ALSTON & BIRD

HEALTH & WELFARE PLAN LUNCH GROUP

February 13, 2025

One Atlantic Center
1201 W. Peachtree Street
Atlanta, GA 30309-3424
(404) 881-7885
E-mail: john.hickman@alston.com

INDEX

ALSTON & BIRD

0

February 2025 Agenda

- MHPAEA Report to Congress
- News for Account-Based Plans
- Regulatory Update
- Litigation Update
- ACA Reporting and State Mandates
- Proposed HIPAA Security Rule
- Gag Clause Update
- Miscellaneous

1

ALSTON & BIRD

MHPAEA Report to Congress

2

Health & Welfare Benefits
MONTHLY UPDATE

2024 Report to Congress

- Continued Issues with compliance with CAA 2021 Comparative Analysis requirement
  - Failure to prepare a comparative analysis
  - Documents provided without adequate explanation
  - Failure to identify the specific MH/SUD and M/S benefits or MHPAEA benefit classifications affected by an NQTL
  - Conclusory assertions lacking specific supporting evidence
- Six EBSA priority areas comprise the vast majority of reviewed NQTLs:
  1. Prior authorization requirements for in-network (INN) and out-of-network (OON) inpatient services
  2. Concurrent care review for INN and OON inpatient and outpatient services
  3. Standards for provider admission to participate in a network, including reimbursement rates
  4. OON reimbursement rates (methods for determining usual, customary, and reasonable charges)
  5. Adequacy standards for MH/SUD provider networks
  6. Impermissible exclusions of key MH/SUD treatments

ALSTON & BIRD

News for Account-Based Plans

4

Health & Welfare Benefits
MONTHLY UPDATE

2024 Guidance for Account-Based Plans

- IRS Notice 2024-71: Condoms qualify as 213(d) medical care for FSAs/HRAs/HSAs
- IRS Notice 2024-75 recognizes the following as preventive care for HSA HDHP purposes (i.e., reimbursable below the deductible)
  - OTC oral contraceptives and condoms
    - Does not allow male sterilization or other male contraceptives
  - Breast cancer screenings other than mammograms (e.g., MRI, ultrasound) – retro expansion/clarification to Notice 2004-23
  - Continuous glucose monitors (as is the case with other glucometers) – retro clarification to Notice 2019-45
    - Limited to monitors that pierce the skin for a reading (n/a smart watch or rings)
  - Insulin and insulin delivery products – retro expansion to accommodate IRC 223(c)(2)(G)
- Employee Choice Program: IRS approves (in PLR 202434006) an arrangement that allows annual choice to direct employer funds between HSA, HRA, education/tuition/loans, and employer DC plan contribution.
  - Choice made annually before start of calendar year; IRS concluded did not constitute an elective deferral (e.g., for 401(k) purposes); Remaining amounts could not be cashed out
  - Compliance and cost considerations: Employer contribution (not salary reduction); Plan limits and nondiscrimination testing issues ; Administrative complexity

5

ALSTON & BIRD

5

Health & Welfare Benefits
MONTHLY UPDATE

More on HSAs

- Expiration of CARES Act HDHP virtual care exception (unless re-enacted retroactively) on December 31, 2024
  - Plan year exception so impacts calendar year plans 1/1/25
  - Potential problem areas for any "treatment" below the deductible
  - Possible exceptions
    - Preventive care?
    - Health coach
    - Disease management
    - Treatment that (in the aggregate) is not significant
      - How do you measure significance?

Health & Welfare Benefits
MONTHLY UPDATE

Final Rule for ERISA Investment Advice Fiduciaries

Final ERISA Investment Fiduciary Rule

- DOL Proposed Rule on **Definition of an Investment Advice Fiduciary** and Proposed Changes to Related PTEs (Nov. 3, 2023); comment period ended Jan. 2, 2024; Final Rule published in FR on April 25, 2024.
- **Top Line Review:**
  - HSAs are subject to the Final Rule
    - No exception as a non-investment deposit product
  - HSA service providers who receive compensation in connection with investment recommendations will be considered fiduciaries, and must fit prohibited transaction exemption 2020-02 "Best Interest Contract Exception"
  - BCE PTE expanded to include NBTs and their service providers
- Two court challenges each have resulted in a stay on enforcement
  - ACLI case
  - FACC case
- DOL has filed a motion to pause the two federal court cases.
  - "Due to the recent change in administration on January 20, 2025, DOL is now under new leadership,". . . "New agency officials are still in the process of onboarding and familiarizing themselves with all of the issues presented by pending litigation."

ALSTON & BIRD

Regulatory Update

8

Health & Welfare Benefits
MONTHLY UPDATE

Withdrawn Proposed Regulations

- **Coverage of Certain Preventive Services Under the ACA:** published Feb. 2, 2023; **withdrawn December 30, 2024**.
  - *Background*: Under the 2018 final rule, sponsors with a moral or religious exemption to contraceptive coverage did not have to provide it. They could provide a completely optional accommodation where the objecting employer did not have to contract, arrange, pay, or refer an individual for contraceptive coverage, but contraceptive services are still available through an insurer or TPA. Many objecting employers did not provide the optional accommodation.
  - Proposed Rule:
    - Would have maintained the existing religious objection but eliminated the moral objection.
    - Would have provide a new pathway where individuals in plans of objecting employers that did not provide the accommodation could obtain contraceptives at no cost through an "individual contraceptive arrangement" with a willing provider.
- **Enhancing Coverage of Preventive Services under the ACA:** published Oct, 28, 2024; **withdrawn Jan. 15, 2025**.
  - Clarified and codified an exception process for reasonable medical management techniques for preventive items/services not generally covered by the plan.
  - Proposed to make the current therapeutic equivalence approach mandatory (it is currently optional).
  - Proposed that plans cover OTC contraceptive items without a prescription or imposing cost-sharing.
  - Proposed a disclosure for coverage and cost-sharing for OTC contraceptive items.

9

ALSTON & BIRD

9

Health & Welfare Benefits
MONTHLY UPDATE

Regulatory Freeze and the CRA

- *Regulatory Freeze*: As of January 20, 2025, any federal regulation published in the Federal Register that is not yet in effect is part of a 60-day regulatory freeze as the incoming administration conducts its own reviews.
  - Applies to rules as defined by US Code "that have been issued in any manner but have not taken effect" and "any agency statement of general applicability and future effect that sets forth a policy on a statutory, regulatory, or technical issue or an interpretation of a statutory or regulatory issue."
  - "Effective date" is distinguishable from a compliance or applicability date.
- *Congressional Review Act* (CRA): Congress can negate certain administration actions taken close to the start of a new Congress.
  - A CRA disapproval resolution to eliminate a rule requires a simple majority of the House and Senate and must be signed by the President.
  - The CRA "lookback" period includes the period reaching back 60 "session days" in the Senate, or 60 "legislative days" in the House, before adjournment sine die.
  - The Senate and House Parliamentarians are the sole definitive arbiters of the operation of the CRA mechanism, including its associated time periods.
  - On August 21, 2024, the Congressional Review Service estimated that Biden Administration rules submitted to the House or Senate on or after August 1, 2024, until the end of the second session of the 118th Congress, were likely to be subject to the CRA lookback provisions and will qualify for additional periods of CRA review in the first 60 session days of the 119th Congress (2025).

Health & Welfare Benefits
MONTHLY UPDATE

Regulatory Freeze and the CRA

Recently Finalized Rules—Are they within the scope of the Congressional Review Act?

- **MHPAEA Final Rule:** published in FR on Sept. 23, 2024; effective date November 22, 2024.
- **Nondiscrimination in Health Programs and Activities (1557):** published in FR on May 6, 2024; effective date July 5, 2024
- **HIPAA Privacy Rule and Reproductive Health Care:** published in FR on April 26, 2024; effective date June 25, 2024.
- **Definition of an Investment Advice Fiduciary:** published in FR on April 25, 2024; effective date September 23, 2024
- **STLDI, Independent, Non-Coordinated Excepted Benefits, Level Funded Arrangements:** published in FR on April 3, 2024; effective June 17, 2024

Recently Proposed Rules

- **Enhancing Coverage of Preventive Services under the Affordable Care Act:** published in FR Oct, 28, 2024. **[Withdrawn]**
- **Proposed Modifications to the HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information:** published in FR January 6, 2025.

