COSMOS
Navigate the Compliance Universe

Report on Medicare Compliance Volume 33, Number 43. December 09, 2024
Provider Settles HIPAA Case over Disclosing Too Much of a Patient's PHI

By Nina Youngstrom

When a patient asked Holy Redeemer Family Medicine in Bensalem, Pennsylvania, to send the results of one test to a prospective employer, something unfortunate happened. The practice sent all her medical records, including sensitive information about the patient's reproductive health care, to the would-be employer.

More than a year later, Holy Redeemer Family Medicine agreed to pay $35,581 to settle allegations it impermissibly disclosed the patient's protected health information (PHI) in violation of the HIPAA Privacy Rule, the HHS Office for Civil Rights (OCR) said Nov. 26.[1] Holy Redeemer also must implement an extensive corrective action plan.

The resolution agreement stemmed from an OCR investigation sparked by a September 2023 complaint that Holy Redeemer Family Medicine allegedly disclosed the patient's PHI to the prospective employer, including her surgical history, gynecological history, obstetric history, and other sensitive health information about reproductive health care.[2] The lone test result she wanted disclosed had nothing to do with reproductive health care. OCR said its investigation found that Holy Redeemer didn't have the patient's authorization for the broad disclosure of her PHI "and that there otherwise was no applicable requirement or permission under the Privacy Rule for such a broad release of her medical records."

Consider Retraining Medical Records Staff

The settlement is a reminder for medical record departments to pay close attention to PHI requests and patient authorizations before responding to them, said attorney Jennifer Hennessy, with Foley & Lardner LLP. "The key is having medical record personnel who have been trained and understand the nuances of reviewing the requests that come in," she said. Whether they're responding to authorizations signed by the patient or requests from a third party, such as a subpoena or a request from a law enforcement agency, covered entities should ensure that medical records staffers understand that only the specific information listed should be provided and nothing more. "This is in addition to making sure the authorization or other request is valid under HIPAA to ensure disclosure is permitted in the first place," Hennessy noted.

OCR calling out the reproductive PHI disclosure in Holy Redeemer's settlement echoes the Biden administration's determination to protect what it considers particularly sensitive information, Hennessy said. OCR finalized a HIPAA regulation on reproductive health care privacy in April 2024, although she noted compliance isn't required until Dec. 23 and therefore the patient's allegations predate it. The new rule prohibits covered entities (CEs) from disclosing reproductive health care information to law enforcement agencies, health oversight agencies, or coroners/medical examiners, or in judicial or administrative proceedings, unless CEs get an attestation from the requestor that the information won't be used in prohibited ways. The rule adds a category of prohibited uses and disclosures of PHI that "encompasses the use or disclosure of PHI for any activities conducted for the purpose of investigating or imposing liability on any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care that the regulated entity that has received the

request for PHI has reasonably determined is lawful under the circumstances in which such health care is provided."

But the sands may shift under the rule. For one thing, it's being challenged in a lawsuit filed by the state of Texas, which asked the U.S. District Court for the Northern District to stop HHS and OCR from enforcing the HIPAA reproductive health care rule as well as an aspect of the original 2000 HIPAA Privacy Rule.[3]

And "we are waiting to see whether the Trump Administration will enforce" the rule, Hennessy said.

Holy Redeemer didn't respond to *RMC*'s request for comment. It didn't admit liability in the resolution agreement.

OIG Cites Shortcomings in OCR HIPAA Oversight

The settlement came down the same week as an HHS Office of Inspector General (OIG) report on OCR enforcement of HIPAA violations.[4] OIG looked at OCR's performance of HIPAA audits, which are required by the Health Information Technology for Economic and Clinical Health (HITECH) Act. The bottom line: "OCR oversight of its HIPAA audit program was not effective at improving cybersecurity protections at covered entities and business associates," according to OIG. "OCR's HIPAA audit implementation was too narrowly scoped to effectively assess ePHI protections and demonstrate a reduction of risks within the health care sector." One reason: the audits assessed only 8 of 180 HIPAA requirements, with only two related to security rule administrative safeguards and none related to physical and technical security safeguards.

In its response, OCR noted it has a small budget and its requests for more money have been in vain. It agreed with most of OIG's recommendations, including doing more audits and expanding their scope (budget permitting).

But OCR didn't agree with OIG's suggestion that "OCR document and implement standards and guidance for ensuring that deficiencies identified during the HIPAA audits are corrected in a timely manner." Again, money plays a role here. "OCR does not have the financial or staff resources to pursue corrective action plans or potential civil money penalties against every audited entity where OCR finds HIPAA deficiencies."

Although OCR indicated in February it would ramp up its audits later this year, "the end of the year is quickly approaching at this point," Hennessy said. OCR had expressed its plans to restart audits akin to audits it did in 2016 and 2017, the last time they were conducted. OCR's enforcement is based on complaints and breach reports.

Contact Hennessy at jhennessy@foley.com.

1 U.S. Department of Health and Human Services, "HHS Office for Civil Rights Settles with Holy Redeemer Hospital Over Disclosure of Patient's Protected Health Information, Including Reproductive Health Information," news release, November 26, 2024, https://bit.ly/49eXMoK.
2 U.S. Department of Health and Human Services, Office for Civil Rights, "Holy Redeemer Hospital Resolution Agreement and Corrective Action Plan," content last reviewed November 26, 2024, https://bit.ly/3ZczhnF.
3 Nina Youngstrom, "Texas Asks Court to Kill HIPAA 2024 Rule and Part of 2000 Rule; Loper Bright Is Lurking," *Report on Medicare Compliance* 33, no. 33 (September 16, 2024), https://bit.ly/3Vp39w1.
4 U.S. Department of Health and Human Services, Office of Inspector General, Office of Audit Services, *The Office for Civil Rights Should Enhance Its HIPAA Audit Program to Enforce HIPAA Requirements and Improve the Protection of Electronic Protected Health Information*, A-18-21-08014, November 2024, https://bit.ly/3ZsHTrB.