Is a COBRA TPA a HIPAA Business Associate?

By Connie Gilchrest

“To be or not to be,” that was the key question in William Shakespeare’s play, Hamlet.

A similar question arises regarding HIPAA privacy and security requirements: Whether a third-party administrator of COBRA needs to be, or not to be, viewed as a business associate. In order to do this, you must first determine if there is access to protected health information. If so, more than likely, the TPA is a business associate.

What Exactly Is a Business Associate?
A business associate is defined as a person or entity, who, on behalf of a covered entity:

1) creates, receives, maintains or transmits PHI (for example, claims processing or administration, data analysis, billing, benefits administration and management); or

2) provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services to or for the covered entity, or to or for an organized health care arrangement in which the covered entity participates, involving PHI.

What Is Individually Identifiable Health Information?
Under the HIPAA regulations, PHI is defined as “[i]ndividually identifiable health information that is maintained or transmitted either electronically or via any other medium.” The regulations specifically exempt this category of information: “[e]mployment records held by a covered entity in its role as employer.”

Individually identifiable health information is a type of health information that is created by a covered entity, such as a health care provider, a health plan or its business associate. This pertains to the past, present or future health condition, provision of care or payment for care of an individual.

Does COBRA Administration Deal with Accessing PHI?
First, we will address if COBRA administration typically involves accessing PHI. The U.S. Department of Health and Human Services indicated that enrollment and disenrollment data is not PHI since it is provided by a non-covered entity (that is, the employer sponsoring the plan) in the employment context.

COBRA records are generally beyond the reach of HIPAA. There are four ways to check to make sure the COBRA information is not PHI:

1) COBRA information does not include health information. Usually COBRA information pertains to eligibility and the payment for continuation of coverage under the group health plan. For example, electing and paying for medical coverage does not include a specific health condition. Therefore, it can be treated as a simple “enrollment” function (see #4 below)

2) The employer provides the information. The HIPAA regulations specifically exclude employment records and COBRA administration. Employment information is needed to process a COBRA qualifying event; for example name, address and benefit coverage levels are not considered PHI, they are considered identifiers.

3) Employers are responsible for the COBRA requirements. ERISA makes it clear that COBRA is a plan sponsor duty; generally the employer is the plan sponsor. The Internal Revenue Code states the liability for the excise taxes fall to the employer.

4) Enrollment and disenrollment information is exempt from the privacy rule. The preamble to the HIPAA privacy regulations specifically states:

See Business Associate, p. 6
“Plan sponsors that perform enrollment functions are doing so on behalf of the participants and beneficiaries of the group health plan and not on behalf of the group health plan itself.”

COBRA information constitutes enrollment and disenrollment information, which is not protected health information under HIPAA. This type of COBRA information does not contain health information (that is, relating to a condition, provision of health care or payment for provision of health care) as defined in Section 160.103 of the HIPAA regulations. In addition, COBRA information relates to activities performed on behalf of an employer/plan sponsor, not a health plan that is a covered entity.

This fact was proven in the lawsuit Cooney v. Chicago Public Schools. (See the Guide, ¶1900.) This is not a COBRA case that involves COBRA coverage; it pertains to HIPAA privacy issues.

The COBRA open enrollment mailings contained the names, Social Security numbers, addresses and other personal information of more than 1,750 qualified beneficiaries. This resulted in the employer, Chicago Public Schools, and a printing company being sued for HIPAA privacy and other claims.

Since the school board held plaintiffs’ health insurance elections in its role as an employer, the board’s disclosure fell outside HIPAA’s coverage. Therefore, all claims were dismissed.

What May Implicate PHI

HIPAA did not change nor eliminate the requirement that under COBRA, employers are to inform a provider of the status of a qualified beneficiary. Disclosing that the qualified beneficiary currently does not have coverage but will have, retroactively, once COBRA is elected and the first payment is received would not be providing any PHI. The employer could even disclose the specific dates of the election period and when the premiums are due.

Although for HIPAA purposes, most COBRA information is not considered PHI, one should still proceed with caution. The HIPAA rules require plan sponsors (that is, employers) to safeguard any information provided by the health plan. This would be the same for a COBRA administrator; safeguards and confidentiality are a must. In addition, some TPAs may perform other services for an employer beyond COBRA, services that could make the TPA a business associate.

