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

March 6, 2025

***Submitted Electronically via:*** ***www.regulations.gov***

U.S. Department of Health and Human Services
Office for Civil Rights
Attention: HIPAA Security Rule NPRM – RIN Number 0945–AA22
Hubert H. Humphrey Building
Room 509F
200 Independence Avenue, SW
Washington, DC 20201

**RE: Comments on the Proposed Amendments to HIPAA's Security Rule and the Requirement to Obligate Plan Sponsors to Comply With the Proposed Security Requirements**

To Whom It May Concern:

The ERISA Industry Committee ("ERIC") respectfully submits the following comments in response to the Notice of Proposed Rulemaking, setting forth proposed requirements intended to better protect the confidentiality, integrity, and availability of electronic protected health information ("ePHI") and increase the cybersecurity for ePHI by revising HIPAA's Security Rule. The Department of Health and Human Services (the "Department") also proposes to require a plan sponsor to include additional information in their group health plan document that would obligate the plan sponsor to comply with HIPAA's Security Rule and adopt the proposed security requirements.

ERIC is the only national trade association that advocates exclusively on behalf of large employers on health, retirement, and compensation public policies on the federal, state, and local levels. ERIC's member companies offer comprehensive group health benefits to their employees in compliance with the myriad federal laws including the Internal Revenue Code ("Code"), the Employee Retirement Income Security Act ("ERISA"), and the Public Health Service ("PHSA"). ERIC supports the ability of its large employer member companies to tailor retirement, health, and compensation benefits to meet the unique needs of their workforce, providing benefits to millions of workers, retirees, and their families across the country.

## COMMENTS

### I. Arbitrary and Unauthorized: The Department Cannot Require the Plan Document to Obligate a Plan Sponsor to Comply With HIPAA's Security Rule and Adopt the Proposed Security Requirements

Whether intended or not, this proposed rule is a back-door way of requiring plan sponsors to comply with the HIPAA Security Rule and adopt all the proposed security requirements.

As the Department rightly points out, plan sponsors are ***not*** directly liable for compliance with the HIPAA Security Rule because plan sponsors are ***not*** "regulated entities" (i.e., they are not a "covered entity" or a "business associate").[1]

As the Department also ***correctly*** points out, the HIPAA statute and corresponding regulations require plan sponsors to include specific information in their plan document,[2] which is intended to ensure that when the plan sponsor is handling PHI and ePHI, the plan sponsor is well aware that they must take action to keep ePHI secure or be subject to penalties under HIPAA. For example, plan sponsors must implement safeguards that reasonably and appropriately protect the confidentiality of ePHI, ensure that individuals handling ePHI agree to follow these safeguards, and notify the group health plan of any security breach the sponsor becomes aware of.[3]

However, the Department is ***incorrect*** in assuming that plan sponsors are not reasonably and appropriately protecting the confidentiality of ePHI,[4] which is an assumption that appears to be the motivation behind the Department's efforts to impose the HIPAA Security Rule and new security requirements on plan sponsors through this proposed rule. As stated, plan sponsors must already have safeguards in place to protect ePHI, and plan sponsors have already deployed robust cybersecurity programs[5] – not only to protect ePHI, but to keep other personally identifiable information ("PII") confidential in accordance with a myriad of State and Federal privacy laws, along with industry standards.[6]

Importantly, an "assumption" is ***no*** legal basis for subjecting plan sponsors to HIPAA's Security Rule and the proposed security requirements, especially when the HIPAA statute does ***not*** require direct compliance with the Security Rule.

Moreover, a court of law would ***never*** allow this Department to use another Federal law that they do ***not*** have jurisdiction over as the means for forcing compliance with HIPAA's Security Rule and adoption of the proposed security requirements.

