Frequently asked questions

Q: I have a patient portal. Doesn’t that make me HIPAA compliant?

A: Not necessarily. Under HIPAA, patients have the right to receive more information than is available in the patient portal and through alternative means, such as email or on a CD or USB drive.

Q: Do I need to buy any new technology or pay any fees to my EHR vendor based on a patient’s request?

A: No. While you are required to provide patient records in the format specified by the patient, HIPAA only requires you to do so if the form and format are readily producible. You do not need to purchase new technology to accommodate a patient’s request. You also do not need to pay thousands of dollars to your EHR vendor for a new feature, but you must know what formats your EHR technology is able to readily produce.

Q: Do I have to pay my EHR vendor each time a patient wants me to connect to a new app?

A: No. The Promoting Interoperability Programs require certified EHR technology to include APIs that allow for secure communications between apps, allowing third parties to connect to the EHR without you having to pay a fee. Recent regulations also set conditions around the permitted fees EHR vendors may charge for the development, deployment, and usage of APIs.

Q: My state has a law stating how much patients can be charged. Can I charge this to my patients?

A: HIPAA permits you to charge “reasonable” and “cost-based fees” for records. If the state law sets a limit on fees, then this amount is considered “reasonable” and you cannot exceed this amount. Remember, you are still limited to your costs and so even if your state permits you to charge more than what HIPAA allows, you cannot charge the higher state fee schedule amount if your actual cost is
less than the statutory amount.

**Q: Am I required to provide a copy of a patient’s medical record?**

A: Yes, if the request comes directly from the patient or their personal representative (such as a parent for a minor patient), you must provide the record under HIPAA unless applicable state law provides otherwise, such as in the case of a minor seeking care for something that the minor may do confidentially.

**Q: Do I have to provide the records electronically if the patients want them that way?**

A: HIPAA provides that they are entitled to an electronic copy. However, if the records are stored in a manner that is not electronic (such as on paper), you are not required to procure hardware or software to convert the paper records into electronic records. If you already have a scanner or some other mechanisms to allow the conversion or if the records are already stored electronically, you must provide the records in electronic form if requested by the patient to do so.

**Q: Do I have to use the USB drive provided by my patient?**

A: Under the HIPAA Security Rule, you should conduct a risk analysis that identifies the risks of connecting foreign USB drives to your systems. It is advisable to be cautious about using a USB drive that is foreign to your systems. In most cases, plugging an unfamiliar USB drive into one of your computers is not a good idea because the USB drive may contain malware unbeknownst to the patient. If you determine that the risk is too high, then you should work with the patient to identify an alternative way to obtain the patient’s records, such as providing the records on a USB drive provided by the practice.

**Q: How much time do I have to respond to a patient’s request for their records?**

A: Under HIPAA, you have 30 days to comply with the request. You are permitted to grant yourself an additional 30-day extension (only once), but you must notify the patient of this extension within the initial 30 days. This means you have a maximum of 60 days to comply with a request. That being said, you should still look at the rules for the specific state(s) in which you practice because many states have more restrictive time frames with which you must comply. You should also consider your policies around electronic requests for records. New regulations require that patients are given “timely” access to their electronic records which may mean providing patients access to test results in parallel to the availability of the test results to the ordering clinician. The AMA has developed resources to help physicians understand these new requirements.
Q: Do I have to comply with a patient’s request that I email records?

A: Email is often not encrypted and can be intercepted; however, you cannot require that a patient use an alternative if that patient is comfortable with email’s risk. In this case, give the patient a basic warning related to email risks and obtain a verbal or written confirmation from the patient that the patient is aware of the risk and still wants to receive the records via email. Document the patient’s consent.

Q: Can I require that a person appear in person when they make a request for records? How do I verify a patient’s identity?

A: It is important to verify the identity of the patient, particularly when the request for access comes from an individual that you do not know. Identification, however, should not become an unreasonable obstacle to the patient accessing medical records. You may not require an in-person verification when you receive a request for records. You should, however, still seek to verify the patient’s identity, such as by obtaining information that is not publicly known (such as the last four digits of the patient’s social security number) or having the patient transmit a copy of a form of identification (ID). That said, clinicians should be aware of and sensitive to the fact that some patients may not have a social security number or government ID and may not wish to disclose that to a practice. Practices should offer a variety of methods for patients to verify their identity.

