COSMOS
Navigate the Compliance Universe

Report on Medicare Compliance Volume 27, Number 33. September 17, 2018
PHI Disclosures May Be Curveballs; OCR Gives Technical Assistance

By Nina Youngstrom

When a physician walked into a hospital room to tell the patient test results, the physician didn't think twice about disclosing the protected health information (PHI) in front of the two women there because he assumed they were the patient's wife and daughter. But the truth was a bit more complicated. The patient intended to shield his daughter from the news so she wouldn't worry, and he was recently widowed, with no plans to share the results with the other woman, who was a neighbor.

Fortunately, the physician was the bearer of good news—the test was negative—but he shouldn't have disclosed the results in front of other people without the patient's permission, says Barbara Duncan, HIPAA privacy officer at Stormont Vail Health in Topeka, Kansas. "We try to reinforce with our providers that if they walk into a room with test results, even if they know the person in the room, they should ask the patient if it's a good time to talk" or if they prefer visitors to step out in the hallway, she says.

To minimize the risk of improper disclosures, physicians and other clinicians and employees are encouraged not to make assumptions about their patients and the people who accompany them to Stormont Vail Health and to avoid talking about their patients in earshot of other patients, Duncan says.

HIPAA permits the use and disclosure of PHI for treatment, payment and operations (TPO), but covered entities must have patient authorization outside of TPO with some exceptions described in the privacy regulation (see tip sheet, p. 4). An impermissible use or disclosure of PHI is automatically a breach unless covered entities can show there is a low probability the PHI has been compromised, according to the HIPAA Breach Notification Rule. They are required to evaluate risk using four 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."