rather than setting an overly-prescriptive government standard. Government-recommended practices are not just a guide for employers and plans, but for hackers too. Having a set standard will give hackers the upper hand in knowing what strategy to take in getting their desired result. It is ERIC's understanding that while security standards and best practices are constantly evolving, so too are the tactics and strategies used by hackers – which necessitates a nimble approach that is neutral as to the exact tactics used, but instead focuses on having a robust process and keeping up with new developments, exactly as current HIPAA rules do.

Carrier Actions and Common Employer Contract Provisions

Depending on the size of the employer, it may not have internal staff who are experts on group health plan cybersecurity practices or requirements. This leads plan fiduciaries to engage with third-party cybersecurity vendors to evaluate the plan's vendor's cybersecurity practices. Plan fiduciaries and their third-party cybersecurity vendors may benefit from working hand in hand with the plan sponsor's IT professionals to develop a uniform response to cybersecurity threats. About 71 percent of ERIC member companies delegate cybersecurity for their group health plans (for active employees and dependents, as well as for retirees) to carriers and third-party administrators, but are actively engaged in monitoring and testing the security measures.

Often, in practice this means that a group health plan's cybersecurity practices will be a combination of both the company's more general IT security policies, as well as added layers of security provided by (primarily) a health insurance carrier. In discussions with carriers and consultants, ERIC heard a number of common practices that seem to be the most commonly used at this time. Additionally, ERIC learned that cybersecurity is now a common factor in contract negotiations between plan sponsors and carriers, and that often times these back-and-forths are headed off by common language used in carrier contracts, which address some of the most pressing cybersecurity concerns that employers have.

Common examples of security measures that carriers have adopted to improve cybersecurity include, but are not limited to:

- Multifactor identification, requiring more than a single set of credentials to log in to secure systems;
- Account password updates and strength requirements, which lead to more complex and harder to hack passwords, that turn over more often so as to diminish the risks of a potentially compromised credential;
- Secure portals that require credentials before viewing any potentially confidential information, which avoid the risk of PHI or PII being viewed improperly in, for instance, an email or text message;
- Password-protected messages that require additional credentials even after a user has clicked through an alert and potentially logged into a system; and

- Zero-trust protocols, in which a user (either a beneficiary, plan sponsor staff, or carrier staff) is required to authenticate credentials every time they use a system, with no saved or remembered credential shortcuts.

Common provisions that carriers agree to in their contracts with plan sponsors include, but are not limited to:

- Define key terms related to information security so there is no confusion about the representations made by the vendor;
- The description of a product or service to be delivered by the vendor, including the aspects of this product where security protocols will be applied;
- Representations and warranties in which the vendor agrees to protect the plan sponsor and beneficiaries, as part of the services being provided;
- Confidentiality for beneficiaries;
- Detailed descriptions of what is included in a security program;
- Monitoring or assessment of vendor performance, often including the right to audit or test the security of the vendor's products and services, or to view regular reports from trusted third parties who conduct penetration testing and other security auditing;
- Remedies in the case of failure to form, or in the case of a significant breach;
- The right to terminate the contract if security problems arise or persist;
- Coordination related to the plan sponsor's cybersecurity insurance (more on this below);
- Indemnification of the plan sponsor in the case of a significant security breach;
- Guarantees to provide services that will enable business continuity in the case of down or compromised systems;
- Notices related to compliance with the myriad cybersecurity laws and rules that apply in various situations; and
- Specifications on the software, hardware, or other products and services that the plan sponsor wants the carrier to use in carrying out the mutually agreed-to cybersecurity protocols.

Already you can see that demand for stronger security from plan sponsors has led carriers to vastly increase their cybersecurity measures. And while technology continues to advance, contracts will be improved and likely strengthened in areas such as risk assessments, third-party audits, and unique language in meeting a plan sponsor's request.

