Testimony Before the ERISA Advisory Council on Health Plan Cybersecurity Issues

Carol Buckmann, Partner, Cohen & Buckmann p.c. September 9, 2022

Thank you for the opportunity to discuss special challenges small and medium size businesses face in developing appropriate cybersecurity practices and ways in which the Department of Labor (DOL) could assist them in better protecting health plan data. This is particularly important because data maintained in connection with health plans may provide a gateway for cybercriminals to steal retirement benefits and other assets, and any health plan security breach may have far-reaching consequences.

Executive Summary.

The Employee Benefits Security Administration (EBSA) is to be commended for issuing guidance in April of 2021 setting out tips and best practices for maintaining cybersecurity for ERISA plans. However, small and medium size plan sponsors face special challenges in developing appropriate cybersecurity protections that are not typically faced by large employers. They are much more likely to outsource their own cybersecurity needs to third parties and less likely to have internal IT departments. They are less likely to know how to obtain or to afford regular systems audits. Almost all of these plans are already subject to HIPAA's Security Rule (at 45 CFR Part 160 and Subparts A and C of Part 164), which establishes national standards for protecting personal health information held or transferred in electronic form (ePHI), and have taken steps to comply. The Security Rule does not prescribe specific actions that all covered entities must take to comply, but rather allows the flexibility to tailor a security program to reflect the size and organization and risks of a specific entity. Any further guidance from EBSA beyond its package of recommended practices issued in 2021 should similarly permit flexibility in compliance, but should clearly state in binding authority such as a regulation that plan fiduciaries who fail to take appropriate steps to adequately secure participant data may be personally liable to restore resulting participant losses, a remedy not provided under HIPAA. In addition, certain suggestions are provided of ways in which EBSA could assist small and medium sized plan sponsors to implement its recommendations and better fulfill their cybersecurity responsibilities, including providing the type of compliance tools that have been made available under HIPAA.

Differences between large and smaller plan sponsors.

The Security Rule requires covered entities to fulfill the following primary obligations:

1. Ensure data confidentiality
2. Identify and protect against reasonably anticipated cybersecurity threats
3. Protect against impermissible uses or disclosures of ePHI; and
4. Ensure compliance by the workforce.

The Security Rule also requires a risk analysis including documenting security measures and designation of a security officer.

Compliance with this existing rule presents challenges for small and medium-sized employers. It is much easier for large plan sponsors who typically have their own networks and internal IT departments to maintain internal security and assist in evaluating service provider systems. Smaller businesses such as my law firm are more likely to outsource their internal cybersecurity responsibilities to third parties and

to rely on those third parties to maintain adequate controls at the entity level. These plan sponsors are less familiar than large employers with good cybersecurity practices, the voluntary cybersecurity framework for small businesses put out by the National Institute of Standards and Technology (NIST) at the United States Chamber of Commerce (at NIST.gov/CyberFramework), and the availability of third parties to assist in requests for proposals (RFPs) and audits of existing providers. They may also lack the resources to do full-scale cybersecurity rfps. For example, we were informed by one vendor that it would cost $30,000 to $50,000 (depending on complexity) for a cybersecurity provider/auditor search. For all of these reasons, smaller plan sponsors will have a sharper learning curve in this area and would greatly benefit from more practical guidance, as explained below.

A Potential Role for Further EBSA Guidance.

Not All Plans May Have Good Procedures to Comply with the Security Rule.

While it is typically assumed that health plans are already complying with HIPAA/HITECH Act Security Rule, and plans exempt from the market requirements of ACA are subject to the Security Rule, HIPAA does not apply to those few self-funded and self-administered health plans that may have fewer than 50 participants or to a few so-called "excepted benefits". Sponsors of smaller plans may not be aware of all of the HIPAA Security Rule requirements, may mistakenly believe that they are exempt if they have a third party administrator, or may not have established good HIPAA protocols.

Additional Remedies for Participants.

