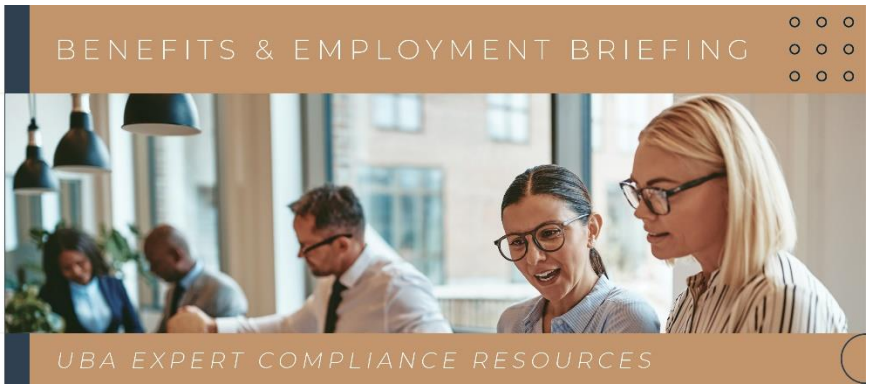

Stay compliant

Welcome to the UBA Partner Firm exclusive quarterly newsletter delivering insights about employee benefits and labor law compliance.

Benefits & Employment Briefing | Winter 2022

IRS Announces Adjusted Patient-Centered Outcomes Research Institute Fee

The IRS recently released Notice 2022-59 to announce the inflation-adjusted amount group health plans must use to calculate the amount due to fund the Patient Centered Outcomes Research Institute (PCORI). Plans ending between October 1, 2022, and December 31, 2022, must use the adjusted amount to calculate the fee that will be due by July 31, 2023. The new per capita amount is $3.00 – increased from $2.79 for plans ending after September 30, 2021, and before October 1, 2022 – which plan sponsors and issuers will multiply by the average number of covered lives under the relevant plan to derive the total amount due.

Background

The Affordable Care Act (ACA) created PCORI, which is an independent, nonprofit research organization that seeks to empower patients and others with information, including comparative clinical effectiveness research, to help patients make better informed health care decisions. PCORI is funded through insurer and

plan sponsor contributions to be reported and remitted annually on IRS Form 720. Plans and issuers began paying the PCORI fee for plan or policy years ending after September 30, 2012. Though originally scheduled to sunset for plan years ending after September 30, 2019, Congress extended the fee to plan or policy years ending before October 1, 2029.

Calculating PCORI Fees

Insurance carriers will calculate and pay the fees on behalf of fully insured plans, but carriers typically pass those fees through to the plan. Self-funded plans, including health reimbursement arrangements (HRAs), must calculate the fee. Self-funded plans may engage a third-party administrator to assist with PCORI fee calculation, but the plan sponsor ultimately bears the burden of filing IRS Form 720 and paying the applicable fee.

Plans may determine the number of covered lives by one of four acceptable methods:

1. Actual Count Method – Count the covered lives on each day of the plan year and average the result.
2. Snapshot Count Method – Determine the number of covered lives on the same day (plus or minus three days) of each quarter or month and average the result.
3. Snapshot Factor Method – Determine the number of covered employees/retirees/COBRA participants on the same day (plus or minus three days) of each quarter or month who have self-only coverage and the number who have other than self-only coverage. Multiply the number of employees/retirees/COBRA participants with other than self-only coverage by 2.35 to approximate the number of covered dependents (rather than actually counting them) and add that to the number of employees/retirees/COBRA participants with self-only coverage. Average the result.
4. Form 5500 Method – Determine the number of participants at the beginning and end of the plan year as reported on Form 5500. If dependents are covered, add the participant count for the start and the end of the plan year. If dependents are not covered, add the participant count for the start and the end of the plan year and average the result. Bear in mind a plan sponsor must file the applicable Form 5500 by July 31 to use this option.

Conclusion

Plan sponsors with plan years ending between October 1, 2022, and December 31, 2022 (including calendar year plans) should be aware of the higher amount they will need to use when reporting and paying the PCORI fee for the 2022 plan year. Plans that ended before October 1, 2022, will use the lower $2.79 per covered participant amount. Plan sponsors should ensure they take the necessary steps – including coordinating with carriers or TPAs – to calculate the fees, remit Form 720 with their payment, and, if using the Form 5500 Method, to complete and file Form 5500 by July 31.

