COSMOS
Navigate the Compliance Universe

Compliance Today - July 2021
Common HIPAA mistakes made by physician practices: Part 1

By Marti Arvin

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

The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule has been enforceable for more than 18 years, the HIPAA Security Rule has been enforceable for more than 15 years, and the Breach Notification Rule was finalized more than eight years ago.[1] Even after all this time, there are still common issues that occur in physician practices. Some issues apply generally to implementation of the rules, while other issues are specific to an individual rule.

General areas of concern under the rules

There are three sets of obligations under the rules that are often of concern: policies and procedures, training, and business associate relationships.

Policies and procedures

When looking at the HIPAA regulations, there is an expectation that covered entities will have policies and procedures addressing all the requirements of the rules applicable to the way in which the covered entity uses and discloses protected health information (PHI). However, many covered entities do not have policies and procedures that address all the provisions of one or more of the rules. Physician practice compliance professionals should review their policies and procedures against all the provisions of the Privacy, Security, and Breach Notification rules to ensure every regulatory criterion applicable to them is covered.

Even when policies do exist, they might not be sufficient. This can be the result of using templated policies and procedures that were drafted by someone else (e.g., a professional association, a consultant, or a law firm). Templated policies and procedures tend to take a one-size-fits-all approach, which means it is not customized to a particular type of healthcare entity. There is nothing wrong with using such templates as long as the organization customizes and changes the policies and procedures to its actual operational practices. This means making sure there are no places where it says, "insert practice name here" in the final approved policies. This also means reviewing the policy and procedure template carefully to make sure all appropriate changes are made.

Once the policies and procedures are customized to the organization, consideration should be given to having a review by the organization's attorney to ensure that changes to the template do not create potential noncompliance. Changing one or two words could change the whole meaning of the policy. Consideration should also be given to the readability of the policy and procedure. Always keep the end user in mind. If an organization has policies and procedures that meet the legal requirements of the regulations, but the average workforce member can't understand them, it will be difficult for employees to follow the policy. It can be a delicate balance between meeting the organization's legal and compliance obligations and having policies and procedures that are useful to the workforce.

One more shortcoming is the failure to routinely review policies and procedures. The routine review helps the

organization ensure the policies are current for any changes to laws or regulations. It is also a good check to ensure that the policies and procedures are aligned with the organization's actual practices. Organizations may change practices over time for a variety of reasons. The change might be based on changes in technology, improvements around efficiency, mergers and acquisitions, or new personnel. A practice that is inconsistent with the organization's policies and procedures does not necessarily mean the organization is doing something illegal or noncompliant. But these types of inconsistencies may need to be explained during regulatory inquiry. Such inconsistencies may also create an environment where staff feel it is ok to not follow a policy because they see it being routinely done. Policies and procedures should be reviewed on a routine basis (i.e., at least once every three years and when there is a new law passed or a change to an existing law).

One specific policy that is routinely problematic is a policy on sanctions for noncompliance. Outlining the organization's approach to sanctions is required by the rules. Several of the Office for Civil Rights (OCR) enforcement actions have identified the lack of such a policy.[2] They have also identified failures to follow the policy when one does exist. A sanction policy should be drafted so that any applicable sanction can be applied in a consistent manner regardless of the offender. This may be a challenge in a physician's practice. Often the ultimate deciding body is one or more members of physician leadership. While there may be no reluctance to have a strong sanction policy for staff, physician leaders may be less willing to apply the same policy to a physician colleague for a similar act of noncompliance. A sanction policy should be drafted to account for a method to apply a consistent comparable sanction to both staff and physicians for similar offenses.

Training the workforce

Training on the rules is an area where a number of organizations have had issues when the OCR pursues investigations or compliance inquiries. A common finding is that the organization did not do training at all or has not done any for a number of years. The Privacy Rule mandates training on the policies and procedures of the organization for both new and existing employees.[3] The Security Rule focuses more on security awareness,[4] which is not explicitly formal training but can be. Making sure there is training for all employees is important. In physician practices, it can be difficult to ensure the physicians complete the required training. If the training is mandatory, there should be sanctions for anyone who fails to complete the training.

