RICHELLE MARTING, JD, MHSA, CPC

CME

# HIPAA: Answers to Your Frequently Asked Questions

**Does your organization interpret HIPAA too strictly, too loosely, or just right? Find out with these FAQs.**

Since its inception more than 20 years ago, the Health Insurance Portability and Accountability Act (HIPAA) has seemed to elicit more questions than answers. When HIPAA's privacy rule was initially proposed in 1999, the U.S. Department of Health & Human Services (HHS) received more than 52,000 public comments and questions about it, and there was "substantial confusion and misunderstanding" about how the rule would operate and "great concern" over its complexity.[1] Over the years, HHS has offered further guidance on both the privacy and security rules, yet many questions, myths, and misinterpretations remain. This article answers some frequently asked questions to help you be better informed.


**ABOUT THE AUTHOR**
Richelle Marting is an attorney practicing with Forbes Law Group in Overland Park, Kan., where she focuses on regulatory compliance and health care reimbursement. Author disclosure: no relevant financial affiliations disclosed.

## PATIENT PRIVACY

**Q: Does HIPAA prohibit the use of sign-in sheets?**

A: Your practice can use sign-in sheets as long as the information collected is appropriately limited. For example, sign-in sheets can include the patient name, check-in time, and provider name if necessary but should omit medical information such as the reason for the visit. This reduces incidental disclosure of patients' health information to others.[2]

**Q: Can I leave messages about a patient's care via voicemail or with family members?**

A: When leaving a message, you must reasonably safeguard information, for example, by disclosing the minimum information necessary in the message or verifying the identity of the person receiving the information.[2,3,4] The HHS Office for Civil Rights (OCR) suggests leaving only the provider's name and number and asking the patient to call back, in order to reasonably protect information being left in a voicemail. You can talk with family members or even close personal friends of the patient to the extent these individuals are involved in the patient's care or payment for care as long as the patient has had an opportunity to agree or object.[5] A patient's verbal permission for you to speak with his or her spouse, parent, or child is sufficient; a formal authorization form is not required.

**Q: Can I discuss patients' care at a nursing station or other location where the conversation may be overheard?**

A: You and your staff can discuss patients' care, even if there is a possibility the conversation may be overheard, if you take reasonable safeguards to prevent unnecessary disclosures.[2,3] For example, coordinating care at the nursing station, discussing care over the phone, and talking to patients in semiprivate rooms or to family in waiting rooms are all permitted. To help reduce the chance of conversations being overheard, you and your staff can lower your voices, turn your back toward others in common areas, or take similar reasonable safeguards.[2]

## PATIENT RIGHTS

**Q: Are we limited to charging patients $6.50 for copies of their medical record?**

A: Your practice may charge reasonable, cost-based fees to provide patients copies of their medical records.[6] HIPAA regulations are very specific about what these fees can include — only the costs of labor for copying the information, supplies for creating the paper copy or electronic media, and postage.[6,7]

A patient's verbal permission for you to speak with his or her spouse, parent, or child is sufficient.

The OCR offers three options for determining what to charge patients who request copies of their own records. First, you can calculate *actual costs* for each and every request from a patient for access to his or her information. Alternatively, you may choose to develop a schedule of *average costs*. Average costs can only be charged as a per-page fee when protected health information (PHI) is maintained in paper form and the patient requests a hard copy or asks that the hard copy be scanned to an electronic format.[7] Per-page fees cannot be charged for PHI maintained electronically.[7] Finally, charging a *flat fee* of $6.50 is permitted when PHI is maintained electronically and requested in an electronic format, but this is not the maximum you may charge if you elect to charge actual or average costs instead.

Practices are expected to notify the individual in advance of the approximate fee for the copies.[7] Some states prohibit providers from withholding records until fees are

### KEY POINTS

- Although HIPAA has existed for more than 20 years, medical practices and other health care organizations still struggle to interpret the law correctly due to its complexity.
- Some organizations are overly strict in their interpretation of HIPAA and prohibit the use of sign-in sheets or phone messages.
- Other organizations are too loose in their interpretation of HIPAA and have never conducted the required security risk assessment.

paid, such as when records are needed for patient care purposes.

These limitations on fees apply only when a patient requests access to or copies of his or her own information. If the request is from someone other than the patient and requires authorization, these fee limitations do not apply. However, state law fee schedules may still apply.

**Q: Do patients have a right to know who has viewed their medical record?**

A: Patients have a right to an accounting of disclosures showing where their information has been sent outside your organization in the last six years.[8] In other words, you must track instances in which you release, transfer, provide access to, or divulge information to those outside your organization.[9] Certain disclosures do not have to be tracked, such as those provided to carry out treatment, payment, or health care operations; those made to the individual patient; and incidental disclosures that are otherwise permitted.[8] At this time, patients do not have a right to a report detailing which specific individuals have accessed their electronic information, such as employees;[10] however, a proposed rule from May 2011 could, if finalized, create this right for patients.

