Advisory Council on Employee Welfare and Pension Benefit Plans

Report to the Honorable Martin Walsh, United States Secretary of Labor

Cybersecurity Issues Affecting Health Benefit Plans

December 2022

NOTICE

This report was produced by the Advisory Council on Employee Welfare and Pension Benefit Plans, usually referred to as the ERISA Advisory Council (the Council). The Council was established under Section 512 of the Employee Retirement Income Security Act of 1974, as amended (ERISA) to advise the Secretary of Labor (the Secretary) on matters related to welfare and pension benefit plans. This report examines cybersecurity issues affecting health benefit plans.

The contents of this report do not represent the position of the Secretary or of the Department of Labor (DOL or the Department).

LIST OF COUNCIL MEMBERS

Peter J. Wiedenbeck, Council Chair

Megan Broderick, Council Vice Chair

James G. Haubrock, Issue Chair

Shaun C. O'Brien, Issue Vice Chair

Dave Gray, Drafting Team Member

Marcelle J. Henry, Drafting Team Member

Mercedes D. Ikard, Drafting Team Member

Jeffrey Lewis, Drafting Team Member

Tonya Manning, Drafting Team Member

Glenn E. Butash

Beth Halberstadt

John R. Harney

Alice Palmer

Edward A. Schwartz

Holly Verdeyen

ABSTRACT

The 2022 ERISA Advisory Council examined cybersecurity issues affecting health benefit plans. The examination identified issues and vulnerabilities affecting these plans and faced by plan sponsors, fiduciaries, and service providers, as well as how those may differ by plan size. The Council also examined existing relevant frameworks, approaches and initiatives tailored to health care and health plan cybersecurity concerns and the interaction between overlapping regulatory regimes for health plans.

Health-care-related privacy and cybersecurity challenges may also be implicated in the administration of disability or other welfare plans. The Council's examination did not generally address cybersecurity issues affecting welfare benefit plans other than health plans, such as long-term disability plans. The Council expects, however, that some of its findings and recommendations will be relevant to those plans.

After hearing from our various witnesses, the Council made six recommendations for DOL to consider.

ACKNOWLEDGEMENTS

The Council recognizes the following individuals and organizations who provided testimony or information that assisted the Council in its deliberations and the preparation of its report. Notwithstanding their contributions, any errors in the report rest with the Council alone. The witnesses are shown in alphabetical order. Any written testimony submitted by them can be found at https://www.dol.gov/agencies/ebsa/about-ebsa/about-us/erisa-advisory-council.

Kathryn Bakich, Segal

Adam Beck, AHIP

Mariah M Becker, National Coordinating Committee for Multiemployer Plans

David Berger, Gibbs Law Group

Mimi Blanco-Best, AICPA

Carol Buckmann, Cohen & Buckmann, P.C.

James Gelfand, ERIC

Nicholas P. Heesters, Jr., Office for Civil Rights, U.S. Department of Health and Human Services

Dennis Lamm, Fidelity Investments

Kirk J. Nahra, WilmerHale

Michael Stoyanovich, Segal

Alan Thierfeldt, Cigna

Marilyn Zigmund-Luke, AHIP

TABLE OF CONTENTS

I. PRIOR COUNCIL REPORTS

The ERISA Advisory Council has twice previously addressed privacy and security issues affecting employee benefit plans. In 2011, the Council examined Privacy and Security Issues Affecting Employee Benefit Plans.[1] With regard to this topic (which expressly *excluded* examining health benefit plans), the Council noted "dramatic changes in technology" relating to administering employee benefit plans and examined issues arising from potential security breaches and the misuse of plan data. The Council also took on the question of whether plan fiduciaries had a duty under ERISA to reduce the risk of personal employee information being disclosed to unauthorized persons. As a result of its work, the Council recommended that the Department (1) provide guidance on the obligation of plan fiduciaries to secure and keep private the personal identifiable information of plan participants and beneficiaries; (2) develop educational materials and engage in outreach to plan sponsors, plan participants and beneficiaries on the issues of privacy and the security of such personal information; and (3) include in such outreach and materials information regarding elder abuse related to benefit plans.[2]

In 2016, the Council expanded on its 2011 work, examining Cybersecurity Considerations for Benefit Plans.[3] In its report, the Council noted that there was no clear guidance or standards for plan sponsors or fiduciaries to follow regarding how to develop and implement an appropriate cybersecurity plan. In this regard, the Council noted that, although the Department had not at that time determined whether cybersecurity was indeed a responsibility of plan fiduciaries, the Council nonetheless recommended that such standards should be established.

---

[1] Available at https://www.dol.gov/sites/dolgov/files/EBSA/about-ebsa/about-us/erisa-advisory-council/2011-privacy-and-security-issues-affecting-employee-benefit-plans.pdf.

[2] The topic of elder abuse was later studied (in part) by the Council in 2020. See *Considerations for Recognizing and Addressing Participants With Diminished Capacity*, https://www.dol.gov/sites/dolgov/files/EBSA/about-ebsa/about-us/erisa-advisory-council/2020-considerations-for-recognizing-and-addressing-participants-with-diminished-capacity.pdf.

[3] Available at https://www.dol.gov/sites/dolgov/files/EBSA/about-ebsa/about-us/erisa-advisory-council/2016-cybersecurity-considerations-for-benefit-plans.pdf.

II. BACKGROUND

A. Cybersecurity Threats and Health Plans

Cybersecurity continues to be a top priority issue for governments and the private sector in the U.S. and around the world due to the increasing frequency and high costs of cyberattacks. According to IBM, the average cost of a data breach in the U.S. is $9.44 million in 2022, a 4.3 percent increase from 2021.[4] Ransomware attacks in which criminals encrypt a system's data and hold it hostage until the system owner pays a sizable ransom, usually in cryptocurrency, have become an especially big problem. According to the Financial Crimes Enforcement Network of the U.S. Department of the Treasury, suspicious activity reports filed by financial institutions showed there were 1,489 ransomware-related incidents in 2021 involving nearly $1.2 billion in payments to cybercriminals, compared to $416 million in 2020.[5]

The health care sector, which has been designated as one of 16 critical infrastructure sectors in the U.S., has been and continues to be one of the biggest targets for cyberattacks. The U.S. Department of Health and Human Services (HHS) Office of Civil Rights (OCR) reported that since 2015, cybersecurity breaches among health care providers have affected the greatest number of individuals.[6] According to the Federal Bureau of Investigation, the Healthcare and Public Health Sector was the U.S. critical infrastructure sector most victimized by ransomware in 2021.[7] In a continuation of this, CommonSpirit Health, the second-largest non-profit health system in the U.S., suffered a ransomware

[4] IBM Security, *Cost of a Data Breach Report 2022* 10 (2022), https://www.ibm.com/reports/data-breach. The calculation of average cost excluded very small breaches (<2,200 compromised records) and very large breaches (>102,000 compromised records). To calculate the average cost of a breach, the authors "used activity-based costing, which identifies activities and assigns a cost according to actual use." Costs were determined for four categories of activity: detection and escalation (e.g., forensic investigative activities); notification (e.g., letters and other communications to individuals whose data has been affected by a breach); post breach response (e.g., credit monitoring and identity protection services); and lost business (e.g., business disruption and revenue losses from system downtime). Id at p. 54. The report did not include ransom payments to cybercriminals in the average cost of a breach. Eleven percent of studied breaches were ransomware attacks. Id at p. 6.

[5] Financial Crimes Enforcement Network, U.S. Department of the Treasury, *Financial Trend Analysis: Ransomware Trends in Bank Secrecy Act Data Between July 2021 and December 2021* 4 (Nov. 1, 2022), https://www.fincen.gov/sites/default/files/2022-11/Financial%20Trend%20Analysis_Ransomware%20FTA%202_508%20FINAL.pdf.

[6] U.S. Government Accountability Office, *Electronic Health Information* 20 (May 2022), https://www.gao.gov/assets/gao-22-105425.pdf.

[7] Federal Bureau of Investigation, Internet Crime Complaint Center, *Internet Crime Report 2021* 15 (2022), https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf.

attack in October 2022, which affected the system for weeks afterward and resulted in the loss of access to some medical records.[8]

Health plans and insurers are no exception to these attacks and have experienced some of the largest breaches in the U.S. A 2015 cyberattack against Anthem Inc. affected 78.8 million people.[9] In a 2014 attack against health insurer Premera Blue Cross, cybercriminals reportedly "gained access to claims data, including clinical information, along with banking account numbers, Social Security numbers, birth dates and other data" for 11 million people.[10] More recently, in March 2022, Partnership HealthPlan of California reported a cyberattack that potentially resulted in the theft of 854,913 current and former health plan members' data including diagnoses and treatment and prescription information.[11]

Health care data breaches are also the costliest. According to IBM's annual look at worldwide data breach costs, the health care industry has been the highest cost industry for 12 years in a row, with the average cost totaling $10.1 million in 2022, up 9.4% compared to 2021.[12]

Health care is a prime target for attacks, in part, because of the value of health data to patients, providers and plans, as well as to criminals. Cyberattacks on health data can interfere with the delivery of care and therefore give cybercriminals greater leverage over data owners. For example, DOL was contacted by a health plan participant who was denied approval for surgery and for whom payments for prior treatment were not made because plan data needed to verify the individual's coverage had been encrypted as part of a ransomware attack. Also, a May 2022 ransomware attack on Costa Rica's public health agency led to the cancellation of scheduled procedures and stopped the filling of prescriptions for some.[13]

---

[8] Andrea Fox, *CommonSpirit Still Working to Restore EHR Systems After ransomware Attack Confirmed*, Healthcare IT News (Oct. 14, 2022), https://www.healthcareitnews.com/news/commonspirit-working-restore-ehr-systems-after-ransomware-attack-confirmed.

[9] Marianne Kolbasuk McGee, *A New In-Depth Analysis of Anthem Breach*, Bank Info Security (Jan. 10, 2017), https://www.bankinfosecurity.com/new-in-depth-analysis-anthem-breach-a-9627.

[10] Reuters, *Premera Blue Cross Says Data Breach Exposed Medical Data*, New York Times (Mar. 17, 2015), https://www.nytimes.com/2015/03/18/business/premera-blue-cross-says-data-breach-exposed-medical-data.html.

[11] HIPAA Journal, *Over 850,000 Individuals Affected by Partnership HealthPlan of California Cyberattack* (May 24, 2022), https://www.hipaajournal.com/over-850000-individuals-affected-by-partnership-healthplan-of-california-cyberattack/.

[12] IBM Security, *supra* note 4, at 11. Country-specific costs by industry were not provided.

[13] Javier Córdoba, *Costa Rica Public Health System Targeted by Ransomware*, AP (May 31, 2022), https://apnews.com/article/russia-ukraine-covid-politics-technology-health-0e24e6644b09e2737af96814635fcd22.

The critical, sometimes life-and-death nature of this information means cyber criminals potentially can demand higher ransom payments than they otherwise might. In the Costa Rica case, the criminals demanded a payment of $5 million in Bitcoin to decrypt the data. Stolen personal health information (PHI) is also very valuable to criminals. As one article recently noted:

> [PHI] is worth a fortune to cybercriminals and is one of the hottest commodities on the dark web. Experian tags stolen patient records as going for $1,000 each, while credit card numbers are selling for around $5 each, a hacked Instagram account is $7, and Social Security numbers are worth a paltry $1.
>
> In addition, criminals experienced in drug trafficking and money laundering eagerly buy medical records to obtain prescription medications, file bogus medical claims, or steal the information to open credit cards and take out fraudulent loans. Medical records are a rich resource of valuable and permanent data points, while accounts and credit cards are quickly canceled.[14]

Use of stolen data for these purposes, in turn, can result in financial costs to health plan participants, just as identity theft can harm individuals.

Perhaps more than with other kinds of data, the theft of PHI can result in broader harms that are not easily quantified in dollars and cents but can be equally or more harmful to a person. As a 2009 Institute of Medicine (IOM) report noted, PHI may be "sensitive and potentially embarrassing." Elaborating further, the IOM report stated:

> If security is breached, the individuals whose health information was inappropriately accessed face a number of potential harms. The disclosure of personal information may cause intrinsic harm simply because that private information is known by others. Another potential danger is economic harm. Individuals could lose their job, health insurance, or housing if the wrong type of information becomes public knowledge. Individuals could also experience social or psychological harm. For example, the disclosure that an individual is infected with HIV or

[14] Shawn Dickerson, *Why Is Healthcare a Top Target for Cybersecurity Threats?*, Security (Sept. 13, 2022), https://www.securitymagazine.com/articles/98324-why-is-healthcare-a-top-target-for-cybersecurity-threats.

another type of sexually transmitted infection can cause social isolation and/or other psychologically harmful results.[15]

The rules implementing the civil money penalties for violations of the privacy and security standards and related provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) acknowledge the unique nature of individually identifiable health information. In particular, the rules direct the Secretary of Health and Human Services to consider as a mitigating or aggravating factor (as appropriate) in determining the amount of a penalty the nature and extent of the harm that resulted from the violation and provide that this may include "[w]hether the violation resulted in harm to an individual's reputation."[16]

B. DOL Cybersecurity Guidance for Employee Benefit Plans

DOL issued its first guidance on cybersecurity for ERISA-covered employee benefit plans in 2021.[17] DOL's release included three separate documents addressed to different audiences:

- *Cybersecurity Program Best Practices* (*Best Practices*) describes 12 categories of best practices that plans' service providers should follow, such as having a formal, well documented cybersecurity program; having a reliable annual third-party audit of security controls; and implementing strong technical controls in accordance with best security practices.[18] This guidance is addressed to "recordkeepers and other plan service providers responsible for plan-related IT systems and data and…plan fiduciaries when making prudent decisions on the service

[15] Institute of Medicine Committee on Health Research and the Privacy of Health Information: The HIPAA Privacy Rule, *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research* 93 (Sharyl J. Nass et al. eds., 2009), https://www.ncbi.nlm.nih.gov/books/NBK9578/pdf/Bookshelf_NBK9578.pdf (citations omitted).

