Brown & Brown

EMPLOYEE BENEFITS

HHS Office of Civil Rights Releases Proposed Rules under the HIPAA Security Rule

Background

In 1996, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) was enacted to ensure health insurance coverage would remain continuous for covered participants and to simplify the process for health insurance transaction administration. In 1999, the HIPAA Privacy Rule was developed, which set the stage for the definition of Protected Health Information (PHI) and established certain standards related to the use and disclosure of PHI by covered entities (defined as health plans, data clearinghouses, and healthcare providers). In 2003, the Privacy Rule became effective, and the HIPAA Security Rule was adopted (which is one of several rules collectively referred to as "the Security Rule" or "the HIPAA Security Rule" throughout this document). The Security Rule required covered entities (and later, business associates) to implement administrative, physical, and technical safeguards to protect ePHI. The Security Rule defines ePHI as "individually identifiable health information (IIHI) transmitted or maintained in electronic media." Specifically, the Security Rule requires covered entities (and later business associates) to "ensure the confidentiality, integrity, and availability of all ePHI they create, receive, maintain, or transmit; protect against reasonably anticipated threats or hazards to the security or integrity of the information and reasonably anticipated impermissible uses or disclosures; and ensure compliance by their workforce."

In 2009, the Health Information Technology and Economic and Clinical Health (HITECH) Act was enacted to strengthen the HIPAA Privacy and Security Rules and promote the transition to ePHI. In 2013, the HIPAA Omnibus Rule was introduced, which revised the HIPAA Rules, implemented several provisions of the HITECH Act, extended the HIPAA requirements to business associates (defined as "a person or entity that performs activities for a covered entity that involves the use or disclosure of PHI") and increased penalties for HIPAA non-compliance. In 2019, the Office of Civil Rights (OCR) turned its focus to individuals' rights as it relates to their health records under the Patient Right of Access Initiative. Final rules were later adopted to support and protect reproductive health rights and privacy, effective December 23, 2024.

Proposed Changes to the HIPAA Security Rule

In January of 2025, the proposed rules titled "Health Insurance Portability and Accountability Act Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information" (hereinafter referred to as the "proposed rules") were published, which are intended to address the current need for more cybersecurity protection surrounding ePHI under the HIPAA Security Rule. Due to the widespread use of computers and network technologies in health care, the Office of Civil Rights (hereinafter referred to as "the Department") believes that due to the risks of bad actors (e.g., hackers implementing ransomware attacks on health care information), covered entities and business associates (collectively referred to as "regulated entities") should implement further protections to ePHI that may not have been necessarily clear or applied under the previous HIPAA Security Rule. The Department is attempting to take proactive measures to adapt current regulations (and adopt new regulations) to address technology advances in the last decade since the HIPAA Security Rule was last revised. The Department also released revisions to the HIPAA Security Rule because it found significant inconsistencies between the enforcement and implementation of the HIPAA Security Rule among many regulated entities.

The proposed rules include significant changes and additions to the current definitions and terms sections of the HIPAA Rules (including the adoption of terms such as Artificial Intelligence (AI), Augmented Reality (AR), Virtual Reality (VR), Multi-factor Authentication (MFA), Electronic Information System, Risk, Technical Controls, Security Measures, Vulnerability) and update the current definition of the following terms: Access, Authentication, Confidentiality, Malicious Software, Physical Safeguards and Security/ Security Measures. In addition, the Department sought the advice of other agencies and organizations (e.g., the National Committee on Vital and Health Statistics, National Institute of Standards and Technology, and Office of the National Coordinator for Health Information Technology) to assist it in shaping the policy for a more effective process in protecting ePHI, while still providing flexibility to regulated entities when implementing these cybersecurity rules.

