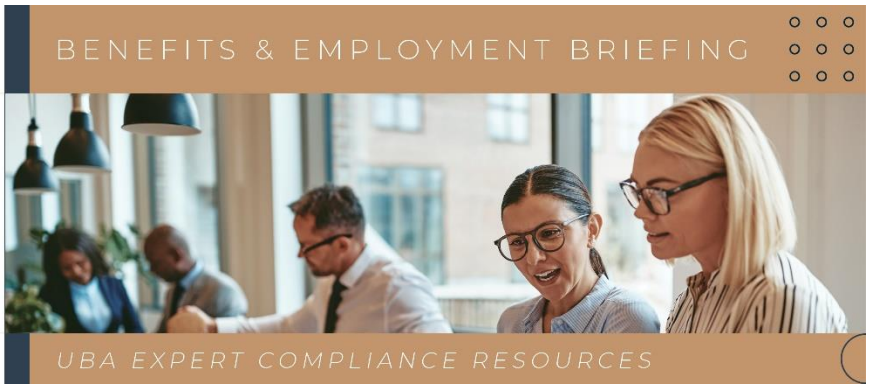
Acadia BENEFITS

UBA PARTNER FIRM | Shared Wisdom. Powerful Results.®



Stay compliant

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

Benefits & Employment Briefing | Summer 2022

Into the Breach: Identifying and Addressing a HIPAA Security Breach

Cybercrimes and attacks on personal data continue to escalate, and threats to sensitive employee data maintained by employee benefit plans are at an all-time high. The Office of Civil Rights (OCR) recently disclosed that hacking and information technology incidents remain the largest category of Health Insurance Portability and Accountability Act of 1996 (HIPAA) breaches, comprising an astounding 68% of all reported breaches for 2020.

OCR strongly recommends that covered entities redouble efforts to comply with HIPAA's Security Rule, including standards and implementation specifications for risk analysis and risk management, information system activity review, audit controls, security awareness and training, and authentication. But what happens even when a covered entity has taken required steps to protect its data and a breach still occurs? These helpful tips can help a covered entity deal with a HIPAA breach — in the moment as well as during the aftermath.

Identifying a Breach

Under HIPAA's Breach Notification Rule, a covered entity first must determine whether a reportable breach has occurred. HIPAA defines a breach as any unauthorized acquisition, access, use, or disclosure of protected

health information (PHI) unless the covered entity demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment. This risk assessment must address at least the following factors:

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification
- The unauthorized person or persons who used the PHI or to whom the disclosure was made
- Whether the PHI was actually acquired or viewed
- The extent to which the risk to the PHI has been mitigated

However, HIPAA regulations also specifically exclude any:

- Unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a covered entity or business associate, if made in good faith and within the scope of authority, and if not further impermissibly used or disclosed.
- Inadvertent disclosure of PHI by a person authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate, and the information is not further impermissibly used or disclosed.
- Disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain the information.

This determination is complicated and fact-intensive and should be made through a covered entity's security officer working with expert legal counsel. It will also be important to include your IT department as well as human resources and any other individuals who will help form the content and delivery of required notices to be sure to control the timing and nature of the message.

Individual Notice

Covered entities who identify a security breach must notify affected individuals without unreasonable delay and no later than 60 calendar days following discovering the breach. Covered entities must provide written notice by first-class mail to the last known address of the individual or, if the individual agrees to electronic notice, by email. If the covered entity knows an affected individual is deceased and has the address of the next of kin or personal representative of the individual, then the covered entity must provide written notification to the next of kin or personal representative.

The required notice must include:

- A brief description of what happened, including the date of the breach and the date of discovery of the breach
- A description of the types of unsecured PHI involved in the breach
- Any steps individuals should take to protect themselves from potential harm resulting from the breach
- A brief description of what the covered entity is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches
- Contact information for individuals to ask questions or learn additional information

Media Notice

For breaches involving more than 500 residents in the same geographic area, a covered entity must notify prominent media outlets serving that area. This media notification must be provided without unreasonable delay and no later than 60 calendar days following the discovery of a breach and must include the same information as that required for the individual notice.

Notice to the Secretary

In addition to notifying affected individuals and the media (where necessary), a covered entity must notify the Secretary of the Department of Health and Human Services (HHS) of breaches of unsecured PHI. If a breach involves 500 or more individuals, a covered entity must notify the Secretary at the same time the affected individuals are notified of the breach.

If a breach involves fewer than 500 individuals, covered entities may submit reports of such breaches on an annual basis. Reports of breaches involving fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches were discovered.

Covered entities must notify the Secretary by filling out and electronically submitting a breach report form on the HHS Department website.