A further reason for EBSA to issue guidance in addition to HIPAA requirements is that HIPAA does not provide a private right of action to aggrieved employees as ERISA does, though there may be rights of action under state privacy and security laws.

Small and Medium Sized Plan Sponsors Are Often Not Clear on Their Legal Obligations.

Most employee benefits practitioners have encountered plan sponsors who are not sure that EBSA's 2021 cybersecurity recommendations package applies to health and welfare plans as opposed to just retirement plans. This confusion arose because, while the fiduciary responsibilities discussed in that guidance apply equally to pension and welfare plans, the guidance did not explicitly say that it applied to welfare plans. Small and medium size plan sponsors are also often unaware of the need to provide cybersecurity protections in third party service agreements and of the impact of limits in indemnification provisions on their potential claims against those providers. One of my regular activities is reviewing service agreements for clients, and even today, I often see agreements with no special provisions on cybersecurity and no obligations on the part of the provider to maintain cybersecurity or other insurance to cover breaches. I may have to explain that plan fiduciaries have cybersecurity obligations and that these agreements need to contain appropriate representations and covenants. The smallest businesses may even be unaware that most service agreements are negotiable.

These differences make it particularly important for EBSA to provide more checklists and compliance tools to fiduciaries with responsibility for health benefits similar to the assistance provided under HIPAA. For example, sample business associate contract language and a HIPAA Security Risk Assessment Tool are available on the OCR website. EBSA has previously made available compliance assistance documents

such as a sample service provider fee disclosure for 401(k) plans. EBSA could also direct fiduciaries to helpful HIPAA resources.

Smaller Employers Need Flexibility.

The HIPAA Security Rule protects only e-PHI, a subset of protected health information. While it established responsibilities for covered entities, the Department of Health and Human Services (HHS) says that the rule is "flexible and scalable so that a covered entity can implement policies, procedures and technologies that are appropriate to the entity's particular size, organizational structure and risks to consumers." Similar flexibility should be maintained in any additional DOL guidance issued in this area. Flexibility is also important because the nature of cybersecurity threats keeps evolving.

Ransom Attacks.

Ransomware attacks are increasing and part of maintaining adequate cybersecurity is being prepared to deal with these attacks by having incident response plans, backup documents and systems. Specific guidance in this area would be welcome.

Suggestions for Further Department of Labor Action

Best Practices Guidance. Although the 2021 package of best practice recommendations appears to apply equally to health and welfare plans, there is confusion about this issue at the plan sponsor level. It would be helpful for additional regulatory or subregulatory guidance, perhaps in the form of FAQs, to make clear that sponsors of health plans have cybersecurity obligations under ERISA in addition to any responsibilities they have under HIPAA. Just as state laws may provide more extensive protections than HIPAA, HIPAA compliance should be compared with ERISA standards to determine where ERISA may be more stringent. It is also important for smaller and medium sized employers to have assistance in prioritizing the steps set out in the recent package of best practice recommendations. If they do not have the ability to take all of the recommended steps, which are the most important? Consideration should be given to establishing level or tiers of recommended protections, ranked by importance and guidance on special considerations for plan sponsors who outsource their internal cybersecurity activities to third parties.

Clarifying Fiduciary Responsibility in Regulatory Guidance.

While the 2021 guidance indicates that providing cybersecurity protections is a fiduciary responsibility, that is subregulatory guidance without the status of a regulation. For example, Compliance Assistance Release 2021-01 on missing participants states that "the contents of this document do not have the force and effect of law" and the 2021 guidance has a similar status. It would be an important step in clarifying legal obligations for EBSA to include references to cybersecurity obligations of fiduciaries of both pension and welfare plans in an official regulation subject to the "notice and comment" process under the Administrative Procedure Act. This is particularly important given the lack of a private right of action under HIPAA. It is suggested that EBSA consider amending its prudence regulations to include reviewing and providing cybersecurity protections as a defined fiduciary responsibility and to state that plan sponsors with inadequate protections can be held responsible to make up participant, beneficiary or dependent losses.