Neither the Privacy nor the Security rule mandates the nature of the training, but often it is done in the form of new employee orientation and ongoing annual training. While this may meet the regulatory obligations of the rule, it should not be the only goal of training. The primary goal of training should be to help ensure the workforce understands what they need to do to help the organization maintain compliance. Effective training is more commonly done by the dissemination of shorter, smaller bits of information dispersed at frequent intervals. This allows the individual to more readily digest and retain the information. This may be done via email, an employee newsletter, or some other means.

Regardless of the training method used, the organization should have some way of evaluating the effectiveness of the training. This might be done by tracking the number of compliance concerns or questions raised before and after the training, which can help demonstrate that individuals can identify a particular compliance concern if the reports increase after the education. Even an increase in questions regarding the topic of training can demonstrate the audience retain the material enough to know to ask the question. Organizations may also do a pre- and post-training test. This can inform the organization of the change in the individual's level of knowledge. To test whether employees are retaining the material over time, the organization may consider an employee survey once some time has passed after the training is completed. Another method is to pose a compliance question via email or through a newsletter, ask employees to respond with their answers, and then put the names of everyone who responded correctly in a drawing for some small prize.

Just like with policies and procedures, adopting a templated training platform created by a vendor, law firm, or another party can have issues. There is no reason to reinvent the wheel, so using material created by someone else as a starting point can save time. However, the practice needs to ensure that appropriate changes are made to customize the training to the organization. Compliance professionals are notoriously generous. If a compliance officer asks a colleague for a copy of their training material, it is likely to be shared. Just be careful that the material is rebranded for the organization, an appropriate assessment is performed, and changes made to reflect the organization's policies and procedures, and any necessary changes reflect differing legal requirements that may be needed to comply with state or other federal laws applicable to the organization. Also, don't assume the material is correct.

Business associate issues

Addressing the HIPAA compliance obligations around business associates is a struggle for most covered entities. For physician practices, it may be more of a struggle because they may not have the same resources and bargaining power as larger entities. It can also sometimes be difficult to tease out whether a particular vendor is a business associate. If the compliance professional is not involved in the process of reviewing potential vendor relationships, agreements can be signed without anyone realizing the need for a business associate agreement (BAA). Confusion also remains on whether a BAA is needed when the agreement is between two covered entities. A covered entity can be the business associate of another covered entity, so the fact that both parties are covered entities does not mean the relationship is not a business associate relationship.

In the Phase 2 audit protocol used by the OCR, it became clear there was an expectation that organizations have a method for clearly identifying their business associates.[5] Several of the resolution agreements signed with OCR have identified the lack of a business associate agreement as one of the violations.[6]

The Privacy and Security rules also have specific criteria that must be included in a valid BAA. If the language is not there, it could constitute a violation of one or both rules. Because there is a standard under each rule for the requirements of the BAA language, failure to have the necessary language could constitute a violation of both rules, which means civil monetary penalties could be imposed for each rule violation.[7] Physician practices, particularly smaller practices, may not have the needed expertise to review language to ensure all the necessary components are present. Simply relying on the BAA provided by a vendor might not be sufficient.

Another violation identified in OCR resolution agreements is the lack of an updated BAA to reflect the provisions of the Health Information Technology for Economic and Clinical Health Act.[8] Changes to the law made it necessary to update most organizations' BAAs. It was necessary for covered entities to review BAAs that existed at the time and make the appropriate changes. If the entity has limited resources and lacks a structured process for identifying business associates, this was made more difficult, and thus BAAs might exist that do not reflect the necessary changes.

Implementing a process by which all the appropriate parties know what constitutes a business associate relationship and ensuring that the required language is part of the agreement with the vendor is critical. This is also necessary to monitor the ongoing relationship and engage in appropriate due diligence of the vendor. The lack of due diligence when engaging a vendor could result in an OCR investigation and potential fines if there is a data compromise on the part of the vendor.

