COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 22, Number 9. September 07, 2022 One Security Guard, One Container: Find Unravels Derm Practice's Disposal Failure

By Theresa Defino

When recommending best practices, federal privacy and security officials stress that organizations need to follow their protected health information (PHI) wherever it "lives," as HIPAA rules require safeguarding no matter the location.

"In the dumpster" should now be on that data map if it wasn't already, in light of a new $300,000 settlement between a dermatology practice and the HHS Office for Civil Rights (OCR) that includes a two-year corrective action plan (CAP).[1]

In March 2021, a security guard found a single-specimen container "bearing a label containing PHI" in a parking lot used by New England Dermatology and Laser Center (NEDLC).[2] NEDLC admitted to OCR that such containers were added to its "regular waste, bagged and placed in an exterior dumpster accessible via the parking lot, without alteration to the PHI containing label."

Along with the settlement, OCR issued FAQs about proper disposal of PHI.[3] For privacy attorney Joseph Lazzarotti, the breach and settlement drive home a number of other lessons, including that organizations need to understand the expansiveness of what constitutes PHI.

And although just one was found that day, NEDLC said it disposed of containers this way for 10 years—beginning Feb. 4, 2021, and ending the day the security guard appeared. OCR's online breach reporting website lists 58,106 affected patients, a number that, oddly, is not mentioned in the settlement agreement OCR announced Aug. 23.

Also not included is the fact that this was NEDLC's second breach—of relatively the same type—in four years, which may help explain the size of the settlement. In 2018, NEDLC acknowledged it had "improperly disposed of patient records…by failing to shred them prior to disposal in a dumpster," according to OCR's breach portal.[4]

Founded in 1954, NEDLC has nine physicians operating from four locations in Massachusetts, with a service area that spans western Massachusetts, northern Connecticut and southern Vermont, according to its website.

The settlement documents do not identify the location involved in the 2021 breach, which NEDLC reported to OCR on May 11 of that year. The agency said the labels on specimen containers listed "patient names, dates of birth, dates of sample collection, and name of the provider who took the specimen."

CAP Requires Disposal Policies

OCR investigators concluded NEDLC had potentially violated C.F.R. § 164.530(c)) of the Privacy Rule requiring safeguards for PHI and 45 C.F.R. § 164.502(a)), which prohibits impermissible disclosures.

As noted earlier, the disposal method was in place for a little more than 10 years. OCR provided no information on how it calculated the $300,640 payment and did not respond to *RPP*'s questions on the amount or why the 2018 breach wasn't addressed in the settlement.

Stephen Ieraci, NEDLC's executive director and privacy officer, signed the settlement agreement. He did not respond to repeated requests for comment.

Like others before it, the CAP requires NEDLC to develop new policies and procedures, train workers on them, report breaches and investigations to OCR and submit periodic and annual implementation reports. It is not required to hire a monitor to oversee the CAP.

The "minimum content" of the policies and procedures, which OCR must approve, address:

- "NEDLC's policy for the disposal of all PHI created, received, or maintained by NEDLC.
- "Protocols for training all NEDLC's workforce members that are involved in handling and disposing of PHI as necessary and appropriate to ensure compliance with the policies and procedures" specified in the agreement.
- A "review and [an] update as necessary NEDLC's policy for the physical safeguarding of PHI.
- "Protocols for training all NEDLC's workforce members that are involved with handling PHI to ensure compliance with the policies and procedures provided" in section V(A) above.
- "Application of appropriate sanctions against NEDLC workforce members who fail to comply with policies and procedures provided for" in the agreement.

Déjà Vu With Another Dumpster

NEDLC's 2018 breach affected 16,000 patients and included their "names, mailing addresses, dates of service, and clinical information." OCR took no enforcement action, apparently satisfied by the changes the practice had made, which consisted of implementing "a new procedure for disposal of PHI," training staff and hiring a business associate (BA) "to shred all records containing PHI."

In a 2018 news story, Ieraci said unshredded documents had gone into a dumpster since the Northampton location opened in June 2013.[5] At the time, there was no evidence of the PHI being misused and he noted NEDLC was in contact with OCR about that breach.

In contrast, *RPP* could not find any published reports about the newest breach that led to the settlement, although given the size (more than 58,000), notice to the media was required.

The new settlement provides a good opportunity for covered entities (CEs) and BAs to look a little deeper and address a host of HIPAA compliance basics that some might neglect, said Lazzarotti, a principal in the Berkeley Heights, New Jersey, office of Jackson Lewis P.C., and head of its privacy, data and cybersecurity practice group.

He said the settlement touches on "two really important issues that I think are lost in the practice" of medicine—namely what is PHI and, secondly, what is the process for destroying PHI once it's no longer needed.