Health & Welfare Benefits
MONTHLY UPDATE

Other Challenges

- **MHPAEA Final Rule**
  - 1.17.2025: ERISA Industry Committee (ERIC) filed suit against the tri-agencies, ERISA Industry Committee v. Department of Health and Human Services et al , D.D.C., No. 1:25-cv-00136. Alleges:
    - Exceeds the Departments' statutory authority with respect to meaningful benefits; material differences in access; fiduciary certification.
    - Arbitrary and capricious with respect to meaningful benefits/core treatment; material differences in access, comparative analysis requirements, fiduciary certification requirements; January 1, 2025 applicability date.
    - Violates APA's notice and comments requirements with respect to reference to third-party clinical standards for "meaningful benefits" and the change from the proposed rule in the fiduciary certification requirement.
    - Also includes due process and constitutional claims.
- **Nondiscrimination in Health Programs and Activities (1557)**
  - Nationwide injunction on several provisions of the 2024 Final Rule related to sex discrimination encompassing gender identity, including the notice of nondiscrimination. *Tennessee v. Becerra*, 2024 WL 3283887 (S.D. Miss. 2024).
  - All provisions of the 2024 Final Rule enjoined in Texas and Montana.
  - Several other ongoing lawsuits, including from prior versions of the rule.

Health & Welfare Benefits
MONTHLY UPDATE

Other Challenges

- **HIPAA Privacy Rule and Reproductive Health Care**
  - State of Texas v. United States Department of Health and Human Services et al; on 1.31.2025 the court issued an order holding briefing in abeyance
  - Tennessee v. HHS (filed 1.17.2025)
- **Definition of an Investment Advice Fiduciary**
  - Two federal trial courts in separate cases have placed a hold on the DOL's 2024 investment advice fiduciary regulations and related PTE amendments
- **STLDI, Independent, Non-Coordinated Excepted Benefits, Level Funded Arrangements**
  - On 12.4.24 a Texas court vacated the notice requirement for fixed indemnity (see Manhattan Life Insurance and Annuity Company et al v. United States Department of Health and Human Services et al E.D.Tex. 6:24-cv-00178-JCB); DOJ filed notice of appeal on 2.3.2025
  - A separate challenge on STLDI restrictions is ongoing (see *American Association of Ancillary Benefits et al. v. Becerra et al.*, 4:24-cv-00783, August 29, 2024)

ALSTON & BIRD

Litigation Update

14

Health & Welfare Benefits
MONTHLY UPDATE

Tobacco Surcharge Litigation

- Over 20 lawsuits filed in 2024 over tobacco surcharges.
- At least one case has settled; no rulings in other cases yet.
- Recent lawsuits focus on “no full reward” and explanation of “reasonable alternative.”
- Review programs and communications.
- Plaintiff’s goal is to survive motion to dismiss and settle.

15

ALSTON & BIRD

15

Health & Welfare Benefits
MONTHLY UPDATE

Fiduciary Breach Litigation

- Two lawsuits filed in 2024 allege claims for fiduciary breaches for failure to monitor PBMs and negotiate lowest prescription drug prices
- Both lawsuits allege breach of fiduciary duty for failure to monitor the PBM, including the prices charged and the incentives for which drugs are placed on the formularies.
- Both lawsuits allege harm to the plan as a whole, resulting in not only higher drug costs to individuals but higher premiums for all participants, and even lower wages.
- One lawsuit alleged a prohibited transaction for paying excessive fees and insinuated that even consultants improperly profit from "market derived income" from PBMs.

Health & Welfare Benefits
MONTHLY UPDATE

Lewandowski v. Johnson & Johnson

- Former employee alleged the plan sponsor breached ERISA fiduciary duty for failure to monitor the PBM, including the prices charged and the incentives for which drugs are placed on the formularies.
- Also alleged harm to the plan as a whole, resulting in not only higher drug costs to individuals but higher premiums for all participants, and lower wages.
- On 1.24.25, a NJ federal court dismissed for lack of standing allegations of breaches of fiduciary duty with respect to the Plan's prescription drug costs.
  - Injury in the form of higher premiums—"speculative and hypothetical."
  - Injury in the form of OOP costs for medication—Court acknowledged she paid higher cost for drugs, but the injury is not redressable because she had hit her out-of-pocket max.
- The court did not dismiss the third count for failure to provide plan documents upon request.

Health & Welfare Benefits
MONTHLY UPDATE

What's Next?

- Will this be the end of these types of lawsuits?
  - Probably not. "Better" plaintiffs with standing may file suit.
  - Plaintiffs may be able to show that higher drug prices do increase participant premiums in plans that target express ratios between employer and employee.
  - Similar lawsuit with additional allegations is still pending.
- Can plan sponsors take steps to head off these types of lawsuits?
  - As a general practice, plan fiduciaries should be monitoring their TPAs, including the service providers they hire to assist with monitoring TPAs and assisting with RFPs.
  - Fiduciaries have a duty to determine whether costs are reasonable.
    - Hire experts to assist with understanding pricing.
    - Include in the RFP terms that require more transparency in presentation of pricing, formularies, and rebates.
    - Request bids for alternative pricing structures.
- A similar lawsuit filed last year is still pending.
  - Has the additional allegation of a prohibited transaction for paying excessive fees.
  - None of those plaintiffs allege that they hit their OOP max.

Health & Welfare Benefits
MONTHLY UPDATE

Gender Care Litigation

- Executive Order 14148 (Jan. 20, 2025), rescinded the prior's administrations executive orders requiring federal agencies to interpret Title IX on the basis of gender identity under *Bostock v. Clayton Cnty., GA.*
- Executive Order 14187 (Jan. 28, 2025) limits gender identity care for minors and is being challenged in at least two federal district court cases:
  - *PFLAG v. Trump, (D. Md)* filed Feb. 4, 2025
  - *State of Washington v. Trump (D. Wa)* filed Feb. 7, 2025
- *U.S. v. Skrmetti,* the former administration intervened in a challenge to a Tennessee Law, S.B. 1, banning gender identity care for minors.
  - Former administration challenged S.B. 1 as denying equal protection under the 14th Amendment on the basis of sex, and participated in oral arguments in the US Supreme Court on December 4, 2024.
  - In a letter to the Clerk of the U.S. Supreme Court, dated February 7, 2025, a U.S. Deputy Solicitor General said that the U.S. Justice Department has reconsidered its position on S.B. 1, and does not believe the law violates equal protection on the basis of sex or any other characteristic.
  - The US is now dropping its challenge to the law, but urged the court to issue a decision based on the private parties' challenges to the law.

Health & Welfare Benefits
MONTHLY UPDATE

Gender Care Litigation

- Unclear how the current administration's departure from the prior administration's interpretation of *Bostock* will impact current litigation.
- Some key circuit court cases:
  - *Pritchard et al. v. Blue Cross Blue Shield of Illinois*: 9th Circuit case on whether 1557 applies to insurer/TPA that administered an exclusion for gender-affirming care for its self-insured plans, including a plan of a religious employer seeking protection under the RFRA. Judges indicated that the opinion may be delayed pending the outcome on *Skrmetti,* although one party noted that *Skrmetti* does not directly apply here.
  - *Jane Doe et al. v. Surgeon General State of Florida et al*: 11th Circuit case on whether heightened scrutiny or strict scrutiny applies to Florida law banning gender-affirming care. Judges indicated that the opinion may be delayed pending the outcome on *Skrmetti*.
  - *Lange v. Houston County*: 11th Circuit case on whether a county plan's exclusion of sex change surgery violated Title VII. US DOJ withdrew its amicus brief on this case days before the rehearing.

ALSTON & BIRD

ACA Reporting and State Mandates

Health & Welfare Benefits
MONTHLY UPDATE

ACA and State Reporting

- For 2024 and later tax years, no longer required to automatically furnish a 1095-C to recipients so long as proper notice is provided
  - Expands prior regulatory relief under Code Section 6055 (covered individuals) to now apply to Code Section 6056 (offers of coverage to full-time employees)
  - IRS to issue guidance regarding notice
  - 6055 regulations may provide a guide to future IRS guidance:
    - reporting entity posts the notice prominently in a location on its website that is reasonably accessible to all individuals entitled to receive the form stating that they may receive a copy upon request.
    - The notice must include an email address and a physical address to which a request may be sent, as well as a telephone number for questions.
    - The regulations also require the notice to be retained in the same location on the ALE's website through October 15 following the calendar year to which the statements related (or the first business day after October 15, if October 15 is not a business day).
  - May not satisfy state reporting obligations (California, Rhode Island, New Jersey, and D.C.)