[16] 45 C.F.R. § 160.408(b)(3).

[17] https://www.dol.gov/agencies/ebsa/key-topics/retirement-benefits/cybersecurity (accessed Oct. 31, 2022). In 2002, DOL issued rules governing the use of electronic media and systems to meet certain statutory disclosure and record maintenance and retention obligations under ERISA. Final Rules Relating to Use of Electronic Communication and Recordkeeping Technologies by Employee Pension and Welfare Benefit Plans, 67 Fed. Reg. 17264 (Apr. 9, 2002) (amending 29 C.F.R. § 2520.104b–1 and adopting 29 C.F.R. § 2520. 107–1). While those rules include some provisions that are relevant to cybersecurity, they are narrowly tailored and do not address whether fiduciaries have an obligation to protect against cyberattacks under ERISA § 404 or the steps fiduciaries should take to fulfill such a fiduciary duty.

[18] The full list of best practices is: (1) have a formal, well documented cybersecurity program; (2) conduct prudent annual risk assessments; (3) have a reliable annual third party audit of security controls; (4) clearly define and assign information security roles and responsibilities; (5) have strong access control procedures; (6) ensure 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; (7) conduct periodic cybersecurity awareness training; (8) implement and manage a secure system development life cycle (SDLC) program; (9) have an effective business resiliency program addressing business continuity, disaster recovery, and incident response; (10) encrypt sensitive data, stored and in transit; (11) implement strong technical controls in accordance with best security practices; and (12) appropriately respond to any past cybersecurity incidents.

providers they should hire." In laying out the context for this guidance, DOL states, "Responsible plan fiduciaries have an obligation to ensure proper mitigation of cybersecurity risks."

- *Tips for Hiring a Service Provider With Strong Cybersecurity Practices* (*Tips*) includes six tips to help with selecting and monitoring service providers, such as asking about the service provider's information security standards, practices, and policies and audit results and making sure a service provider contract requires ongoing compliance with cybersecurity and information security standards.[19] This guidance is addressed to sponsors and fiduciaries of "401(k) and other types of pension plans" to help them "meet their responsibilities under ERISA to prudently select and monitor…service providers" on which they rely "to maintain plan records and keep participant data and plan accounts secure."
- *Online Security Tips* provides participants eight basic tips, such as use strong and unique passwords and beware of phishing attacks, to "reduce the risk of fraud and loss to your retirement account."[20]

In releasing this guidance, Acting Assistant Secretary Ali Khawar explained that DOL's objective was to help plan sponsors, fiduciaries and participants "safeguard retirement benefits and personal information."[21] The new guidance got significant attention in the trade press and among benefit plan advisers, and the headlines used by them to describe the guidance to their readers and clients generally followed DOL's lead by describing it as addressing cybersecurity for retirement plans. Some

[19] The full list of tips is: (1) ask about the service provider's information security standards, practices and policies, and audit results, and compare them to the industry standards adopted by other financial institutions; (2) ask the service provider how it validates its practices, and what levels of security standards it has met and implemented, as well as look for contract provisions that give you the right to review audit results; (3) evaluate the service provider's track record; (4) ask whether the service provider has experienced past security breaches, what happened, and how it responded; (5) find out if the service provider has any insurance that would cover losses caused by cybersecurity and identify theft breaches; and (6) make sure the contract requires ongoing compliance with cybersecurity and information security standards, beware provisions that limit the service providers responsibility for IT security breaches, and try to include terms that would enhance cybersecurity protection for the plan and its participants.

[20] The full list of tips is: (1) register, set up and routinely monitor your online account; (2) use strong and unique passwords; (3) use multifactor authentication; (4) keep personal contact information current; (5) close or delete unused accounts; (5) be wary of free wi-fi; (6) beware of phishing attacks; (7) use antivirus software and keep apps and software current; and (8) know how to report identity theft and cybersecurity incidents.

[21] U.S. Department of Labor, News Release, *US Department of Labor Announces New Cybersecurity Guidance for Plan Sponsors, Plan Fiduciaries, Record-Keepers, Plan Participants* (Apr. 14, 2021), https://www.dol.gov/newsroom/releases/ebsa/ebsa20210414 (accessed Oct. 31, 2022).

benefit plan advisers, however, also noted either that it was unclear to what extent any of the guidance applied to non-retirement plans or stated that it was applicable to some extent.[22]

C. Other Relevant Laws Addressing Cybersecurity for Health Plans

In addition to obligations that may be imposed on fiduciaries and plan sponsors by ERISA, other federal and state laws regulating data and cybersecurity practices may apply to ERISA-covered health benefit plans.

HIPAA and HITECH. As part of HIPAA, Congress provided for the establishment of standards and requirements for the electronic transmission of health information that would encourage the development of a nationwide health information system, with the stated purpose of improving the efficiency and effectiveness of the overall U.S. health care system.[23] Among other things, HIPAA (as amended), together with the 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act (as amended):

- Creates a privacy standard for individually identifiable health information (PHI) and a security standard for electronic protected health information (e-PHI).
- Requires certain reporting and notifications when breaches of e-PHI and PHI occur.
- Creates auditing and enforcement regimes with respect to these various requirements.
- Provides for civil monetary penalties when certain violations occur.

With limited exceptions, these standards and requirements for PHI and e-PHI apply to covered entities—health care providers, health plans, and health care clearinghouses—and their business

---

[22] *Compare* Joseph J. Lazzarotti & Joy M. Napier-Joyce, Jackson Lewis, *DOL Issues Cybersecurity Best Practices for Retirement Plans: Plan Fiduciaries Have an Obligation to Ensure Mitigation of Cybersecurity Risks*, www.shrm.org (Apr. 20, 2021), https://www.shrm.org/resourcesandtools/hr-topics/benefits/pages/dol-issues-cybersecurity-best-practices-for-erisa-retirement-plans.aspx ("The U.S. Department of Labor's Employee Benefits Security Administration (EBSA) on April 14 issued much-anticipated cybersecurity guidance for employee retirement plans."), *with* Brian J. Kearney et al., Mercer, *DOL Issues Cybersecurity Guidance for Retirement Plans* (Apr. 26, 2021), https://www.mercer.com/content/dam/mercer/attachments/global/law-and-policy/gl-2021-dol-issues-cybersecurity-guidance-for-retirement-plans.pdf ("The GAO report discussed cybersecurity for retirement plans, and DOL's news release suggests that the new publications likewise focus on those plans. However, the extent to which the guidance applies to other ERISA plans is unclear. The tips on hiring and monitoring service providers are addressed specifically to retirement plan fiduciaries, while the best practices document appears to discuss ERISA plan service providers in general. However, the guiding principles of both documents seem relevant to all ERISA plans, as all fiduciaries have an obligation to prudently select and monitor service providers.")

[23] 42 U.S.C. § 1320d note.

associates (which handle personal health information).[24] The term health plan includes certain group health plans, health insurers, and health maintenance organizations. According to HHS, "A group health plan with less than 50 participants that is administered solely by the employer that established and maintains the plan is not a covered entity."[25] Since self-administration of health plans is rare, there likely are very few health plans that are not HIPAA covered entities.

Under these HIPAA standards, health plan includes account-type arrangements such as health flexible spending accounts (FSAs) and health reimbursement arrangements (HRAs). Certain types of excepted benefit plans, however, are not health plans covered by the HIPAA security or privacy rules:

- Coverage only for accident, or disability income insurance, or any combination thereof.
- Coverage issued as a supplement to liability insurance.
- Liability insurance, including general liability insurance and automobile liability insurance.
- Workers' compensation or similar insurance.
- Automobile medical payment insurance.
- Credit-only insurance.
- Coverage for on-site medical clinics.
- Other similar insurance coverage, specified in regulations, under which benefits for medical care are secondary or incidental to other insurance benefits. [26]

Under the HIPAA security rule, covered entities and business associates are required to:

- Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain, or transmit.

---

[24] HIPAA requirements do not apply to personally identifiable health information held by entities that do not constitute any of these covered entities or business associates.

[25] U.S. Department of Health and Human Services, Office of Civil Rights, *Summary of the HIPAA Privacy Rule* 2 (2003), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf.

[26] HHS.gov, Health Information Privacy, *Are the following types of insurance covered under HIPAA: long/short term disability; workers' compensation; automobile liability that includes coverage for medical payments?,* https://www.hhs.gov/hipaa/for-professionals/faq/364/which-insurances-are-covered-under-hipaa/index.html. An employer's onsite clinic could be considered a health care provider subject to the HIPAA security and privacy standards. Also, if the clinic "provides substantial medical services (i.e., not just first aid)[, it] could get swept in under the definition of a group health plan if it is treated as an ERISA plan by the employer/plan sponsor." Susan M. Nash, McDermott Will & Emery, *View From McDermott: Navigating Legal Issues in Connection with Employer Sponsored On-Site Health Clinics*, Bloomberg Law (Oct. 6, 2015), https://www.bloomberglaw.com/bloomberglawnews/employee-benefits/X5MO7IQO000000?bna_news_filter=employee-benefits#jcite.

- Protect against any reasonably anticipated threats or hazards to the security or integrity of that e-PHI.
- Protect against any reasonably anticipated uses or disclosures of that e-PHI that are not permitted or required under HIPAA.
- Ensure compliance by their workforce with the HIPAA security rule.

The HIPAA security rule requires covered entities and business associates to implement administrative, physical, and technical safeguards (e.g., implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level); organizational requirements (e.g., include certain terms in business associate agreements); and policies and procedures and documentation requirements (e.g., implement reasonable policies and procedures to comply with the security standards).

Flexibility is built into the HIPAA security rule. Covered entities and business associates are permitted to "use any security measures that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation specifications" of the rule.[27] Further, in numerous circumstances, a covered entity or business associate that determines that an implementation specification for a security standard is not reasonable and appropriate can implement an equivalent alternative measure if it is reasonable and appropriate.[28]

In spite of HIPAA's flexible framework for addressing the security of e-PHI, one critique of the rule is that HHS has not updated it to keep up with emerging cybersecurity threats. For example, a recent report by the office of U.S. Senator Mark R. Warner (D-Va.) noted, "HIPAA requirements remain focused on a covered entity and business associate's responsibilities to protect patient confidentiality, but they have not been sufficiently updated to address emerging threats to data integrity and availability (e.g. ransomware)."[29]

HIPAA calls for HHS enforcement of the law's security, privacy and related requirements. HHS can audit plans for compliance, resolve compliance failures through agreements with covered entities and business associates, and impose civil monetary penalties. Individuals can file complaints about

---

[27] 45 C.F.R. § 164.306(b).
[28] 45 C.F.R. § 164.306(d).
[29] Office of Sen. Mark R. Warner, *Cybersecurity is Patient Safety: Policy Options in the Health Care Sector* 15 (Nov. 2022), https://www.warner.senate.gov/public/_cache/files/f/5/f5020e27-d20f-49d1-b8f0-bac298f5da0b/0320658680B8F1D29C9A94895044DA31.cips-report.pdf.

potential HIPAA violations with HHS. They cannot bring a private civil action to enforce these requirements.

HIPAA requires covered entities and business associates to provide notification after a breach of unsecured protected PHI or e-PHI. A covered entity must notify affected individuals of a breach without unreasonable delay (and no later than 60 days after discovery of the breach).[30] If a breach affects more than 500 residents of a state or jurisdiction, the covered entity must notify prominent media outlets that serve that area.[31] If a breach affects 500 or more individuals (regardless of where they live), the covered entity must notify HHS at the same it notifies affected individuals.[32] For breaches affecting fewer people, a covered entity can inform HHS within 60 days after the end of the calendar year in which the breach happened.[33] A business associate must notify a covered entity of a breach without unreasonable delay (and no later than 60 days after discovery of the breach).[34]

In 2021, 349 data breaches affecting the personal health information of 500 or more individuals and involving health care entities and their business associates covered by HIPAA were reported to the U.S. Department of Health and Human Services. More than three-fourths of those involved hacking/IT incidents, including 39 incidents directly involving health plans and affecting 4.7 million people.[35] Through the first 10 months of 2022, there were 38 such incidents involving health plans affecting nearly 1.9 million people.

Cyber Incident Reporting Under the Critical Infrastructure Act of 2022 (CIRCIA). Under the yet-to-be-implemented CIRCIA[36], some health plans and health insurers may be required to report to the U.S. Cybersecurity and Infrastructure Security Agency (CISA) certain significant cyberattacks and all ransom payments to cybercriminals.[37] It appears that only deidentified information from these reports will be made public. Which health plans and health insurers are covered by this requirement will depend on regulations that will be issued by CISA. All entities that are part of any of the 16 critical

[30] 45 C.F.R. §§ 164.402, 164.404.
[31] 45 C.F.R. § 164.406.
[32] 45 C.F.R. § 164.408.
[33] *Id.*
[34] 45 C.F.R. § 164.410.
[35] Calculated from U.S. Department of Health and Human Services, Office for Civil Rights, *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information*, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.
[36] Pub. L. No. 117-103, 136 Stat. 1039.
[37] 6 U.S.C. §§ 681, 681b.

infrastructure sectors could potentially be covered by this requirement. Healthcare and Public Health is one of those sectors, and Health Plans and Payers is a subsector of it.[38]

State Laws. A growing patchwork of state laws regulates the privacy and security of personal information held by private entities, including those that might be considered covered entities and business associates under HIPAA.

According to the National Conference of State Legislatures, all 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have laws requiring private businesses to notify individuals of security breaches of information involving their personally identifiable information.[39] These laws typically define personal information covered by the notice requirements to include information about an individual's health plan coverage, health treatments, and diagnoses.