One significant change in the proposed rules is the removal of the word "addressable" under the HIPAA Security Rule and replacing it with the term "required," no longer allowing regulated entities to subjectively adhere to the HIPAA Security Rule. As an example, under the existing Security Rule a regulated entity's encryption of ePHI is an "addressable implementation specification under the standard for access control," allowing a regulated entity a choice to not encrypt ePHI if it is not reasonable and appropriate. However, in the proposed rules, encryption of ePHI would be required. In addition, the proposed rules seek to replace the term "reasonable and appropriate security measures" that is currently used in the HIPAA Security Rule to assess whether a regulated entity would need to implement any security as it related to ePHI (i.e., some regulated entities interpreted this language to mean that the HIPAA Security Rule was optional due to the rule's previous language) and replace that language with much more stringent language that states "reasonable and appropriate security measures to implement the standards and implementation specifications under the Security Rule." The proposed changes in language seem to indicate that many parts of the HIPAA Security Rule implementation process will be explicitly required of regulated entities and plan sponsors of group health plans (if these rules are adopted in the final regulations) as a part of the Security Rule, with only limited exceptions.

If these rules are adopted under the final rules, some of the security measures could include:

- A requirement that all ePHI at rest and in transit be encrypted, with limited exceptions.
- Regulated entities must establish and administer technical controls in a regular and consistent manner when configuring their electronic information systems and workstations. These requirements would include: 1) implementing anti-malware security on systems; 2) the removal of all non-relevant software from any electronic information systems/workstations; and 3) the disablement of network ports, subject to the entity's overall risk analysis.
- A requirement for multi-factor authentication when accessing ePHI.
- Safety protocols and audits by regulated entities, such as: 1) scanning for vulnerabilities within the electronic information system at least every six months, with penetration testing at least once every 12 months; and 2) reviewing and testing the effectiveness of certain security measures and performing a compliance audit at least once every 12 months (which replaces the previous requirement to maintain security measures, generally).
- Increased specificity when a regulated entity performs a risk analysis, including having a written assessment identifying all potential threats and vulnerabilities related to the "confidentiality, integrity, and availability" of the regulated entity's ePHI.
- Required notification to a regulated entity within 24 hours when a workforce member's access to ePHI is either changed or terminated.
- Strengthen requirements for responding to security incidents and building contingency plans and establishing written procedures for loss of "relevant electronic information systems" and "security incident response plans."
- Require business associates to verify with covered entities, at least once every 12 months, that they have "deployed technical safeguards…to protect ePHI through a written analysis of the business associate's relevant electronic information systems by a subject matter expert and a written certification of that the analysis has been performed and is accurate." Business associates must also notify covered entities (along with subcontractors to business associates) "upon activation of their contingency plans without unreasonable delay, but no later than 24 hours after activation."
- Group health plans must include in their plan documents provisions stipulating that a group health plan sponsor must "comply with the administrative, physical, and technical safeguards of the [revised] Security Rule; ensure that any agent to whom they provide ePHI agrees to implement the administrative, physical, and technical safeguards of the Security Rule; and notify their group health plans upon activation of their contingency plans without unreasonable delay, but no later than 24 hours after activation." (See more specific details related to group health plans later in this article).

The Department believes that even though these proposed rules seem to revise a substantial portion of the current text within the HIPAA Security Rule, the proposed rules have very limited impact on regulated entities' current compliance obligations because these proposed rules would only serve to codify the current obligations and practices in which regulated entities are already engaged (e.g., encryption of email for the transfer of ePHI, or Multi-Factor Authentication access to electronic information systems). The Department's focus, therefore, seems to be on modifications to, and requests for comments on, the codification of practices that were already adopted and developed by regulated entities due to the Security Standards, Administrative Safeguards, Physical Safeguards, Technical Safeguards, and Organizational Requirements that were already in existence under the HIPAA Security Rule. The Department believes that many of the proposed rules only serve to expand and improve the current requirements, with a larger need for written documentation when implementing safeguards to ePHI (e.g., implementation of a written set of procedures for data backups that allow access to ePHI from a remote location in the instance of a total failure of the system), and further ensuring that these measures are more consistently monitored by regulated entities (e.g., auditing their compliance under each standard and specification of the Security Rule, at least once every 12 months).

Proposed Documentation Requirements on Regulated Entities

The proposed rules specifically address a new requirement for all regulated entities to adhere to certain documentation standards.

