GROOM LAW GROUP

Publications

Biden Administration Proposes Beefed-Up HIPAA Security Rule… But Prognosis Uncertain

ATTORNEYS & PROFESSIONALS

Shanna Cramer
scramer@groom.com
202-861-6636

Christy Tinnes
ctinnes@groom.com
202-861-6603

Viv Hunter Turner
vturner@groom.com
202-861-6324

PUBLISHED
02/17/2025

SOURCE
Groom Publication

SERVICES
Employers & Sponsors
- Health & Welfare Programs

Health Services
- ERISA
- Privacy & Security
- Federal Insurance Regulation

On January 6, 2025, the Biden Administration issued a new proposed rule updating the HIPAA Security Standards ("Proposed Rule"). The original HIPAA Security Standards were issued in 2003 and updated in 2013 and require that covered entities and business associates establish procedures to protect the security of electronic protected health information ("ePHI") ("Security Standards"). These rules followed the HIPAA Privacy Rules, which govern the confidentiality of PHI ("Privacy Rules").

Comments on the Proposed Rule are due March 7, 2025.

GROOM INSIGHT: On January 20, 2025, President Trump issued a "regulatory freeze" on proposed regulations. However, for regulations that were already published in the Federal Register, the language says that executive departments should "consider" postponing the effective date for 60 days and "consider" opening a new comment period. So far, the Department of Health & Human Services ("HHS") has not commented, so it appears that the March 7th comment period deadline currently holds.

Below we provide a background of the current rules, highlights of the new Proposed Rule, our predictions on whether the Proposed Rule will move forward under the Trump Administration, and what HIPAA covered entities and business associates should be considering now.

We also created an in-depth Compliance Tool outlining the Standards and Implementation Specifications under the new Proposed Rule. Covered entities and business associates can use this Compliance Tool as a reference point when comparing the Proposed Rule to the existing rules. If you would like a courtesy copy of our Compliance Tool outlining the requirements of the Proposed Rule, please contact the authors of this alert here or reach out to any of our Groom attorneys.

I. Background of Existing Security Standards

The existing Security Standards apply to HIPAA covered entities – health care providers, clearinghouses, and health plans (i.e., fully insured and self-funded group

health plans, health insurance issuers, and any arrangement that pays or provides for medical care). The Security Standards also apply directly to business associates.

The current Security Standards include general "Standards" and specific "Implementation Specifications" in three categories: administrative, physical, and technical safeguards.

The Implementation Specifications are labelled as either "Required" or "Addressable,"

- **Required** –The covered entity or business associate must establish and document its procedure to comply.
- **Addressable** – The covered entity or business associate must assess whether the safeguard is "reasonable and appropriate" when analyzed with reference to the likely contribution to protect ePHI and either implement the Implementation Specification or, if it determines the Implementation Specification is not reasonable and appropriate, document why and establish and document an equivalent alternative measure if reasonable and appropriate.

Covered entities and business associates are required to document compliance with the Standards and Implementation Specifications in a "Security Risk Assessment" (sometimes referred to as an "SRA"). HHS may request a copy of the covered entity's or business associate's SRA in an audit or investigation.

II. Proposed Rule Highlights

The Proposed Rule utilizes the same general framework as the Security Standards but goes into much greater detail on the specific procedures that a covered entity or business associate must implement with more prescriptive deadlines, including a requirement to update these procedures annually. In addition, all Standards and Implementation Specifications would be "Required" (no more "Addressable" Standards or Implementation Specifications).

Covered entities and business associates would be required to comply within 8 months of publication of the final rule in the Federal Register, with a more extended transition period for updating business associate agreements ("BAAs").