IRS Releases Critical 2023 Employee Benefit Plan Limits

The IRS recently published Revenue Procedure 2022-38 in which it announced its list of annual key employee benefit limits based on periodic inflation or cost-of-living adjustments. The newly announced limits represent

higher than normal increases for contributions to, and permitted carryovers from, health flexible spending arrangements (HFSAs).

Effective for tax years beginning in 2023, the IRS imposes the following maximums:

HFSA individual contribution	$3,050/year
HFSA maximum permitted carryover amount	$610
Qualified transportation fringe benefits	$300/month
Adoption assistance program expenses	$15,950/year (subject to phase out for individuals with adjusted gross income starting at $239,230)
Qualified Small Employer Health Reimbursement Arrangement (QSEHRA)	$5,850/year ($11,800/year for family coverage)

Employers should be mindful of the adjusted limits as they prepare for 2023 and communicate with their employees regarding available benefit options. Plan sponsors also may need to amend plan documents and summary plan descriptions (SPDs) and update all payroll and human resources systems with the new dollar amount limitations. Plan sponsors will need to communicate with all necessary third-party vendors to ensure they have correctly accounted for the increased amounts.

The IRS also announced in Notice 2022-55 the increased amounts relating to retirement plans:

Maximum 401(k) employee elective deferral	$22,500
Maximum employee catch-up contribution (age 50 or older by end of year)	$7,500
Defined contribution maximum limit, employee + employer	$66,000 ($73,500 including age 50 and older catch-up contribution)
Employee compensation limit for calculating contributions	$330,000
Key employees' compensation threshold for top-heavy plan testing	$215,000
Highly compensated employees' threshold for nondiscrimination testing	$150,000 (2022 compensation)

Also, the maximum earnings subject to Social Security FICA payroll tax in 2023 will be $160,200.

Finally, the IRS has announced that employers who fail to file ACA Forms 1095 in 2024 (reporting for 2023) can be subject to a $310 penalty per form. The updated penalty for failure to provide individual statements to employees also will increase to $310 per statement. Since the penalties are cumulative, an employer who fails to provide an employee statement and fails to file with the IRS can be penalized up to $620 for each required form.

The IRS continues to be less lenient with late ACA report filers. As fines continue to increase, employers with filing obligations should take great care to ensure that their reporting processes ensure timely filing and timely distribution of individual statements.

Agencies Seek Public Comment on No Surprises Act Good Faith Estimate and Advanced Explanation of Benefits Provisions

Congress enacted the Consolidated Appropriations Act, 2021 (CAA), which includes the No Surprises Act (NSA), in December 2020. The NSA seeks to protect health care consumers against surprise billing and limits out-of-network cost sharing under many of the circumstances in which surprise bills typically arise.

To help accomplish this goal, the NSA requires health care providers and facilities to inquire whether an individual who has scheduled an item or service is enrolled in a group health plan. If so, and the individual plans to submit a claim for such item or service, providers and facilities must provide to the plan, issuer, or carrier a good faith estimate (GFE) of the expected charges for furnishing the scheduled item or service, along with the relevant expected billing and diagnostic codes.

The NSA further requires group health plans that receive a GFE to send a covered individual, by mail or electronically (as requested by the covered individual), an advanced explanation of benefits (AEOB) in clear and understandable language. The AEOB must include:

- The network status of the provider or facility
- The contracted rate for the item or service, or if the provider or facility is not a participating provider or facility, a description of how the covered individual can obtain information on providers and facilities that are participating
- The GFE received from the provider or facility
- A GFE of the amount the plan or coverage is responsible for paying
- The amount of any cost sharing which the covered individual would be responsible for paying with respect to the GFE received from the provider or facility
- A GFE of the amount that the covered individual has incurred toward applicable deductibles and out-of-pocket maximums under the plan as of the date of the AEOB
- Disclaimers indicating whether coverage is subject to any medical management techniques (e.g., concurrent review, prior authorization, and step-therapy or fail-first protocols)

The AEOB also must state that it is only an estimate based on the items and services reasonably expected to be furnished, at the time of scheduling or requesting an item or service and is subject to change; and any other information or disclaimer the plan, issuer, or carrier determines is appropriate and consistent with NSA's goals.