Business associate due diligence

The failure to conduct sufficient due diligence is not unique to physician practices. However, physician practices, particularly smaller practices, may not have adequate resources to conduct the needed due diligence when

engaging the vendor and are even less likely to have the resources to conduct ongoing due diligence. The assessment necessary at the initiation of a business associate relationship can vary depending on the services the business associate will be providing and the volume of PHI the vendor will be accessing, maintaining, transmitting, or receiving on behalf of the practice. Vendors who will handle larger volumes of PHI should get more scrutiny than those who might only occasionally touch PHI.

The practice should not only be asking what the vendor has in place regarding appropriate controls to protect its PHI, but also conducting some verification of key aspects. For example, if the vendor will be hosting the practice's electronic health record, the practice may want to confirm the vendor has done routine risk assessments. Ideally, the vendor will be able to demonstrate not only that the routine risk assessments have been performed, but also that there has been some form of recent independent third-party assessment to validate what the vendor has done internally. Another component of the due diligence it so to ensure any significant risk identified by the vendor's risk assessment has been appropriately mitigated.

Both of the steps require some level of expertise in information security practices that may not be present in a physician's practice. This could be a function that the physician practice wants to outsource. If the practice does not know how to assess a risk the vendor has identified and evaluate whether the mitigation approach seems appropriate, due diligence will not exist.

Breach Notification Rule issues

Physician practices may have several issues with compliance under the Breach Notification Rule. This starts with identifying the breach and continues through the stages of evaluating a data compromise to determine whether it is a breach.

Failure to identify a breach

When a compromise of protected health information (PHI) occurs, there will always be a need to evaluate whether the compromise is a breach. The obvious first step is the identification that the PHI has been compromised. This can be a challenge for any covered entity, but when the organization is smaller and likely more resource constrained, the challenge becomes even more daunting.

There are a number of ways that organizations can miss a data compromise. Users accessing records for personal reasons have already been discussed in the context of monitoring systems. The failure to conduct this type of monitoring is not only an issue, but it can result in organizations failing to identify that a breach has occurred and thus failing to provide the required notification to the patient and OCR. This means the potential for additional violations of the rules and an increased exposure to civil monetary penalties and other legal actions.

Practices may not have other necessary controls such as a method to identify unauthorized access to their system. There should be security controls in place that alert the practice to unusual activity. The lack of such controls can allow an unauthorized actor to be in the system for quite some time before being detected. This allows the bad actor to gain access to more and more information, which can make the response to the data compromise much broader.

Another temptation is to rely on the assessment by a business associate that a data compromise does not constitute a breach. The practice's BAA should require any business associate to notify the practice of a security incident and any breach. However, to notify the practice of a breach requires the business associate to perform the analysis of the data compromise to determine whether a breach has occurred. This can be a bit of a gamble since the Breach Notification Rule puts the obligation of notifying the patient and OCR on the covered entity.[9] The business associate is only obligated to notify the covered entity under the rule.

Covered entities, including physician practice, should not blindly rely on the business associate's assertion that a data compromise is not a breach but rather follow the standard compliance mantra of "trust but verify." When a business associate notifies of a data compromise, the practice should ask about the circumstances of the compromise, what data were involved, what the business associate did to mitigate any damage, and any other questions deemed necessary for the practice to feel confident in the business associate's analysis. If the practice can't reach a sufficient level of confidence, it should conduct and document an independent assessment to reach its own conclusions.

Analyzing the data compromise

Even if a data compromise is identified, there are still common mistakes in the analysis process. The OCR has issued guidance that when covered entities are subject to ransomware, it is a breach, with some very narrow exceptions.[10] A common mistake when ransomware or other malware is used against a covered entity is to reach the conclusion that if data were not exfiltrated from the organization, there was no breach. However, the Breach Notification Rule states a breach is "acquisition, access, use, or disclosure" of PHI.[11] So the bad actor's ability to access the PHI is sufficient to constitute a potential breach. An analysis of this type of situation often requires a level of expertise that might make outside support necessary. The physician practice does not want to get this wrong.