Our Compliance Tool goes into greater detail (with new requirements noted), but as highlights, covered entities and business associates must:

- Update HIPAA Security Procedures at least annually;
- Establish written procedures related to the use of patches and review at least annually (must update patches within 15 days of a "critical" risk and 30 days of a "high" risk);
- Establish written procedures to authorize or terminate access to ePHI by HIPAA workforce members and update at least annually;
- Terminate a HIPAA workforce member's access within 1 hour after their termination of employment;
- Notify business associates of a change in access authorization by a HIPAA workforce member within 24 hours;
- Conduct security training at least annually;
- Perform a compliance audit at least annually (can be an external or internal audit);
- Require business associates to verify compliance annually with these rules, with a certification from a person within the business associate with authority to act (applies to subcontractor business associates, too);
- Encrypt all ePHI at rest or in transit (some exceptions, in which case must use compensating controls);
- Annually review and test the effectiveness of technology controls, access controls, and audit trails;
- Deploy multi-factor authentication to all technology assets (some exceptions, in which case must use compensating controls);
- Conduct vulnerability scanning every 6 months and penetration testing at least annually;
- Create backups to ensure copies are not more than 48 hours old; test backups every 6 months;
- Update HIPAA BAAs; and
- Update HIPAA plan amendment language allowing disclosure to plan sponsors.

GROOM INSIGHT: Currently a health plan may disclose PHI to its employer plan sponsor for plan administration functions (such as to review claims data or where a plan sponsor decides certain appeals in-house), as long as the plan document has been amended to allow the disclosure and the plan sponsor certifies certain compliance with the Privacy Rules and Security Standards. For example, the plan sponsor must certify that it will safeguard the PHI and only use the PHI for plan administration functions, and it must require any service providers to do the same.

The current Security Standards require that the plan sponsor agree to implement administrative, physical, and technical safeguards that "reasonably and appropriately" protect ePHI but do not mandate how that is done. The Proposed Rule would require that plan sponsors implement the specific administrative, physical, and technical safeguards spelled out in the Proposed Rule This change appears to mean that a plan sponsor would have to have a Security Risk Assessment of its own, undergo an annual compliance audit, establish security procedures, and comply with the more prescriptive security measures and deadlines of the Proposed Rule (and require that its own service providers that access ePHI do the same).

While the employer plan sponsor would not be directly subject to HIPAA and HHS enforcement, it appears that the health plan could be subject to enforcement if the plan sponsor does not comply since the health plan would have relied on the certification to disclose the ePHI to the plan sponsor. This is an area where plan sponsors and health plans may want to comment.

III. Predictions: Will the Proposed Rule Be Finalized?

That is the big question.

On January 31, 2025, President Trump issued an Executive Order (referred to as the "10 for 1" rule), which requires that, for each new regulation issued, the issuing agency identify at least 10 prior regulations for elimination. So, HHS may have some pressure not to finalize the Proposed Rule since it may be difficult to identify 10 prior regulations to repeal.

That said, cybersecurity is a bipartisan issue, so the Trump Administration may have an appetite for finalizing rules strengthening HIPAA's security framework. However, the Trump Administration may want to align the rules with its own priorities.

As far as predictions . . .

- HHS could do nothing – the Proposed Rule is only proposed, so the Trump Administration would not need to rescind it.
- HHS could review any comments that are submitted and issue final rules. However, the final rules could not differ significantly from the Proposed Rule or there would be risk that HHS could be seen as going beyond its authority without notice and comment.
- HHS could re-issue the Proposed Rule with modifications that are more in line with the Trump Administration's priorities, which would require a new comment period.

IV. What Should Health Plans and Business Associates Be Doing?

While we suggest that health plans and business associates follow the status of the Proposed Rule and familiarize themselves with the requirements generally, we think it is too soon to commit to full compliance. The final rules could differ from the Proposed Rule, or the Trump Administration could decide to issue its own proposal or ignore the Proposed Rule altogether.

However, certain aspects of the Proposed Rule could be considered a "best practice" to work toward, which would make future compliance easier. In addition, HHS has noted that one of the most frequent HIPAA violations is noncompliance with the current Security Standards, particularly the requirement for a covered entity or business associate to document compliance with the rules in an SRA. We suggest that health plans and business associates take this year to ensure that their "HIPAA houses" are in order and that they are fully compliant with the current Security Standards. Not only will that mitigate current risk of a security breach or enforcement by HHS, but it will be that much easier to build on the current rule if a final rule is issued in the next year or two.

Right now, plans have time to review their current compliance, fill in any gaps, and make sure their SRA is updated. Once final rules are issued, there will be a deadline to comply, so some legwork on the front end can pay off by making that lift a little less heavy.