Health & Welfare Benefits
MONTHLY UPDATE

ACA Reporting and State Reporting

- Codifies the rule that date of birth for a dependent may be used if TIN not provided
  - Does NOT modify/alleviate solicitation requirement
  - Good time to reevaluate solicitation process

ALSTON & BIRD

Proposed HIPAA Security Rule Updates

24

Health & Welfare Benefits
MONTHLY UPDATE

Proposed HIPAA Security Rule

Plan amendment for Security Rule (plan and plan sponsors)

- Plan amendment required unless the only ePHI disclosed to the plan sponsor is: (1) summary health information about an individual's participation in or enrollment or disenrollment in a health plan, (2) summary health information for premium bids or modifying, amending, or terminating the plan, or (3) authorized by the individual.
- The plan amendment must require the plan sponsor to:
  - Implement the administrative, physical, and technical safeguards that covered entities and business associates must implement under 45 C.F.R. §§ 164.308(a), 164.310, and 164.312.
  - Ensure adequate separation from the plan is supported by the administrative, physical, and technical safeguards.
  - Ensure that any agent to whom the plan sponsor provides the plan's ePHI implements the administrative, physical, and technical safeguards.
  - Report to the plan any security incident of which it becomes aware.
  - Report to the plan without unreasonable delay and in no case later than 24 hours any activation of the plan sponsor's contingency plan adopted consistent with the proposed Security Rule's administrative safeguard requirements.

25

ALSTON & BIRD

25

Health & Welfare Benefits
MONTHLY UPDATE

Proposed HIPAA Security Rule

Contingency Plan (plan and their business associates; plan sponsor and their agents)

- The proposed rule requires the contingency plan to consist "of written policies and procedures for responding to an emergency or other occurrence— including but not limited to fire, vandalism, system failure, natural disaster, or security incident—that adversely affect[] relevant electronic information systems."
- The written contingency requirements include:
  - Criticality Analysis – Perform and document an assessment of the relative criticality of relevant electronic information systems and technology assets.
  - Data Backups – Establish and implement written procedures to create and maintain exact retrievable copies of ePHI, including verification that the ePHI has been copied accurately.
  - Information Systems Backups - Establish and implement written procedures to create and maintain backups of relevant electronic information systems, including verification of success of backups.
  - Disaster Recovery Plan - Establish (and implement as needed) written procedures to restore loss of: (1) critical relevant electronic information systems and data within 72 hours of the loss; and (2) other relevant electronic information systems and data in accordance with the criticality analysis.

Health & Welfare Benefits
MONTHLY UPDATE

Proposed HIPAA Security Rule

Contingency Plan (plan and their business associates; plan sponsor and their agents)

- The written contingency requirements include (continued):
  - Emergency mode operation plan - Establish (and implement as needed) written procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode.
  - Testing and revision procedures - Establish written procedures for testing and revising contingency plans. Review and test contingency plans at least once every 12 months, document the results of such tests, and modify such contingency plans as reasonable and appropriate in accordance with the results of those tests.

Health & Welfare Benefits
MONTHLY UPDATE

Proposed HIPAA Security Rule

New Business Associate Agreements

- At least every 12 months obtain a business associate's written verification that it has deployed the Security Rule's technical safeguards that includes:
  - A ***written analysis*** of the business associate's relevant electronic information systems by a person with appropriate knowledge of and experience with generally accepted cybersecurity principles and methods for ensuring the confidentiality, integrity, and availability of ePHI to verify compliance with each standard and implementation specification for technical safeguards.
  - A ***written certification*** that the analysis has been performed and is accurate by a person who has the authority to act on behalf of the business associate.

Health & Welfare Benefits
MONTHLY UPDATE

Proposed HIPAA Security Rule

Notable new administrative, physical, and technical safeguards

- The proposed Security Rule eliminates the distinction between "addressable" and "required" safeguards, so plans might find less flexibility.
- These standards include detailed implementation specifications that plans, other covered entities, and business associates (and their subcontractors) must follow. Most implementation specifications require ongoing review every 12 months, 6 months, or when changes are or will be made.
- A few examples of safeguards that might be difficult for plans:
  - *Evaluation* - Perform a written technical and nontechnical evaluation to determine whether a change in environment or operations may affect the confidentiality, integrity, or availability of ePHI. Note that the rule requires this to be done "within a reasonable period of time ***before making a change*** in the environment or operations", which will require careful coordination among different departments of plans and their sponsors.
  - *Workforce Security* - Implement written policies and procedures to ensure that all workforce members have appropriate access to ePHI and relevant electronic information systems, and to prevent those workforce members who are not authorized to have access from obtaining access to ePHI and relevant electronic information systems. Significantly, a "**workforce member's access must be terminated as soon as possible but no later than *one hour* after the employment of, or other arrangement with, a workforce member ends**[,]" which might be difficult to implement in situations where employment terminations are sudden and unexpected (among many other common workplace scenarios). Additionally, **other covered entities and business associates must be notified no later than 24 hours after a workforce member's change in or termination of access to ePHI** or relevant electronic information systems.

Health & Welfare Benefits
MONTHLY UPDATE

Proposed HIPAA Security Rule

Plan amendment, contingency plan, and compliance with most new Security Rule requirements will be required within 240 days after the Final Rule is published

- Updated Security Rule compliance, including adoption of plan amendment and contingency plan, required within 180 days after the effective date of the final rule.
- The final rule's effective date effective is the date 60 days after publication in the Federal Register

Health & Welfare Benefits
MONTHLY UPDATE

Proposed HIPAA Security Rule

Business associate agreement may be eligible for transition period

- a limited deemed compliance period is available if:
  - the written contract with the business associate (or subcontractor) complies with the requirements for business associate agreements under the current rule; and
  - the business associate agreement is not renewed or modified from 60 days after publication of the final rule in the Federal Register until 240 days after publication.
- A business associate (or subcontractor) agreement that meets those requirements shall be deemed compliant until the earlier of:
  - the date the contract or arrangement is renewed on or after 240 days after the final rule's publication, or
  - 1 year and 60 days after the final rule's publication.

ALSTON & BIRD

Tri-Agency FAQ 69: Gag Clause Prohibitions and Attestations; No Surprises Act

32

Health & Welfare Benefits
MONTHLY UPDATE

FAQs Part 69 - Gag Clause Prohibition and Attestation

Downstream contracts

- A plan or insurer violates the gag clause prohibition if its TPA or other service provider has a contract that prohibits sharing relevant information with the plan or insurer
- To avoid violating the gag clause prohibition, **the departments expect that plans and insurers will include provisions in their direct contracts prohibiting TPAs and other service providers from executing downstream agreements with other parties that restrict the plan or insurer from sharing information or data**.

33

ALSTON & BIRD

33

Health & Welfare Benefits
MONTHLY UPDATE

FAQs Part 69 - Gag Clause Prohibition and Attestation

Downstream contracts (continued)

- Gag clause prohibition does not apply directly to TPAs or other service providers, but departments are indirectly requiring their compliance
- TPAs and other service providers will want to ensure their contracts with downstream entities allow plan and insurer clients to meet compliance attestation obligations, as plans and issuers are likely to require contractual representations about downstream contracts

Health & Welfare Benefits
MONTHLY UPDATE

FAQs Part 69 - Gag Clause Prohibition and Attestation

Discretionary sharing of de-identified claims with BAs prohibited

- An agreement has a prohibited gag clause if it permits the plan or insurer to share de-identified claims data with a business associate only at the discretion of a health care provider, network, association of providers, TPA, or other service provider offering network access

Health & Welfare Benefits
MONTHLY UPDATE

FAQs Part 69 - Gag Clause Prohibition and Attestation

Examples of prohibited restrictions on de-identified claims or data

- Prohibited gag clauses include limitations on the scope, scale, or frequency of electronic access to de-identified claims and encounter information or data to the extent such limitations place unreasonable limits on access to the information upon request. Unless the information or data is otherwise electronically accessible to the plan or insurer, prohibited gag clauses related to audit or claims review include:
  - Limitations on access to a statistically significant or the minimum necessary number of de-identified claims.
  - Limitations on the scope of access to the data to specific, narrow purposes (such as limiting access to an audit).
  - Unreasonable limitations on the frequency of claims reviews (for example, no more than once per year).
  - Limitations on the number and types of de-identified claims that a plan or issuer may access.
  - Restrictions on the data elements of a de-identified claim that a plan or issuer may access.
  - Limiting access to de-identified claims data to the TPA's or service provider's physical premises.
- This is not an exclusive list and agencies may provide additional examples.

