COSMOS
Navigate the Compliance Universe

Compliance Today - August 2021
Common HIPAA mistakes made by physician practices: Part 2

By Marti Arvin

Marti Arvin (marti.arvin@cynergistek.com) is an Executive Advisor at CynergisTek in Austin, TX.

Part one of this series, published in last month's issue,[1] discussed general Health Insurance Portability and Accountability Act (HIPAA) mistakes and issues under the Breach Notification Rule by physician practices. This article will discuss the issues physician practices have that are unique to the Privacy and Security rules.

Common Privacy Rule mistakes

In order to comply with the Privacy Rule, a basic level of understanding regarding appropriate uses and disclosures of protected health information (PHI) is critical. Sometimes in the environment of a smaller, more close-knit organization, this can be easy to overlook or forget. There are several areas where users may not understand the limitation on their use and disclosure of PHI.

Access to their own record

Organizations vary in their approach to allowing users to access their own record directly if the user otherwise has access to the electronic health record (EHR). If the policy is that access is prohibited, the practice should have a process for monitoring this to help ensure users do not access their record in this manner.

If the policy is to allow users to look at their own record, this should still be monitored. It is likely that users who can look also have some ability to modify the record. A process should be in place to review user's access to their own record to ensure it is a view-only access and that no changes were made to the record. Whether the policy is to allow or not allow access, it should be applied equally to physicians and staff. In a smaller physician practice, it may prove difficult to enforce consistent sanctions if the individuals who will ultimately invoke the sanctions—the physician leadership—are some of the individuals who are engaging in the misconduct. If a staff member would be given a written warning for accessing their own record, a similar sanction should be imposed against a physician who does the same.

Accessing a minor child's record

Under the HIPAA regulations, a parent is commonly the personal representative of the minor child. This means the parent has the same rights to access PHI the child would in most circumstances. However, it is not always true that the parent is the personal representative of the minor child. There can be circumstances where the minor child has the exclusive access right to certain portions of the record related to specific healthcare services. Allowing self-access to the record is not equivalent to allowing access to the record of another person when the user serves as the personal representative.

It can be very tricky to control access to a minor child's record when the right to access is mixed. If a personal representative directly accesses a record as the personal representative, it might not be considered as egregious as accessing the portion of the record for which they are not considered the personal representative. Unfortunately, in most EHRs, the record is not neatly segregated in this manner. If a covered entity allows the

personal representative to use their direct access rights to access their minor child's record, it could result in a data compromise and possibly a breach if the individual accesses information that they do not have a right to see without an authorization.

This is another case when there should be monitoring to ensure the access is not occurring and that changes are not being made to the record. A best practice is to have a policy that clearly defines whether a user can directly access their own record. The policy should clearly prohibit direct access to a record (except the user's own record if that is the practice's decision) other than to perform the user's job. The policy should also address the process for monitoring and the sanctions applicable to improper accesses. As discussed in Part 1 of this series, the organization's policies should be clear that sanctions will be applied in a consistent manner regardless of the user's status.

Very similar provisions apply to access a family member's record. Organizational policies should be clear that if a user wants access to a family member's record, they are to follow the organization's policies on requesting access. Users are granted direct access to the organization's EHR to perform their job duties. These duties would not include using that access to sidestep other organizational policies regarding how patients and other third parties gain access to the system.

Disclosing information outside the covered entity

There are a number of places that users may be tempted to share patient information with no ill intent. Social media is a common place users share information. This may be to share information about the hard day at work or it may be specific to a patient. Often users don't understand that a patient granting them "permission" to share is not sufficient to meet the requirements of the Privacy Rule.

Even with a patient authorization, it is probably not consistent with the organization's policies and procedures because of the user's role. If the individual's role is not to promote the organization on social media, it is unlikely the organization views such shares as within the scope of employment. Another factor is the nature of the information shared. While users may think they have deidentified the information, it is not uncommon that a date is mentioned or unique aspects of the individual's care are discussed. Sharing photos is another common practice. Even if the user has become close to the patient or knows them through other interactions, there still needs to be a separation between the personal and the professional.