Plans must issue an AEOB no later than one business day after receiving a GFE. However, when an item or service is scheduled at least 10 business days before it is to be furnished (or if the covered individual requested

the information) the plan must provide an AEOB to the covered individual within three business days after the date on which the plan receives the GFE or request.

These provisions generally apply to plan years beginning on or after January 1, 2022. However, the agencies who oversee and enforce NSA compliance have announced that until they issue final regulations, they will not enforce these provisions.

Plans, carriers, and other stakeholders have raised concerns over the burdens associated with the GFE and AEOB requirements. In response, the agencies enforcing the NSA have sought comments from interested parties that the agencies will consider when drafting final rules to implement these requirements. Specifically, the agencies seek information to help them frame prudent rules to address the following important areas.

HIPAA Considerations

The Agencies are concerned about additional HIPAA risks associated with requiring transfer of protected health information to comply with GFE and AEOB requirements and have asked for comments as to what privacy concerns the transfer of AEOB and GFE data raise, considering these transfers would list the individual's scheduled (or requested) item or service, including the expected billing and diagnostic codes for that item or service. Further, the Agencies seek to understand whether the exchange of AEOB and GFE data creates new or unique privacy concerns for individuals enrolled in a plan and whether they should weigh special factors for individuals who are enrolled in a plan or coverage along with other members of their household.

Coordination with NSA Price Transparency Tool Requirement

The Agencies recognize that there could be significant overlap in the price transparency tool requirements coming online for plans beginning on or after January 1, 2023, for 500 initially identified items or services, and January 1, 2024, for all other items or services. Thus, they have sought input as to:

- How the final rule could coordinate with the internet-based self-service tool requirement to help minimize the burden on plans, issuers, and carriers in implementing both.
- Whether plans, issuers, and carriers can leverage technical work completed to comply with the internet-based self-service tool requirements to help streamline the process for complying with AEOB requirements.
- What, if any, obstacles will plans, issuers, and carriers face if required to provide AEOBs to covered individuals for all covered items or services (rather than a specified subset, as with the first year of the internet-based self-service tool requirement) beginning with the first year of the AEOB requirement.

Mandatory AEOB Notice to Provider or Facility

Are there reasons why the Agencies should or should not propose a requirement that plans, issuers, and carriers provide a copy of the AEOB to the provider or facility, as opposed to allowing such a transfer but not requiring it?

Plan Coverage Verification

What, if any, additional burden would be created by requiring providers, facilities, plans, issuers, and carriers to verify:

- Whether an individual is uninsured, self-pay, or enrolled in a health plan or coverage for AEOB and GFE purposes
- Coverage for each item or service expected to be included in an AEOB or GFE
- Coverage from multiple payers

Should the final rules allow providers and facilities, for purposes of verifying coverage, to rely on an individual's representation regarding whether the individual is enrolled in a health plan or coverage and seeking to have a claim for the items or services submitted to the plan or coverage?

Language Access

Should the Agencies adopt an AEOB language access requirement similar to existing requirements for group health plans and health insurance issuers, such as the internal claims and appeals and external review and Summary of Benefits and Coverage (SBC) requirements to provide oral language services, notices in non-English languages, and non-English language statements in English versions of notices indicating how to access language services? And, if so, what is the best way to ensure information about language access services is communicated with enough time to facilitate the provision of the AEOB in the language that is most accessible to the individual?

Conclusion

The specific areas noted above will shape the final requirements that plans will need to address when the GFE and AEOB rules become final. We expect the agencies also will address the extent to which plans may rely on carriers or third-party administrators to meet these requirements.

The comment period recently closed, so we would expect the agencies to issue final rules in 2023, possibly as early as the first quarter. Having said that, we also would expect that such rules would not be immediately effective or enforceable, and that plan sponsors will have time to digest the final rules and take whatever steps they will need to ensure compliance.