Health & Welfare Benefits
MONTHLY UPDATE

FAQs Part 69 - Gag Clause Prohibition and Attestation

Submitting gag clause attestation with non-compliant agreements

- If a plan or issuer has an agreement that violates the gag clause prohibition and has been unable to remove the noncompliant provision from their agreement, the plan or insurer must identify the noncompliant provision as part of their attestation. This includes both direct contracts and downstream agreements. The attestation must include:
  - Any prohibited gag clauses that a service provider has refused to remove.
  - The name of the TPA or service provider with which the plan or insurer has the agreement containing the prohibited gag clause.
  - Conduct by the service provider that shows the service provider interprets the agreement to contain a prohibited gag clause.
  - Information on the plan's or insurer's requests that the prohibited gag clause be removed from such agreement.
  - Any other steps the plan or insurer has taken to come into compliance with the provision.

Health & Welfare Benefits
MONTHLY UPDATE

FAQs Part 69 - Gag Clause Prohibition and Attestation

Submitting gag clause attestation with non-compliant agreements (continued)

- Scope of this FAQ (FAQ-9) is unclear:
  - First Interpretation: Statute applies to agreements between a plan or insurer and TPA or service provider
    - Practical effect is that the service provider must ensure that it can provide access to plan or insurer
    - If an agreement does not provide this assurance, then it appears to have a gag clause
  - Second Interpretation: Plan or issuer must identify gag clauses in downstream agreements to which they are not a party
    - If this is what the departments mean, then this would appear to be contrary to the statute.
    - Unclear if/how departments will wage that battle.
    - Cautious plans/issuers might consider carefully drafted contract terms.

Health & Welfare Benefits
MONTHLY UPDATE

FAQs Part 69 - No Surprises Act

- Calculating QPA after Fifth Circuit's decision in Texas Medical Association v. HHS (aka TMA III)
- Disclosures of QPA to nonparticipating providers, facilities, and providers of air ambulance service within initial payment or notice of denial of payment, and in a timely manner upon request
- Timing of required disclosures when an initial payment or notice of denial is sent electronically while required disclosures are sent using paper
- After a certified IDR entity makes a payment determination for a qualified IDR item or service, may a plan or insurer recalculate cost-sharing if the recalculation results in a cost-sharing amount that exceeds the amount calculated using the lesser of the billed charge or the QPA?
  - Cannot recalculate or increase a participant's cost-sharing based on the amount of the certified IDR entity's payment determination (or for any other reason) if it would result in a cost-sharing amount that exceeds the permitted amount calculated using the recognized amount (or lesser of the billed charge or the QPA for out-of-network ambulance services).
  - Payments made after a certified IDR entity makes a payment determination must be made in full and cannot be reduced based on any prohibited increase in cost-sharing displayed on an EOB generated after an IDR payment determination.

ALSTON & BIRD

Miscellaneous

40

Health & Welfare Benefits
MONTHLY UPDATE

Disaster Relief: IRS Filing Extensions

Deadlines vary depending upon the disaster and locality. Details on all recent disaster relief for presidentially-declared disasters are on the Around the nation page on IRS.gov. Currently:

- Taxpayers in the following states and affected areas have until May 1, 2025, to file 2023 tax year returns:
  - Taxpayers in **all of** Alabama, Florida, Georgia, North Carolina, South Carolina.
  - Taxpayers in affected parts of Alaska, New Mexico, Tennessee, Virginia and West Virginia.
- Taxpayers in parts of California affected by fires have until October 15, 2025 to file various federal individual and business tax returns and make tax payments. See the link below.
- The IRS automatically provides filing and penalty relief to any taxpayer with an IRS address of record located in the disaster area. The DOL automatically recognizes these extensions for Form 5500 filing. Visit https://www.irs.gov/newsroom/tax-relief-in-disaster-situations for more information.

Health & Welfare Benefits
MONTHLY UPDATE

Disaster Relief: Extensions of Timeframes

- DOL/EBSA and Treasury/IRS published **Extension of Time Frames** in FR on Nov. 8, 2024 for Hurricane and Tropical Storm Helene and Hurricane Milton. *Note: "Disaster areas" are those areas designated as eligible for Individual Assistance by FEMA due to a particular storm. It is narrower in some states than the IRS tax filing relief.*
- Extensions for Participant, beneficiary, qualified beneficiary, or claimant apply to Special Enrollment requests (30 or 60 days); COBRA 60-day election period; COBRA premium payment deadlines; Deadline for disability determination notices; Claim filing deadline; Deadline for filing appeals of adverse benefit determinations; Deadline for filing requests for external review; Deadline for filing information to perfect a request for external review.
- Extensions for GHP, sponsor or TPA: Providing COBRA election notice.
- EBSA also published Disaster Relief Notice 2024-01, as well as general FAQs for participants and beneficiaries impacted by Hurricane Helene or Hurricane Milton.
  - EBSA Notice 2024-01 extends deadlines for furnishing notices, disclosures, and other documents required by provisions of Title I of ERISA to plan participants, beneficiaries, and other persons so that employers, plan fiduciaries, and plan sponsors have additional time to meet their obligations.

Health & Welfare Benefits
MONTHLY UPDATE

Medicare Creditable Coverage: New Proposed Methodology

- On January 10, 2025, Centers for Medicare & Medicaid proposed an update to its simplified Rx drug creditable coverage determination methodology.
- Currently, group health plans that do not receive retiree drug subsidy have two methodologies available for determining creditable coverage:
  - Actuarial Equivalence Test
  - Simplified Determination Methodology
- Current proposal is for the simplified determination methodology only and would consider Rx drug coverage to be equal to or exceed the standard Part D benefit if it meets ***all*** of the following:
  - Provides reasonable coverage for brand name and generic prescription drugs and biological products;
  - Provides reasonable access to retail pharmacies; and
  - Is designed to pay on average at least 72 percent (up from 60%) of participants' prescription drug expenses.
- The proposed updated method would do away with some of the current requirements (some of which are obsolete due to changes in other laws or changes in the group health plan market) but would add biological products and increase the plan's share from 60% to 72% of expenses.
- Comments were due by February 10, 2025; CMS intends to finalize by April 7, 2025.

44

ALSTON & BIRD

Employee Benefits & Executive Compensation Advisory | Changes to Employer Reporting Requirements Under the ACA

January 6, 2025

Advisories

By: Ashley Gillihan, Laurie Kirkwood, Bria Smith

The new year is off to a good start for plan sponsors required to distribute Forms 1095-B and 1095-C under the Affordable Care Act (ACA). Congress passed two new laws – the Paperwork Burden Reduction Act and the Employer Reporting Improvement Act – which together ease compliance burdens for plan sponsors. These changes include:

- *Alternative manner of furnishing Forms 1095-B and 1095-C to employees upon request*: Entities required to furnish Forms 1095-B and 1095-C to employees may now provide these statements upon request only. These statements no longer have to be furnished to employees automatically.
- *Statutory changes to electronic delivery of Forms 1095-B and 1095-C*: The duration of consent to electronic delivery of statements lasts until the employee revokes consent in writing. Regulations require the consent to state the scope and duration of consent, but this statutory change allows the consent to be valid until withdrawn in writing.
- *More time to respond to penalty assessment letters from the IRS*: Certain large employers now have more time – 90 days rather than 30 days – to respond to letters from the IRS that propose to assess an employer shared responsibility payment (ESRP).
- *Fixed statute of limitations for ESRP assessments under Code Section 4980H*: Congress set a six-year statute of limitations for the IRS to assess the ESRP penalty.
- *Codifies the birthdate substitution for TINs*: Congress made the flexibility for using a full name and birthdate instead of the taxpayer identification number (TIN) on Forms 1095-B and 1095-C a statutory provision rather than just regulatory provision.

We focus on what these changes mean under the ACA for large employers, which typically file and furnish Forms 1095-C to report information on employer-provided health insurance offerings and coverage. However, these changes also apply to reporting entities for Forms 1095-B (e.g., insurers and employers sponsoring self-insured plans).