Using the wrong discovery date is another way to get the analysis wrong. The Breach Notification Rule defines the discovery date as the "first day on which such breach is known to the covered entity, or, by exercising reasonable diligence would have been known."[12] Determining when the compromise of PHI occurred can be complicated. If the bad actor got into the system on September 5, 2020, and the covered entity discovered their presence on December 8, 2020, but did not identify any access to PHI until February 24, 2021, what is the discovery date? Under this scenario, there is a solid argument that the discovery date was February 24, 2021.

The covered entity will want to ensure it was attentive to the matter between the date the actor was identified in the system and the date the access to PHI was known. If OCR were to find the practice did not exercise reasonable diligence in that time, the discovery date could be identified as December 8, 2020. This is important because breach notification must occur without undue delay but not more than 60 days after the discovery date. The discovery date is when the clock starts.

Improperly evaluating low probability of compromise

Any unauthorized access to unsecure PHI is presumed to be a breach and notification is necessary. This is true unless the organization does an analysis of the facts and circumstances surrounding the data compromise and determines there was a low probability that the PHI was compromised. If the organization can support a low probability of compromise, there is no breach, and the notification is not required. Determining if there is a low probability of compromise is a subjective process, but the organization will want to ensure it was followed and that it documented the risk assessment process outlined in the Breach Notification Rule.

Other considerations for data compromises

A practice's analysis of a data compromise does not necessarily end with evaluating the Breach Notification Rule. There may be a need to consider state laws. Often, if a state law is applicable, the standards that need to be evaluated are different from HIPAA. State laws may encompass data beyond PHI. So, individuals other than patients may also require notification, including state authorities such as the state attorney general. There may also be different breach notification timelines. These laws may also be stricter than HIPAA. This means an

organization may determine it is not required to notify of a breach under HIPAA but is obligated to notify under state law.

Conclusion

There are multiple ways a physician practice should be addressing general issues associated with compliance with the HIPAA Privacy, Security, and Breach Notification rules. Making sure the person or persons responsible for oversight of compliance are appropriately resourced and have sufficient authority to effectively perform their duties is a key aspect to meeting all the compliance obligations. Part two of this series will discuss specifics of the Privacy and Security rules that are common missteps in physician practices.

Takeaways

- Having policies and procedures covering all aspects of the HIPAA Privacy, Security, and Breach Notification rules is important.
- Understanding the discovery date for a breach of protected health information is critical to complying with the timeline for breach notification.
- Covered entities need a structured process for ensuring business associate agreements are in place when appropriate.
- A Health Insurance Portability and Accountability Act (HIPAA) sanctions policy should be consistently enforced for all users.
- Healthcare entities may need to consider state law, not just HIPAA, for breach notification requirements.

1 "When Was HIPAA Enacted?" HIPAA Journal, March 9, 2018, https://bit.ly/3tUuXYq.
2 "Resolution Agreements," OCR, U.S. Department of Health & Human Services, last reviewed March 26, 2021, https://bit.ly/2QDQV4o.
345 C.F.R. § 164.530(b) .
445 C.F.R. § 164.308(a)(5) .
5 "HIPAA Privacy, Security, and Breach Notification Audit Program," OCR, last reviewed December 17, 2020, https://bit.ly/3tSKVCs.
6 "Resolution Agreements," OCR.
745 C.F.R. §§ 164.308(b)(1), 164.504(e)(1) et. seq.
8 Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, § 13,001, 123 Stat. 226 (2009).
945 C.F.R. §§ 164.400–414 .
10 U.S. Department of Health & Human Services, OCR, "FACT SHEET: Ransomware and HIPAA," accessed May 20, 2021, https://bit.ly/2z0IabO.
1145 C.F.R. § 164.402 .
1245 C.F.R. § 164.404(a)(2) .