with current regulations and best practices." ■

SOURCES

- Erin Dunlap, JD, Coppersmith Brockelman, Phoenix. Telephone: (314) 255-5988. Email: edunlap@cblawyers.com.
- Angela Matney, JD, Reed Smith, Washington, DC. Telephone: (202) 414-9343. Email: amatney@reedsmith.com.
- Jeremy Mathis, Vice President of Client Success, Fathom, Cleveland, OH. Telephone: (216) 369-2220.
- Kristen Rosati, JD, Coppersmith Brockelman, Phoenix. Telephone: (602) 381-5464. Email: krosati@cblawyers.com.

Unique Identifier Rule Can Be Confusing

HIPAA's Unique Identifier Rule mandates the use of standardized codes to provide unique identification of healthcare organizations, employees, and patients in an effort to enhance efficiency and security. The requirements and use of the codes can be confusing.

The unique identifier rule was part of the administrative simplification part of HIPAA, explains **Amy M. Magnano**, JD, partner with the Morgan Lewis law firm in Seattle. The goal was to make the identification process more efficient by ensuring that patients, health plans, and providers would all have a unique identifier to use in standard transactions, she explains.

"The thing to know about it, though, is, although the rule originally envisioned two unique identifiers for four categories, ultimately, now there are two categories currently in existence," she says. "So, as a healthcare entity, you have to have an Employer Identification Number [EIN], which is actually something that came out of the tax code. So, this is where this gets kind of complicated, because you have to have an EIN to submit standard transactions as a healthcare entity.

The National Provider Identifiers [NPI] is a unique 10-digit identification number covered entities use with standard HIPAA electronic transactions, says **Henry Norwood**, JD, an attorney with the Kaufman Dolowich law firm in San Francisco. One common pitfall health providers face with their NPI numbers involves locum tenens providers — a temporary provider covering at a facility for another provider who is unavailable, he notes. Should the facility bill under the normal provider's NPI or the locum tenens provider's NPI? The answer can vary depending on whether the patient is covered by Medicare, Medicaid, or private insurance, Norwood says.

He explains that if billing through Medicare, the facility can bill under their normal provider's NPI if the normal provider is unavailable, the Medicare patient is seeking care from the normal provider, the locum tenens provider is paid per diem, and the locum tenens provider cannot bill under the normal provider's NPI continuously for more than 60 days.

"Medicaid plans typically follow this same rule, but facilities should confirm with their state Medicaid rules. Private plans generally allow billing services by locum tenens providers under the normal provider's NPI, but facilities should confirm with each patient's plan in advance," Norwood says. "Misusing an NPI number can cause issues ranging from billing headaches to potential fraud actions by the government, so health providers should plan to avoid issues in advance." ■

SOURCES

- Amy M. Magnano, JD, Partner, Morgan Lewis, Seattle. Telephone: (206) 274-6451. Email: amy.magnano@morganlewis.com.
- Henry Norwood, JD, Kaufman Dolowich, San Francisco. Telephone: (628) 219-9814. Email: henry.norwood@kdvlaw.com.

Hospital Terminates Employees for Allowing Another To Do Their Jobs

A Boston hospital recently announced that it terminated two employees over a privacy breach after an investigation determined that they allowed a third person, not an employee of the hospital, to perform some of their job duties. That person might have accessed patient protected health information (PHI), the hospital said.

The incident holds lessons for covered entities, says **Ashley Algazi**, JD, partner with the Rivkin Radler law firm in Uniondale, NY. Although it is difficult to control your

employees' every move, especially if they are working remotely, covered entities can reduce the risk of a similar breach occurring by monitoring their information technology systems for unusual activity and implementing training that specifically addresses keeping usernames and passwords confidential, she says.

Since all employees should have a unique username and password, covered entities should have the ability to track unusual activity and identify potential breaches, she notes.

"Ultimately, good employee management is required to identify if your employee is offloading their work to an outside party," Algazi says.

She advises watching for these top four red flags:

- employees not being able to answer questions about their work or being evasive in their answers;
- employees who are unavailable during regular business hours;
- a sudden change in the quality of work product of an employee; and
- regular unusual communications or file transfers to parties outside of your organization.

Understand HIPAA Limitations

With how busy a typical hospital gets, and considering the staff shortages that most healthcare operations face, it is understandable that some staff may need backup or assistance to help meet the demands of their jobs, says **John F. Howard**, JD, senior attorney with the Clark Hill law firm in Scottsdale, AZ.

"In these situations, it is important that they understand the limitations of what is permitted around the access and use of PHI, specifically, the PHI they need to access and use to perform their jobs," he says. "Just because two employees work in the same facility does not mean they are authorized to all PHI within that facility's possession or control."

For example, a staff member in the pediatric unit of a hospital will not have the same access to PHI that a staff member in the cardiothoracic unit will have, he says. While this seems to make logical sense, it also is required under HIPAA. Internal uses are required to be governed by policies and procedures that control and restrict access to PHI based on the specific roles of the staff or workforce members, Howard says.

These policies and procedures must identify the roles or classes of people in the workforce that need access to PHI and what PHI they need access to. All of this is required to be based on what the individual needs to be able to do their job, he says.

"One type of HIPAA violation we have all become used to seeing that relates to these requirements is employee snooping. Where a person with some level of authorized access, based on their job role, exceeds that access and starts looking at PHI belonging to individuals that they do not need to access to do their jobs," Howard says. "We have seen many cases where this has led to fines against covered entities and actions taken against employees. Granted, this is different than an employee getting assistance from another employee to do their job, as arguably the use is for [treatment, payment, and healthcare operations], but it is essentially a violation of the same restrictions. A person's access rights are required to be restricted based on that person's role."

Covered entities can avoid these issues by making sure that their staff are appropriately trained on what role-based access rules and procedures the organization has put in place, he says. Covered entities also can put technical controls, where reasonable and possible, to limit access based on each individual. This will help limit the possibility of staff crossing over into operational areas where they are not permitted to do so, he says.

"Essentially, the best way to combat these types of breaches is to train your workforce not just on the requirements, but also on the purpose of such requirements," he says. "Patients expect some level of confidentiality of their health information, even within healthcare operations. If a workforce member does not have a 'need to know' or have access to certain PHI, then they are not allowed to have access to it. This not only makes sense from a public policy perspective in helping keep trust in the healthcare system. It is also required under HIPAA." ■

SOURCES

- Ashley Algazi, JD, Partner, Rivkin Radler, Uniondale, NY. Telephone: (516) 357-3528. Email: ashley.algazi@rivkin.com.
- John F. Howard, JD, Senior Attorney, Clark Hill, Scottsdale, AZ. Telephone: (480) 684-1133. Email: jfhoward@clarkhill.com.