Current Law

Under the ACA, applicable large employers (ALEs) – or large employers who have employed an average of at least 50 full-time equivalent employees in the prior year – are required to provide Form 1095-C to all full-time employees. Employers of all sizes with self-insured plans must also provide the form to all employees enrolled in the employer's health plan, regardless of full-time status. Although employers have the option to either mail these statements or furnish them electronically, employers must distribute them automatically. Electronic delivery requires employee consent, and one of the consent requirements is to define the scope and duration of the consent. This can result in the employee limiting the consent to, for example, only the upcoming Form 1095-C, or to a span of 12 months. The difficulty of managing the consent requirements (e.g., different durations for each employee) has resulted in many ALEs choosing to mail these forms to their employees. In either case, automatic distribution must be done by January 31 each year (or March 1, if using an extension).

ALEs also send these Forms 1095-C to the IRS, which in turn uses some of that information to determine whether to assess an ESRP penalty against the employer. If that happens, the IRS sends a letter to the ALE informing the employer of the potential penalty (these are called 226-J letters). These letters usually include a response form that must be returned to the IRS within 30 days, which can be a tight turnaround time if the letter takes a while to move through the employer's organization and get into the hands of someone authorized to reply. Failure to respond by the deadline could result in the IRS assessing the penalties against the employer. Although the IRS grants extensions for these responses when the request is made within the 30-day period, employers are at risk of not getting an extension for requests made after the 30-day deadline.

ALEs also never know when they may receive a 226-J letter from the IRS for a given year proposing an ESRP assessment because, according to the IRS, there is no statute of limitations for assessing the ESRP. Not knowing when an assessment of ESRP may be proposed from a prior year can affect the employer's standard record retention policies and procedures.

Changes in 2025

Under the newly enacted laws, ALEs have a substantially reduced burden for distributing Form 1095-C to employees and have much more breathing room to

respond to 226-J letters from the IRS. Changes include:

- **Alternative manner of furnishing statements.** ALEs now have an alternative to automatically providing Form 1095-C to employees by January 31. Instead of automatically furnishing the statement, either by mail or electronic delivery (if consent has been obtained), ALEs can now provide the statement upon request. ALEs will be treated as providing the Form 1095-C timely so long as:
  - The employer "provides clear, conspicuous, and accessible notice" to employees entitled to receive the Form 1095-C that they can request a copy of it.
  - The employer satisfies the request for the statement no later than the later of:
    - January 31 of the year following the calendar year for which the return was required to be made, or
    - 30 days after the date of the request.

  The ALEs would still have to mail the Form 1095-C to the employee requesting the statement unless the employee consented to electronic delivery.

  Effective date: This alternative manner of furnishing statements is available for statements for returns for calendar years after 2023, which includes 2024 Forms 1095-C. Although Congress deferred the time and manner of the required notice to the Secretary of the Treasury, a good-faith compliance standard would likely apply until further guidance is provided.

  Practice Pointer: Until the IRS provides further guidance on the time and manner of notice, ALEs wishing to use this alternative manner for distributing their 2024 Forms 1095-C may want to look at regulations for similar notice provisions for guidance. For ALEs with self-insured plans, the IRS already provides an alternative manner of furnishing Form 1095-C to covered nonemployees and covered employees who were not full-time employees at any time during the year. Under those regulations, the notice requirement is met if the reporting entity posts the notice prominently in a location on its website that is reasonably accessible to all individuals entitled to receive the form stating that they may receive a copy upon request. The notice must include an email address and a physical address to which a request may be sent, as well as a telephone number for questions. The regulations also require the notice to be retained in the same location on the ALE's website through October 15 following the calendar year to which the statements related (or the first business day after October 15, if October 15 is not a business day).

- **Proper electronic consent is valid until it is revoked**. Under the current regulations, consent from employees for electronic distribution of the Form 1095-C must state the scope and duration of the consent. Under the new statutory provision, an individual is deemed to have consented to receive the Form 1095-C in electronic form if they have affirmatively consented "at any prior time" to the employer (or to the entity required to provide the Form 1095-C). The consent is valid until the individual revokes the consent in writing.

  Effective date: This change applies to Forms 1095-C due after December 31, 2024.

- **More time to respond to ESRP assessment letters.** ALEs now have 90 days, instead of just 30 days, to respond to the "first letter" (i.e., the 226-J letter) from the IRS proposing an assessment of the ESRP against the employer. The new law does not indicate whether an ALE can still request an extension beyond 90 days.

  Effective date: This change applies to assessments proposed in taxable years beginning after December 23, 2024.

- **Six-year statute of limitations ESRP assessments under Code Section 4980H.** Congress added a six-year statute of limitations on assessments of the ESRP under Code Section 4980H. The six-year period begins on the due date for filing the return or, if later, the date the return was filed for the calendar year for which the ESRP penalty is determined.

  Effective date: This change applies for returns due after December 31, 2024. Note that this change does not necessarily affect the IRS's position on the statute of limitations for prior years.

- **Codifies the birthdate substitution for TINs.** Congress made the flexibility for using a full name and birthdate instead of the TIN on Forms 1095-B and 1095-C a statutory provision rather than just a regulatory provision. Regulations already permitted the birthdate rather than the TIN to be used if "reasonable efforts" had been made to obtain the TIN. The statutory language states that if the person required to make a return "is unable to collect information on the TINs," the Secretary of the Treasury "may allow" the individual's full name and birthdate to be substituted for the TIN (note the discretionary wording of "may allow" rather than "shall allow").

  Effective date: This statutory change applies for returns with due dates after December 31, 2024, although technically it is already permitted under the regulations.

If you have any questions about these changes, contact your employee benefits counsel.

Meet the Authors

Ashley Gillihan

Partner

Phone: +1 404 881 7390
Email: ashley.gillihan@alston.com

Laurie Kirkwood

Senior Attorney

Phone: +1 404 881 7814
Email: laurie.kirkwood@alston.com

Bria Smith

Associate

Phone: +1 404 881 7559
Email: bria.smith@alston.com

ALSTON & BIRD

Employee Benefits & Executive Compensation Advisory | New Year Brings New Tri-Agency FAQs About Gag Clause Prohibitions and Attestations, No Surprises Act

January 22, 2025

Advisories

By: Steven C. Mindy, John R. Hickman, Ashley Gillihan, Laurie Kirkwood

On January 14, 2025, the departments of Labor, Health and Human Services, and Treasury, as well as the Office of Personnel Management, issued FAQs About Consolidated Appropriations Act, 2021 Implementation Part 69. The FAQs provides guidance on both the gag clause prohibition compliance and the No Surprises Act. Health plans and their vendors, including third-party administrators (TPAs), will want to be aware of a new requirement to ensure that contracts do not have prohibited gag clauses.

Gag Clause Prohibition and Attestation FAQs

Generally, group health plans and health insurers offering group or individual cover cannot enter into an agreement with a provider, association of providers, network, TPA, or other service provider offering access to a network that directly or indirectly restricts the plan or insurer from:

1. Making provider-specific cost or quality-of-care information or data available to active or eligible participants, beneficiaries, and enrollees of the plan or coverage, plan sponsors, or referring providers.
2. Electronically accessing de-identified claims and encounter information or data for each participant, beneficiary, or enrollee in the plan or coverage consistent with applicable privacy regulations, upon request.
3. Sharing such information or data described in (1) and (2), or directing such data be shared, with a business associate consistent with applicable privacy regulations.

By December 31 of each year, plans and insurers must submit a gag clause prohibition compliance attestation (GCPCA) to the departments.

Does a plan or issuer have a contract with a prohibited gag clause if its TPA or other service provider has an agreement with another party that restricts the plan or insurer from providing, electronically accessing, or sharing information?

Yes. A plan or issuer violates the gag clause prohibition if its TPA has a contract that prohibits the TPA from sharing relevant information with the plan or insurer even though it is not a party to the TPA's other agreement. To avoid violating the gag

clause prohibition, **the departments expect that plans and insurers will include provisions in their direct contracts prohibiting TPAs and other service providers from executing downstream agreements with other parties that restrict the plan or insurer from sharing information or data**. The departments view such downstream agreements as an "indirect" restriction on the plan or issuer. Plans, insurers, and their service providers will want to be mindful of this new requirement. Although the gag clause prohibition does not apply directly to TPAs and other service providers, the departments have indirectly required their compliance by requiring plans and insurers to achieve their compliance contractually. Thus, TPAs and other services providers will want to ensure their contracts with downstream entities allow their plan and insurer clients to meet their GCPCA obligations since plans and issuers are likely to require contractual representations about whether those contracts comply with the gag clause prohibition.

