COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 19, Number 12. December 04, 2019 'Misinterpretation' of Breach Rule, Lack of Internal BAA Cost Hospital Group $2.1M

By Theresa Defino

Sentara Hospitals, a nonprofit group of 12 medical centers in Virginia and North Carolina, will implement a fairly minimal two-year corrective action plan (CAP)[1] and pay the HHS Office for Civil Rights (OCR) nearly $2.2 million, a surprisingly high amount for what the organization refers to as a single billing "error." OCR Director Roger Severino, however, used unusually strong language in announcing the settlement a day before Thanksgiving, accusing the hospitals of misinterpreting what constitutes a breach and refusing to comply with reporting requirements even when warned.

Sentara's settlement, which also concerns the alleged lack of an internal business associate agreement (BAA), is the third enforcement action OCR issued[2] in a single month and among the speediest complaints it has formally resolved.

According to OCR's Nov. 27 announcement, the $2.175 million settlement was triggered by a complaint it received April 17, 2017, that "Sentara Hospitals sent a bill to the complainant with another patient's protected health information (PHI) enclosed." The agency offered no explanation for how it arrived at the settlement amount nor why a CAP was necessary. OCR typically requires CAPs when it finds an organization has multiple HIPAA violations, such as failing to conduct a security risk analysis, which it did not find in this case.

OCR said Sentara "reported this incident as a breach" that affected eight people, while the agency's investigation "determined that Sentara mailed 577 patients' PHI to wrong addresses that included patient names, account numbers, and dates of services."

The agency contended that Sentara "concluded, incorrectly, that unless the disclosure included patient diagnosis, treatment information or other medical information, no reportable breach of PHI had occurred." OCR added in the announcement that Sentara "persisted in its refusal to properly report the breach even after being explicitly advised of their duty to do so by OCR."

Said Severino: "HIPAA compliance depends on accurate and timely self-reporting of breaches because patients and the public have a right to know when sensitive information has been exposed. When health care providers blatantly fail to report breaches as required by law, they should expect vigorous enforcement action by OCR."

OCR's own investigation "revealed that the billing statements for 577 patients were merged with 16,342 different guarantor's mailing labels." In contrast to the OCR news release, the settlement itself does not give a reason as to why Sentara only reported eight patients as being affected.

This settlement came 20 months after an individual complained to OCR that he or she received someone else's medical bill, a quick resolution. Similarly, in September, OCR announced a settlement agreement with a hospital in Florida barely a year after receiving a complaint that a mother had been denied her unborn child's medical records.[3] It is not uncommon for the agency to issue resolutions five or more years after a suspected HIPAA violation.

Sentara Seeks to Prevent Repeat of 'Error'

Sentara sent *RPP* a statement in response to questions about the settlement. The hospital group indicated that what it called "the incident" occurred when "a vendor who prints and mails our bills accidentally printed some patients' billing information on other patients' statements. Upon discovering the error, we took immediate action to halt bill printing and mailing and later notified the affected patients."

The hospital group "cooperated fully" with OCR, the statement to *RPP* said. "Since the incident, we have implemented more stringent quality control measures, required our vendor to enhance their quality control processes and hired a new privacy director. We also are in the process of updating employee training and education and assessing our privacy program as a whole. Sentara is committed to the security of our patients' personal information and working hard to prevent this error from happening again."

Sentara did not use the word "breach" to describe what happened, and it did not admit wrongdoing as part of the settlement.

The misdirected bills were not the only problems OCR found and that underlie the payment.

Corporate BAA Lacking

"OCR also determined that Sentara failed to have a business associate agreement in place with Sentara Healthcare, an entity that performed business associate services for Sentara," the agency announced.

Ten Sentara hospitals are "affiliated covered entities" (CEs) under the common ownership of Sentara Healthcare, the "parent corporation and business associate" of Sentara Hospitals, according to the settlement agreement, which does not explain the status of the other two hospitals in the 12-medical-center group.

"Sentara Hospitals allowed their parent corporation and business associate, Sentara Healthcare, to create, receive, maintain, or transmit PHI on their behalf and to provide services involving the disclosure of PHI without obtaining satisfactory assurances," OCR said in the settlement agreement.

The agency stopped short of accusing Sentara of impermissible disclosures specifically, but may simply have failed to spell this out. Because there is no breakdown of how OCR arrived at the $2.175 million, it is not possible to tell how much the lack of a BAA contributed to the total, nor what category of penalties any of the alleged infractions fell into (e.g., reasonable cause, willful neglect).

Previous Settlement Focused on Same Issue

The question of when affiliated organizations within the same corporate structure need BAAs with each other has been a somewhat vexing issue, and one that was the subject of a previous OCR settlement.

In 2016, Care New England settled with OCR for $400,000 and agreed to implement a two-year CAP.[4] Care New England is the parent and business associate for Women & Infants Hospital in Rhode Island, itself the CE. OCR accused the hospital of impermissible disclosures to Care New England; OCR alleged that, while there was a BAA, it was not updated.