Q: Can I charge for paper records? How about other electronic media, e.g., a CD?

A: Under HIPAA, you are allowed to charge the lesser of either a “reasonable” fee as defined under state law or the actual costs to you of copying the records. Your copying costs may include employee wages associated with copying time, the cost of supplies, the cost of the media (e.g., the CD cost) and postage. You should avoid charging a retrieval and review fee or a fee associated with the electronic maintenance of the records. Records access should not be viewed as a revenue-generating opportunity.

Q: What do I need to include in response to a patient’s request for records? What about a request for “a list of the patient’s medical records disclosure”?

A: You need to include what the patient asked for, to the extent the information is contained within the “designated record set.” This includes medical and billing records and any other record that is used to make decisions about the patient. The term does not include business records that solely relate to the practice. Furthermore, under HIPAA, there is a provision called the “accounting of disclosures.” This is a list of how health information has been disclosed outside of the organization and covers items like when you have to disclose information to public health authorities or law enforcement. There are
regulatory exceptions for disclosures for treatment, payment and health care operations.

**Q: How do I find out what other methods are available for my EHR vendor to produce records?**

**A:** If your EHR is certified EHR technology (i.e., it has been certified for use under what previously was called the “meaningful use” programs), then it will have a view/download/transmit function in the patient portal, which permits patients to remotely obtain certain information without having to contact your staff. The EHR will probably also allow for secure “Direct Messaging” and creation of a PDF, which can be printed or sent using encryption technology. It may also allow documents to be saved in the CDA format, which is a format specifically created for health information. Your certified EHR will eventually support APIs allowing patients and other clinicals to more easily access electronic records. Contact your EHR vendor to find out all their capabilities.

**Q:** What do I do if the patient requests the diagnostic imaging tests, such as MRI scans?

**A:** If the images are in your system and you are relying on them for diagnosis and treatment decisions, you must produce them to the patient if requested to do so. If you are relying on a link to another health care provider’s systems, then you can direct the patient to the other health care provider for the information. However, please note that, even where you are not the originator of the image, if it is in your system, you must produce it.

**Q:** How do I know if it is safe for patient records to be available through the EHR portal? Does a certification mean that the EHR is HIPAA compliant?

**A:** No, EHR certification does not mean that the EHR is HIPAA compliant. Software cannot be HIPAA compliant but can support a health care provider’s HIPAA compliance. For example, your EHR’s patient portal likely has password protection and other security features that support your HIPAA compliance. But it falls to you to include the EHR software in your information security “risk analysis” and to identify potential security risks. This does not mean you have to review software coding, but you should discuss with your EHR vendor what the company does to identify security vulnerabilities in the patient portal, such as whether an independent third party has assessed the vendor’s systems for security flaws. You can also ask if there are security features that you are responsible for turning on.

**Q:** The patient wants me to send her medical information to an app, but my EHR does not appear to support or be compatible with this app. Do I need to send the record to her app?

Copyright 1995 - 2021 American Medical Association. All rights reserved.
A: There are applications that manage personal health records (PHR) for the consumer by collating information from various health providers and that can allow sharing of information. The government is pushing to make it easier for the patient to be able to use such apps. If your EHR is certified to the “2015 Edition,” then it should include API features that allow third-party apps to obtain medical information from your EHR. There should be minimal, if any, action needed on your part for information to be available through your EHR to patients’ apps. Future updates to your EHR will enable more advanced API features allowing you and your patients to select, connect or install apps that best fit your needs. Your EHR vendor should already have an established timeline for when these updates will be made available to you.

**Download the playbook**

The Patient Access Playbook (PDF) focuses on dispelling HIPAA myths and helping physicians understand their obligations to provide patients with access to their health information.


Copyright 1995 - 2021 American Medical Association. All rights reserved.