Does an agreement violate the gag clause prohibition if it allows the plan or insurer to share de-identified claims data with a business associate only at the discretion of a health care provider, association of providers, TPA, or other service provider offering network access?

Yes. An agreement has a prohibited gag clause if it permits the plan or insurer to share de-identified claims data with a business associate only at the discretion of a health care provider, network, association of providers, TPA, or other service provider offering network access.

What restrictions on access to de-identified claims and encounter information or data violate the gag clause prohibition?

Prohibited gag clauses include limitations on the scope, scale, or frequency of electronic access to de-identified claims and encounter information or data to the extent such limitations place unreasonable limits on access to the information upon request. Unless the information or data is otherwise electronically accessible to the plan or insurer, prohibited gag clauses related to audit or claims review include:

- Limitations on access to a statistically significant or the minimum necessary number of de- identified claims.
- Limitations on the scope of access to the data to specific, narrow purposes (such as limiting access to an audit).
- Unreasonable limitations on the frequency of claims reviews (for example, no more than once per year).
- Limitations on the number and types of de-identified claims that a plan or issuer may access.
- Restrictions on the data elements of a de-identified claim that a plan or issuer may access.
- Limiting access to de-identified claims data to the TPA's or service provider's physical premises.

The departments noted that this is not an exhaustive list and that they may provide additional examples of prohibited gag clauses.

How do plans and insurers submit a GCPCA if they entered into an agreement that violates the gag clause prohibition?

If a plan or issuer has an agreement that violates the gag clause prohibition and has been unable to remove the noncompliant provision from their agreement, the plan or insurer must identify the noncompliant provision as part of their attestation. This requirement applies to both a direct agreement between the plan/issuer and the service provider and a downstream agreement between the service provider and another entity that restricts the use of such relevant information or data. Once the plan or issuer has identified the noncompliant provision, it may use the text box labelled "Additional Information" in the

GCPCA webform system on step 3 to include the provision as part of its attestation. The additional information includes:

- Any prohibited gag clauses that a service provider has refused to remove.
- The name of the TPA or service provider with which the plan or insurer has the agreement containing the prohibited gag clause.
- Conduct by the service provider that shows the service provider interprets the agreement to contain a prohibited gag clause.
- Information on the plan's or insurer's requests that the prohibited gag clause be removed from such agreement.
- Any other steps the plan or insurer has taken to come into compliance with the provision.

The prohibited gag clauses might still prompt enforcement action by the departments. The departments will take into account good-faith efforts to self-report a prohibited gag clause in the event of any enforcement action. Nonetheless, a plan or insurer submitting such additional information is considered to satisfy their obligation to submit a GCPCA.

We note that the scope of this FAQ (FAQ-9) is unclear. The departments state that this requirement applies to both a direct agreement between the plan/issuer and the service provider and a downstream agreement between the service provider and another entity that restricts the use of such relevant information or data. However, reading the FAQs in the context of the statute, which is limited in scope to an agreement to which the plan or issuer is a party, the departments appear to be saying that an agreement between a plan or issuer and a service provider must contain assurances from the service provider that the plan or issuer will have the access required by the statute. The practical effect is for the service provider to ensure that it can, in fact, provide such access. If an agreement does not contain such an assurance, the agreement would appear to have a gag clause under these FAQs. Another interpretation of these FAQs is that the plan or issuer must identify gag clauses in downstream agreements to which they are not a party. If that is what the departments are saying, that would appear to be counter to the terms of the statute.

No Surprises Act FAQs

The No Surprises Act protects group health plan or group or individual health insurance participants, beneficiaries, and enrollees against surprise medical bills for certain out-of-network services. The departments established a federal independent dispute resolution (IDR) process to resolve disputes between plans or insurers and providers, facilities, or providers of air ambulance services about the out-of-network rate for certain items and services. The departments' regulations and guidance provided methodology for calculating the qualifying payment amount (QPA) for those out-of-network services. In *Texas Medical Association v. United States Department of HHS* (also known as *TMA III*), the Eastern District of Texas vacated and remanded certain parts of these regulations and guidance. In response, the departments issued several FAQs (FAQs About Consolidated Appropriations Act, 2021 Implementation Part 62 and FAQ About Consolidated Appropriations Act, 2021 Implementation Part 67). On October 30, 2024, in *TMA III*, the Fifth Circuit issued an opinion and order that partially reversed the district court's decision. The latest FAQs provide guidance in response to that decision.

How should plans and insurers calculate the QPA after the Fifth Circuit's TMA III decision?

Unless the Fifth Circuit decides to rehear its panel's *TMA III* decision and alters its judgment, plans and insurers must calculate QPAs using a good-faith, reasonable interpretation of applicable statutes and regulation that remain in effect after the decisions of both the Fifth Circuit and district court once the Fifth Circuit issues its mandate. However, the departments

recognize the significant amount of time and resources it will again take to review and recalculate QPAs. For items and services furnished before August 1, 2025, the departments will extend the enforcement discretion provided in FAQs 62 and 67 under the relevant No Surprises Act provisions for any plan, insurer, or party to the IDR payment dispute process that uses a QPA calculated under the departments' 2021 methodology (in other words, the regulations and guidance in effect before the district court's *TMA III* decision).

Because the Fifth Circuit has not yet issued its mandate, plans and issuers can continue to rely on QPAs that have already been calculated using a good-faith, reasonable interpretation of the departments' 2023 methodology (in other words, FAQ 62). Once the Fifth Circuit issues its mandate, the departments will exercise enforcement discretion for QPAs calculated using a good-faith, reasonable interpretation of the 2023 methodology for items and services furnished before August 1, 2025. This enforcement discretion for QPAs using the 2021 or 2023 methodology applies to (1) patient cost-sharing; (2) providing required disclosures with an initial payment or notice of denial of payment; and (3) providing required disclosures and submissions under the IDR process. The FAQ notes that HHS will exercise enforcement discretion for a provider, facility, or provider of air ambulance services that bills, or holds liable, a participant, beneficiary, or enrollee for a cost-sharing amount based on a QPA calculated using the 2021 or the 2023 methodology, for items and services furnished before August 1, 2025.

How should plans and insurers make disclosures about the QPA to nonparticipating providers, facilities, and providers of air ambulance services with an initial payment or notice of denial of payment, and in a timely manner upon request?

Plans and insurers should make these disclosures about the QPA consistent with prior guidance, which was not affected by the Fifth Circuit's decision. A plan or insurer may certify that it determined a QPA in compliance with the applicable rules if it used a good-faith, reasonable interpretation of the applicable statutes and regulations that remain in effect after the decisions of both the Fifth Circuit and the district court in *TMA III*.

The departments will exercise enforcement discretion for disclosures regarding a QPA provided with an initial payment or notice of denial of payment. Specifically, for items and services furnished before August 1, 2025, the departments will exercise enforcement discretion when the plan or insurer using the 2021 or 2023 methodology certifies that the QPA was determined consistent with the applicable regulations. However, the plan or insurer must disclose in a timely manner upon request that it is using a QPA calculated using the 2021 or 2023 methodology, as applicable.

When must a plan or insurer provide the required disclosures when an initial payment or notice of denial is sent electronically while required disclosures are sent using paper?

The departments note that a plan or insurer is not relieved from sending required disclosures with each initial payment or notice of denial when the plan's or issuer's method of electronic transmission of the initial payment or notice of denial does not allow for the disclosures to be sent with the transmission. When sending an initial payment or notice of denial electronically and required disclosures on paper *for out-of-network emergency services and applicable non-emergency items*, a plan or insurer must transmit the required disclosures on or near the date it sends the initial payment or notice of denial of payment. The plan or insurer must ensure that it sends all this no later than 30 calendar days after receipt of the information necessary to decide the claim. *For out-of-network air ambulance services*, the plan or insurer must transmit the required disclosures on or near the date that it sends the initial payment or notice of denial. The plan or insurer must ensure that it sends all this no later than 30 calendar days after the provider of air ambulance services transmits the bill for services.

What is the deadline to initiate open negotiation when required disclosures are received on paper after the initial payment or notice of denial is sent electronically?