Ongoing Application of Certain COVID-19 Guidance

The COVID-19 global pandemic at times can seem like it is in the rearview, but certain laws, regulations, and agency guidance remain in effect and will continue to apply for the foreseeable future. This point has been highlighted twice this year when President Biden extended the National Emergency until March 1, 2023, as well as when the Secretary of Health and Human Services (HHS) recently extended the existing public health emergency related to COVID-19 for 90 days to January 11, 2023.

The ninth extension of the public health emergency from its initial declaration in January 2020 bridges the midterm election cycle and the end of the benefits year for calendar year plans. Though Secretary Becerra could

end the public health emergency earlier, he has previously announced that HHS will give 60 days' advance notice prior to doing so.

COVID-19 Vaccines

Among other things, the extension means that group health plans will continue to be required to cover the costs associated with COVID-19 vaccinations under rules issued during the pandemic. Currently non-grandfathered plans must cover the cost of approved vaccines with no cost-sharing requirements (including a reasonable rate for non-network providers). However, at the end of the public health emergency, such plans will be permitted to limit coverage to in-network providers. Plan sponsors will need to carefully monitor HHS announcements going forward to take necessary steps to amend plan documents and SPDs to account for any planned changes to how their plans will cover vaccines.

Extended Plan Deadlines

Until the Biden administration declares an end to the National Emergency, plans will continue to have to permit extended deadlines for actions including COBRA elections, HIPAA special enrollment periods, and plan claims and appeals procedures during the so-called Outbreak Period for COVID-19. The Outbreak Period will not end until 60 days after the end of the National Emergency.

Employers will need to keep in mind guidance that applies the extended deadlines to the earlier of one year from the date an individual or plan was first eligible for relief, or 60 days after the announced end of the National Emergency. This potentially will create multiple rolling deadlines impacting numerous plan participants.

Plan sponsors also should remember that the Employee Benefit Security Administration has previously announced that the guiding principle for administering employee benefit plans is to act reasonably, prudently, and in the interest of plan participants and beneficiaries. Plans and fiduciaries may wish to consider putting participants on notice that certain deadlines are expiring both during the National Emergency and when the Outbreak Period is about to expire.

Education Assistance Plan Student Loan Reimbursement

Another COVID-related benefit employers can continue through 2025 is reimbursing the costs of student loans through a qualified education assistance plan under Code section 127. Section 127 plans historically had been limited to reimbursing certain qualifying education expenses related to tuition, books, and related fees. However, the CARES Act in 2020 expanded the list of permitted reimbursable expenses to include qualifying student loans, and the Consolidated Appropriations Act, 2021 (CAA) extended the student loan provision through 2025. As a result, employers who establish and properly administer a bona fide section 127 plan can reimburse up to $5,250 annually in student loans.

Employers can adopt or expand a Section 127 plan to include student loan repayment assistance but must do so according to IRS rules. An education assistance plan must be formalized in writing and must:

- Be limited to tuition, fees, and textbook expenses for any educational course taken by the employee, regardless of whether it is related to the employee's job.

- Exclude reimbursements for education involving sports, games, or hobbies, as well as meals, lodging, transportation, and any tools or supplies an employee may keep following the course.
- Limit loan repayment to principal or interest on any qualified education loan (i.e., a loan taken solely to pay qualified higher education expenses) incurred by the employee for their own education.
- Cap benefits at $5,250 per year (combined between tuition and loan repayment expenses).
- Not discriminate in favor of highly compensated employees or their dependents.
- Pay no more than 5% of the total amounts paid during the year to significant shareholders.
- Reasonably notify eligible employees of the plan's availability and terms, including, for example, any reasonable conditions such as required repayment if an employee terminates employment within a certain period after receiving reimbursement.