Physician practices may also have an organizational website. To share information about a patient on this website would likely require an authorization. Again, users may not remember that a full-face photo is an identifier under the Privacy Rule. For example, sharing a patient's pictures to depict a before and after would need authorization.

Physician practices also may promote and sponsor online patient support groups. This is a tricky scenario. If the patient freely offers information on the support group, the practice might be tempted to view that as information that is not PHI for their practice. The support group might also have nonpatient family members participating and sharing their own health information. All of this is arguably PHI if the practice is hosting the site for the support group. The Privacy Rule does not identify PHI as only the individually identifiable information created or received by a covered entity for patients. At minimum, if a support group is hosted by the physician practice, there should be a terms of use document that any participant agrees to that makes them aware the information they share may be viewable by current and future members of the support group. The practice may also consider requiring a username and password for participants.

Sharing information for education of the organization's workforce and others

Practices need to be sure that if information is shared to provide education, it is done in an appropriate way. The Privacy Rule permits a covered entity to use PHI for its own educational purposes. This may include its workforce and trainees, such as students in nursing and allied health or medical students and residents. The caution is to be aware if others will be present. If the practice allows other community providers to participate in its educational programs, those providers may not be entitled to PHI. The presentation may need to be deidentified. A best practice is to use deidentified information or only the bare minimum identifiers necessary to provide the educational experience. For example, instead of saying, "Susie Smith, date of birth 10/21/72," the presenter would say, "an XX-year-old female." Habitually using deidentified information makes it less necessary to worry about who is in the room.

If the practice does not have any formal affiliation agreement for the educational activity, there should be a policy and procedure that addresses this. Observers are an example of this. If the observer is a high school or college student, the practice can likely still fit this within the HIPAA exception, but care should be taken to make sure the patient's permission is obtained before the individual is allowed to participate in an encounter. There should also be some minimal education for the person regarding patient confidentiality and HIPAA.

Notice of Privacy Practices issues

The Privacy Rule provisions for the notice of privacy practices (NPP) require that all direct treatment providers give the NPP to patients at the first episode of care.[2] The regulations say it must be provided, not simply made available. It is very common for registration staff to ask patients to sign an acknowledgment that the NPP was received when it has not actually been provided to patients. There is a notice of proposed rulemaking (NPRM) that was published by the Office for Civil Rights (OCR) in January that proposed to eliminate the requirement to obtain an acknowledgment.[3]

The Privacy Rule also requires that the notice be posted in a prominent place where patients are likely to see it.[4] In the preamble to the final regulations under the Health Information Technology for Economic and Clinical Health Act, OCR clarified that a summary of the notice could be posted as long as the full notice was readily available in a nearby location.[5] For example, the summary could be posted on the wall, and the full notice available in brochures on a table below the summary. The key to this requirement of the rule is that it be posted in a prominent place. If a visitor to the practice cannot locate the posted NPP, it is probably not in a prominent place. The Privacy Rule also requires that the current NPP be posted on the website if the practice maintains one.

The Privacy Rule permits the NPP to be updated when the law changes or a practice's use and disclosure of PHI changes. When this occurs, it is important to ensure that the notice is updated everywhere (i.e., the summary, the brochure, and the website). Practices should take care to also educate staff on the importance of disposing of the old notices and not just using them until they run out and then start using the new NPP.

Failure to provide patients timely access to their PHI

An area of enforcement focus for the OCR is the patient's right of access. As of March 26, the OCR had entered into 18 resolution agreements and corrective action plans over violations of the patients' right to access.[6] The indication is that more such agreements will follow. Most of the resolution agreements are with physician practices.

The Privacy Rule gives patients the right to access not only to their medical record but also to billing information and any other information used to make a decision about them. This combination of information is what the Privacy Rule defines as the designated record set.[7] The regulations require that a patient's request for access be

fulfilled within 30 days, with the option for one 30-day extension.[8] The NPRM mentioned earlier proposed to change the time period to 15 days to respond, with the possibility of one 15-day extension. The heightened enforcement focus by OCR makes it critical that practices have a strong process for responding to patients' request for access. This is also important under the Information Blocking Rule from the Office of the National Coordinator for Health Information Technology.[9] The compliance date for that rule was April 5.