Breach notification laws are sometimes combined with broader laws regulating data security and cybersecurity practices in the private sector. For example, the National Association of Insurance Commissioners (NAIC) Insurance Data Security Model Law requires insurers and other entities licensed by a state department of insurance to develop, implement, and maintain an information security program and investigate cybersecurity events, as well as notify the state insurance commissioner if a cybersecurity event occurs. According to the NAIC, 21 states had adopted some version of this model law as of July 2022.[40]

The NAIC model law exempts a HIPAA-covered insurer from the state law requirement that it establish and maintain an information security program so long as the insurer has met the HIPAA security requirements and certifies that it has. Some states, however, have taken a broader approach. In 2017, New York's Superintendent of Financial Services promulgated Cybersecurity Requirements for Financial Services Companies.[41] This regulation generally requires financial services companies — including health insurers — to maintain a cybersecurity program designed to protect the confidentiality, integrity, and availability of their information systems.

---

[38] *See id.*; U.S. Department of Homeland Security, *Healthcare and Public Health Sector-Specific Plan* 5, fig. 2 (May 2016), https://www.cisa.gov/sites/default/files/publications/nipp-ssp-healthcare-public-health-2015-508.pdf.

[39] National Conference of State Legislatures, *Security Breach Notification Laws* (Jan. 17, 2022), https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (accessed Nov. 7, 2022).

[40] NAIC Center for Insurance Policy and Research, *Cybersecurity* (July 9, 2022), https://content.naic.org/cipr-topics/cybersecurity (accessed Nov. 7, 2022).

[41] N.Y. Comp. Codes R. & Regs. tit. 23, § 500 et seq.

While HIPAA can preempt state laws, it only does that to the extent a HIPAA security, privacy or related requirement is contrary to a state law. HIPAA is contrary to a state law if a covered entity or business associate would find it impossible to comply with both the state and federal requirements or the state law otherwise is an obstacle to accomplishing and executing the full purposes and objectives of HIPAA. HHS has broad authority to except state laws from preemption if certain conditions are met, and other exceptions also apply.[42]

D. Cybersecurity Frameworks

In 2016, the ERISA Advisory Council examined governmental and private cybersecurity frameworks used by organizations to evaluate and navigate cybersecurity risks.[43] While the 2022 Council did not undertake a comprehensive examination of all cybersecurity frameworks in use, these frameworks are an important part of understanding how health plans, insurers and their business associates are addressing cybersecurity risks. Commonly used frameworks include the National Institute of Standards and Technology (NIST) Cybersecurity Framework; the Health Information Trust Alliance (HITRUST) Common Security Framework; and the ISO/IEC 27001 standard. These frameworks generally provide flexible approaches to assessing cybersecurity risks and adopting and implementing policies, practices, controls and other measures for protecting data and responding to cyber threats.

While HIPAA and other laws regulating cybersecurity practices generally do not require organizations to use a cybersecurity framework, regulators and others may consider their use in evaluating whether an organization is meeting its obligations to protect data. For example, a 2021 amendment to the HITECH Act directs HHS to consider whether a covered entity or business associate had so-called "recognized security practices" in place for not less than the previous 12 months when deciding whether to lessen HIPAA fines, terminate a HIPAA audit early and favorably, or mitigate other agreed upon remedies for resolving potential violations of the HIPAA security rule.[44] The law defines recognized security practices as including the NIST cybersecurity framework; approaches contained in *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients*, which was developed by HHS in collaboration with the public-private partnership of the Healthcare and Public

[42] 42 U.S.C. § 1320d–7; 45 C.F.R. § 160.203.

[43] Advisory Council on Employee Welfare and Pension Benefit Plans, *Cybersecurity Considerations for Benefit Plans* (Nov. 2016), https://www.dol.gov/sites/dolgov/files/ebsa/about-ebsa/about-us/erisa-advisory-council/2016-cybersecurity-considerations-for-benefit-plans.pdf.

[44] 42 U.S.C. § 17941.

Health (HPH) Sector of Critical Infrastructure; and other cybersecurity programs and practices developed, recognized, or promulgated through regulations under other statutory authorities.

III. WITNESS TESTIMONY

A. Government

Nicholas P. Heesters, Jr., Office for Civil Rights, U.S. Department of Health and Human Services, described cybersecurity issues affecting health benefit plans. He provided an explanation of the HIPAA security rule and discussed the compliance challenges faced by employers and data breach reporting.

OCR's approach to the HIPAA security rule is that organizations must have processes and safeguards that ensure the confidentiality, integrity, and availability of e-PHI. The size and complexity of the organization determines the appropriate safeguards and processes. Safeguards should be flexible, scalable, and technology neutral and provide administrative, physical, and technical protections. Safeguards under the security rule form a minimum standard for protecting e-PHI.

According to Mr. Heesters, risk analysis and risk management — particularly risk analysis — is frequently found to be deficient in OCR's investigations and compliance reviews. Often, OCR determines the risk analysis performed by the organization is not accurate or thorough and does not consider all e-PHI risk factors. The risk analysis process is important because it should help inform what security protocols will be implemented based on identified risk profiles. Once risks are identified action should be taken to reduce risk. Heesters also noted that organizations should ensure e-PHI is properly disposed of, sufficiently backed up and disaster recovery plans are in place.

Regarding breach notifications, Heesters stated organizations have an obligation to report electronic and unsecured PHI breaches to OCR and affected individuals. A breach is defined as "The acquisition, access, use, or disclosure of PHI in a manner not permitted by the HIPAA Rules which compromises the security or privacy of the PHI."

B. Attorneys

Kirk Nahra, Partner, WilmerHale, provided background on HIPAA and a historical perspective on the creation of the privacy and security rules.

The HIPAA statute was passed in 1996 and applies to "covered entities" — health care providers, health plans, and health care clearinghouses. HIPAA was initially primarily focused on allowing insurance coverage to be portable and to remove pre-existing medical conditions as a barrier to changing jobs. Ultimately, the final law contained provisions that addressed standardizing electronic transactions containing health information along with data privacy and data security.

Mr. Nahra indicated that because the law only applies to "covered entities", there are gaps in protection under the law. A primary example is that health insurance is covered under the law, but disability and life insurance are not.

Under HIPAA, HHS was instructed to develop a standardized format for certain electronic transactions containing health information. It is important to note the law does not require the electronic submission of health information. It requires that if electronic means are used, then those transactions be in standard format. Standardized transactions brought about privacy and security concerns associated with health care information being maintained and transmitted in electronic form. Ultimately, this gave rise to the HIPAA privacy rule and the HIPAA security rule.

The HIPAA privacy rule regulates group health plans, but not employers. Mr. Nahra shared in his written testimony that:

> *This history and the resulting scope of the HIPAA Privacy and Security Rules drives the challenges today for employers and their health plans. HHS had authority to impose obligations on employer sponsored group health plans because such group health plans were defined as "health plans" in the HIPAA statute – because of their involvement with "portability." However, based on the same definitions, HHS did not have the authority to regulate employers directly. So, the group health plan (essentially a benefits contract) is a HIPAA covered entity, but the employer is not.*

When writing the rules, HHS recognized hospitals and health insurers use vendors to provide services and many of the services involve protected patient information. And HHS realized that they had

no authority to regulate service providers. Because of the core use of service providers and HHS's inability to regulate them, HHS created the concept of "business associate" and "business associate agreement." A business associate is defined as an entity that provides services to the health care industry where the performance of those services involves the use or disclosure of patient information. HHS required covered entities to implement specific contracts (i.e., business associate agreements) with service providers, (i.e., business associates), that would create contractual privacy and security obligations. The failure to execute a business associate agreement would mean that the covered entity violated HIPAA rules.

In 2013, HHS issued regulations (as a result of the 2009 HITECH law) that extended the scope of compliance obligations under HIPAA to business associates. As a result, business associates have contractual, legal and compliance obligations and are subject to enforcement.

HHS also recognized employers provide much of the nation's health insurance and they wanted to ensure, as much as possible, that protected health information (as defined by HIPAA) was not used by employers to make employment-related decisions. Since HHS is unable to regulate employers, HHS included provisions under the HIPAA privacy rule limiting who can access protected health information.

Regarding data security controls, Mr. Nahra stated the challenge faced by most companies is they have one system that may require many internal groups to access it — IT, finance, payroll, legal, etc. Their security protocols are designed to protect the entire organization and are not HIPAA centric.

David Berger, Partner, Gibbs Law Group, who has been involved in representing those covered by health plans in litigation arising out of data breaches, discussed four key vulnerabilities that increase the cybersecurity risk posture of health plans. First, some health plans rely on legacy or "end of life" computer systems, which are no longer supported, to manage their data. These legacy systems oftentimes receive no security patches or updates from their manufacturers and are limited in terms of growth. These systems are old and outdated and present significant vulnerabilities because they are not set up to battle Internet intruders. To boot, legacy systems are usually excluded from or carved out of a health plan's cybersecurity risk assessment via the subject entity giving itself a pass. Instead of upgrading or replacing the legacy systems, the entity excludes the system from review because the entity knows that the system is not capable of satisfying the assessment requirements and, therefore, excluding it allows the entity to take the position that it is (otherwise) fully complaint with its security systems. Mr.

Berger urged that future guidance address (i) legacy systems and (ii) the security exceptions that allow for such systems to be carved out of the cybersecurity risk assessment.

The second cybersecurity vulnerability to health plans is a health plan's failure to properly secure its databases. Mr. Berger indicated that this is the most severe vulnerability and yet the easiest to prevent. He noted that health plans oftentimes maintain a data repository that houses easily sorted/filtered data that is attractive to hackers. Mr. Berger explained that there are off-the-shelf commercial technologies that health plans could purchase that would assist them in mitigating this vulnerability by providing notification of odd activity.

The next cybersecurity health plan vulnerability comes as a result of data sharing with affiliates, business associates and other third parties. Mr. Berger explained that health plan IT systems are set up to communicate constantly with other entities. He noted that the failure to restrict inbound communications to a secure environment has been the cause of major cybersecurity incidents. A health plan simply trusting a service provider to have adequate cybersecurity protections "is not good enough" according to Mr. Berger. To mitigate the risk of being breached, he advised that health plans should implement processes that have a "zero trust environment."

The final health plan cybersecurity vulnerability relates to vendor security reviews and Mr. Berger offers suggestions for improving same. Mr. Berger reported that there is an increased use of pro forma security reviews which are not tailored to the risk profiles of the subject plans. Responses to the questions on these general questionnaires are oftentimes inadequate or nonresponsive, but nevertheless they are overlooked in favor of moving forward with the contracting process. Mr. Berger advised that when contracting, health plans should take time and invest resources into obtaining answers that fully address questions regarding a service provider's security practices. Similarly, it is important to have appropriate documentation on file to substantiate the claims made by the providers regarding their cybersecurity practices. For example, plans could require that vendors provide a SOC2 report. If necessary, plans can sign a confidentiality agreement with the vendors to protect privileged information.

In closing, Mr. Berger provided two final thoughts:

- Cybersecurity insurance alone is not a panacea. Even if the health plan is insured, it may not adequately cover the individual whose information is being held for ransom.

- Health plan size does not matter because if a health plan is not equipped to keep data secure it should not "keep the data." If the health plan chooses to maintain a lot of data on its system, it is making a choice, and it should ensure that controls are in place to secure such data regardless of entity size.

Carol Buckmann, Partner, Cohen & Buckmann, PC, who represents small and medium-sized employers and advises regarding their plans, focused her testimony on the challenges small and medium-sized businesses face in developing appropriate cybersecurity practices and ways in which DOL could assist them in better protecting health plan data.

Ms. Buckmann delineated the challenges faced by small and medium-sized employers due to a greater prevalence of outsourcing cybersecurity to third parties because they lack in-house IT capacity. They are also less likely to know how to obtain cybersecurity services and systems audits, and less able to afford them. Almost all these plans are already subject to HIPAA's security rule and have taken steps to comply with it. 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 of, nature of and risks confronting a specific entity.

Ms. Buckmann observes from her practice that compliance with the security rule presents challenges for small and medium-sized employers. She noted that such employers are less familiar than large employers with good cybersecurity practices, including the NIST cybersecurity framework and the third parties qualified to provide cybersecurity services.

Ms. Buckmann believes that small employers would greatly benefit from practical guidance from the Employee Benefits Security Administration (EBSA). To that end, she made several recommendations to the Council:

- 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.
- Clarifying Fiduciary Responsibility in Regulatory Guidance: While the 2021 guidance indicates that providing cybersecurity protections is a fiduciary responsibility, that guidance lacks the

status of a regulation. 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 rulemaking process under the Administrative Procedure Act. This is particularly important given the lack of a private right of action under HIPAA. Ms. Buckman suggested that EBSA consider amending its prudence regulations to expressly include cybersecurity as a 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: EBSA should consider indirectly improving service provider security practices by requiring hiring fiduciaries to obtain cybersecurity disclosures from potential or current service providers. This would be like the current requirement for hiring fiduciaries to obtain fee disclosures from service providers under ERISA section 408(b)(2). Plan fiduciaries could be required to obtain such disclosures before entering or renewing a service agreement and their failure to do so could be evidence of imprudence in engaging the providers.
- Provide Sample Contract Language: The Internal Revenue Service (IRS) often provides sample plan language illustrating provisions the Service considers satisfying certain legal requirements. 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: EBSA should create minimum compliance standards that will be the focus of audits and investigations. Any penalties assessed should reflect the size of the plan sponsor and the efforts made to provide appropriate protections to participants.
- Outreach educational meetings: Small and medium-sized employers would benefit from EBSA providing educational meetings and materials.

C. Plan Sponsors

James Gelfand, President of the ERISA Industry Committee (ERIC), a national nonprofit organization exclusively representing the largest employers in the United States in their capacity as employee benefit plans sponsors, provided the perspective of large, self-insured plan sponsors. About

110 million of the estimated 181 million people who receive health care through their jobs (pre-COVID) receive it through self-insured plans like those sponsored by ERIC members.