Risk assessments usually identify functions, activities, products, and services and their relative importance to the organization. Employers are also advised to evaluate the inherent cybersecurity risk presented by the people, processes, technology, and data that support the identified function, activity, product, or service and assess the existence and effectiveness of controls to protect against the identified risk. Risk assessments are important as they can provide the basis for the selection of appropriate controls and the development of remediation plans so that risks and vulnerabilities are reduced to a reasonable and appropriate level. Obviously, there will always be some risk, but regular review of where the vulnerabilities are, is a critical aspect of minimizing and controlling that risk.

Third-party audits are usually done on internal controls, reporting, contract performance, security, technical features, and more. Security audits may occur periodically, or they might be event-driven. Audit provisions may provide that the results of third-party audits be made available to the plan sponsor upon request, or according to an agreed upon schedule, together with evidence of remediation of risks identified, and explanation of any risks accepted. From a plan sponsor perspective, this is exactly what employers want – not only to verify that a carrier is testing their own cybersecurity, preferably with the help of outside entities, but also to learn about the steps the carrier is taking to address any vulnerabilities that are discovered.

Employers commonly will make unique and specific requests about the cybersecurity practices of a carrier, and it is ERIC's understanding that these requests are usually agreed to and codified within the carrier contract, at least depending on the size of the client. ERIC's member companies are all very large employers with many employees and many more covered lives in their group health plans, so it is usually worth it for a vendor to make changes necessary to get and keep contracts with these plan sponsors. One of the most common requests that one carrier described to ERIC has to do with penetration testing. The carrier reported that they (and presumably other major carriers) usually came to an agreement on these requests to run penetration testing more than once a year. This is a good example of standards evolving and improving due to pressure from plan sponsors. Previously. It was common for penetration tests to be run annually by the carrier and their own third-party contractors, rather than tests taking place throughout the year, and being carried out at times by agents of the client, not the carrier.

The Council should note that the very existence of these commonly requested contractual provisions to beef up carrier cybersecurity, show that plan sponsors are being proactive in protecting beneficiary health information, and are willing to work with their vendors in contract negotiations. However, it is important to note that not all vendors may be meeting every plan sponsor's requests, including requests to align with DOL's 2021 guidance on established practices. This is likely because there is still confusion about whether the guidance applies to health plans. A clarification in this regard would therefore be likely to improve plan sponsors' and carriers' adherence to the best cybersecurity practices.

And a note on cybersecurity insurance: Most large employers obtain, at great cost, some degree of cybersecurity insurance, which is not specific to their employee benefits plans. This is an enterprise-wide insurance product, that covers the employer in innumerable different ways and instances. The vendors of these cybersecurity insurance products are themselves at great risk, and as such, they make significant demands upon the plan sponsors. In order to be fully protected by the cybersecurity insurance, or even to obtain the policy, the plan sponsor will have to certify compliance with many best practices and standards far beyond the "minimums" that might be suggested in various government rules and guidance.

While we know this is not the focus of the Council's inquiry today, it is important to take this into account, because it is evidence that the private sector is indeed addressing this issue in a constructive manner.

As such, while the 2021 guidance does not specifically mention group health plans, we urge the Council to recommend that DOL clarify whether the guidance applies to group health plans through a set of "frequently asked questions" or a "field assistance bulletin." As DOL endeavors to align their own guidance with the myriad other privacy and cybersecurity rules that govern group health plans, this clarification would provide certainty to plan sponsors, as well as to the carriers and other vendors, and to the consultants and other advisors, who are critical in designing and carrying out benefits.

Conclusion

In conclusion, employers are acutely aware of the ever-changing landscape of cybersecurity, and we are committed to protecting employees' protected health information, and their personally identifiable information. We are dedicated to helping improve this dynamic for patients, and believe that employers are an integral part of the solution.

Thank you for this opportunity to share our views with the Council. The ERISA Industry Committee and our member companies look forward to working with you to meaningfully improve health plan cybersecurity for our employees, their families, and retirees. We are confident that this can be done without burdensome new mandates and penalty regimes, by leveraging a quickly-evolving and innovative tech sector, and aligning and clarifying existing rules and regulations. I am happy to take any questions, and appreciate your inclusion of plan sponsors' voices in this conversation.