Understand the Definition of PHI

Much of health care is delivered by small practices, and staff is "not always thinking about compliance," he added. In health care, "compliance is sometimes difficult to manage consistently across all parts of the business. I think people are not as vigilant as they could be or should be."

Workers "on the front lines" are often confused about PHI and mistakenly think that if there is no diagnostic information—like there was not on NEDLC's containers—then it's not PHI, Lazzarotti said. "I thought it was

interesting to see there was some enforcement action with respect to data that doesn't happen to be very sensitive PHI, but it's PHI nonetheless."

Addressing the new OCR FAQs, Lazzarotti said they are useful, particularly because OCR's website contains a "wealth of information," but it can sometimes be difficult to find something specific.

The guidance doesn't suggest removing the labels themselves or using a marker to black out the information, but these are additional steps CEs could take, especially with sensitive data.

OCR is "trying to be practical" while still offering suggestions on data protection, Lazzarotti said, adding, "it's probably a lot easier, a lot more efficient, to just put the bottles into a bag that you can't see through and secure [them] until you can otherwise get rid of them."

It's Not About Harm Anymore

The definition of PHI "is quite broad," Lazzarotti noted. As he wrote on his blog, it "starts with the definition of 'individually identifiable health information,' which generally means identifiable health information transmitted or maintained in electronic media or any other form or medium that 'relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.'"[6]

As OCR explains,[7] an "impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

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

If an item or items with PHI are disposed of improperly, and there is a breach, notification to patients is usually required. Under the revised Privacy Rule, organizations must notify patients, the media (depending on the number of patients affected) and OCR.

Whether an inappropriate use or loss results in harm is no longer an issue in notification as it was prior to the final rule issued in 2013. Now there is presumed to be a reportable breach unless certain conditions are met—and they must be documented.

But it's unlikely that all providers and other CEs have shifted to this standard, Lazzarotti said.

"People will naturally say, 'Oh, no harm, no foul.' That's a common-sense approach and you can't blame people, especially when many, many state breach notification [requirements] have exactly that [risk of harm] analysis. But HIPAA takes a different view," Lazzarotti said.

In that regard, CEs and BAs will need to consider whether state breach laws apply and the analysis those may require related to notification.

Don’t ‘Stonewall’ If OCR Calls

Lazzarotti had no knowledge about why OCR settled with NEDLC for $300,640, but noted that agency officials frequently say—and Lazzarotti has found them to be true to their word in his dealings—that one way to reduce a penalty is to cooperate.

“Things happen. Breaches happen. It’s not the end of the world, and it doesn’t mean anybody’s going to jail,” he said.

When dealing with OCR or any agency on behalf of a client, “we try to be as responsive as possible,” Lazzarotti said. “We try to resolve the matter as much as possible to the extent we can. We zealously represent our clients, but if you're not as cooperative as the agency would like you to be…maybe you stonewall, maybe you don’t provide the documents they want, you argue back and forth…they may take an approach where instead of just saying, ‘Okay, let’s settle for a hundred thousand,’ they may say, ‘We are going to go through all the penalty provisions and we are going to count every violation,’” which can lead to a much higher penalty.

OCR staff usually “want to be helpful” and will work to close a complaint “without any penalty,” he said.

Lazzarotti also reminds CEs and BAs to document all corrective actions they take following a breach, which can be helpful, particularly if OCR is alerted following a patient complaint or other means, such as a news story.

Contact Lazzarotti at joseph.lazzarotti@jacksonlewis.com.

1 U.S. Department of Health & Human Services, “OCR Settles Case Concerning Improper Disposal of Protected Health Information,” news release, August 23, 2022, https://bit.ly/3AMK1wH.
2 U.S. Department of Health & Human Services, “New England Dermatology Resolution Agreement and Corrective Action Plan,” resolution agreement, last reviewed August 22, 2022, https://bit.ly/3wUHDTA.
3 Theresa Defino, “OCR Disposal Guidance Follows Three Settlements,” *Report on Patient Privacy* 22, no. 9 (September 2022).
4 U.S. Department of Health & Human Services, “Office for Civil Rights Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information,” last accessed September 6, 2022, https://bit.ly/3CWwc1u.
5 Bera Dunau, “Northampton dermatology center improperly disposed of thousands of medical records,” *Daily Hampshire Gazette,* July 20, 2018, https://bit.ly/3Qk4Y7U.
6 Joseph J. Lazzarotti, “Recent HIPAA Settlement Offers Lessons on Data Disposal and the Meaning of PHI,” JacksonLewis Workplace Privacy, Data Management & Security Report, August 24, 2022, https://bit.ly/3D2dRA8.
7 U.S. Department of Health & Human Services, “Breach Notification Rule,” last reviewed July 26, 2013, http://bit.ly/2tcFpPc.