It is ERIC's understanding that health data is the most valuable information that most hackers seek, and that this information is a valuable commodity that can be used to enable improper access to other data and potentially aid in accessing participants' financial information and accounts.

Self-insured employers take an active role in contracting with major health plan carriers and are increasingly focused on ensuring the protection of their workers' health information.

ERIC recommends the following:

- DOL should coordinate with HHS, including OCR, as well as other relevant agencies – such as the IRS, the Equal Employment Opportunity Commission (EEOC), and others to harmonize cybersecurity rules that might be conflicting or overlapping.
- DOL should 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 up an overly prescriptive government standard. Stated another way, DOL should rely on the health care and technology industries to continue to evolve and update best practices. Overly specific guidelines can provide a guide for hackers, whose strategies and tactics are constantly evolving. DOL should focus on requiring a robust process and keeping up with current developments, as the HIPAA rules do.
- Rather than issue new cybersecurity guidance or standards, DOL should clarify whether the 2021 sub-regulatory guidance applies to all group health plans and continue to provide useful information to plan sponsors regarding best practices. This should be done through a set of Frequently Asked Questions or a Field Assistance Bulletin.

The DOL guidance issued in 2021, while characterized as "tips" and "best practices", uses strong language and provides thorough steps a plan sponsor should take, including significant processes that should be in place to vet vendors and performance. Mr. Gelfand noted that ERIC is always concerned about agency "best practices" and sub-regulatory guidance issued without notice and comment.

The DOL guidance leaves open questions, including the following:

- How should fiduciaries and service providers address existing arrangements that don't comply with the guidance?
- Does DOL believe that ERISA preempts state data privacy laws as they relate to ERISA benefit plans?
- Does DOL expect fiduciaries to communicate online security tips to participants and beneficiaries, and, if so, how often?

DOL is currently auditing cybersecurity programs of plan sponsors and fiduciaries. These audits include highly detailed information requests, which Mr. Gelfand described. In light of this, plan sponsors are eager to meet DOL's expectations and to avoid unnecessary audits or reprimands; therefore, they think carefully about their current cybersecurity practices and contracts with service providers.

ERIC believes that there is substantial confusion among plan sponsors and outside experts (whom ERIC canvassed) as to whether DOL's 2021 guidance applies to health plans. ERIC believes that many plan sponsors, as well as their consultants and lawyers, are currently under the impression that the guidance does not apply to health plans.

Even without DOL guidance, there are multiple frameworks and standards that health plan sponsors and fiduciaries already comply with, including HIPAA, the strongest federal law covering patients' health information, but also the Genetic Information Nondiscrimination Act of 2008 (GINA) and HITECH, which strengthened and updated HIPAA. Plan sponsors are keenly aware of two HIPAA rules updated by HITECH: (1) privacy standards, which are enforced by the HHS OCR, and which are flexible and comprehensive because of the complexity of the health care market; and (2) the Security Standards for Protection of Electronic Protected Health Information, also enforced by the OCR, which ensure that covered entities would have specified administrative safeguards. State laws contrary to HIPAA regulations are preempted.

Because of these existing standards, DOL cybersecurity guidance could add a layer of compliance beyond HIPAA and HITECH requirements unless carefully crafted to align with existing rules.

In addition, the Federal Trade Commission (FTC) and EEOC, as well as the IRS, have rules impacting employee privacy rights, as do states. State cybersecurity laws are not uniform and therefore present compliance challenges. Vendors tend to think that these state laws are not preempted by federal law and therefore try to comply with both state and federal standards.

ERIC members routinely go above and beyond what all of these rules require. Many plan sponsors voluntarily comply with the NIST guidelines. Nevertheless, better coordination among the various agencies is necessary to make sure that the rules are cohesive. And care should be taken not to disincentivize plan sponsors from continuing to voluntarily comply with enhanced standards such as NIST's.

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 with regard to health plans. More frequently, hackers gain access to PHI by posing as participants by guessing or obtaining a user's credentials. Plan sponsors continue to work to improve verification requirements, but it is challenging to protect this information if users adopt an easily guessed password or leave their credentials open to view (e.g., noted on paper).

He believes that plan fiduciaries engage with third-party cybersecurity vendors to evaluate their plans' cybersecurity practices. About 71 percent of ERIC member companies delegate cybersecurity for their group health plans to carriers and third-party administrators, but nevertheless actively engage in monitoring and testing security measures. This will often include a company's more general security practices but add layers of security provided primarily by a health insurance carrier.

Cybersecurity is now a common factor in contract negotiations between the large plan sponsors that belong to ERIC and carriers. He outlined several common examples of carrier practices improving cyber security and also listed common provisions in contracts between carriers and plan sponsors. Large plan sponsors' demand for greater security has led carriers to vastly increase their cybersecurity measures and, as technology advances, contracts will be strengthened in areas such as risk assessments (including but not limited to regular review of vulnerabilities), third-party audits (periodic and/or event driven, with evidence of resulting remediation of risks), and language to meet sponsors' special requests (such as penetration testing throughout the year, rather than just annually).

Although plan sponsors are being proactive in protecting their participants' information, including in contract negotiations, not all vendors may be meeting all plan sponsors' requests, including requests to align with the Department's 2021 guidance. This is likely because there is confusion as to whether the guidance applies to health plans.

Most large employers obtain, at great cost, some degree of cybersecurity insurance which is not specific to their plans. Insurers make significant demands on plans sponsors because of the great risk to the insurers. Sometimes plan sponsors have to certify compliances with standards and practices that go beyond the minimums required by government agencies.

He believes (although he has no survey data to offer on this) that all of ERIC's members have insurance covering cybersecurity breaches, and that insurance carriers have imposed strong cybersecurity underwriting requirements uniformly, which benefits small employers as well. However, he did not have specific information as to what members' insurance covers.

Mariah Becker, Director of Research and Education for the National Coordinating Committee for Multiemployer Plans (NCCMP), and Kathryn Bakich, the National Health Compliance Practice Leader for Segal and an NCCMP consultant, provided the perspective of multiemployer health plan sponsors. The NCCMP is a non-profit, non-partisan organization dedicated to advocacy for and the protection of multiemployer plans, their sponsors, participants and beneficiaries. Segal is a benefits and HR consulting firm that supports multiemployer plan trustees in the delivery of health care and for which Ms. Bakich specializes in providing research and analysis on federal laws and regulations affecting health coverage.

Based on current regulatory guidance (in particular, HIPAA), there is already sufficient protection and oversight of ERISA group health plans. There exists sufficient guidance on what group health plans need to do to protect the valuable data and information with which they are entrusted. The 2021 sub-regulatory guidance published by the Department is almost identical to existing HIPAA and HITECH guidance, so its principles were already being used by group health plans to enhance their cybersecurity stance. Significant internal risk mitigation concerns coupled with external commercial pressures have also resulted in most group health plan sponsors reviewing and enhancing their cyber risk management practices (via NIST, ISO or other cybersecurity risk mitigation frameworks).

Multiemployer plans have taken significant steps to address the privacy and security rules and issues that are presented within a multiemployer plan's structure. These include but are not limited to:

- Conduct HIPAA security risk assessments periodically (every 2-3 years) and whenever new technology is introduced (e.g., a new benefits system, new mobile devices, or a cloud conversion).
- Require business associate agreements for all entities that use or disclose plan PHI.
- Maintain a notice of privacy practices.
- Establish and maintain privacy and security policies and procedures.
- Maintain plan documents that are amended in accordance with the privacy rule.
- Utilize secure transmissions for PHI and e-PHI between service providers.
- Redact identifiable information from all appeals heard by the Board of Trustees.
- Train staff and fiduciaries on the HIPAA and HITECH rules and threats to PHI and e-PHI.

As already noted, a statutory and regulatory framework for cyber security is provided through HIPAA and HITECH. NIST standards provide guidelines for protection and use of PHI and e-PHI. Further, HITECH makes multiemployer health plan partners (known as "business associates") directly liable for compliance with the security rule's administrative, physical, and technical safeguards and documentation requirements.

Enforcement is provided by HHS through regular monitoring for breach reports and complaints, and its OCR has a detailed enforcement process. OCR also works in conjunction with the Department of Justice (DOJ) to refer possible criminal violations of HIPAA, and there are civil and criminal penalties for violations.

Under current processes and agreements, reporting of security incidents is also taking place. Particularly since HITECH was put in place, service agreements with business associates typically require reporting to the plan. These agreements include audit requirements, monetary requirements, and requirements on reporting. The agreement further specifies when to report a security incident, when to report a breach, and how many days are allowed before reporting. There are also official notifications to the government, but who does the reporting varies between the plan or the service provider.

At the core of a multiemployer fund's approach to cybersecurity is the HIPAA security risk assessment. This periodic assessment is required, regardless, of size, by the HIPAA security rule. Risk

assessments must also be done when there is a change in technology, because new or heightened risks and vulnerabilities can be introduced through changes in technology.

Changes in business operations due to COVID-19 amplified the risk environment. Increased prevalence of remote workers using home computer equipment and cell phones, and reliance on website communications with participants, compounded threats. Remote work can also create an environment where there is a lack of stable internet access or security of paper files and documents. All of this has been further complicated by a general heightened risk of cyber-attacks.

Multiemployer funds range from small fully insured arrangements, to large, self-insured plans, to self-administered plans. Fortunately, HIPAA and HITECH rules are designed to be scalable to the size and needs of the organization. But having scalable requirements does not equate to allowing some plans to be out of compliance. It instead is simply recognizing that there are different administrative arrangements that require different compliance. In the HIPAA structure, for example, a fully insured plan that does not use PHI to administer claims has fewer requirements than a self-insured plan, and a self-insured plan has very different needs than a self-administered plan that might have servers onsite holding PHI with multiple claims processors. Since the exposures vary, the compliance requirements should scale up or down accordingly.

Another aspect of multiemployer systems is that the pension and health fund offices are often run very similarly and might share employees and office space. While HIPAA doesn't apply to pension funds, the pension funds are often building their processes for compliance based on what has already been put in place for the health funds. As such, it would be best to have the requirements between pension and health remain as consistent as possible.

Current DOL guidance outlines best practices for pension, but here is some confusion as to whether the best practices for pensions apply to health plans as well. The best practices are almost identical to the HIPAA requirements, but a key difference is HIPAA’s allowance for self-audit.

NCCMP does not have official survey data to support their view of the multiemployer space, but feel they are sufficiently connected with and in communication with a variety of plans to make a fair representation.

D. Health Insurers, Service Providers and Consultants

Adam Beck, Marilyn Zigmund-Luke and Alan Thierfeldt provided the perspective of health insurers. Mr. Beck is Vice President for Employer Health Policy and Initiatives at AHIP, Ms. Zigmund-Luke is a Vice President with AHIP, and Mr. Thierfeldt is the Director of Information Protection for Cigna Healthcare. The panel presented six cybersecurity-related recommendations for the Council's consideration. First, AHIP recommended that the Council clarify whether the focus of the cybersecurity guidance will be on employer-sponsored self-funded plans, employer-sponsored fully insured plans, both, or some other structure (*e.g.*, Multiple Employer Welfare Arrangements (MEWAs)). It was noted that AHIP believes that employer-sponsored health and welfare plans that comply with HIPAA, the HITECH Act, and other federal and State laws and regulations understand cybersecurity risks and the importance of implementing reasonable and appropriate protections.

Second, AHIP recommended that the Council clarify the scope of its cybersecurity recommendations to DOL and focus recommendations on any "gaps" or current concerns that may not be covered by the existing legal protections. For context, AHIP explained that employer-sponsored health plans that are fully-insured will rightly rely on health insurance providers to protect information from a cybersecurity perspective. The employer itself cannot legally access protected health information held by a health insurance provider under HIPAA and should not be expected to prepare for, respond to or remediate a cyber-attack. The health insurance provider is and should be the entity to plan for, respond to and remediate cybersecurity attacks.

Third, AHIP recommended that DOL consider working with HHS OCR to issue guidance explaining any cybersecurity concerns and the existing roles and responsibilities between employers and health insurance providers in fully insured plans. They noted, for employer-sponsored health plans that are self-funded, often these arrangements involve an administrative-services-only (ASO) agreement through which an entity oversees the administrative services for the plan. AHIP noted that, anecdotally, they have received information indicating that cybersecurity is a common contractual provision in modern ASO contracts and entities have been proactive in arranging cyber planning and response in these arrangements. It was further noted that they do not know whether all ASO arrangements have consistently and routinely prepared for cybersecurity risks.

Fourth, AHIP recommended that DOL conduct a limited and concentrated informal inquiry to research and discover whether ASO contracts have adequate provisions for cybersecurity. If such

provisions are not commonplace, DOL should issue guidance setting forth expectations between employers and ASO providers in self-funded health and welfare plans. If no ASO contract exists and the employer functions as the administrator, AHIP believes the Council should recommend ways (using the resources highlighted above) for self-funded health plans to address cybersecurity risks in their business environments and operations. AHIP noted that, in their assessment, despite the funding arrangement of a health and welfare plan, smaller or mid-sized companies frequently find cybersecurity guidance helpful as their resources are often limited when compared to larger, more robust operations.

Fifth, AHIP recommended that DOL provide educational outreach to help smaller and mid-sized self-funded health plans understand the risks and benefits to promote building cyber protections into their business operations. Where possible, the Department should partner with other agencies or leverage the cybersecurity guidance and materials that have been developed to date. AHIP cautioned against DOL prescribing guidance or future regulations that are prescriptive or that would remain static and create an inability to keep pace with new cyber threats, industry trends for protections and new technological developments that promote better detection, response, and remediation.