---

[1] *See* 90 Fed. Reg. 898, 983 (Jan. 6, 2025).
[2] *Id*.; *see also*, 45 CFR 164.315(b)(1).
[3] *See* 45 CFR 164.315(b)(2).
[4] *See* 90 Fed. Reg. at 983 (Jan. 6, 2025).
[5] By way of example, virtually all plan sponsors obtain cybersecurity insurance as a risk mitigation tool to protect against any attack on their electronic systems. When obtaining cybersecurity insurance, the plan sponsor must undergo an extensive review of the sponsor's risk management programs, security systems and policies, along with incident response plans before a cybersecurity insurance policy can even be issued. For purposes of renewing such cybersecurity insurance coverage (or obtaining new coverage through a different distribution channel), the plan sponsor must undergo a rigorous audit of their existing programs and policies each year.
[6] The Department actually acknowledges that plan sponsors have already implemented the CISA Cross-Sector Cybersecurity Performance Goals to protect their existing electronic information systems to protect PII, as well as ePHI, which the Department admits is "consistent with the Security Rule and the proposed security requirements." *See* 90 Fed. Reg. at 984 (Jan. 6, 2025). So, if the proposed security requirements are consistent with existing safeguards plan sponsors have in place, why mandate that plan sponsors must implement the proposed security requirements?

More specifically, the Department proposes to require plan sponsors to include additional information in the plan document that would ***obligate*** plan sponsors to comply with HIPAA's Security Rule and adopt the proposed security requirements. But, as noted above, plan sponsors are ***not*** required by the HIPAA statute to comply with the Security Rule, and by extension, the proposed security requirements. However, as a back-door way of requiring such compliance with HIPAA's Security Rule and adoption of the proposed security requirements, the Department is using the Employee Retirement Income Security Act ("ERISA"), a Federal law that this Department does ***not*** have jurisdiction over (note, the Department of Labor (DOL) is the appropriate Federal Department that has jurisdiction over ERISA).

ERISA requires plan sponsors to administer their group health plan in accordance with the plan document.[7] ERISA also provides that if a plan sponsor ***does not*** administer their plan in accordance with the plan document, the plan sponsor ***would be*** subject to fiduciary liability[8] and potential monetary penalties imposed by the DOL.[9]

For example, if (1) this proposed rule is finalized thereby requiring amendments to the plan document to ***obligate*** the plan sponsor to adopt all the proposed security requirements, and if (2) the plan sponsor ***does not*** adopt all of the proposed security measures, the plan sponsor would ***breach*** their fiduciary duty and expose themselves to potential penalties under ERISA.

This Department is effectively using ERISA – and ERISA's fiduciary liability provisions – as the means for ***obligating*** plan sponsors that are not otherwise required by the HIPAA statute to comply with the Security Rule and adopt all the proposed security requirements.[10]

Congress can change the HIPAA statute to require plan sponsors to comply with the Security Rule and adopt the proposed security requirements. But, in the absence of Congressional action, this Department does ***not*** have the authority to ***obligate*** plan sponsors to comply with the Security Rule and adopt the proposed security requirements through regulations, and especially by leveraging ERISA.

---

[7] Section 404(a)(1)(D) of the Employee Retirement Income Security Act ("ERISA").
[8] *See, e.g.,* ERISA section 502(a)(2), (3), (5) and (6).
[9] *See* ERISA section 502(l) penalties and related DOL enforcement activities.
[10] Importantly, the DOL is already using ERISA's fiduciary provisions to require plan sponsors to implement robust cybersecurity programs to protect all PII, including ePHI. *See* Employee Benefits Security Administration, *Compliance Assistance Release No. 2024-01* at https://www.dol.gov/agencies/ebsa/key-topics/retirement-benefits/cybersecurity/compliance-assistance-release-2024-01. In addition, the DOL has already begun – and will continue to – audit plan sponsors and investigate the steps taken to mitigate their health plans' cybersecurity risks. So, even if this Department had the authority to obligate plan sponsors to comply with the proposed security requirements (which as discussed above, this Department does not), there is a level of overlap and duplication between two Federal Departments that is unnecessary and extremely costly for the Federal government and both public and private sector plan sponsors.

## II. Significant Administrative and Cost Burden: The Department Underestimates the Feasibility of Compliance, Along With the Upfront and Ongoing Costs

The cost of employer-sponsored health coverage for a family exceeded $25,000 in 2024.[11] In response to this finding, the President and CEO of the Kaiser Family Foundation stated, "***Employers are shelling out the equivalent of buying an economy car for every worker every year to pay for family coverage***."[12] Such a profound statement underscores the exceedingly high costs plan sponsors face when offering health coverage to their employees and their family members, and health care costs continue to rise unabated.