Office for Civil Rights Reiterates HIPAA Requirements and Responses to Cybersecurity Incidents

The HHS Office for Civil Rights (OCR) recently reported that a national cybersecurity firm observed a 42% increase in cyber-attacks for 2022 compared to 2021, and a 69% increase in cyberattacks specifically targeting the health care sector. Further, breaches of unsecured protected health information (PHI), including ePHI, affecting 500 or more individuals and reported to OCR increased from 663 in 2020 to 714 in 2021, with 74% of reported breaches involving hacking or information technology (IT) incidents. OCR noted that hacking is now the greatest threat to the privacy and security of PHI in the health care sector and that timely response to a cybersecurity incident is one of the best ways to prevent, mitigate, and recover from cyberattacks.

As we have recently completed National Cybersecurity Awareness Month, now is a great time for group health plans subject to the HIPAA Security Rule to review their policies and procedures that address security incidents to make sure they follow the guidelines OCR recently reiterated.

Regulated entities must implement and document their plan for responding to security incidents (suspected or known) to include:

- Identifying security incidents
- Responding to security incidents
- Mitigating harmful effects of security incidents
- Documenting security incidents and their outcomes

In preparing their security incident response process, regulated entities like group health plans should consider forming a security incident response team that is organized and trained to effectively respond to security incidents. Among the items to consider in forming a team are:

- Selecting a team structure and staffing

- Establishing relationships and lines of communication between the security incident response team and other internal and external resources
- Identifying internal groups that may need to participate in incident handling (management, IT support, legal, public affairs and communications, human resources, business continuity/disaster recovery, physical security, facilities management)
- Identifying points of contact at external groups that may be helpful to include in the event of an incident (network service providers, software and hardware vendors, local and federal law enforcement, incident handling teams of business partners and customers)
- Determining what services the security incident response team should provide (such as intrusion detection, advisory distribution, education and awareness, information sharing)

The security incident response team should regularly test its security incident procedures. This could involve conducting tests involving different types of potential security incident scenarios like a cyber-criminal's infiltration and deployment of ransomware, for example. Updating security incident procedures based on this testing will help protect against, and improve efficiency in responding to, actual security incidents.

The HIPAA Security Rule regulations also require a regulated entity to:

- Identify the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.
- Maintain and regularly review audit logs.
- Implement hardware, software, and procedural mechanisms to record and examine access and other activity in information systems that contain or use electronic protected health information.
- Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

When responding to a security incident, a regulated entity should contain the security incident and any threat it may pose to ePHI and take appropriate action to ensure the confidentiality, integrity, and availability of its ePHI by:

- Determining the nature and extent of the damage caused by the security incident.
- Identifying and removing any malicious code and components that the security incident may have left behind.
- Mitigating any vulnerabilities that may have permitted the security incident to occur.
- Collecting and preserving data relevant to investigating the security incident, such as log files, registry keys, and other artifacts.

After the security incident has been neutralized and any malware removed, the next steps should include mitigating the harmful effects of the security incident including recovery and restoration of systems and data to return to normal operations. The HIPAA Security Rule requires that regulated entities establish a contingency plan to include data backup and recovery processes.

Frequent backups and verification of the integrity of the backed-up data are crucial to being able to recover data that may have been deleted or had its integrity compromised as a result of a security incident. Backup logs should be reviewed regularly, and test restorations of backups conducted periodically to ensure the integrity of backups and provide confidence in the regulated entity's ability to restore its data. Because some malware, including some ransomware variants, are known to delete or otherwise disrupt online backups, regulated entities should consider maintaining at least some of their backups offline and unavailable from their networks.

Once a security incident has ended, systems and data have been restored, and operations have returned to normal, regulated entities should document their response and analysis into a record of the security incident. A regulated entity's security incident procedures should include a section on documenting security incidents and what information to include in the documentation (e.g., discovery of the security incident, systems and data affected, response and mitigation activities, recovery outcomes, root cause analysis, forensic data collected).

Finally, when considering their security incident procedures and how to respond to security incidents, regulated entities must understand their duty to report breaches of unsecured PHI. The Breach Notification Rule requires covered entities to report breaches affecting 500 or more individuals to the affected individuals, to OCR, and (in certain cases) to the media without unreasonable delay and no later than 60 calendar days from the discovery of the breach. Covered entities are required to report breaches affecting fewer than 500 individuals to the affected individuals without unreasonable delay and no later than 60 calendar days from the discovery of the breach, and to OCR no later than 60 days after the end of the calendar year in which the breach was discovered.