Last, AHIP recommended that future guidance or regulations be flexible and allow for technology-neutral, scalable solutions based on an entity's business operations, risk assessment, available resources, and new developments that promote better detection, response, and remediation. AHIP noted that a cost-benefit analysis should be an essential part of the process. AHIP advised that a key function for public and private entities to combat cyber-attacks is to share information when possible as a campaign or infiltration is detected. Federal laws have attempted to help in this regard, but oftentimes information cannot be shared or if it is shared, it is "watered down."

In closing, the panel noted that international efforts are important for mitigating threats and campaigns, particularly from nation states and part of global "infection" processes as can occur with malicious code and viruses.

Mimi Blanco-Best, Associate Director of Attestation and Methodology and Guidance, Insurance Services Executive Committee, Association of International Certified Professional Accountants (AICPA), provided testimony on the various ways in which CPAs can support clients' cybersecurity efforts by informing clients as to the cybersecurity risks faced by health benefit plans, evaluating their cybersecurity risks and controls, and assisting in the assessment of their service providers' cybersecurity posture, including SOC reports for Cybersecurity.

Ms. Blanco-Best noted that health benefit plans may be attractive targets for hackers seeking access to plan assets and participant personal information. The factors contributing to the risks include but are not limited to the large amount of sensitive employee information that is shared with multiple third parties; benefit plans often falling outside the scope of a sponsor organization's cybersecurity planning; the absence of cybersecurity regulations; and the risk that plan sponsors and administrators may mistakenly believe that the SOC 1 adequately addresses cyber risks. She further noted that the consequences of a cybersecurity breach can be substantial for plan sponsors, service providers, and participants and can include costs such as monetary damages, reputational risk, HIPAA notification obligations, and fiduciary breach claims.

In discussing plan auditor's responsibility for evaluating cybersecurity risk and controls in the audit of plan financial statements, she made clear that cybersecurity risks and controls are a concern of the financial statement auditor *only* to the extent they could impact financial statements to a material extent. The auditor's primary focus is on the controls and systems in the closest proximity to the data presented in the financial statements. Even when a breach of participant information occurs, it may have no substantial impact on the plan's financial statements, making it of little relevance to the audit.

Ms. Blanco-Best further testified that CPAs can provide critical cybersecurity services beyond financial statements to help management assess the effectiveness of an organization's controls. The AICPA developed the System and Organization Controls (SOC) Suite of Services. The SOC suite of services includes:

- SOC 1® — SOC for Service Organizations: ICFR. Service organizations may provide services that are relevant to their user entities' internal control over financial reporting and, therefore, to the audit of financial statements.
- SOC 2® — SOC for Service Organizations: Trust Services Criteria. To identify, assess and address the risks that arise from doing business with a service organization, customers and business partners want information about the design, operation, and effectiveness of security controls, and in some cases controls over system availability, processing integrity, and the protection of confidential or private information used by the service organization's system. To support their risk assessments, customers and business partners may request a SOC 2® report from the service organization.

- SOC for Cybersecurity: As part of an entity's cybersecurity risk management program, an entity designs, implements, and operates cybersecurity controls. A SOC for Cybersecurity is an engagement to examine and report on an entity's cybersecurity risk management program and the effectiveness of controls within that program.

The SOC for Cybersecurity report includes three key components:

- Management's description of the entity's cybersecurity risk management program: The description is designed to provide information about how the entity identifies its information assets, the ways in which the entity manages the cybersecurity risks that threaten it, and the key security policies and processes implemented to protect the entity's information assets against those risks. The description provides the context needed for users to understand the conclusions expressed by management in its assertion and by the practitioner in his or her report.
- Management's assertion: The report includes an assertion provided by management, which addresses whether: (a) management's description is presented in accordance with DC section 100, *Description Criteria for Management's Description of the Entity's Cybersecurity Risk Management Program*; and (b) the controls within the entity's cybersecurity risk management program were effective to achieve the entity's cybersecurity objectives based on the control criteria. The 2017 trust services criteria may be used as the measurement criteria; alternatively, other criteria considered suitable for the examination may also be used to evaluate the effectiveness of cybersecurity processes and controls.
- CPA's report: The report also includes a CPA's opinion that evaluates management's assertion.

In summary, Ms. Blanco-Best stressed to the Council that is paramount that employee health benefit plans understand how service organizations to which they have outsourced services are managing their cybersecurity risks. Failure to do so can have devastating consequences to the plan, plan sponsor, administrator, and plan participants.

Michael Stoyanovich, Vice President and Senior Consultant in Segal's Administration & Technology Consulting practice, described how Segal's group health plan clients are addressing cybersecurity risks and the kinds of cybersecurity reviews Segal provides to group health plans with respect to e-PHI. He also provided his recommendations about whether additional DOL guidance is needed and what kinds of guidance would be helpful.

Based on his work with Segal's clients, which include a wide variety of plan sponsor types, Mr. Stoyanovich noted that plan fiduciaries have a heightened awareness of "the cyber security risk environment that they are operating in." He also described group health plans' relatively long experience complying with the HIPAA security rule for e-PHI and applying voluntary cybersecurity frameworks, such as the NIST Cybersecurity Framework, along with their growing sophistication in addressing these issues. He noted that cyberinsurance carrier underwriting is also prompting group health plans to take additional voluntary steps. Stoyanovich stated that among Segal's clients there is a strong level of awareness of HIPAA and "pretty good compliance with it"; he did not address the degree of awareness and compliance beyond Segal's clients. He noted that all of Segal's group health plan clients now request service provider information about their cybersecurity policies and practices, such as SOC 2 Level 2 assessments, and remarked that this reflects a change in practice compared to earlier periods.

Segal performs comprehensive HIPAA assessments for its clients, which it recommends be performed every two to three years and more frequently if there is a change in service providers, such as a third-party administrator. Assessments include significant data and information requests made of clients via a questionnaire of approximately 300 questions, follow-up interviews and even a physical review of the client's premises. In performing assessments, Segal determines whether clients have appropriate technical, physical and administrative safeguards in place and provides recommendations for strengthening safeguards.

Mr. Stoyanovich recommended against DOL issuing additional cybersecurity guidance for group health plans, stating that "based on a [sic] current regulatory guidance, and in particular HIPAA, there's already sufficient protection and oversight of ERISA group health plans." He noted that although HIPAA's Security standard only applies to e-PHI, the measures put into place for e-PHI generally would apply broadly and therefore protect other data, too. If DOL were to issue guidance, he urged just clarifying DOL's 2021 cybersecurity guidance, which he noted some group health plan decisionmakers have already begun to use in reviewing their plans. He also encouraged DOL to coordinate HHS on any guidance, recognize differences in plans (e.g., based on their differing financial, human and technological resources) and provide flexibility, including by providing guidance that is technology neutral.

Dennis Lamm, Senior Vice President and Head, Customer Protection, Workplace Investing, at Fidelity Investments, described why group health plans are at risk, what cyber risks plans

are facing, how plans are mitigating those risks and what plans are experiencing in practice. He also offered recommendations for plans and DOL.

According to Mr. Lamm, the health sector is the most breached sector in the U.S. economy, and health plans account for one-in-seven breaches in that sector, with plan breaches increasing by 10-20% each year. Health data is seen by cyber criminals as having the weakest controls protecting it and being the most valuable kind of data for sale on the internet's black market, known as the dark web. He noted that a personal health record sells for 300 times the average Social Security number or individual credit card information, about $350. A full health record enables cyber criminals to "attempt financial fraud, your bank accounts, your retirement accounts, your brokerage accounts because they attempt to impersonate you by knowing all the sensitive indicative data about you." Health data is also a bigger target for cyberattacks because of underfunded controls, antiquated systems and a critical need for the data which can be exploited.

The vast majority of successful cyberattacks are of two types: phishing and exploitation of zero-day vulnerabilities. The former account for 90% of breaches, and most organizations do not have the right controls to prevent them or the right technology (which is fairly sophisticated) to quarantine them so they do not spread to other systems. The latter occurs when software companies release patches for newly identified vulnerabilities and bad actors rush to exploit those announced vulnerabilities before users download the software updates. According to Mr. Lamm, solid, consistent cyber hygiene will stop 90-95% of breaches. He noted that there are two major risks from cyberattacks against health plans: theft of personal health information and disruption of the organization's ability to provide services, typically for a three-week period, due to ransomware.

Mitigating the risk of successful cyberattacks is a matter of adopting and implementing appropriate processes and controls. He stated that the HIPAA Security standard is a "baseline," "an absolute minimum." The HIPAA Security controls do not get you everything you need and have not been updated in nine years. As a result, "the sorts of things that are causing health benefits to be compromised would still be compromised even if you implemented HIPAA compliance." It is important for an organization to use other cybersecurity frameworks, such as AICPA's SOC 2, ISO 27000 or HITRUST, which have many more controls than HIPAA Security.

In the health care space, Mr. Lamm noted that there is an expectation of cyber due diligence especially among major health insurers, and they generally prefer using the HITRUST framework,

though they will accept SOC 2 or ISO 27000. They are not satisfied with a service provider just being HIPAA compliant. Many Fidelity health benefit plan clients have established formal vendor oversight programs; 75% of them audit Fidelity every two years, with requests for attestations that adequate controls are in place. Some ask to see third-party audits, such as the SOC 1 and SOC 2. Others submit their own detailed questionnaires, which could be between 50 and 250 questions. Cybersecurity is also integrated into vendor searches, not just a part of monitoring existing vendors. Mr. Lamm noted, however, that despite health plans being more aware of their cybersecurity obligations than retirement plans, not all plans are doing what they should.

Mr. Lamm made two specific recommendations. First, he suggested that group health plans should ensure that service providers have a third-party audit of and can attest to their cybersecurity controls. He noted that Fidelity's clients have differing preferences for which assessment is used (e.g., SOC 2, HITRUST or ISO 27000) and plans should be given flexibility as to which cybersecurity framework they use. Second, he stated that a lot more information and awareness about the need for cybersecurity protections is needed within the benefits community and that will require active outreach, not simply posting information online. He suggested that DOL could partner with the Department of Health and Human Services, which already has an active outreach program about HIPAA Security focused on small and medium-sized businesses, or CISA, which is an arm of the U.S. Department of Homeland Security and also has a focus on risks to small and medium-sized businesses.

Regarding DOL's 2021 cybersecurity guidance, Lamm said it is the perception of some Fidelity clients that the guidance does not apply to health plans. He noted that some of the 2021 guidance has been referenced in DOL audits of retirement plans. He also said that although the 2021 DOL guidance was a constructive step forward, there are limitations to it. He noted that in the guidance, "you don't see the word phishing once and there's nothing really about server patching or ransomware, which are the evolving threats now." He raised concerns about the guidance creating confusion about which frameworks should be applied and resulting in the duplication of effort. Regarding the possibility of additional DOL guidance, he warned against guidance that is too prescriptive because it can quickly become outdated without a commitment to update it frequently, and he noted the helpfulness of using formal notice and comment in developing guidance in order to provide for stakeholder input.

IV. COUNCIL OBSERVATIONS

Health plan information is prized by cyber criminals. Health data is the most valuable information sought by hackers.[45] The personally identifiable information (PII) and PHI held by health plans, their insurers, and service providers can provide the gateway to identity theft, credit fraud, and access to participants' financial accounts, including retirement savings such as 401(k) accounts. The Council heard testimony indicating that the health care sector (including medical care providers as well as insurers and health plans) is the most frequently breached sector in the U.S. economy, and that one in seven health-care-related breaches involves a health plan.[46] As of September 2022, approximately 50 health plans had been breached year-to-date in 2022.[47] That malicious focus is understandable in light of the relative value of the data: An individual's PHI sells on the dark web for an amount that is more than 300 times greater than a Social Security Number (SSN).[48] The Council was told that phishing attacks account for about 90 percent of security breaches overall, and that data exfiltration (sometimes on a massive scale) occurs in 70 percent of ransomware events.[49]

An important thread running through much of what the Council heard from witnesses concerned the relationship between the obligations of health plan fiduciaries with respect to cybersecurity under the HIPAA and ERISA. The privacy rule and the security rule issued under HIPAA impose some safeguards surrounding health information in the hands of health care providers, health plans, and service providers (known as "business associates" in the HIPAA context).[50] These protections are not displaced by ERISA,[51] which raises the question whether ERISA's fiduciary responsibility requirements demand more.[52] HIPAA focused on portability and electronic claim processing; it was not centrally concerned

---

[45] James Gelfand, *Understanding Health Plans and Cybersecurity Activities* 2 (July 20, 2022) (written statement submitted to the ERISA Advisory Council (Council) on behalf of the ERISA Industry Committee), https://www.dol.gov/sites/dolgov/files/EBSA/about-ebsa/about-us/erisa-advisory-council/2022-cybersecurity-issues-affecting-health-benefit-plans-gelfand-07-20.pdf.

[46] Council Hearing of Sept. 9, 2022, Transcript of Testimony of Dennis Lamm, Fidelity Investments, at 184.

[47] *Id.* at 189 (observing that 2022 health plan data breaches will increase 10% to 15% over 2021 levels).

[48] *Id.* at 187 (stating that the going price of a PHI record is about $350, while an individual SSN trades for about $1).

[49] *Id.* at 192; Council Hearing of Sept. 9, 2022, Transcript of Testimony of Timothy Marlin, Marsh McLennan, at 17.

[50] Pub. L. No. 104-191, 110 Stat. 1936; 45 C.F.R. Part 164.

[51] ERISA § 514(d), 29 U.S.C. §1144(d) (providing that ERISA Title I does not impair any law of the United States).