Address Deficiencies

After discovering and, if necessary, communicating a breach, affected covered entities should carefully analyze the findings of any breach investigation. Covered entities should perform a security risk assessment (or review the most recent risk assessment) and incorporate any items gleaned from the breach investigation. This will demonstrate good faith compliance in the event of any future investigation or audit, and it also will make it less likely that an entity remains vulnerable to the same or similar security threat that resulted in a breach. This will allow a covered entity to modify its breach incident policies and procedures and reeducate members of an entity's HIPAA security and beach response team.

Conclusion

OCR continues to ramp up enforcement efforts and is currently considering public comments on how to best distribute monetary penalties and other settlement amounts to affected individuals. As data security continues to drive the agency's agenda, now is a perfect time for employer plan sponsors to make sure they have comprehensive HIPAA policies and procedures in place, including a thorough security risk assessment and breach response plan.

Delaware, Maryland Latest to Require Paid Family Leave

Measures aimed at passing a federal law requiring paid family leave continue to falter in Washington. Thus, a growing number of states continue to pass laws requiring employers to provide paid family leave. Delaware and Maryland are the latest two states to dictate paid leave.

Delaware

Delaware recently enacted the Healthy Delaware Families Act (Act) that will require covered employers to make payroll contributions beginning January 1, 2025, to provide benefits to eligible employees who may take up to 12 weeks of job-protected leave starting January 1, 2026. The law will provide for up to 80% of an eligible employee's average weekly wages, with a maximum weekly payout of $900 in 2026 and 2027. Employers can either cover the full contribution or withhold up to 50% of the cost from employee paychecks and pay the balance. The Delaware Department of Labor will regulate deductions, withholdings, and payments.

The Act establishes a statewide paid family and medical leave insurance program that will cover employees who need leave for their own serious health condition; a serious health condition affecting a spouse, parent, or child; bonding with or caring for a child during the first year following birth, adoption, or foster-care placement; or due to a family member's military deployment. Similar to the Family and Medical Leave Act (FMLA), Delaware employees are eligible for leave if they worked 1,250 hours during the previous 12-month period and have worked for their employer for at least a year.

Employees who qualify for leave can take up to 12 weeks in a year for parenting, and a total of six weeks in a two-year period for their own medical care, family caregiving, or a family members' military deployment. The maximum benefit per year is 12 weeks for all reasons combined.

Employers with at least 25 employees in Delaware during the prior 12-month period must provide job-protected leave for all parental, family, and medical leaves. Employers with 10 to 24 employees during the previous 12 months will only need to provide qualifying parental leave. Seasonal business that completely shut down for at least 30 consecutive days a year are exempt. Also, an employer that already provides paid leave benefits that are at least as generous as the provisions under the act may be able to opt out.

Eligible employees have the right to keep their healthcare benefits while on leave and to be reinstated to their job when the leave period ends. Additionally, an employer can face significant penalties for discriminating or retaliating against an employee for requesting, applying for, or using family and medical leave benefits.

Maryland

Maryland's legislature recently enacted a law under which any employer that employs at least one individual in Maryland must provide eligible employees with up to $1,000 per week for up to 12 weeks of leave annually. Further, qualifying leave will be job-protected which means an employer cannot discharge, demote, or otherwise discriminate or take adverse action against an individual who has filed for, applied for, or received benefits under the new law, inquired about rights and responsibilities under the new law, communicated an intent to file a claim, complaint, or appeal under the new law, or testified or intents to testify in a proceeding under the new law.

Under the new law, any employee (part- or full-time) who has worked at least 680 hours over the 12-month period immediately preceding the date on which leave begins may take up to 12 weeks of paid time off annually to care for a new child, address their own medical problems, or deal with a family member's serious illness or military deployment. Moreover, a parent could get up to 24 weeks if they require medical leave during pregnancy, followed by parental leave after their child is born.

Employers and employees will split the cost for paid leave through a payroll tax that will go into effect on October 1, 2023, to fund the Family and Medical Leave Insurance Fund. Benefits will become available starting January 1, 2025.

An employer can comply with the requirements of the new law through a private employer plan consisting of employer-provided benefits, insurance, or a combination of the two, if the private employer plan is offered to all eligible employees and meets or exceeds the new law's benefits. Maryland will require employers to submit their private plan to the Maryland Department of Labor for approval.

In addition to Delaware and Maryland, employers should be aware of similar paid leave laws in California, Colorado, Connecticut, Massachusetts, New Jersey, New York, Oregon, Rhode Island, and Washington, as well as the District of Columbia. As more employers continue to modify remote work policies to cope with the lingering effects of the COVID-19 pandemic, they will need to be vigilant regarding state laws that might impact them for the first time.

IRS Announces 2023 HSA and HDHP Amounts

The IRS recently issued Revenue Procedure 2022-24 to announce the 2023 inflation-adjusted amounts that apply to health savings accounts (HSAs) and high-deductible health plans (HDHPs). The newly announced figures include the maximum contribution limit for an HSA, the minimum permissible deductible for an HDHP, and the maximum limit on out-of-pocket expenses (e.g., deductibles, copayments, and other amounts aside from premiums) for qualifying HDHPs. These limits will differ depending on whether an individual is covered by a self-only or family coverage tier under an HDHP.