When the plan or insurer sends disclosures in a timely manner, the period to initiate open negotiation ends 30 business days after the provider, facility, or provider of air ambulance services has received both the initial payment or notice of denial of payment and the required disclosures. However, at its discretion, a provider, facility, or provider of air ambulance services may initiate open negotiation after receiving the initial payment or notice of denial even if it has not yet received the required disclosures. If a provider, facility, or provider of air ambulance services receives an initial payment or notice of denial but has not received the required disclosures at all, or has received disclosures sent outside the required timeframe, then it may initiate open negotiation or request an extension to initiate the IDR process.

After a certified IDR entity makes a payment determination for a qualified IDR item or service, may a plan or insurer recalculate cost-sharing if the recalculation results in a cost-sharing amount that exceeds the amount calculated using the lesser of the billed charge or the QPA?

No. The cost-sharing amount for out-of-network emergency services and applicable non-emergency items and services must be calculated using the recognized amount under the No Surprises Act (or lesser of the billed charge or QPA for out-of-network air ambulance services). The departments noted that the have received reports of some plans and insurers generating new explanations of benefits (EOBs) after an IDR payment decision was made. The FAQ states that a plan or insurer cannot recalculate or increase a participant's, beneficiary's, or enrollee's cost-sharing based on the amount of the certified IDR entity's payment determination (or for any other reason) if it would result in a cost-sharing amount that exceeds the permitted amount calculated using the recognized amount (or lesser of the billed charge or the QPA for out-of-network ambulance services). The departments remind plan and insurers that payments made after a certified IDR entity makes a payment determination must be made in full and cannot be reduced based on any prohibited increase in cost-sharing displayed on an EOB generated after an IDR payment determination.

Conclusion

It is likely that the departments will issue further guidance on gag clauses and the No Surprises Act in the future. Gag clause prohibition compliance and reporting is not impacted currently by any court cases but, due to the FAQs, will require careful attention by plans and issuers. In particular, plans and insurers will need to ensure that their contracts with TPAs and other service providers contain representations that the TPA or other service provider does not have any contracts with other parties that might prevent the plan or issuer from receiving required information or data. Meanwhile, TPAs and other service providers should make sure that their contracts with other parties do not have terms that prevent them from representing that they do not have any contracts with downstream entities that might cause a plan or insurer to violate the gag clause prohibition since plans and insurers will likely be requesting such representations after the departments' new FAQ.

Notably, *TMA III* is still making its way through the courts, so compliance with the No Surprises Act might be impacted by future decisions. In the meantime, plans and insurers should be certain to follow the updated guidance in the departments' FAQs.

Meet the Authors

Steven C. Mindy

Partner

Phone: +1 202 239 3816
Email: steven.mindy@alston.com

John R. Hickman

Partner

Phone: +1 404 881 7885
Email: john.hickman@alston.com

Ashley Gillihan

Partner

Phone: +1 404 881 7390
Email: ashley.gillihan@alston.com

Laurie Kirkwood

Senior Attorney

Phone: +1 404 881 7814
Email: laurie.kirkwood@alston.com

ALSTON & BIRD

Employee Benefits & Executive Compensation Advisory | Health Plan Impact of HHS's Proposed HIPAA Security Rule Update

February 11, 2025

Advisories

By: Steven C. Mindy, John R. Hickman, Laurie Kirkwood

At the close of 2024, the Department of Health and Human Services (HHS) Office of Civil Rights issued a proposed update to the HIPAA Security Rule. While these proposed rules have the attention of many health care providers, health plans and their business associates also should pay close attention. In addition to new technological and documentation requirements, the proposal requires plan amendments and new business associate agreements. Public comments on the rule are due by March 7, 2025.

Health plans will need to comply with most of the new Security Rule requirements 180 days after the final rule's effective date. Health plans have more obligations under the proposed rule than other HIPAA covered entities (health care providers and health care clearinghouses), as well as areas where they might find compliance more difficult than other HIPAA covered entities.

Business associates of health plans will also want to pay attention to the proposed rule because they will also be subject to the revised Security Rule. The rule requires business associates to notify plans (or other covered entities) without unreasonable delay and no later than 24 hours after activation of the new contingency plan that the proposed Security Rule requires.

Plan Amendment Requirement Imposes Compliance Obligations on Both Plans and Plan Sponsors

Under the proposed rule, health plans will be required to adopt a plan amendment that applies the Security Rule to both the plan and the plan sponsor. A group health plan must ensure that its plan documents require the plan sponsor to reasonably and appropriately safeguard electronic protected health information (ePHI). This requirement applies unless the only ePHI disclosed to the plan sponsor is: (1) summary health information about an individual's participation in or enrollment or disenrollment in a health plan; (2) summary health information for premium bids or modifying, amending, or terminating the plan; or (3) authorized by the individual. To implement this requirement, the plan amendment must require the plan sponsor to:

- Implement the administrative, physical, and technical safeguards that covered entities and business associates must implement under 45 C.F.R. §§ 164.308(a), 164.310, and 164.312.

- Ensure adequate separation from the plan is supported by the administrative, physical, and technical safeguards.
- Make sure that any agent to whom the plan sponsor provides the plan's ePHI implements the administrative, physical, and technical safeguards.
- Report to the plan any security incident of which it becomes aware.
- Report to the plan without unreasonable delay and in no case later than 24 hours any activation of the plan sponsor's contingency plan adopted consistent with the proposed Security Rule's administrative safeguard requirements.

Plans, Plan Sponsors, Business Associates, and Agents Must Adopt a Contingency Plan

As a result of the plan amendment requirement, both the plan (and its business associates) and the plan sponsor (and its agents) will need a written contingency plan. The proposed rule requires the contingency plan to consist "of written policies and procedures for responding to an emergency or other occurrence, including, but not limited to, fire, vandalism, system failure, natural disaster, or security incident, that adversely affects relevant electronic information systems." The written contingency plan requirements include:

- **Criticality Analysis.** Perform and document an assessment of the relative criticality of relevant electronic information systems and technology assets.
- **Data Backups.** Establish and implement written procedures to create and maintain exact retrievable copies of ePHI, including verification that the ePHI has been copied accurately.
- **Information Systems Backups.** Establish and implement written procedures to create and maintain backups of relevant electronic information systems, including verification of success of backups.
- **Disaster Recovery Plan.** Establish (and implement as needed) written procedures to restore loss of: (1) critical relevant electronic information systems and data *within 72 hours of the loss*; and (2) other relevant electronic information systems and data in accordance with the criticality analysis.
- **Emergency Mode Operation Plan.** Establish (and implement as needed) written procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode.
- **Testing and Revision Procedures.** Establish written procedures for testing and revising contingency plans. Review and test contingency plans at least once every 12 months, document the results of such tests, and modify such contingency plans as reasonable and appropriate in accordance with the results of those tests.

Plan Amendment, Contingency Plan, and Compliance with Most New Requirements Required Within 240 Days After Final Rule Published

Like most of the new or updated requirements in the proposed Security Rule, the plan amendment and contingency plan will need to be adopted within 180 days after the effective date of the final rule. The final rule's effective date will be the date 60 days after its publication in the *Federal Register*. As a result, plans and plan sponsors will need to move quickly to establish and implement the new Security Rule once it is finalized.

New Business Associate and Subcontractor Agreements Required, but Longer Transition Period Might Be Available

The proposed Security Rule requires plans and their business associates to execute new business associate or

subcontractor agreements. However, this requirement has a longer transition period under the proposed rule. As proposed, a limited deemed compliance period is available if: (1) the written contract with the business associate (or subcontractor) complies with the requirements for business associate agreements under the current rule; and (2) the business associate agreement is not renewed or modified from 60 days after publication of the final rule in the *Federal Register* until 240 days after publication. A business associate (or subcontractor) agreement that meets those requirements shall be deemed compliant until the earlier of: (1) the date the contract or arrangement is renewed on or after 240 days after the final rule's publication; or (2) one year and 60 days after the final rule's publication.