[52] Acting Assistant Secretary Ali Khawar observed that in developing EBSA's 2021 cybersecurity guidance the agency did not explicitly address its application to health plans, in part because of differences in the legal regime applicable to health plans (compared to retirement plans) and the sensitivity of health plan data. Council Hearing of Sept. 8, 2022, Transcript of Statement of Ali Khawar, at 249.

with health care privacy or security.[53] Preventing employer misuse of health data in employment decision-making was the core objective of HHS rulemaking.[54] Those concerns, being distinct from and largely orthogonal to ERISA's worker protection policy, leave plan fiduciaries with wide latitude to preserve the confidentiality and integrity of plan data.

The overriding fiduciary obligation to "discharge his duties with respect to a plan solely in the interests of the participants and beneficiaries and … with the care, skill prudence and diligence under the circumstances then prevailing that a prudent man acting in like capacity and familiar with such matters would use"[55] may sometimes require precautions more stringent than the HIPAA baseline. A Fidelity witness observed that the HIPAA security rule sets a baseline that is not sufficient in practice, consistent with other critiques of HIPAA's effectiveness.[56] A witness for employee benefits consulting firm Segal, however, opined that HIPAA provides enough oversight of cybersecurity issues for ERISA-covered health plans.[57]

Another important thread running through much of the testimony, statements, and other information received by the Council was the lack of clarity about and knowledge of ERISA fiduciary duties regarding cybersecurity for health plans, especially among some segments of fiduciaries and their advisers. While no witness questioned whether health plan fiduciaries have a duty to act prudently regarding cybersecurity risks and some stated explicitly that they believe such a duty exists[58], it was also apparent that there is a wide range of understanding among health plan sponsors and other fiduciaries about whether they have a duty and what it requires of them.

Some uncertainty and confusion appear to arise out of the fact that DOL has not made a sufficiently direct statement, whether in a regulation or guidance, declaring the basic principle that

---

[53] Kirk J. Nahra, *Cybersecurity Issues for Health Plans* 1-2, 4-5 (July 20, 2022) (written statement submitted to the ERISA Advisory Council), https://www.dol.gov/sites/dolgov/files/EBSA/about-ebsa/about-us/erisa-advisory-council/2022-cybersecurity-issues-affecting-health-benefit-plans-nahra-written-statement-07-18.pdf. Council Hearing of July 18, 2022, Transcript of Testimony of Kirk Nahra, WilmerHale, at 11-15.

[54] Nahra, *Cybersecurity Issues for Health Plans*, *supra* note 9, at 4-5; Council Hearing of July 18, 2022, Transcript of Testimony of Kirk Nahra, WilmerHale, at 22-23.

[55] ERISA § 404(a)(1), 29 U.S.C. § 1104(a)(1).

[56] Council Hearing of Sept. 9, 2022, *supra* note 46, at 196.

[57] Council Hearing of July 18, 2022, Transcript of Testimony of Michael Stoyanovich, Segal, at 97 ("Thus, what I would say and in Segal in general, is based on current regulatory guidance, and in particular HIPAA, there's already sufficient protection and oversight of ERISA group health plans.")

[58] *E.g.*, Council Hearing of July 20, 2022, Transcript of Testimony of James Gelfand, ERIC, at 72 ("[I]t is our understanding that plan sponsors do believe that they have a fiduciary responsibility to ensure the privacy and confidentiality of the data obtained by group health plans.").

health plan fiduciaries have a duty to act prudently regarding cybersecurity risks. As one experienced employee benefit plan attorney told the Council, "If you read the [2021] guidance, it seems clear that the fiduciary responsibilities that are discussed there apply equal[ly] to health and welfare plans, but the guidance doesn't say clearly that it does."[59] That same attorney recommended DOL issue "a regulation that is clearly binding" and stating explicitly that ERISA fiduciaries' duty to act prudently extends to cybersecurity.[60]

The U.S. Government Accountability Office (GAO) has made a similar recommendation regarding defined contribution pension plans. In early 2021, before DOL released its package of cybersecurity guidance, GAO called on DOL to "formally state whether cybersecurity for private sector defined contribution plans is a plan fiduciary responsibility under ERISA."[61] Release of the 2021 guidance, however, did not address this recommendation to GAO's satisfaction. Appearing before the Council in July 2022, a GAO representative called for DOL to "formally clarify[] that mitigating cybersecurity risk is a fiduciary responsibility under ERISA…[to] help ensure that plan fiduciaries are clear about their responsibilities," after noting that DOL has already "issued best practices for protecting PII, and financial data."[62]

Added uncertainty and confusion about the basic principle of whether and to what extent any fiduciaries have a duty with regard to cybersecurity may have been caused by the approach taken by DOL in its 2021 cybersecurity guidance. In its *Best Practices*, DOL implied, but did not expressly state, that adopting prudent cybersecurity practices was a fiduciary duty, stating that the included practices were "for use by service providers responsible for plan-related IT systems and data, and for plan fiduciaries making prudent decisions on the service providers they should hire." In the accompanying *Tips*, DOL stated, "[T]o help owners and fiduciaries meet their responsibilities under ERISA to prudently select and monitor service providers, we prepared the following tips for plan sponsors of all sizes…." In other words, DOL couched its *Best Practices* and *Tips* in terms of plans' dealings with service providers and never flatly stated that exercising prudence with regard to cybersecurity of

[59] Council Hearing of Sept. 9, 2022, Transcript of Testimony of Carol Buckmann, Cohen & Buckmann, PC, at 216.
[60] *Id.* at 220.
[61] GAO, *Defined Contribution Plans: Federal Guidance Could Help Mitigate Risks in 401(k) and Other Retirement Plans* (GAO 21-25, Feb. 11, 2021), https://www.gao.gov/assets/gao-21-25.pdf. In its response to GAO, DOL neither agreed nor disagreed with this recommendation. *Id.* at 31. However, DOL did note that plan fiduciaries' duties to "act prudently and solely in the interest of plan participants and beneficiaries, as set forth in ERISA section 404...require plan fiduciaries to take appropriate precautions to mitigate risks of malfeasance to their plans, whether cyber or otherwise." *Id.* at 34.
[62] Council Hearing of July 19, 2022, Transcript of Testimony of Dan Garcia-Diaz, U.S. GAO, at 9.

participant data was a fiduciary duty generally; i.e., whether that duty applied to data maintained by plans or sponsors themselves as well as in their selection of service providers.

The framing of the 2021 announcement also created confusion about whether the guidance applies to health plans. DOL's April 2021 *News Release*[63]announcing cybersecurity guidance in three forms[64], quotes Acting Assistant Secretary for Employee Benefits Security, Ali Khawar, stating, "The cybersecurity guidance we issued today is an important step towards helping plan sponsors, fiduciaries and participants to safeguard *retirement benefits* and personal information, ... This much-needed guidance emphasizes the importance that plan sponsors and fiduciaries must place on combatting cybercrime and gives important tips to participants and beneficiaries on remaining vigilant against emerging cyber threats." (Emphasis added.) Further, the introductory paragraph for the *Tips* provides "[a]s sponsors of 4*01(k) and other types of pension plans*, business owners often rely on other service providers to maintain plan records and keep participant data confidential and plan accounts secure. Plan sponsors should use service providers that follow strong cybersecurity practices." (Emphasis added.)

Confusion has emerged in the employee plans industry as to whether the *Tips* and the *Best Practices* guidance apply to retirement plan sponsors alone or to both retirement and health benefit plan sponsors and providers.[65] Neither DOL's *News Release* for the cybersecurity guidance nor the guidance itself makes mention of health benefit plans. Further, given the repeated references to "retirement benefits" in the *News Release*, many have read the *Best Practices* and *Tips* as applying to only retirement plan sponsors and leaving health benefit plan sponsors subject solely to non-ERISA regulatory requirements, such as HIPAA privacy and security rules and HITECH.[66] DOL also has provided information to the Council that some stakeholders have inquired as to whether the cybersecurity guidance applies to health benefit plans. The Council heard from multiple witnesses who

[63] U.S. Department of Labor, *supra* note 21.

[64] *Id.* The three forms were: (i) *Tips for Hiring a Service Provider with Strong Cybersecurity Practices*, (ii) *Cybersecurity Program Best Practices* and (iii) *Online Security Tips*.

[65] *E.g.*, Council Hearing of July 20, 2022, *supra* note 58, at 50 ("In fact, ERIC conducted a canvas of experts which showed significant confusion about this guidance, particularly whether or not the guidance is meant to focus solely on retirement plans or also on group health plans.") See also, the discussion of DOL's 2021 cybersecurity guidance in the Background section, including *supra* note 22.

[66] *E.g.*, Council Hearing of Sept. 9, 2022, *supra* note 46, at 204 (Dennis Lamm of Fidelity stating that many benefit plan clients have the perception that the 2021 guidance does not apply to health plans).

recommend that DOL provide clarification on whether the *Tips* and *Best Practices* apply to health plans.[67]

Several witnesses discussed the relationship between DOL's 2021 guidance and HIPAA's security standard. For example, one witness noted that the *Best Practices* list is "almost identical" to HIPAA's security standard requirements.[68] Others suggested that it would be helpful if DOL were to identify where HIPAA requirements and the DOL guidance overlap.[69] The Council determined that DOL could improve ERISA compliance by doing so. Some Council members felt that the correspondence between ERISA and HIPAA's requirements should be specifically identified before the Department applies its 2021 guidance to health plans.

Witnesses highlighted how quickly the cybersecurity threat environment and technology change and therefore the need for regulators, fiduciaries, and service providers to stay up to date and for regulators to provide for flexibility. Underscoring the need to keep up to date, a Fidelity witness noted that because HIPAA controls haven't been updated in nine years, "the sorts of things that are causing health benefits to be compromised would still be compromised even if you implemented HIPAA compliance."[70] That witness further stated, "[U]nless the DOL is prepared to, on an annual basis, continually reach out to industry and update and refresh these controls, they're going to become obsolete."[71] An AHIP witness cautioned against "having very prescriptive recommendations or guidance or setting things in stone, in terms of regulation, because cyber is one of those areas that is not static."[72] She further noted, "And in order to create the ability to keep pace with cybersecurity threats, there needs to be that flexibility to keep up with industry trends, both in terms of protections...as well as any

---

[67] *E.g.*, Council Hearing of July 20, 2022, *supra* note 58, at 65 ("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."); Council Hearing of Sept. 9, 2022, *supra* note 58, at 219 ("[A]lthough the 2021 package of best practice recommendations appears to apply equally to health and welfare plans, I think it would be helpful if there were some specific written indication from [DOL], perhaps in the form of FAQs, it could be some regulatory authority, but something that specifically clarifies this point and eliminates any confusion that the smaller employers have about whether the guidance applies to them.")

[68] Council Hearing of Sept. 8, 2022, Transcript of Testimony of Kathy Bakich, Segal, at 109 ("And the Department's best practices list is almost identical to the HIPAA requirements that already apply to health plans, so I think there's some confusion in implementation.... The only real difference between the two is that under HIPAA, you can self audit.")

[69] *E.g.*, Council Hearing of Sept. 9, 2022, *supra* note 59, at 225 ("[I]t would be extremely helpful for people to know how DOL would be viewing their HIPAA responsibilities. For example, if they had a HIPAA audit and it showed they had good practices, would that be sufficient, satisfying the DOL?")

[70] Council Hearing of Sept. 9, 2022, *supra* note 46, at 196.

[71] *Id.* at 202.

[72] Council Hearing of Sept. 9, 2022, Hearing Transcript of Marilyn Zigmund-Luke, AHIP, at 163-164.

developments that would help promote better detection response mediation."[73] The Council determined that it is important that DOL regularly review and update its cybersecurity guidance, including the *Tips* and *Best Practices*, to ensure it keeps up with the evolving cybersecurity and technological environments.

A third significant thread woven through much of the testimony heard by the Council related to how plans address cybersecurity issues in their dealings with third-party service providers. Modern health plans overwhelmingly deliver benefits by contracting with a health insurance company. Often, the insurance company acts as an expert third-party administrator (TPA) of the employer's self-insured plan under an ASO contract. Alternatively, and most often in the case of small employers, the employer will purchase a health insurance policy covering its workers and their beneficiaries. Because the health plan does not itself administer benefits, most of the action, most of the information, and most of the security risk lies with TPAs, insurers, and other service providers. Or, as one witness stated, "One of the largest risks to employee benefit plans is actually the risk of doing business with...third-party service providers."[74]

Organizing benefit delivery in this fashion makes good security practices by service providers an essential component of the plan's data security posture. As one commentator, in observing that best practices "now require evidence of robust monitoring," has noted about the need to pay careful attention to service providers' cybersecurity policies and practices:

> *The modern EBP [employee benefit plan] committee should have written cybersecurity rules for hiring, monitoring, and re-engaging vendors as recordkeepers, investment firms, healthcare plans, payroll operations, and any other service provider possessing PII or PHI. It is also essential for committees to know if any of their EBPs' service providers utilize agents or subcontractors to perform the services, and to examine such providers' data security policies and procedures.*[75]

[73] *Id.* at 164.
[74] Council Hearing of July 18, 2022, Transcript of Testimony of Mimi Blanco-Best, AICPA, at 60.
[75] Ronald E. Hagan, *Cybersecurity in the Committee Room*, J. Comp. & Benefits 30, 32, 33 (July/August 2022).

