PEOs Need to Prepare for Increased Cybersecurity Requirements Thanks to Proposed HIPAA Security Rule Revisions

Insights
1.08.25

With the HIPAA Security Rule set to undergo a massive overhaul to boost cybersecurity protections, PEOs need to take note. After all, as stewards of worksite employee and client company data – and as sponsors of group health plans – PEOs will be greatly impacted by the revised requirements for data classification, security, contractual requirements, and operational workflows. PEOs face unique challenges and should therefore pay close attention to these potential regulatory changes from the Department of Health and Human Services (HHS).

Proposed Rule in a Nutshell

Earlier this week, HHS published a proposed rule aimed at securing the confidentiality and integrity of electronic protected health information (ePHI) in response to growing breaches and cyberattacks against healthcare organizations and other keepers of confidential data. Thanks to the significant increase in cyberattacks against healthcare data, the agency is proposing to enhance protections for ePHI by implementing robust cybersecurity requirements and addressing the increasing sophistication of cyberattacks.

You can read a full review of the proposed changes in our comprehensive Insight here. Some key changes include:

- Making all cybersecurity obligations **mandatory**, eliminating the exception that allowed some rules to be ignored if not appropriate in certain circumstances.
- Requiring covered entities to create and maintain a **written inventory of technology assets and a network map** that tracks the movement of ePHI through its electronic systems.
- Mandating that covered entities develop a **detailed written risk assessment** that identifies reasonably anticipated threats and potential vulnerabilities.

This is just the tip of the iceberg. Our Insight provides an in-depth summary that we suggest you review.

Why Should PEOs Care?

Given the extent of these proposed changes, PEOs that are considered covered entities should familiarize themselves with the new rules and requirements. If the rule is finalized as proposed, you must be prepared to:

- Ensure proper classification of data in your possession and map all ePHI workflows;
- Implement advanced security measures to safeguard ePHI within health plan documents and ensure agent compliance;
- Monitor and address emerging cybersecurity threats; and
- Evaluate third parties that qualify as business associates, and review and inventory business associate agreements.

While PEOs should always strive to maintain an excellent compliance and security posture, you should especially consider efficiency and scalability issues when preparing to implement any necessary changes. And, of course, you will need to reevaluate your PEO's current HIPAA compliance practices to ensure you are in line with the proposed changes.

What's Next?

As explained in our Insight, the proposed rule is now open for public comments by interested parties until March 7. If your PEO is interested in taking part in the conversation and submitting comments, consider contacting your Fisher Phillips PEO attorney or FP Advocacy to assist with any rulemaking comments.

Conclusion

Fisher Phillips will continue to monitor developments and provide updates as warranted, so make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information direct to your inbox. For further information, contact your Fisher Phillips attorney, the authors of this Insight, or any attorney on the firm's PEO Advocacy and Protection Team. You can also rely on our Data Protection and Cybersecurity Team for guidance and support.

Related People

Usama Kahf, CIPP/US
Partner
949.798.2118
Email

Anne Yarovoy Khan
Of Counsel
949.798.2162
Email

Daniel Pepper, CIPP/US
Partner
303.218.3661
Email

Service Focus

Privacy and Cyber

Data Protection and Cybersecurity

Employee Benefits and Tax

Industry Focus

PEO

Healthcare