Conclusion

The policies and procedures regulated entities create to prepare for and respond to security incidents can pay dividends in the long run with faster recovery times and reduced compromises of ePHI. A well-reasoned, well-tested security incident response plan is integral to ensuring the confidentiality, integrity, and availability of a regulated entity's ePHI.

Recent Court Decisions Should Put Employers on Notice Regarding COBRA Administration

Two cases recently decided in federal courts in Illinois and Alabama, respectively, provide cautionary tales for employers and how they administer COBRA continuation coverage, particularly how they provide election notices following a COBRA qualifying event. In both cases, the courts determined that claims of COBRA notice violations could not be denied because the responsible employer could not demonstrate that it had properly issued COBRA election notices.

Sending COBRA Election Notice to Incorrect Address

In *Howard v. Ivy Creek of Tallapoosa, LLC*, the U.S. District Court for the Middle District of Alabama considered a case in which a disabled employee was terminated from active group health coverage following an extended absence due to a brain aneurysm. The employer communicated detailed plan information to the employee at her current address, but the TPA responsible for COBRA notices had only an outdated address for the former employee in its system. Even though the notice was returned to the TPA as undeliverable, the TPA never informed the employer.

The former employee sued the employer for the employee sued the employer and TPA under ERISA, including claims for:

- Failing to mail her a COBRA election notice at her last known address (that is, her residence address)
- ERISA statutory penalties for failing to provide her plan documents in response to a written request
- Equitable relief under ERISA consisting of the employee's health premiums, outstanding medical bills, interest, and attorney's fees

The court disagreed with the employer's assertion that it had no liability since it had instructed the TPA to send the COBRA election notice to the employee's last-known address in its files. The court held that the employer could not absolve itself by delegating the notice responsibility to a third party when it neglected to inform that third party of a more recent address of which the employer was aware. Moreover, the service agreement between the employer and TPA obligated the employer to notify the TPA of any changes in employees' addresses, which the employer failed to do in this case.

This case illustrates the importance of an employer building fail-safe processes to properly exchange information relevant to COBRA notices and elections. This is especially true when an employer changes COBRA vendors, and the data migrates from one vendor to another without the employer or new vendor performing an audit to ensure the data is updated and correct. Further, it is important for an employer to review its COBRA administrative services agreement to be sure it complies with any obligations it has to the COBRA administrator.

Insufficient Evidence to Prove COBRA Election Notice Mailing

In *Earl v. Jewel Food Stores, Inc.*, a former employee sued an employer for failing to provide timely COBRA election notices. The employer attempted to show that it had followed COBRA rules and made a good faith effort to provide a timely election notice. However, the court held that the evidence the employer offered was insufficient to demonstrate a good faith notification effort.

ERISA plan administrators must generally be able to show that a COBRA notice has been provided, but the law does not require proof of receipt. Where an employer can clearly demonstrate that it followed COBRA rules and issued a proper and timely COBRA election notice, it generally can demonstrate good faith compliance and avoid liability. In this case, however, the court noted that the employer's evidence of having sent the disputed COBRA election notice was inadequate. The court specifically reasoned that the employer failed to show any evidence that the COBRA notice was sent by certified or first-class mail; that the employer had detailed standard COBRA notice procedures; or that the employer followed any standard procedures in this

case. The court also rejected an argument the employer made that the employee did not need COBRA or could not have afforded COBRA in any event even if he had received proper COBRA notice.

This case aligns with other similar cases in which an employer argued that it has sent a proper COBRA notice following a qualifying event. In the cases where a court sided with the employer, there has been direct evidence that the employer sent the notice by first class or certified mail, or that the employer had regimented and routine notice generation and mailing procedures, and that the employer followed the standard procedures in the matter in question. Often an employer can demonstrate compliance with its internal procedures through an affidavit of the individual responsible for adhering to COBRA procedures.

Conclusion

COBRA continues to pose challenges that result in litigation – even class actions in some cases. It is important for employers to routinely examine their COBRA processes and any governing third-party vendor agreements to clearly define duties and obligations and to set procedures to periodically audit processes to ensure full compliance with COBRA election rules.