For example, in the case of a self-funded plan such as a health flexible spending account or health reimbursement arrangement, an employer generally outsources the claim substantiation to TPAs. Following are examples of what contains PHI:

- Reports
- Claim forms
- Substantiation documents
- Some communication notes
- Account information
- Data at rest and data in transmission
- Paper-based and electronic data

In this context, since TPAs definitely receive, maintain and transmit PHI, they are considered a business associate and have many requirements under the HIPAA privacy/security rules to be in compliance.

Preventing Breaches

HIPAA now applies with equal force to a business associate as it has in the past for a covered entity. Therefore, a TPA must put into practice the same measures as a covered entity to prevent privacy and security breaches.

The definition of a breach is “the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protect health information.”

An example of a possible breach for a TPA would be when an explanation of benefits was sent to an incorrect participant and was not returned as undeliverable. This should throw up a red flag and action should be taken quickly to correct the issue.
Some Self-funded Plans to Escape Reinsurance Fees in Future Reform Rules

Self-funded plans that are also self-administered will be made exempt from paying reinsurance contributions under the health care reform law for the 2015 and 2016 benefit years, the Centers of Medicare and Medicaid Services said in final program integrity rules.

The promised relief will occur in future rulemaking, according to the preamble of the program integrity rules. The change will remedy an imbalance under which self-funded plans, which operate without an insurer that funds the risk, would be paying into a fund they could not draw from. (Only insurers can draw payments from state reinsurance funds.)

The program integrity rules were published in the Oct. 30 Federal Register (78 Fed. Reg. 65045). Those rules deal with systems for financial integrity and oversight for participants in health insurance exchanges and how states must operate risk adjustment and reinsurance programs.

In announcing the upcoming reinsurance program relief for certain self-funded plans, CMS noted that there will be caveats. The change will only be applied if the major medical component of the plan is self-insured, CMS states in the integrity rule preamble. It would not be applied if the plan carves out, say, a prescription drug benefit, to be self-insured and self-administered, while keeping a fully insured policy for major medical coverage, the preamble added.

CMS agreed to develop a more specific definition of “major medical coverage” for this purpose, which would add certainty for entities unsure whether they will need to contribute or not.

Those self-funded plans would be required to pay the first-year fee for the program in 2014, and that fee is $63 per plan life that is covered for all 12 months of the year.


Cumulative Index, Volume 26

This cumulative index covers the Guide newsletter, Volume 26, Nos. 1-12. Entries are listed alphabetically, and provide the article by subject and a listing of court cases, followed by the volume, issue number and page number of the newsletter in which the entry appeared. For court cases, this index can be used in conjunction with the Table of Cases and Index of Cases found in Tab 1900 of the Guide.

Articles by Subject
Alternative coverage, 26:5/10
Attorney’s fees, 26:3/8, 26:6/8
CHAMPUS/TRICARE, 26:5/4
Class action, 26:3/2, 26:6/6, 26:8/2, 26:10/2
COBRA compliance tips, 26:5/3
Contributing Editor columns
As feds begin reform frenzy, learn how new fees and W-2 rules implicate COBRA, 26:1/4
Can taking COBRA cost you your health care reform subsidy?, 26:10/6
COBRA class actions are now a real threat, 26:11/2
COBRA compliance: Getting back to basics, 26:9/5
COBRA counts under reform’s shared responsibility rules, 26:2/2
DOL eliminates the old and brings in the new with revised model qualifying event notices, 26:6/3
Having a retiree-only health plan does not end your COBRA obligation, 26:3/6

Business Associate (continued from p. 6)

If an EOB was sent to an incorrect participant and the post office returned it unopened, this would not be considered a breach.

Conclusion
In closing, here are three issues business associates and covered entities should keep in mind to avoid any breaches that could initiate fines and penalties:

1) This statement clarifies that a TPA is considered a business associate: “If you’re a TPA, you are, in effect, running the health plan. We would expect that kind of business associate to operate just as a covered entity would,” Susan McAndrew, HHS deputy director in the Office for Civil Rights, recently stated.

2) In addition, a TPA’s subcontractors are also considered business associates. Now, companies must look not only to their direct contractors, but to their subcontractors of those entities to ensure that they are HIPAA compliant.

3) Furthermore, HIPAA requires that “[u]ses, disclosures and requests for PHI must be limited to the minimum necessary amount needed to carry out the purposes of the use or disclosure.”