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.

Common Security Rule mistakes

The HIPAA Security Rule has numerous provisions for appropriate administrative, physical, and technical safeguards for electronic PHI (ePHI) that could be stumbling blocks for physician practices. There are a few pretty common ones.

Risk assessments and risk mitigation plans

OCR has settled numerous cases since the HIPAA regulations were finalized. A significant number have found violations of the HIPAA Security Rule. In virtually all of those cases, the failure to have a routine risk assessment as required by the rule was a finding. This is true for physician practices. Performing a routine risk assessment is identified as a required implementation specification. While the regulations do not define routine, the industry standard is considered once every three years as the maximum length of time between risk assessments. In some of the cases settled by OCR, the organizations could not demonstrate that an assessment had ever been performed, and in others, it was not done on a routine basis.

The idea behind performing routine risk assessment is that the threat landscape is ever-evolving. To keep up with the risks, an organization facing it needs to evaluate them. But performing an adequate risk assessment is no small undertaking. It requires expertise that the physician practice staff might not have. It may also not be cost-effective for the physician practice to employ someone with the expertise, depending on the practice's size. However, this is not a reason not to perform the assessment. Practices need to understand their obligation and resource the function in a manner that makes sense for them.

It is not enough to perform the risk assessment. The Security Rule also requires covered entities to create a risk mitigation plan based on the risk identified in the assessment.[10] The expectation is that a mitigation plan will be a road map for determining the process for and steps needed to mitigate risks. It is rare that an organization has the resources to mitigate all risks, so the plan would serve as the tool to prioritize risk and distinguish which risks will be accepted and the degree to which others will be mitigated. Organizations may not be able to eliminate a risk, but a determination will need to be made on the right risk-reduction strategy that is based on the organization's resources and risk tolerance.

Review of audit trails

Another common Security Rule violation is a lack of routine reviews of audit logs. Under the rule, covered entities should have policies and procedures in place to "prevent, detect, contain, and correct security violations."[11] The regulations also require covered entities and business associates to implement "procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports."[12] It also requires the covered entity to implement hardware, software, and/or procedural processes that *record and examine* activity in information systems containing ePHI.[13]

The only review of audit trails done by many organizations is prompted by patient complaints or some other event triggering the need to conduct an investigation. This is reactive, or for-cause access monitoring and auditing, which is necessary, but organizations should also be doing proactive, not-for-cause auditing and

monitoring. Many physician practices do not engage in a proactive monitoring and auditing program of user access.

The regulations do not specify how much monitoring and auditing is enough to meet the criteria of the rule. However, the regulatory language leads to the clear conclusion that doing nothing will not meet the requirements. Moreover, the OCR has not issued specific guidance regarding how much is sufficient. It shared the following recommendations in its January 2017 Cybersecurity Newsletter: a plan tied to the organization's risk assessment and the technical infrastructure, regular review of system activity, and reasonable and appropriate audit controls to record and examine system activity.[14]

Physician practices should ensure any system that contains ePHI has an audit trail capability that captures user activity, including what files were opened and closed as well as whether the user created, read, edited, or deleted records. Understanding the organization's major risks based on the risk assessment and the overall environment in which it operates is key to determining an appropriate proactive access monitoring and auditing program.

If an organization is currently doing nothing, then it will be important to identify the necessary resources to implement a proactive monitoring and auditing program. Evaluating access logs is a daunting task if it has to be done manually. Consideration should be given to evaluating technology solutions that are available to allow for a more effective and efficient program.

Other common Security Rule issues

Physician practices may have individuals wearing multiple hats and staff that work closely together. This can increase the temptation to take shortcuts, such as sharing usernames and passwords. Staff may not stop to consider that they are responsible for what happens in their user account. In the often close-knit environment, it is easy to be less diligent. If a user has been given a certain level of access because of their role, it would not be appropriate for them to allow someone else who does not have that same level of access to use their account. The role-based access has been granted for a reason. But if the practice is short staffed and certain work needs to be done, it could be tempting to share one's account information to expedite getting the work done.

The sharing of user accounts is tied to another issue—creating generic user accounts and passwords. This is often seen as an expeditious and efficient way to get work accomplished, but it is a violation of the Security Rule, which requires unique user accounts.[15] Practices should review systems and ensure there are no generic accounts.

Data exfiltration

Physicians often view the information about their patients as their data. This is generally not the case. The data belongs to the practice. So, when a physician decides to leave a practice, there should be a process for determining whether the physician will be allowed to take patient information. Part of the agreement with the physician when they join a practice should include the ground rules for what will happen with patient information if the physician leaves the practice. While patients may choose to follow a physician to a new practice, this should not be assumed. There should be a process to allow patients to request a transfer of their records to any new practice rather than have the physician simply copy records to an external hard drive, for example.

If the physician is moving to another location where it is unlikely that patients will follow, consideration should be given to whether the physician should be allowed to take any information. There may be some information that it would be appropriate for the physician to take, such as the data necessary for any board certification or to

obtain privileges in a new location. However, this would not likely require the entire patient record, so minimum necessary should be kept in mind. Allowing physicians to exfiltrate information without a structured process could lead to a data compromise and a potential breach.

Conclusion

Compliance with the HIPAA regulations is a complex process. There needs to be sufficient resourcing and expertise to do this well. This is not always something that physician practices have in place. It continues to be important to recognize what is in place and what may be needed when an issue arises. Diligence in all areas is necessary. And remember, there are compliance colleagues there to help and support when questions arise.

Takeaways

- Users must clearly understand a policy allowing access to their own record doesn't allow access to records of other patients.
- A strong proactive user access monitoring program is important to comply with the Security Rule.
- Posting a summary notice of privacy practices must be accompanied by having the full notice available nearby.
- Patient information should not be shared on social media unless that is part of the individual's job.
- Physicians should not be allowed to take protected health information when they leave a practice unless it is properly authorized.

1 Marti Arvin, "Common HIPAA mistakes made by physician practices: Part 1," *Compliance Today*, July 2021, https://bit.ly/366rpc9.
245 C.F.R. § 164.520(c)(2)(i)(A) .
3 Proposed Modifications to the HIPAA Privacy Rule To Support, and Remove Barriers to, Coordinated Care and Individual Engagement, 86 Fed. Reg. 6,446 (January 21, 2021) , https://bit.ly/3asDtpI.
445 C.F.R. § 164.520(c)(2)(iii)(B) .
5 Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5,566, 5,625 (January 25, 2013) , https://bit.ly/35shQE1.
6 U.S. Department of Health & Human Services, "OCR Settles Eighteenth Investigation in HIPAA Right of Access Initiative," news release, March 26, 2021, https://bit.ly/2U5Gh7T.
745 C.F.R. § 164.501 .
845 C.F.R. § 164.524(b)(2)(i), (ii) .
9 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program, 85 Fed. Reg. 25,642 (May 1, 2020) , https://bit.ly/32vJ6RI.
1045 C.F.R. § 164.308(a)(1)(ii)(B) .
1145 C.F.R. § 164.308(a)(1)(i) .
1245 C.F.R. § 164.308(a)(1)(ii)(D) .
1345 C.F.R. § 164.312(b) .
14 U.S. Department of Health & Human Services, Office for Civil Rights, "Understanding the Importance of Audit Controls," January 2017, https://bit.ly/3iUrE1A.
1545 C.F.R. § 164.312(a)(2)(i) .