The proposed rules require a regulated entity to have **written** policies and procedures as they relate to the Security Rule and also require a regulated entity to review and test its security measures on a regular basis. Therefore, the Department proposes to "revise other provisions of the Security Rule to clarify that a regulated entity is required to implement and maintain its administrative, physical, and technical safeguards, including its policies and procedures. These proposals clarify that such maintenance requires the review, testing, and modification of the regulated entity's security measures on a regular cadence, meaning that the regulated entity's security measures can be modified at any time."

In addition to the requirement that a covered entity must have written policies and procedures for complying with the HIPAA Security Rule, the proposed rules would also require a regulated entity to document what factors it considered in the development of its policies and procedures. The proposed rules provide a list of factors regulated entities should consider when deciding which security measures to implement. Also, under the proposed rules, a regulated entity is responsible for documenting all of its "actions, activities, and assessments." For example, even verbal reports of a suspected/known security incident/ breach, would need to be documented in writing. This documentation must be updated at least once every 12 months "and within a reasonable and appropriate period of time after a security measure is modified."

If the proposed rules are finalized, regulated entities would be responsible for retaining all relevant written documentation required under the revised HIPAA Security Rule for a period of no less than six years from the date of its genesis or the last date it was in effect, whichever is later. This rule already exists within the current HIPAA Security Rule and is not modified under the proposed rules.

The written documentation requirements discussed in this section may be created and maintained in an electronic, written format.

Proposed Rules to Further Integrate the HIPAA Security Rules into Group Health Plans

The proposed rules include a specific section addressing group health plans subject to the HIPAA Security Rule. This was due to the Department's concern that group health plans may not recognize that they are also required to implement security measures that may be equivalent to other covered entities under the HIPAA Security Rule. The proposed rules would rename the current implementation specifications within the current HIPAA Security Rule to include such topics as "Safeguard implementation," "Separation," and "Agents," and also include within these three specifications a requirement that plan sponsors (or any agent of the plan sponsor to whom the group health plan provides ePHI) implement the "administrative, physical, and technical safeguards" of the HIPAA Security Rule. As an example, for the Department to ensure that plan sponsors are implementing the administrative safeguards and performing the required risk analysis, plan sponsors would be beholden to the same security measures as regulated entities through the obligations imposed on them under the plan documents of their group health plan. In addition, the Department proposes to include a requirement that plan sponsors include a policy related to "security incident awareness" within their plan documents to add a "new implementation specification for contingency plan activation…that…a plan sponsor [is required] to report to the group health plan without unreasonable delay, but no later than 24 hours after activation of its contingency plan." The proposed rules do not provide a template for the language that would be included in the plan documents to comply with these obligations, but only state that the Department "permit[s] the group health plan and plan sponsor to negotiate the form, content, or manner of the notice…"

The following are topics the Department is seeking comment on from stakeholders and are contained within the group health plan section of the preamble to the proposed rules:

"a. How group health plans currently ensure that plan sponsors implement reasonable and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of ePHI.

b. Whether it is appropriate for group health plans to require plan sponsors to implement the administrative, physical, and technical safeguards of the Security Rule. If not, please explain and provide alternatives for how the Department should ensure the confidentiality, integrity, and availability of ePHI when it is disclosed to plan sponsors.

c. Whether business associates currently notify covered entities (or subcontractors notify business associates) upon activation of their contingency plans, and if so, the manner and timing of such notice.

d. Whether plan sponsors currently notify group health plans upon activation of their contingency plans, and if so, the manner and timing of such notice.

e. Whether it would be appropriate to require a business associate to notify a covered entity (or a subcontractor to notify a business associate) within 24 hours of activating its contingency plan. If not, please explain why and what would be an appropriate amount of time for such notification.

f. Whether it would be appropriate to require a plan sponsor to notify a group health plan within 24 hours of activating its contingency plan. If not, please explain why and what would be an appropriate amount of time for such notification.

g. The manner, timing, frequency, and process used by business associates to report security incidents to a covered entity (or subcontractors to business associates).

h. The manner, timing, frequency, and process used by a plan sponsor to report security incidents to a group health plan."