If a patient requests that you *not* send his or her information to a health plan and the patient has paid for services in full, you must agree *not* to do so.

**Q: If patients do not want their information sent to their insurance company, do I have to agree not to submit a claim for payment?**

A: If a patient requests that you *not* send his or her information to a health plan and the patient has paid for services in full, you must agree *not* to do so, unless the disclosure is required by law.[11] For example, some state laws may prohibit a provider from receiving a cash payment from a patient who belongs to a health maintenance organization; therefore, the provider would need to submit a claim to the health plan for payment and would thereby disclose the patient's information.[12] Although Medicare generally requires providers to submit claims for services provided to Medicare beneficiaries, there is an exception when patients refuse to authorize the submission of the bill to Medicare.[12] Providers are allowed to bill Medicare patients directly in these instances, subject to any limiting charges.[12,13]

If the patient has not paid in full for his or her services (e.g., if the check bounces, the credit card is declined, or the patient does not otherwise make payment), you may send a claim to the patient's insurance company as long as you make some attempt to resolve the payment dispute with the patient first.[12]

## DATA SECURITY

**Q: How often must we perform a security risk assessment?**

A: All providers covered by HIPAA must perform an assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI.[14] (For guidance about how to conduct this assessment, see "The HIPAA Security Rule: Are You in Compliance?" *FPM*, March/April 2017, https://www.aafp.org/fpm/2017/0300/p5.html.) The security rule does not specify how frequently you must perform a risk analysis, but OCR guidance suggests the risk analysis process should be ongoing.[15] Reviewing or updating a security risk analysis may be done annually or as needed, depending on whether you have made significant changes to your electronic systems, such as implementing a new electronic health record (EHR).

**Q: Can I send patient information by email?**

A: You can send PHI by email, but you must implement safeguards under the security rule[2] to ensure the information is secure, accessed only by authorized individuals, and not altered, edited, or deleted.[16] The best way to do this is to encrypt your emails; however, patients have the right to request access to their own information via unencrypted email. You may send patient information by unencrypted email if you have advised the patient of the risks and the patient still prefers unencrypted email.[12]

**Q: If my practice is targeted by ransomware, is it automatically a HIPAA breach?**

A: Ransomware is a type of malicious software, or malware, that attempts to deny access to a computer user's data, usually by encrypting the data until a ransom is paid.[17] A breach occurs when PHI is acquired, accessed, used, or disclosed in a manner not permitted under the HIPAA privacy rule, compromising the privacy or security of the information.[18] When an electronic system is infected by ransomware, it is not necessarily a breach of PHI. According to HHS, "Whether or not the presence of ransomware would be a breach under the HIPAA Rules is a fact-specific determination."[18] If electronic PHI becomes encrypted as the result of a ransomware attack, the OCR presumes a breach to have occurred because an unauthorized individual has taken possession or control — in other words, acquired — the information.[18] The breach of information must be reported unless the practice can demonstrate through a thorough risk assessment that there is a low probability that PHI has been compromised.[18] The breach risk assessment should include the following:

- The nature and extent of the information involved, such as the types of identifiers and likelihood of re-identification,
- The name of the unauthorized person who acquired the information,
- Whether PHI was actually acquired or viewed,
- The extent to which the risk to PHI has been mitigated.[18]

Additional factors to consider for all malware incidents are the exact type and variant of malware, communications between the malware and the attackers' command and control servers, and whether the malware infected other systems.[17] Other considerations include whether there is a high risk of unavailability of the data, which can be an indication of compromise, and whether the information was already encrypted when the attack occurred.[17] If, at the time of the malware attack, information was encrypted or otherwise rendered unreadable, unusable, and indecipherable to unauthorized persons, this may be an exception to a breach.[17,18]

## BUSINESS ASSOCIATES

**Q: Do I need a business associate agreement with all entities I do business with?**

A: A business associate is a person or entity that creates, receives, maintains, or transmits PHI on your behalf for a function or activity regulated by HIPAA.[9] These functions or activities can include claims processing or administration, data analysis, utilization review, quality assurance, patient safety activities, billing, benefit management, practice management, and repricing.[9] A business associate may also provide legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services involving your disclosure of PHI.[9] When a person or entity meets the definition of a business associate, a business associate agreement must be in place between you and the business associate in order to share PHI.[3]

> You do not have to monitor your business associates for compliance with HIPAA. You must, however, have business associate agreements in place.

Here are some common relationships that have caused confusion:

**Maintenance services.** Business associate agreements are not required if a person's services do not involve the use or disclosure of PHI.[2] Where access to PHI is possible but only incident to the person's or organization's services to the covered entity, the relationship does not rise to the level of a business associate.[2] Examples include janitors, plumbers, electricians, or photocopy machine repair technicians who enter your premises for work.[2]

**Communications services.** When practices use communication services, such as phone companies, the U.S. Postal Service, or couriers, a business associate agreement is generally not required.[2,19] Typically, these organizations are merely conduits for the transportation of information and do not access PHI routinely as part of their services. As a result, they do not meet the

definition of a business associate.