Proposed Security Rule Requirements

As our Health Care and Privacy, Cyber & Data Strategy teams discussed in their advisory about the proposed Security Rule updates that are generally applicable to HIPAA covered entities (i.e., health plans, health care providers, and health care clearinghouses) and their business associates, the proposed rule eliminates the distinction between "required" and "addressable" implementation specifications in favor of compliance with *all* standards (see New Year, New HIPAA Security Rule: OCR Adds to Health Care Entities' New Year's Resolutions). These standards include:

Administrative safeguards

- **Technology Asset Inventory.** Conduct and maintain an accurate and thorough written inventory and a network map of electronic information systems and all technology assets that may affect the confidentiality, integrity, or availability of ePHI.
- **Risk Analysis.** Conduct an accurate and comprehensive written assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all ePHI created, received, maintained, or transmitted.
- **Evaluation.** Perform a written technical and nontechnical evaluation to determine whether a change in environment or operations may affect the confidentiality, integrity, or availability of ePHI. Note that the rule requires this to be done within a reasonable period of time *before making a change* to the environment or operations, which will require careful coordination among different departments of plans and their sponsors.
- **Patch Management.** Implement written policies and procedures for applying patches and updating the configuration(s) of relevant electronic information systems.
- **Risk Management.** Implement security measures sufficient to reduce risks and vulnerabilities to all ePHI to a reasonable and appropriate level.
- **Sanction Policy.** Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures.
- **Workforce Security.** Implement written policies and procedures to ensure that all workforce members have appropriate access to ePHI and relevant electronic information systems, and to prevent those workforce members who are not authorized to have access from obtaining access to ePHI and relevant electronic information systems. Significantly, a "workforce member's access must be terminated as soon as possible but no later than one hour after the employment of, or other arrangement with, a workforce member ends," which might be difficult to implement in situations when employment terminations are sudden and unexpected (among many other common workplace scenarios). Additionally, *other covered entities and business associates must be notified no later than 24 hours after a workforce member's change in or termination of access to ePHI* or relevant electronic information systems.
- **Information Access.** Establish and implement written policies and procedures for authorizing access to ePHI and relevant electronic information systems.
- **Security Awareness Training.** Implement security awareness training for all workforce members as necessary and appropriate for the workforce members.

- **Security Incident Procedures.** Implement written policies and procedures to respond to security incidents.
- **Compliance Audit.** Perform and document an audit at least once every 12 months of compliance with each of the Security Rule's standards and implementation specifications.
- **Business Associate Agreement.** The business associate agreement requirement is familiar to health plans but is updated to require that covered entities such as the plan *obtain the business associate's written verification that it has deployed the Security Rule's technical safeguards at least once every 12 months* . The business associate's written verification must include:
  - A *written analysis* of the business associate's relevant electronic information systems by a person with appropriate knowledge of and experience with generally accepted cybersecurity principles and methods for ensuring the confidentiality, integrity, and availability of ePHI to verify compliance with each standard and implementation specification for technical safeguards.
  - A *written certification* that the analysis has been performed and is accurate by a person who has the authority to act on behalf of the business associate.

  If finalized, this requirement effectively adds a new duty for plans and other covered entities to monitor compliance by the business associates on a regular, ongoing basis.
- **Delegation to Business Associate.** A plan, other covered entity, or business associate may delegate a business associate to serve as their security official but will remain liable for compliance with all Security Rule requirements.

Physical safeguards

- **Facility Access Controls.** Establish and implement written policies and procedures to limit physical access to all relevant electronic information systems and the facilities in which they are housed, while ensuring that properly authorized access is allowed.
- **Workstation Use.** Establish and implement written policies and procedures that govern the use of workstations that access ePHI or relevant electronic information systems.
- **Workstation Security.** Implement and modify physical safeguards for all workstations that access ePHI or relevant electronic information systems.
- **Technology Asset Controls.** Establish and implement written policies and procedures that govern the receipt and removal of technology assets that maintain ePHI into and out of a facility, and the movement of these assets within the facility.

Technical safeguards

- **Access Control.** Deploy technical controls in relevant electronic information systems to allow access only to users and technology assets that have been granted access rights. Note that this requires separate user identities from identities used for administrative and other increased access privileges, among other requirements.
- **Encryption and Decryption.** Deploy technical controls to encrypt and decrypt ePHI using encryption that meets prevailing cryptographic standards. Note that this requires encryption of all ePHI at rest and in transit. The proposed rule provides a few exceptions to this requirement. Health plans should note that they can provide unencrypted ePHI to individuals who request unencrypted access to their PHI, but the individual first must be informed of the risks associated with the transmission, receipt, and storage of unencrypted ePHI. Note that this exception does not apply when the individual receiving the ePHI is using technology controlled by the plan or its business associate.
- **Configuration Management.** Establish and deploy technical controls for securing relevant electronic information systems and technology assets, including workstations, in a consistent manner, and maintain such electronic information systems and technology assets according to established secure baselines.

- **Audit Trail and System Log Controls.** Deploy technology assets and/or technical controls that record and identify activity in the covered entity's or business associate's relevant electronic information systems.
- **Integrity.** Deploy technical controls to protect ePHI from improper alteration or destruction, both at rest and in transit; and review and test the effectiveness of such technical controls at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, and modify as reasonable and appropriate. Among other things, this requirement makes use of multi-factor authentication mandatory for accessing electronic information systems that contain ePHI or changing user privileges to systems with ePHI.
- **Transmission Security.** Deploy technical controls to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network; and review and test the effectiveness of such technical controls at least once every 12 months or in response to environmental or operational changes, whichever is more frequent, and modify as reasonable and appropriate.
- **Vulnerability Management.** Deploy technical controls in accordance with the required patch management policies and procedures to identify and address technical vulnerabilities in relevant electronic information systems.
- **Data Backup and Recovery.** Deploy technical controls to create and maintain exact retrievable copies of ePHI.
- **Information Systems Backup and Recovery.** Deploy technical controls to create and maintain backups of relevant electronic information systems; and review and test the effectiveness of such technical controls at least once every six months or in response to environmental or operational changes, whichever is more frequent, and modify as reasonable and appropriate.

These standards include detailed implementation specifications that plans, other covered entities, and business associates (and their subcontractors) must follow. Most implementation specifications require ongoing review every 12 months, six months, or when changes are or will be made. While it is uncertain when HHS might publish the final rule or what the final rule will contain after HHS reviews public comments, plans, other covered entities, and their business associates should start making themselves aware of the proposed requirements and prepare accordingly because they will have only 240 days to document and implement the new Security Rule once it is finalized.

Reminder: HIPAA applies to almost all group health plans regardless of whether they are subject to ERISA, but the Department of Labor's cybersecurity guidance applies to *all* ERISA employee benefit plans of any kind.

Almost all health plans must comply with HIPAA. However, *all* employee benefit plans subject to ERISA, including health plans, other welfare plans, and retirement plans, must comply with the cybersecurity guidance by the Department of Labor (DOL). In September 2024, the DOL clarified that its April 2021 cybersecurity guidance generally applies to *all* employee benefit plans and not only retirement plans. The DOL intended the 2021 guidance to help plan sponsors, fiduciaries, service providers and participants in plans safeguard plan data, personal information, and plan assets. The guidance has three parts:

1. **Tips for Hiring a Service Provider.** Includes recommended RFP questions and contract terms for plan sponsors.
2. **Cybersecurity Program Best Practices.**
    1. Lists 12 cybersecurity best practices for service providers that the DOL would expect to see if auditing the plan or a service provider.
    2. States that pension and health and welfare plans are tempting targets for cyber criminals because the plans: (1) often hold millions of dollars in assets; and (2) store and/or transfer participants' personally identifiable data.
3. **Online Security Tips.** Tips for participants and beneficiaries to reduce the risk of fraud.

The DOL's 2024 guidance also referenced HHS cybersecurity publications to help plans and their service providers maintain good cybersecurity practices:

- Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients.
- Technical Volume 1: Cybersecurity Practices for Small Healthcare Organizations.
- Technical Volume 2: Cybersecurity Practices for Medium and Large Healthcare.

Health and welfare plans should ensure compliance with the DOL's cybersecurity guidance now that the department has clarified that the guidance does not apply only to retirement plans. Additionally, due to HHS's updates to the new Security Rule, plans should watch for updates to the HHS cybersecurity publications that the DOL cites.

You can subscribe to future advisories and other Alston & Bird publications by completing our publications subscription form.

If you have any questions, or would like additional information, please contact one of the attorneys on our Employee Benefits & Executive Compensation team.

Meet the Authors

Steven C. Mindy

Partner

Phone: +1 202 239 3816
Email: steven.mindy@alston.com

John R. Hickman

Partner

Phone: +1 404 881 7885
Email: john.hickman@alston.com

Laurie Kirkwood

Senior Attorney

Phone: +1 404 881 7814
Email: laurie.kirkwood@alston.com