Proposed Rules for Transition to Revised Security Rule

Originally, the HIPAA Security Rule had an initial implementation period dating back to 2005 and 2006. The Department proposes to replace that initial implementation period after nearly 20 years and replace it with a different deadline period to include a transition period for the revised HIPAA Security Rule (if the proposed rules are finalized). The Department recognizes that this creates a significant concern for regulated entities due to the anticipated administrative burden and increased cost of revising business associate agreements and other written documents that would need to comply with these new rules. Examples of these changes include the inclusion of the need for a business associate to report to the covered entity within 24 hours of activation of its contingency plan or the expiration of the business associate agreement after the compliance date of the HIPAA Security final rules, which would be released in the future. Due to this recognition by the Department of these and other factors, the Department has included a transition period within the proposed rules when and if these rules are finalized.

The transition provisions would allow regulated entities to operate under previous business associate agreements (or other written arrangements) until the earlier of:

1) The date the business associate agreement/contract renews on or after the compliance date of the final rules; or

2) A year after the final rules' effective date.

This transition period would only apply if both of the following conditions apply to the regulated entities:

1) Prior to the date the final rules are published, the regulated entities had an existing business associate agreement (or other written arrangement) with a business associate or subcontractor that is compliant under the previous HIPAA Security Rule (that was adopted prior to the effective date of the new HIPAA Security final rules); and

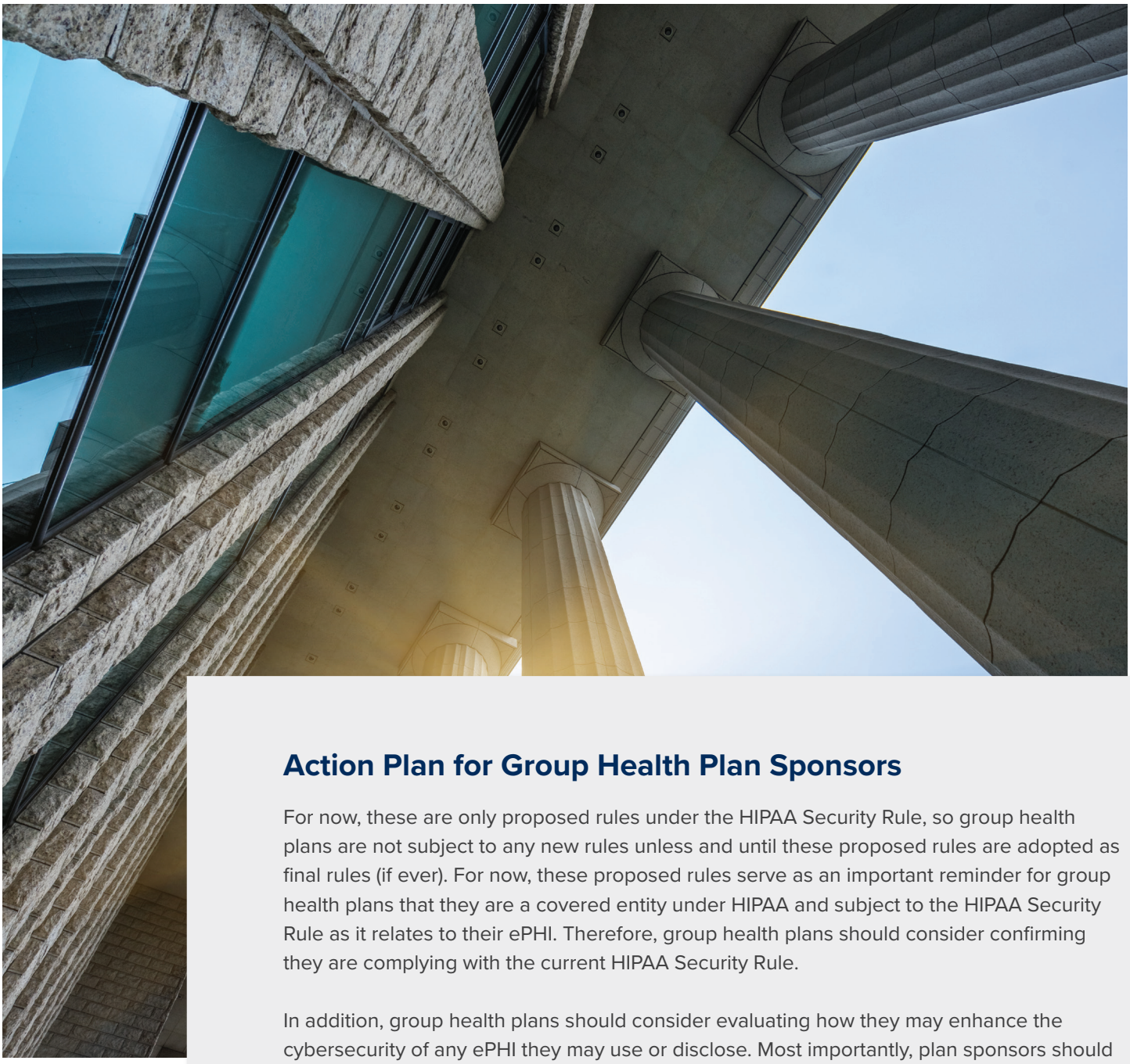
2) The renewal date of such business associate agreement (or other written arrangement) is not renewed or modified between the effective date and the compliance date set forth in the revised HIPAA Security final rules.

