Advice from OCR's Breach Parade Reviewing Stand: Verify Whether Your Business Associate is also an Independent Covered Entity

A recent post in this blog series has discussed the valuable guidance for covered entities ("CEs") and business associates ("BAs") that can be contained in the U.S. Department of Health and Human Services list (the "HHS List") of breaches of unsecured PHI affecting 500 or more individuals ("List Breaches"), especially within the "brief summaries of the breach cases that OCR [the federal Office of Civil Rights] has investigated and closed. . . ." ("Summaries").
An example is List Breach number 265 ("LB 265"), which reported a theft of a laptop in Alaska from Trisha Elaine Cordova, a BA of Catholic Social Services ("CSS"), the related CE, on February 1, 2011. The laptop reportedly contained approximately 493 adoption home studies affecting 1,700 individuals. LB 265 also happens to be the most recent List Breach involving a BA for which a Summary has been provided by OCR. (As an aside, LB 265 actually appears on line 266 of a chronological schedule of List Breaches because the first line was used by HHS for column headings.)

According to the LB 265 Summary: "T**he protected health information involved in the breach included names, addresses, phone numbers, dates of birth, driver's license numbers, and health information; 20% of the files contained social security numbers.**"

While the PHI involved covered a broad range, there was nothing unusual about the items. What makes LB 265 Summary worthy of discussion is its final two sentences:

The covered entity did not have a business associate contract with the contractor at the time of the breach. OCR's investigation resulted in the covered entity developing policies and procedures for obtaining business associate contracts when required by the Privacy Rule and verifying that the contractor involved was not an independent covered entity.

The LB 265 Summary identified what OCR deems to be two related important elements of compliance with the HHS Privacy Rule when a CE contracts with another person with respect to PHI – the first of which is obvious and well-known but the second of which is more subtle and less recognized:

1. The requirement that a CE have a business associate agreement or contract ("BAA") with the contractor and

2. The need for the CE to verify in what capacity the contractor is serving with respect to the CE's PHI, that is, whether the contractor is only a BA or is a CE as well as a BA (a "BA/CE").

In its LB 265 Summary, OCR is pointing out its expectation that a contractor like Ms. Cordova may be a BA with respect to the PHI of CSS, but, depending upon her status and activities with respect to such PHI, she could also be a BA/CE. Furthermore, it is viewed by OCR to be the obligation of CSS as a CE (and presumably Ms. Cordova as a BA as well) to

have policies and procedures in place to verify if Ms. Cordova was a BA/CE with respect to the PHI.

Ms. Cordova was apparently provided with PHI by CSS for the purpose of conducting adoption home studies for CSS respecting applicants seeking to adopt children through the auspices of CSS. It is conceivable that the CSS P**HI in Ms. Cordova's hands could have been reformulated and processed by her in her BA activities to such an extent that she could have been a BA/CE. The discussion by OCR in LB 265 of the need by a CE for a BAA under the HIPAA Privacy Rule in the same sentence as the verification activity is consistent with OCR's sentence in its "OCR Privacy Brief" section on CEs as follows: "A covered entity can be the business associate of another covered entity." In requiring a CE to establish policies and procedures to verify whether a BA is also a BA/CE, OCR would appear to have extended CE obligations. However, because no further comment was made on the matter by OCR in LB 265, it would appear that Ms. Cordova was not deemed to be a BA/CE.**

Separate and apart from OCR's position on verification, unless a CE (and its contractor as well) has done sufficient analysis of the status of its BA and the character of the BA's activities, how can the CE properly draft applicable provisions of its BAA? One form of BAA does not necessarily fit all BAs, as much as CEs would like to believe. For example, if a BA of a CE is also a BA/CE with respect to specific PHI, the BA/CE has primary reporting and/or documentation obligations to HHS in the event of a privacy breach, even to the extent of a separate report to HHS for a List Breach. If a BA/CE were to fail to notify HHS of a List Breach, the BA/CE may incur significant penalties and sanctions.

The BAA should take cognizance of whether the BA is deemed by the parties to be a BA/CE and in such case, discuss procedures and methods to confront, among other things, a List Breach, other breaches and the parties' relative investigation, documentation and reporting responsibilities under HIPAA/HITECH, and even data breach insurance. Without proper coordination, in the event of a List Breach or other breach, there can be (i) unnecessary and costly duplication of investigation efforts and evaluation of risk of harm, (ii) inappropriately inconsistent reporting of the event to affected individuals, HHS and state agencies, (iii) inconsistent statements to the media, etc.

In summary, the OCR deems it a requirement for a CE to verify the status of its BA and the character of the BA's activities with respect to the CE's PHI; in turn such CE and BA and their respective counsel should use the verification process to develop provisions in the BAA.