Requiring Fiduciaries to Obtain Cybersecurity Disclosures from Service Providers.

Many small and medium sized plan sponsors do not know what to ask for when they hire providers (mostly recordkeepers and contract administrators) who will handle health plan data or when they engage in a provider review. Since most recordkeepers are not fiduciaries under current law, and contract administrators and pharmacy benefit managers often disclaim fiduciary responsibility in their contracts, they would not be directly affected by a regulation redefining fiduciary responsibilities. However, even though the Department of Labor cannot generally define the responsibilities of non-fiduciary service providers, EBSA could indirectly affect the level of nonfiduciary recordkeeper regulation and contract administrator compliance by requiring hiring fiduciaries to obtain cybersecurity disclosures from potential or current providers. This would be similar to the current requirement for hiring fiduciaries to obtain fee disclosures from service providers under ERISA section 408b-2. Fiduciary administrators could be directly required to provide such disclosures. Plan fiduciaries could be required to obtain such disclosures before entering into or renewing a service agreement and their failure to do so could be evidence of imprudence in engaging the providers.

Suggested Disclosure Information.

The disclosures could require a service provider to describe its procedures for following HIPAA's Security Rule in handling of data, whether it has entered into business associate agreements with all subcontractors it hires, whether its cybersecurity systems are subject to regular third party audits, whether it has suffered past breaches, its backups and procedures for handling ransomware attacks, and whether it maintains cybersecurity insurance, including the provider and extent of such coverage. More extensive disclosures could require information such as whether the service agreement indemnification provisions would cover cybersecurity losses and whether the provider offers any type of cybersecurity warranty. These would greatly assist fiduciaries of smaller plans in evaluating and comparing providers, as recommended in "Tips for Hiring a Service Provider with Strong Cybersecurity Practices", which urges hiring fiduciaries to compare security practices, standards and audit results of a provider "to the industry standards adopted by other financial institutions."

Provide Sample Contract Language.

EBSA also recommends in the 2021 guidance that hiring fiduciaries "try to include terms in the contract that would enhance cybersecurity protection for the plan and its participants." Provisions regarding audit rights and review of limits in indemnification clauses are also specifically mentioned. Smaller employers in particular, who may not have internal legal counsel, may be unsure how to do this.

The Internal Revenue Service often provides sample plan language illustrating provisions the Service considers to satisfy certain legal requirements. As previously indicated, sample HIPAA business associate provisions are also available online. It would greatly assist small and medium sized plan sponsors if some sample cybersecurity contract provisions were made available to them on EBSA's website.

Standards for Review in Examinations and Investigations.

The April 21 package appears to create some minimum compliance standards that will be the focus of audits and investigations going forward. Any penalties assessed should reflect the size of the plan sponsor and the efforts made to provide appropriate protections to participants. HIPAA penalties have been tiered to reflect whether there was reasonable cause for a violation, whether it was due to willful neglect, and similar factors. In this respect, a new penalty standard established in a 2021 amendment

(H.R. 7898) to the HITECH Act could be appropriately applied in the ERISA sphere as well, particularly given that some breaches are inevitable no matter how diligent the plan fiduciaries may be. H.R. 7898 is not a safe harbor, but it requires the Department of Health and Human Services to take into consideration "the recognized security practices" of covered entities and business associates that were in place for the previous 12 months when determining fines, audit results or other remedies for potential HIPAA violations. In particular situations, the result of this consideration could be no liability for a past violation or violations and a focus on future correction.

Outreach educational meetings.

The Department of Labor has held plan education meetings in the past in sessions such as "Know Your Fiduciary Responsibiities". There has also been focused outreach on reviewing plan fees. Similar programs focused on cybersecurity would be very helpful to small and medium size employers.

It is respectfully suggested that all or some of these steps be considered to reinforce and supplement the 2021 guidance. Some suggestions would be equally helpful for retirement plans, and they would ease the compliance burden of small and medium size employers while increasing cybersecurity protections.