The IRS's new higher HSA contribution limit and HDHP out-of-pocket maximum will take effect January 1, 2023. HDHP deductible limits will increase for plan years that begin on or after January 1, 2023.

The chart below shows the old 2022 limits as well as the new 2023 limits. Also note that the maximum permitted catch-up HSA contribution for eligible individuals who are 55 or older remains unchanged for 2022.

	2023		2022	
Applicable Limit	Self-Only	Family	Self-Only	Family
HSA Maximum Contribution	$3,850	$7,750	$3,650	$7,300
HSA Maximum Catch-up Contribution	$1,000	$1,000	$1,000	$1,000
HDHP Minimum Deductible	$1,500	$3,000	$1,400	$2,800
HDHP Maximum Out-of-Pocket Expense	$7,500	$15,000	$7,050	$14,100

Employers that sponsor HDHPs may need to make plan design changes as they finish 2023 planning. Additionally, affected employers will need to ensure that they update all plan communications, open

enrollment materials and other documentation that addresses these limits to be sure participants and beneficiaries are adequately informed.

The IRS also announced that the maximum amount that can be made newly available in 2023 for an Excepted Benefit HRA (EBHRA) is $1,950.

SECURE 2.0 Act to Bolster Retirement Savings Clears First Hurdle

The U.S. House of Representatives recently passed the Securing a Strong Retirement Act of 2022 (SECURE 2.0) by a 414-5 vote. The bill now moves to the Senate, where it is expected to be addressed in the coming months.

SECURE 2.0, as passed by the House, expands on certain aspects of the Setting Every Community Up for Retirement Enhancement (SECURE Act) that became law in 2019. SECURE 2.0 similarly intends to give American workers greater access to retirement savings opportunities.

Mandating Automatic Retirement Plan Enrollment

For plan years beginning after December 31, 2023, SECURE 2.0 would require new 401(k) plans to automatically enroll participants upon becoming eligible. Employees would be permitted to decline participation. All current 401(k) plans, and plans sponsored by businesses with 10 or fewer employees, businesses in existence for fewer than three years, church plans, and governmental plans would be exempt.

Creating Student Loan Repayment "Matching" Contributions

SECURE 2.0 would allow an employer to make contributions under a 401(k) plan to match certain student loan repayments made by employees as if the repayments were elective deferrals to the 401(k) plan. Only payments made by an employee solely to pay for certain qualified higher education expenses would be eligible for this treatment. The new rule would apply to contributions made for plan years beginning after December 31, 2022.

Raising Required Minimum Distribution Age

SECURE 2.0 would increase the required minimum distribution (RMD) age on a sliding scale as follows:

- Age 73 starting on January 1, 2023, for anyone who turns 72 after December 31, 2022, and turns 73 before January 1, 2030)
- Age 74 starting on January 1, 2030, for anyone who turns 73 after December 31, 2029, and turns 74 before January 1, 2033
- Age 75 starting on January 1, 2033, for anyone who turns 74 after December 31, 2032

These changes would apply starting with distributions required to be made after December 31, 2022, for anyone who turns 72 after that date.

Increasing Catch-up Limits

For tax years starting after December 31, 2023, the current $1,000 catch-up IRA contribution allowed for those 50 and older would be indexed and increased for inflation. Additionally, the current catch-up contribution

limits on retirement plans would increase to $10,000 ($5,000 for SIMPLE plans) and be indexed to account for inflation for individuals who are at least 62 but not yet 65.

Expanding Eligibility for Certain Part-time Employees

The SECURE Act requires employers to let long-term, part-time workers into their 401(k) plans except for collectively bargained plans. Employers must have a dual eligibility requirement whereby an employee must complete either one year of service under the standard 1,000-hour rule or three consecutive years of service where the employee completes at least 500 hours of service. SECURE 2.0 would shorten that period for part-time workers to two years for plan years starting after December 31, 2022.

Creating Retirement Savings "Lost and Found"

SECURE 2.0 would, as of its enactment date, create a virtual lost and found where workers would be able to potentially locate retirement funds they might have forgotten they had. The Act also requires the U.S. Department of Labor, along with the Department of the Treasury, to issue regulations on how plan fiduciaries can meet their fiduciary duties to locate missing participants.

Expanding Employee Plans Compliance Resolution System

SECURE 2.0 would, as of its enactment date, expand the Employee Plans Compliance Resolution System (EPCRS) to permit employer plan sponsors to correct more types of errors (such as plan loan errors) via self-correction. SECURE 2.0 also would remove certain errors (such as failure to make required minimum distributions) from otherwise applicable excise tax liability.