UBA ComplianceAdvisor

Compliance Recap

April 2017

In April, government agencies ramped up their activities by issuing a final rule, updating guidance, and announcing increased Health Insurance Portability and Accountability Act of 1996 (HIPAA) enforcement.

The Internal Revenue Service (IRS) updated its webpage that summarizes employer shared responsibilities payments and their calculation. The Department of Health and Human Services (HHS) Centers for Medicare & Medicaid Services (CMS) released its ACA Market Stabilization Final Rule and its 2018 Medicare Part D Benefit Parameters. The Treasury Inspector General released its report on the IRS' processing of Forms 1094-C and 1095-C.

The IRS released an information letter on HSA ineligibility due to Medicare entitlement. HHS' Office of Civil Rights (OCR) released guidance on electronic protected health information (ePHI) attacks. The Department of Labor (DOL) released its annual report on self-insured group health plans. The Congressional Research Services updated its Patient Protection and Affordable Care Act (ACA) Resources for FAQs.

UBA Updates

UBA released two new advisors in April:

- ACA Market Stabilization Final Rule
- Section 105(h) Nondiscrimination Testing

IRS Updates Its Webpage on Employer Payments and Calculations

On April 6, 2017, the IRS updated its webpage on Types of Employer Payments and How They are Calculated. It provides a summary of the employer shared responsibility provisions, the penalties amounts adjusted for calendar year 2017, examples of employer liability, and description of the IRS' process for assessing and collecting the employer shared responsibility payment.

CMS Releases Its ACA Market Stabilization Final Rule

On April 18, 2017, CMS issued its final rule regarding ACA market stabilization. The regulations are effective on June 17, 2017.

The rule amends standards relating to special enrollment periods, guaranteed availability, and the timing of the annual open enrollment period in the individual market for the 2018 plan year, standards related to network adequacy and essential community providers for qualified health plans, and the rules around actuarial value requirements.

The changes primarily affect the individual market. However, to the extent that employers have fully-insured plans, some of the changes will affect those employers' plans because the changes affect standards that apply to issuers.

Read more about the final rule.

CMS Releases Its 2018 Medicare Part D Benefit Parameters

On April 3, 2017, the Centers for Medicare & Medicaid Services (CMS) released its Announcement of Calendar Year (CY) 2018 Medicare Advantage Capitation Rates and Medicare Advantage and Part D Payment Policies and Final Call Letter and Request for Information.

Most group health plan sponsors offering prescription drug coverage to Part D eligible individuals must disclose whether the plan is creditable or non-creditable. For coverage to be creditable, the coverage's actuarial value must equal or exceed the actuarial value of the standard Medicare prescription drug coverage. Practically speaking, coverage is creditable if it's at least as good as standard Medicare prescription drug coverage.

Group health plan sponsors will use the parameters below to determine whether their plans' prescription drug coverage is creditable for 2018:

Part D Benefit Parameters -- Standard Benefit	**2017**	**20**
Deductible	$400.00	$40
Initial Coverage Limit	$3,700.00	$3,75
Out-of-Pocket Threshold	$4,950.00	$5,00
Total Covered Part D Spending at Out-of-Pocket Threshold for Non-Applicable Beneficiaries	$7,425.00	$7,50
Estimated Total Covered Part D Spending for Applicable Beneficiaries	$8,071.16	$8,41
Minimum Cost-Sharing in Catastrophic Coverage Portion of the Benefit		
Generic	$3.30	$
Other	$8.25	$

Treasury Inspector General Releases Report on IRS' Processing of Forms 1094-C and 1095-C

On April 7, 2017, the U.S. Department of the Treasury Inspector General released its Affordable Care Act: Efforts to Implement the Employer Shared Responsibility Provision that describes the results of its audit of the IRS' preparations for ensuring compliance with the Employer Shared Responsibility Provisions and its related information reporting requirements.

The Inspector General determined that some of the IRS' processes and procedures do not function as intended. As a result, the IRS has been unable to accurately and completely identify noncompliant employers who are potentially subject to the employer shared responsibility payment, unable to process paper information returns timely and accurately, and unable to identify validation errors correctly. Further, the IRS' implementation of a post-filing compliance validation system is being delayed until May 2017.

IRS Releases Information Letter on HSA Ineligibility Due to Medicare Entitlement

The IRS issued Letter 2017-0003 that explains the consequences of health savings account (HSA) ineligibility due to Medicare entitlement. Under the facts, an employee retired and enrolled in Medicare Parts A and B. Later, the employee resumed working and enrolled in the employer's health plan and was provided with an HSA.

The IRS determined that the employee never had a valid HSA because the employee's Medicare enrollment disqualified him from establishing an HSA. Per the IRS, the employee must withdraw the funds from his account and include them in his income; the withdrawal is not subject to a fine.

HHS OCR Releases Guidance About Man-in-the-Middle Attacks on ePHI

The U.S. Department of Health and Human Services Office for Civil Rights (OCR) issued its Man-in-the Middle Attacks and "HTTPS Inspection Products" guidance. The OCR warns organizations that have implemented end-to-end connection security on their internet connections using Secure Hypertext Transport Protocol (HTTPS) about using HTTPS interception products to detect malware over an HTTPS connection because the HTTPS interception products may leave the organization vulnerable to man-in-the-middle (MITM) attacks. In an MITM attack, a third party intercepts internet communications between two parties; in some instances, the third party may modify the information

or alter the communication by injecting malicious code.

OCR provides a partial list of products that may be affected. Also, OCR provides a method that organizations can use to determine if their HTTPS interception product properly validates certificates and prevents connections to sites using weak cryptography.

OCR emphasized that covered entities and business associates must consider the risks presented to the electronic protected health information (ePHI) transmitted over HTTPS. Further, OCR encouraged covered entities and business associates to review OCR's recommendations for valid encryption processes to ensure that ePHI is not unsecured and the U.S. Computer Emergency Readiness Team's recommendations on protecting internet communications and preventing MITM attacks.

DOL Releases Its Annual Report to Congress on Self-Insured Group Health Plans

The Department of Labor (DOL) released its Report to Congress - Annual Report on Self-Insured Group Health Plans. The report provides statistics on self-insured employee health benefit plans and financial status of employers that sponsor such plans. The report uses data from the Form 5500 that many self-insured health plans are required to file annually with the DOL.

Congressional Research Services Updates Its ACA Resources for FAQs

On April 3, 2017, the Congressional Research Service updated its Patient Protection and Affordable Care Act (ACA): Resources for Frequently Asked Questions. The report lists contacts for questions about employer-based coverage and sources on taxes, congressional efforts to repeal or amend the ACA, ACA agency audits and investigations, insurance coverage statistics, and legal issues.

Question of the Month

Q. Under what circumstances do HIPAA's breach notification requirements not apply when a breach of protected health information (PHI) occurs?

A. Generally, breach notification must be provided when a breach of *unsecured* PHI is discovered. HHS provides only two methods of creating "secured PHI" that would not be subject to the notification requirements if there is a breach:

- Encryption
- Destruction

This means that if PHI/ePHI is encrypted or destroyed and a breach occurs, HIPAA's notification requirements are not triggered.

5/1/2017

The UBA Compliance Advisors help you to stay up to date on regulatory changes to help simplify your job and mitigate compliance risk.