Recognizing this fact, the accounting profession has developed a mechanism (the SOC 2 report) to test and validate the accuracy and effectiveness of service provider security controls.[76] For defined contribution pension plans, SPARK's Data Security Oversight Board developed a set of Industry Best Practices for Data Security Reporting to provide a standard framework for recordkeepers to report their cybersecurity capabilities to plan sponsors.[77] Cybersecurity, the Council was told, is an essential element in vendor searches, and is one of top three criteria health plans use in contracting decisions.[78]

HIPAA security rules now directly apply to plan service providers as business associates under the HITECH Act, and the obligations flow downstream to subcontractors.[79] Because business associates are independently subject to HIPAA, the security rule contains no express requirements with respect to business associate monitoring and oversight by health plans.[80] In theory, plan sponsors should be protected against security breaches by downstream vendors under the HIPAA business associate agreement rules, but in practice fiduciaries often do not have sufficient information to know about the cybersecurity practices of remote vendors down the chain to assure themselves that plan members' PII and PHI are reasonably secure.[81] One attorney advised the Council that trusting outside entities to be secure is not enough. He recommended that when dealing with service providers, plans should not only rely solely on contractual provisions for data protection but should also have the ability to validate that contract terms are being met.[82] Similarly, Fidelity's cybersecurity expert recommended that plans obtain third party attestation or an audit to test the reliability of a service provider's system and environment.[83]

Despite the importance of robust service provider security controls and practices, differential capacity presents a challenge. Small and mid-sized plans are often unsure about the need to cover cybersecurity practices in service agreements. Their business associate agreements may say only that the

---

[76] Mimi Blanco-Best, *Testimony*, 5-8 (July 18, 2022) (written statement submitted to the ERISA Advisory Council on behalf of the AICPA), https://www.dol.gov/sites/dolgov/files/EBSA/about-ebsa/about-us/erisa-advisory-council/2022-cybersecurity-issues-affecting-health-benefit-plans-blanco-best-written-statement-07-18.pdf.

[77] Council Hearing of July 19, 2022, Transcript of Testimony of Timothy Rouse, SPARK Institute, at 195-96; SPARK Inst. Inc., Industry Best Practice Data Security Reporting, rel. 2.0 (Aug. 30, 2022), https://www.sparkinstitute.org/wp-content/uploads/2022/10/SPARK-Data-Security-Industry-Best-Practice-Standards-Version-2022.11-082922.pdf.

[78] Council Hearing of Sept. 9, 2022, *supra* note 46, at 208.

[79] Council Hearing of July 18, 2022, Transcript of Testimony of Kirk Nahra, WilmerHale, at 40-41.

[80] Nicholas Heesters, *HIPAA Security Rule, Breach Notification, and Cybersecurity* 37-38 (Sept. 8, 2022) (presentation submitted to the ERISA Advisory Council on behalf of the Office of Civil Rights, Department of Health and Human Services), https://www.dol.gov/sites/dolgov/files/EBSA/about-ebsa/about-us/erisa-advisory-council/2022-cybersecurity-issues-affecting-health-benefit-plans-heesters-written-statement-09-08.pdf.

[81] Council Hearing of July 18, 2022, *supra* note 57, at 112-13.

[82] Council Hearing of July 20, 2022, Transcript of Testimony of David Berger, Gibbs Law Group, at 99-103.

[83] Council Hearing of Sept. 9, 2022, *supra* note 46, at 199-200.

contractor will follow HIPAA.[84] Representatives of health insurers also observed that small and mid-size plans may need help in formulating contract terms concerning cybersecurity practices in ASO agreements.[85] Even if they are attuned to the risk, small employers cannot always succeed in negotiating protections in their contracts with service providers, due to insufficient bargaining power.[86]

In light of the important role service providers have in keeping health plan data secure, the Council considered the value of DOL issuing a clear declaration that health plan fiduciaries' duty to act prudently with regard to cybersecurity risks includes the duty to ascertain that their health plan service providers have practices and procedures in place to deal with these risks and that agreements with service providers adequately address this issue. A majority of Council members believe providing such a statement, whether through a regulation or other guidance, is an essential complement to a statement by DOL that fiduciaries' duty to act prudently includes addressing cybersecurity risks.

Depending on the circumstances, the review of service agreements might include, for example, commitments by the service provider to take one or more of the following steps:

- Maintain a program that meets specified standards, such as those articulated by DOL through guidance or otherwise.
- Regularly undertake outside reviews of its practices and procedures and provide reports generated by those reviews to the plan.
- Promptly notify the plan of any breaches or security incidents in a timely fashion and inform the plan of steps being taking to investigate and remediate those breaches.

---

[84] Council Hearing of Sept. 9, 2022, *supra* note 59, at 231-32.

[85] Adam Beck, *Cybersecurity in the Context of Health and Welfare Benefit Plans* 9 (Sept. 9, 2022) (written statement submitted to the ERISA Advisory Council on behalf of America's Health Insurance Plans (AHIP)), https://www.dol.gov/sites/dolgov/files/EBSA/about-ebsa/about-us/erisa-advisory-council/2022-cybersecurity-issues-affecting-health-benefit-plans-ahip-written-statement-09-09.pdf; AHIP, *Health Plan Cybersecurity Presentation* 10-11 (Sept. 9, 2022) (suggesting that DOL consider issuing a request for information on the subject), https://www.dol.gov/sites/dolgov/files/EBSA/about-ebsa/about-us/erisa-advisory-council/2022-cybersecurity-issues-affecting-health-benefit-plans-ahip-written-statement-presentation-09-09.pdf.

[86] Council Hearing of Sept. 9, 2022, *supra* note 59, at 227-28. Similarly, in the case of defined contribution pension plans, experts noted a distinction between large and small plans in their approaches to dealing with data security service providers, with large plans being more sophisticated. Council Hearing of July 19, 2022, Transcript of Testimony of Richard S. Betterley, Betterley Risk Consultants, Inc., at 93. And when it comes to the related issue of cybersecurity insurance, the Council was told that small plans rely on the coverage of recordkeepers or other service providers. Timothy Marlin, *Statement*, at 4 (Sept. 9, 2022) (written statement submitted to the ERISA Advisory Council on behalf of Marsh & McLennan Cos.) (observing that smaller companies often "outsource plan administration and rely on their fiduciary insurance and the cyber, professional liability, and other coverages that could potentially respond to a cyber event that impacts the provider"), https://www.dol.gov/sites/dolgov/files/EBSA/about-ebsa/about-us/erisa-advisory-council/2022-cybersecurity-insurance-and-employee-benefit-plans-written-statement-marlin-09-09.pdf.

- Provide proof of adequate insurance covering cyber breaches.
- Confirm whether any contractual provisions would limit the provider's liability to the plan, via indemnification rights, inadequate insurance policy limits, or otherwise.

In so doing, DOL should recognize that small and medium-sized plans may have limited ability to negotiate these terms.

The Council also noted that existing DOL guidance for health plan fiduciaries might create the impression that their fiduciary duties do not include ensuring cybersecurity risks are adequately addressed by service providers. The September 2021 version of M*eeting Your Fiduciary Responsibilities*, the core DOL compliance education publication for retirement plans, advises fiduciaries to ask service providers about "information security standards, practices and policies, and annual audit results available to plan clients; how it validates its practices; and whether it has insurance policies that cover losses caused by cybersecurity and identity theft breaches (whether caused by internal or external threats)" and cites the 2021 guidance on its list of resources for employers.[87] In contrast, the current health plan fiduciary counterpart, *Understanding Your Fiduciary Responsibilities under a Group Health Plan,* is silent on the issue,[88] raising some question about how or whether health plan fiduciaries need to attend to cyber risks presented by service provider information handling.

The Council is convinced that careful contracting with and ongoing monitoring of TPAs, insurers, and other service providers is an integral — indeed, indispensable — component of benefit plan cybersecurity (see Recommendation 2). While most large plans have the ability to get this information, smaller plans may not. To ensure that all health plans have access to the information needed to make prudent decisions concerning service provider selection and contracting and assist plan fiduciaries in evaluating the propriety of additional safeguards, the Council discussed additional steps beyond DOL clarifying the scope of fiduciaries duty to act prudently with respect to service provider selection and monitoring and cybersecurity. The Council considered, but set aside, a recommendation

[87] U.S. Department of Labor, Employee Benefits Security Administration, *Meeting Your Fiduciary Responsibilities* 5, 13 (Sept. 2021), https://www.dol.gov/sites/dolgov/files/EBSA/about-ebsa/our-activities/resource-center/publications/meeting-your-fiduciary-responsibilities.pdf.

[88] U.S. Department of Labor, Employee Benefits Security Administration, *Understanding Your Fiduciary Responsibilities Under a Group Health Plan* 4-6 (Sept. 2019), https://www.dol.gov/sites/dolgov/files/ebsa/about-ebsa/our-activities/resource-center/publications/understanding-your-fiduciary-responsibilities-under-a-group-health-plan.pdf.

that DOL consider requiring disclosure of health plan service providers' practices and performance on cybersecurity matters to facilitate the selection and monitoring of service providers.

As discussed by the Council, regulations could require that any service provider with access to plan participants' PII or PHI must inform plan fiduciaries of its cybersecurity practices and experience at regular intervals. This disclosure mandate could be modelled on the fee disclosure rule issued under ERISA §408(b)(2), specifically, 29 CFR § 2550.408b-2(c)(1) (effective 2012).[89] That is, a regulation could prescribe that a contract with a service provider that has or will have access to a plan participant's or beneficiary's PHI or PII is not a reasonable contract or arrangement unless the contract requires that the service provider inform plan fiduciaries of its cybersecurity practices and experience before contracting and at regular intervals or upon appropriate occasions thereafter. Such a disclosure rule should include safeguards to prevent public dissemination of information that might compromise cybersecurity. Rulemaking of this sort was suggested by one witness.[90] While no members of the Council felt they were equipped with sufficient information to recommend rulemaking on this subject, some believed the issue is important enough to warrant serious consideration of that action. The Council did not move forward with this recommendation for a variety of reasons, including a belief that this issue was not sufficiently ripe for action. Further, some Council members questioned whether DOL has the authority to issue a rule requiring this disclosure.

The Council heard testimony from a variety of witnesses explaining the need for additional guidance for small and medium-sized health plans regarding how to address cybersecurity. However, after some discussion it was decided that this concern is adequately addressed by Recommendations 2 and 6 below.

Although the Council heard testimony from HHS that awareness of the HIPAA security rule is "fairly broad" even among small health care providers, HHS's presentation to the Council also noted recurring security compliance problems of a serious nature, suggesting awareness too often does not

[89] The fee disclosure mandate was extended to group health plans by the Consolidated Appropriations Act, 2021, Pub. L. No. 116-260, Div. BB, § 202, which added ERISA § 408(b)(2)(B), 29 U.S.C. § 1108(b)(2)(B). The statute tracks the DOL's pension plan fee disclosure rule closely. So closely, in fact, that EBSA announced in Field Assistance Bulletin 2021-03, Q&A-8 (Dec, 30, 2021), https://www.dol.gov/agencies/ebsa/employers-and-advisers/guidance/field-assistance-bulletins/2021-03, that it "does not believe that comprehensive implementing regulations are needed."

[90] Carol Buckmann, *Testimony on Health Plan Cybersecurity Issues* 4 (Sept. 9,2022) (written statement submitted to the ERISA Advisory Council), https://www.dol.gov/sites/dolgov/files/EBSA/about-ebsa/about-us/erisa-advisory-council/2022-cybersecurity-issues-affecting-health-benefit-plans-buckmann-written-statement-09-09.pdf; Council Hearing of Sept. 9, 2022, *supra* note 59, at 222.

translate into critical data security practices.[91] The Council also heard testimony from a private-sector cybersecurity expert that many organizations have not implemented the controls (i.e., the processes, policies, devices, practices, or other actions that modify risk) needed to defend against current cybersecurity threats.[92] Further, the Council heard testimony that while awareness among health plan sponsors of the need to investigate service provider cybersecurity policies and practices is higher than among retirement plan sponsors, it is still not enough.[93] That same witness recommended there be "a lot more information and awareness with the broader benefits plan community about the need" and that DOL needs to actively engage plan sponsors and others on cybersecurity.[94]

Witnesses identified small and medium-sized plans and plan sponsors as deserving a special focus in education and outreach efforts. One witness stated small and mid-sized employers need additional compliance tools and information about what DOL looks for in investigations given they often lack the internal expertise and have less familiarity with good cybersecurity practices and where to find help to develop them.[95] That same witness remarked that there is a "great deal of confusion" about which plans are covered by HIPAA's security standard and other requirements.[96] The Council received a statement from another witness suggesting that the Council recommend that DOL "begin educational outreach to help smaller and mid-sized self-funded health and welfare plans understand the risks and benefits to promote building cyber protections into their business operations."[97]

Witnesses also recommended DOL collaborate and coordinate its education and outreach efforts with other federal agencies and entities with leading roles on cybersecurity. Suggested partner

---

[91] Council Hearing of Sept. 8, 2022, Transcript of Testimony of Nicholas P. Heesters, Jr., U.S. Dep't of Health and Human Services, Office of Civil Rights, at 52; Nicholas P. Heesters, Jr., HIPAA Security Rule, Breach Notification, and Cybersecurity 53 (Sept. 8, 2022) (written presentation submitted to the Council on behalf of the U.S. Dep't of Health and Human Services, Office of Civil Rights), https://www.dol.gov/sites/dolgov/files/EBSA/about-ebsa/about-us/erisa-advisory-council/2022-cybersecurity-issues-affecting-health-benefit-plans-heesters-written-statement-09-08.pdf.

[92] Council Hearing of Sept. 9, 2022, *supra* note 46, at 192 (stating that "[m]any organizations do not have the right set of controls for threat or theft or to quarantine" when a breach occurs).

[93] *Id.* at 198 (stating that about 75% of Fidelity health benefit plan clients audit Fidelity on cybersecurity every two years, compared to about 50% of retirement plan clients and commenting that all health plans should do it).

[94] *Id.* at 200.

[95] Council Hearing of Sept. 9, 2022, *supra* note 59, at 212-13.

[96] *Id.* at 215.