As an example, the proposed rules state that a business associate agreement (or other written arrangement) would not need to include provisions indicating that the business associate would need to comply with the revised HIPAA Security Rule when creating, receiving, maintaining or transmitting ePHI until the end of the transition period discussed above.

In the instance where an agreement automatically renews (e.g., an evergreen contract), such contract would be eligible for this transition relief if those written agreements/arrangements automatically renew between the effective date and the compliance date outlined in the revised HIPAA Security final rules and would, therefore, be deemed in compliance when these contracts automatically renew.

Despite the above transition relief that would not require a regulated entity to amend any written business associate agreements (or other written arrangements) prior to the compliance date set forth in the revised HIPAA Security Rule, these transition rules do not affect any other compliance obligations that would be required under the revised HIPAA Security Rule. For example, the proposed rules provide that if the final rules are published adopting the proposed rules, a business associate would still be required to implement and document the implementation of "the administrative, physical, and technical safeguards required by [the] revised Security Rule..., even if the business associate's contract with the covered entity has not yet been amended."

The Department also considered transition rules for group health plans and plan document requirements but ultimately did not include them as proposed rules. According to the preamble of the proposed rules, the reason the Department did not formally create a proposed rule for transition relief to group health plans for the adoption of these plan document requirements is that the plan sponsor would only be subject to these new plan document rules under the revised HIPAA Security Rule if and at the time the amendment/revision is adopted into the plan document(s). The Department did request comments on how transitional guidance could be implemented for group health plans and plan sponsors so that plan sponsors would be subject to the final rules but not be required to include such language in a plan document until the end of a transition period.



Action Plan for Group Health Plan Sponsors

For now, these are only proposed rules under the HIPAA Security Rule, so group health plans are not subject to any new rules unless and until these proposed rules are adopted as final rules (if ever). For now, these proposed rules serve as an important reminder for group health plans that they are a covered entity under HIPAA and subject to the HIPAA Security Rule as it relates to their ePHI. Therefore, group health plans should consider confirming they are complying with the current HIPAA Security Rule.

In addition, group health plans should consider evaluating how they may enhance the cybersecurity of any ePHI they may use or disclose. Most importantly, plan sponsors should begin speaking with their legal counsel and technology consultants (both internal and external) in preparation for these new rules when (and if) they are adopted. Group health plan sponsors should consider working with legal counsel to create adequate business associate agreements (or other written arrangements) pursuant to the current HIPAA Security Rule if they have not done so already, to benefit from the transition rules discussed within the proposed rules.

How Brown & Brown Can Help

Connect with your Brown & Brown service team to learn more about how we can help find solutions to fit your unique needs.

Brown & Brown

Find Your Solution at BBrown.com

DISCLAIMER: *Brown & Brown, Inc. and all its affiliates, do not provide legal, regulatory or tax guidance, or advice. If legal advice counsel or representation is needed, the services of a legal professional should be sought. The information in this document is intended to provide a general overview of the topics and services contained herein. Brown & Brown, Inc. and all its affiliates, make no representation or warranty as to the accuracy or completeness of the document and undertakes no obligation to update or revise the document based upon new information or future changes.*