Although Care New England was the party signing the OCR agreement, it was not accused of any HIPAA violations itself, but signed on behalf of its four hospitals, including Women & Infants.

The Care New England case was also somewhat complicated by the fact that the hospital had experienced a breach in 2012 that was the subject of a 2014 settlement with Massachusetts authorities—likely the reason the

BAA situation came to OCR's attention in the first place.

Both state attorneys general (AGs) and OCR have authority to bring HIPAA cases. In this situation, the Massachusetts settlement, which stemmed from the loss of backup tapes that had PHI for 14,000 patients, was for $150,000. There also was a two-year CAP.

Coming two years after the action, OCR's $400,000 settlement with Care New England caught many by surprise based on the size and the tangential issue of the BAA. At the time, OCR stated that the AG's agreement "sufficiently cover[s] most of the conduct in this breach" involving the tapes.

Sentara's statement to *RPP* made no mention of the BAA issue, and a spokesperson did not respond to questions, citing the unavailability of personnel over the Thanksgiving holiday.

Non-breaches Must Be Reported

As noted earlier, the requirements in the CAP are few. The hospitals are not being asked to sign BAAs with their parent organization, as apparently this occurred on Oct. 17, 2018. Nor is there any mention of a risk analysis being conducted.

The hospital group is required to "develop, maintain, and revise, as necessary, their written policies and procedures" related to the breach notification rule. Revised policies are due to OCR for approval within 90 days of the Nov. 11 effective date of the settlement. The settlement doesn't state how long OCR can take to review them, but Sentara will have 45 days to make changes should OCR find the policies lacking, and then 60 days from that point to implement them. Employees must be trained on the new policies within specified time periods.

The CAP also has a new take on "reportable events." Getting to the core of the breach notification issue OCR said Sentara had, the agency is requiring Sentara to notify it whenever the hospital group investigates an "unauthorized acquisition, access, use or disclosure of PHI [that] may have occurred" and determines the incident is *not* a reportable breach.

In contrast, the other settlement agreement this month obligates the University of Rochester Medical Center to alert OCR in writing within 60 days of any actual HIPAA violations committed by employees.[5]

Sentara must notify OCR within 15 (and no later than 60) days of making a non-breach determination of what OCR is calling a "reportable event," sharing with the agency "a complete description of the incident, including the relevant facts and the persons involved; a copy of any breach risk assessment Sentara Hospitals conducted to evaluate the incident; and a description of the actions taken and any further steps Sentara Hospitals plan to take to address the matter."

Lighter Payment for Previous Late Notice

OCR will then decide for itself whether Sentara made the correct call.

"If OCR disagrees with Sentara Hospitals' breach risk assessment, Sentara Hospitals shall revise the assessment based on technical assistance provided by OCR and provide appropriate breach notification," the CAP states.

The agency also pointed out all the usual breach notification rules continue to apply to Sentara, meaning if it determines there *is* a reportable breach, it had better follow the rules and notify OCR, patients and the media as appropriate.

This is the second settlement in recent months in which a CE was sanctioned for late or inappropriate

notification to OCR. In October, OCR fined Jackson Health System $2.15 million for a variety of HIPAA violations, including that it didn't update the number of patients affected in a 2013 breach until 2016.[6]

Another settlement for late notification brought a far lighter sanction by OCR. In January 2017, a nonprofit health care system in Illinois agreed to a $475,000 payment and two-year CAP for being 45 days past the 60-day requirement in notifying 836 patients, the media and OCR of the loss in 2013 of surgery scheduling sheets.

OCR said the delay was due to "miscommunications between its workforce members."[7]

1 "OCR Secures $2.175 Million HIPAA Settlement After Hospitals Failed to Properly Notify HHS of a Breach of Unsecured Protected Health Information," Office for Civil Rights, November 27, 2019, .
2 "Resolution Agreements and Civil Money Penalties," Office for Civil Rights, last reviewed November 27, 2019, .
3 Theresa Defino, "Just Get It Done: Amid $85K Penalty, CEs Must Address Roadblocks Thwarting Records Release," *Report on Patient Privacy* 19, no. 10 (October 2019), .
4 Theresa Defino, "Citing Outdated BAA, OCR Gets $400,000 From Parent of Hospital That Lost Tapes," *Report on Patient Privacy* 16, no. 10 (October 2016).
5 Theresa Defino, "OCR Warns Against 'Neglecting' Encryption As Hospital Pays $3M for Loss of Mobile Devices," *Report on Patient Privacy* 19, no. 12 (December 2019).
6 Theresa Defino, "New OCR Enforcement Action Shows Risks of Paper Files, Media Leaks, Lax Info Security," *Report on Patient Privacy* 19, no. 11 (November 2019), .
7 Theresa Defino, "Sole Failure of Timely Notification After Breach Costs Covered Entity $475,000,"*Report on Patient Privacy* 17, no. 2 (February 2017).