Regarding this proposed rule, the Department's estimates reveal that the ***mandate***[13] for complying with HIPAA's Security Rule and adopting the proposed security requirements would add $4.6 billion in the first year of implementation to the cost of providing employer-sponsored health coverage.

However, we believe that the Department ***underestimates*** the cost burden for plan sponsors and that the upfront costs would ***exceed*** the estimated $4.6 billion in the first year of implementation. For example, in most if not all cases, amendments to plan documents are prepared by retained ERISA attorneys. While the hourly billing rate varies for those ERISA attorneys drafting the plan amendments, the hourly rate for these attorneys is much, much higher than the rate of $111.08 that the Department uses to develop its $4.6 billion cost estimate. This effectively means that the higher hourly rate for amending a plan document as mandated under this proposed rule will certainly inflate the initial estimate of $4.6 billion for adopting and implementing the proposed security requirements.

Additionally, the cost burden would ***not end after the first year***. This proposed rule would require plan sponsors to conduct periodic audits to assess whether the plan sponsor is complying with HIPAA's Security Rule and the proposed security requirements. Conducting compliance audits periodically (e.g., annually) costs money whereas the plan sponsor must hire a HIPAA compliance firm to conduct the audit. Then, there is cost associated with working hours of the plan sponsor's workforce allocating their time and resources to (1) coordinating with the HIPAA compliance firm, (2) monitoring the compliance firm's activities, and (3) ultimately determining whether the findings of the audit confirm that the plan sponsor remains compliant with the proposed security requirements. Again, all of this costs money, time, and resources, which are costs that would be added to the already out-sized $4.6 billion estimate for adopting and implementing the proposed security requirements.

---

[11] *See* Kaiser Family Foundation ("KFF"), *2024 Employer Health Benefits Survey* at https://files.kff.org/attachment/Employer-Health-Benefits-Survey-2024-Annual-Survey.pdf.

[12] Quote from Drew Altman, President and CEO of KFF at https://www.kff.org/health-costs/press-release/annual-family-premiums-for-employer-coverage-rise-7-to-average-25572-in-2024-benchmark-survey-finds-after-also-rising-7-last-year/.

[13] The Department refers to these proposed requirements a "mandate" on plan sponsors. *See* 90 Fed. Reg. at 1000 (Jan. 6, 2025). As we have pointed out in numerous comment letters, this Department cannot impose mandates on self-insured health plans. ERIC response to "Requirements Related to the Mental Health Parity and Addiction Equity Act (EBSA-2023-0010-0001)" (October 17, 2023).

The above-stated example (i.e., conducting periodic audits) is just one example of the costs plan sponsors would incur in future years. Several other examples would add significant dollars to these ongoing costs (e.g., routinely updating the technology asset inventory and network map; conducting and documenting a comprehensive risk assessment; and producing annual written verification that the plan's business associates have adopted and implemented the proposed security requirements).

As discussed above, incurring these ongoing costs would solely be a result of this Department using a Federal law that they do ***not*** have jurisdiction over (ERISA) to ***obligate*** plan sponsors to comply with HIPAA's Security Rule and adopt the proposed security requirements. By using ERISA – and ERISA's fiduciary liability provisions – the Department would effectively force plan sponsors to (1) spend billions for ongoing compliance with the proposed security requirements or (2) face fiduciary liability and potential penalties under ERISA. A lose-lose proposition that would ultimately hurt plan participants and their families.

The Department also ***underestimates*** the complexity of compliance with the proposed security requirements. For example, even a 180-day compliance transition period is unattainable for any entity subject to the proposed rule. In addition, requiring the restoration of electronic information systems within 72 hours after a breach is arbitrary, unrealistic, and could introduce additional risk into the recovery process. Conducting audits, risk assessments, and document reviews annually is not only costly (as discussed above), but they are so resource-intensive that completing any one of these tasks (let alone completing all these tasks) within a year is unachievable. As a result, the Department should withdraw these proposed rules, and instead engage in a dialogue with covered entities, business associates, as well as plan sponsors to more efficiently and effectively develop rules to protect confidentiality, integrity, and availability of ePHI.

***

Thank you in advance for considering these comments. Please do not hesitate to contact me at 202-789-1400 or jgelfand@eric.org with any questions or if we can serve as a resource on these very important issues.

Sincerely,

James P Gelfand

James P. Gelfand
President & CEO