[97] Adam Beck, AHIP Statement for the Record before the U.S. Department of Labor ERISA Advisory Council: Cybersecurity in the Context of Health and Welfare Benefit Plans 9 (Sept. 9, 2022) (written statement submitted to the ERISA Advisory Council on behalf of AHIP), https://www.dol.gov/sites/dolgov/files/EBSA/about-ebsa/about-us/erisa-advisory-council/2022-cybersecurity-issues-affecting-health-benefit-plans-ahip-written-statement-09-09.pdf.

organizations include HHS, the U.S. Department of Homeland Security, CISA, and the Healthcare and Public Health Sector Coordinating Council.[98]

In considering recommendations that DOL expand its education and outreach to address health plan cybersecurity, the Council took note of DOL's existing education and outreach programs. Providing compliance education and outreach to employers and the regulated community is already a core component of DOL's strategy for promoting ERISA compliance.[99] The Department holds education and outreach events, such as in-person sessions and webinars. In Fiscal Year (FY) 2022, it held more than 1,640 events, including 340 compliance assistance activities.[100] It provides pamphlets, fact sheets, frequently asked questions, and other tools, which are distributed electronically through DOL's website and in print by mail in response to individual requests. In FY 2022, 168,435 publications were distributed, and there were 7.94 million visitors to the EBSA website.[101] DOL also works cooperatively with private- and public-sector organizations such as the AICPA and the NAIC.[102] Further, DOL partners with community-based organizations, especially to educate small business owners about ERISA's requirements, and sees that, among other education efforts, as "an effective way to create broad-based compliance."[103]

DOL already is doing cybersecurity education for retirement plan fiduciaries, sponsors, and advisers. Its 2021 cybersecurity guidance is featured on its own web landing page, "Cybersecurity," as part of the broader "Retirement Benefits" key topic.[104] At least since the release of that guidance, DOL also has integrated cybersecurity into some of its other retirement plan compliance assistance content. For example, the *Best Practices* and *Tips* are featured among the employer and adviser "General Compliance Assistance" resources for retirement plans.[105] DOL also has integrated information about

---

[98] Council Hearing of Sept. 9, 2022, *supra* note 46, at 205-06; Council Hearing of Sept. 9, 2022, *supra* note 72, at 163.

[99] U.S. Department of Labor, Employee Benefits Security Administration, *FY 2023 Congressional Budget Justification: Employee Benefits Security Administration* 22, 26-27, https://www.dol.gov/sites/dolgov/files/general/budget/2023/CBJ-2023-V2-01.pdf.

[100] U.S. Department of Labor, Employee Benefits Security Administration, *Fact Sheet: EBSA Restores Over $1.4 Billion to Employee Benefit Plans*, Participants and Beneficiaries (Dec. 12, 2022), https://www.dol.gov/sites/dolgov/files/EBSA/about-ebsa/our-activities/resource-center/fact-sheets/ebsa-monetary-results.pdf.

[101] *Id.*

[102] U.S. Department of Labor, *supra* note 99, at 24.

[103] *Id.* at 24.

[104] https://www.dol.gov/agencies/ebsa/key-topics/retirement-benefits/cybersecurity (accessed Nov. 17, 2022).

[105] U.S. Department of Labor, Employee Benefits Security Administration, *Retirement Plans,* https://www.dol.gov/agencies/ebsa/employers-and-advisers/plan-administration-and-compliance/retirement (accessed Nov. 17, 2022).

cybersecurity into its core publication for retirement plan fiduciaries, *Meeting Your Fiduciary Responsibilities*. That booklet includes summary information about the prudent selection and monitoring of third-party service providers responsible for maintaining plan records and keeping participant data confidential and plan accounts secure and provides links to the 2021 cybersecurity guidance.[106]

Although DOL also provides materials and programs targeted to health plan fiduciaries and sponsors, that content does not appear to address cybersecurity issues. For example, the core publication for health plan fiduciaries, *Understanding Your Fiduciary Responsibilities Under a Group Health Plan*, does not address cybersecurity issues.[107] While DOL content does address HIPAA, mentions of it are focused exclusively on the HIPAA portability, nondiscrimination and related provisions enforced by DOL.[108] It does not address HIPAA's security standard and related requirements.

V. RECOMMENDATIONS AND RATIONALES

1. **We recommend that DOL make explicit that, although cybersecurity risks may never be completely eliminated, acting prudently with regard to cybersecurity risks is a responsibility of fiduciaries of all employee benefit plans, not just pension plans.**

Rationale: Pursuant to ERISA Section 404(a)(1)(B), plan fiduciaries are required to discharge their duties with respect to a plan "with the care, skill, prudence, and diligence under the circumstances then prevailing that a prudent man acting in a like capacity and familiar with such matters would use in the conduct of an enterprise of a like character and with like aims." Cyberattacks on entities, including, group health plans are an on-going problem. There have been successful cyberattacks on major health care providers that provide or administer benefits for group health plans. Given these prevailing circumstances and as a component of the obligation of prudence, fiduciaries of group health plans must use reasonable efforts to implement cybersecurity practices that will seek to avoid such victimization.

Although DOL has implied in its *Best Practices* that adopting prudent practices as to cybersecurity is a fiduciary duty, at least for pension plans, it has not stated explicitly that this is a

[106] U.S. Department of Labor, *supra* note 87, at 5, 13.
[107] U.S. Department of Labor, *supra* note 88.
[108] *E.g.*, *Id.* at 13; U.S. Department of Labor, Employee Benefits Security Administration, *FAQs on HIPAA Portability and Nondiscrimination Requirements for Employers and Advisers*, https://www.dol.gov/sites/dolgov/files/EBSA/about-ebsa/our-activities/resource-center/faqs/hipaa-compliance.pdf.

fiduciary duty. Expressly stating the general principle, it is hoped, would avoid a problem with the 2021 guidance: Some of the confusion concerning the scope of *Best Practices* seems to stem from its failure to emphasize at the outset that the "obligation to ensure proper mitigation of cybersecurity risks" is not a new duty, but rather is merely a specific application of the general obligation of prudence. Taking this step aligns with specific recommendations made by some witnesses.[109]

2. **We recommend DOL make clear that the fiduciary duty to act prudently with regard to cybersecurity risks includes the duty of health plan fiduciaries to ascertain that their health plan service providers have practices and procedures in effect to deal with such risks. This would include, but not necessarily be limited to, including this in a change to DOL's core publication for health plan fiduciaries, *Understanding Your Fiduciary Responsibilities Under a Group Health Plan*.**

Rationale: Like the first recommendation above, this recommendation emphasizes the important general principle involved: Prudence demands attention to cyber practices of service providers storing or using plan information. In contrast, specific compliance guidance, such as DOL's 2021 *Tips*, offers more granular advice on implementing or operationalizing the general principle. As with the first recommendation, this one aligns with specific recommendations made by some witnesses.[110]

This recommendation expressly applies only to "health plan fiduciaries." In part, that is because of the incongruity between existing EBSA publications (as discussed above in the Observations section), which raises some question about how or whether health plan fiduciaries need to address cyber risks presented by service provider information handling. This recommendation puts any such doubt to rest and highlights an important ambiguity that should be eliminated. It also reflects the focus of this issue group.

Some Council members did not support this recommendation. Some believed it is covered by the first recommendation calling for guidance stating that acting prudently with regard to cybersecurity risks is a responsibility of fiduciaries of all employee benefit plans. Some believed it also is covered by the

[109] Council Hearing of July 19, 2022, *supra* note 62, at 9 (calling for DOL to "formally clarify[] that mitigating cybersecurity risk is a fiduciary responsibility under ERISA…[to] help ensure that plan fiduciaries are clear about their responsibilities" after noting that DOL has already "issued best practices for protecting PII, and financial data"); Council Hearing of Sept. 9, 2022, *supra* note 59, at 220 ("[T]here should be a regulation that clarifies the fiduciary responsibilities of plan sponsors and other internal company fiduciaries in connection with cybersecurity.")

[110] *Id.*

next recommendation calling for DOL to clarify that DOL's *Tips* guidance applies to health plans and that any added statement by DOL about this duty risked creating confusion or being incongruent with the *Tips*. Some were concerned that this recommendation's application only to health plans could be misinterpreted to suggest that the same duty does not exist for fiduciaries of pension plans and other employee benefit plans, while others expressed concern that because the basic principle addressed by this recommendation applies broadly to all ERISA-covered employee benefit plans, this recommendation fell beyond the scope of the working group's charge.

Because modern health plans overwhelmingly deliver benefits by contracting with a health insurance company (either as an insurer or TPA) and do not themselves administer benefits, most of the security risk lies with TPAs, insurers, and other service providers. The reality that cybersecurity risks reside predominately with service providers persuaded a majority of the Council that it would be useful to specifically highlight the need for plan fiduciaries to prudently select and monitor service providers with respect to their posture and practices on this dimension. Some Council members did not support this recommendation.

3. **We recommend DOL clarify that the *Cybersecurity Program Best Practices* and *Tips for Hiring a Service Provider with Strong Cybersecurity Practices* apply to health benefit plan fiduciaries.**

Rationale: The Council heard testimony from multiple witnesses that plan fiduciaries and their advisers of all sizes are unclear about whether the *Best Practices* and *Tips* apply to health plans. Uncertainty about this was reinforced by information provided by DOL that stakeholders have inquired about their applicability and the Council's noting how plan advisers have communicated to their clients about them. The Council also heard testimony from multiple witnesses recommending DOL clarify whether this guidance applies to health plans. Further, witnesses indicated that some health plan fiduciaries are already using the 2021 guidance to assess their cybersecurity practices and those of their service providers and that they find the guidance to be useful in this regard. Some Council members did not support this recommendation.

4. **We recommend that DOL indicate the extent to which compliance with HIPAA and HITECH satisfies any of the recommended practices in *Best Practices* and *Tips*.**

Rationale: There is broad familiarity with HIPAA and HITECH and the requirements of the security standard among health plans and their advisers. Though compliance with those requirements is far from perfect, health plans, insurers, and their service provider-business associates generally have taken steps to implement them. Several witnesses noted the overlap between the requirements of these laws and DOL's 2021 guidance. DOL would facilitate compliance with health plan fiduciaries' duties to act prudently with regard to cybersecurity risks by highlighting the extent to which compliance with HIPAA requirements addresses practices recommended in DOL guidance. A Council member did not support this recommendation.

The Council considered, but set aside, a recommendation that DOL also clarify that compliance with HIPAA and HITECH does not necessarily constitute compliance with ERISA. Although the Council heard testimony that compliance with HIPAA and HITECH provides just a baseline of protection and not enough to protect against some cybersecurity threats, it did not receive testimony or information detailing specific ways in which HIPAA and HITECH fall short of what ERISA requires. In light of this, the Council determined that this important issue requires further study before recommending DOL provide guidance on it.

5. **We recommend DOL review, on a regular and timely basis and update, if necessary, the Best Practices and Tips so that they reflect changes in those practices in light of the evolving nature of cybersecurity threats.**

Rationale: Witnesses testified that the cybersecurity environment is constantly changing and becoming more complex. Cybersecurity threats are constantly evolving, with criminals regularly changing tactics and targets. Technology advances often result in more complex digital environments, introducing new vulnerabilities to exploit. Regularly scheduled reviews and updates are consistent with the *Best Practices* and *Tips* themselves. These recommend annual risk assessments by plan sponsors "facilitate the revision of controls resulting from changes in technology and emerging threats." If this recommendation is not implemented, the *Best Practices* could become irrelevant, not useful, or even misleading. A Council member did not support this recommendation.

6. **We recommend DOL provide education and materials to health plan sponsors and fiduciaries to assist them in understanding and carrying out these duties. This might include:**

a. **Specific tailored and targeted educational programs and materials to inform plan sponsors and fiduciaries about their ongoing responsibilities and obligations related to cybersecurity (e.g., educational meetings and outreach and publishing sample materials, such as model cybersecurity provisions for service provider agreements) and also could be integrated into existing materials, such as *Understanding Your Fiduciary Responsibilities Under a Group Health Plan*, and programs, such as DOL's Health Benefits Education Campaign components that address compliance.**
b. **Informing plan sponsors and fiduciaries of materials available from other agencies, such as the HIPAA SRA Tool which is designed to assist small-to medium-sized organizations. DOL also should consider updating its Outreach, Education and Assistance Program strategic plan to include health plan cybersecurity as a priority topic for its educational programs and outreach.**

To more effectively reach small and medium-sized plan fiduciaries and sponsors who are more likely to be unaware of existing cybersecurity guidance, DOL should consider sending communications targeting them by using DOL's database of Form 5500 filings or otherwise.

Rationale: While awareness of cybersecurity issues and implementation of protective measures is generally considered to be better among health plan sponsors and fiduciaries than those for retirement plans, witnesses testified that they are insufficient and important gaps exists. Gaps are especially apparent among small and medium-sized plans, which are much less likely to have staff dedicated to addressing cybersecurity and ready access to outside advisers. Witnesses suggested the need for additional education and awareness activities as a means to improve compliance.

DOL has a longstanding compliance education and outreach program for plan sponsors and other fiduciaries. Cybersecurity for retirement plans has already been integrated into it. Further, DOL's compliance education program prioritizes smaller plans. Incorporating content and programming targeting health plan fiduciaries, including those of small plans should be relatively straightforward.

Although DOL's education outreach program is robust, the Council considered the challenges in reaching the sponsors and other fiduciaries of all two million ERISA-covered health plans, especially those most likely to need compliance education. For that reason, the Council is recommending DOL consider direct outreach to plan sponsors using the contact information provided in Form 5500 filings.

DOL could target outreach by plan size, such as those in which the number of plan participants is below a certain level. The Council recognizes that this still will not enable DOL to reach the many small plans that are not required to file a Form 5500.

Some Council members did not support this recommendation. Some expressed concerns that DOL or others might seek to enforce compliance with education guidance as if it were a rule established through notice and comment rulemaking, or other formal guidance (e.g., field assistance bulletins or interpretive bulletins). Other Council members disagreed with this as a concern and recognized the important role DOL's compliance education programs and materials play in helping plan fiduciaries comply with ERISA's duties and act in the best interests of participants and beneficiaries.