**Shredding services.** When disclosure of PHI to a person or organization is routine, such as with those handling records or shredding documents, this is often considered a business associate relationship that would require an agreement.[19] However, a limited exception exists if the work is performed on the provider's premises by someone considered to be part of the provider's workforce.[19]

**Hospitals.** Physicians with medical staff privileges at hospitals or other health care facilities do not have to enter into business associate agreements with these facilities. In these situations, the physician and facility are often participating in an organized health care arrangement, which is an exception to the definition of a business associate under the privacy rule.[2,9]

**Software vendors.** Merely selling or providing software to a HIPAA-covered entity does not give rise to a business associate relationship.[2] For example, Microsoft Corp. is not a business associate simply because a practice purchases Microsoft Office products that will be used for the health care business. However, some software companies, such as EHR vendors that host the practice's software on the company's own server, may access PHI to troubleshoot software issues or provide other information technology support. In these cases, the software company *is* a business associate because its services to the practice involve access to or maintenance of PHI.[2]

**Cloud vendors.** Practices using a cloud service provider (CSP) are generally required to enter into a business associate agreement with the CSP.[2] This is true even if the CSP cannot view the practice's PHI because the information is encrypted and the CSP does not have access to the encryption key.[2]

**Q: Do I have to monitor my business associates for compliance with HIPAA?**

A: You do not have to monitor your business associates for compliance with HIPAA.[2] You must, however, have business associate agreements in place before sharing PHI with the business associate. Providers are no longer responsible or liable for the actions of their business associates under HIPAA.[12] Note, however, that the conduct of business associates may still leave providers vulnerable for other reasons.

## TOO STRICT OR NOT STRICT ENOUGH?

With HIPAA, as with many other regulations, it's common for some organizations to interpret the rules too strictly, while others are not strict enough. Both are problematic. This article's answers to frequently asked questions about HIPAA should help practices feel more confident that they are enforcing the regulations correctly. FPM

Send comments to **fpmedit@aafp.org,** or add your comments to the article online.


1. U.S. Department of Health and Human Services. Standards for privacy of individually identifiable health information. *Fed Regist*. 2002;67(157):53182. Codified at 45 CFR §160 and §164.

2. Office for Civil Rights. HIPAA FAQs for professionals. U.S. Department of Health and Human Services website. https://www.hhs.gov/hipaa/for-professionals/faq/. Updated October 12, 2017. Accessed February 2, 2018.

3. U.S. Department of Health and Human Services. Uses and disclosures of protected health information: general rules. 45 CFR. §164.502.

4. U.S. Department of Health and Human Services. Other requirements relating to uses and disclosures of protected health information. 45 CFR. §164.514(h).

5. U.S. Department of Health and Human Services. Uses and disclosures requiring an opportunity for the individual to agree or to object. 45 CFR. §164.510(b)(1)(i).

6. U.S. Department of Health and Human Services. Access of individuals to protected health information. 45 CFR. §164.524(c)(4).

7. Health Information Privacy Division. Individuals' right under HIPAA to access their health information. U.S. Department of Health and Human Services website. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html. February 25, 2016. Accessed February 2, 2018.

8. U.S. Department of Health and Human Services. Accounting of disclosures of protected health information. 45 CFR. §164.528(a).

9. U.S. Department of Health and Human Services. Definitions. 45 CFR. §160.103.

10. U.S. Department of Health and Human Services. HIPAA privacy rule accounting of disclosures under the Health Information Technology for Economic and Clinical Health Act. *Fed Regist*. 2011;76(104):31426, 31430. Codified at 45 CFR §164.

11. U.S. Department of Health and Human Services. Rights to request privacy protection for protected health information. 45 CFR. §164.522(a)(1)(vi).

12. U.S. Department of Health and Human Services. 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. *Fed Regist*. 2013;78(17):5566, 5588, 5626, 5627, 5634. Codified at 45 CFR §160 and §164.

13. Centers for Medicare & Medicaid Services. Medicare Benefit Policy Manual, 100-02, Chapter 15, Section 40. https://www.cms.gov/Regulations-and-Guidance/Guidance/Manuals/Downloads/bp102c15.pdf. July 11, 2017. Accessed February 2, 2018.

14. U.S. Department of Health and Human Services. Administrative safeguards. 45 CFR. §164.308(a)(1)(ii)(A).

15. Office for Civil Rights. Guidance on risk analysis requirements under the HIPAA security rule. U.S. Department of Health and Human Services website. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf. July 14, 2010. Accessed February 2, 2018.

16. U.S. Department of Health and Human Services. Technical safeguards. 45 CFR. §164.312(a)(1), (c)(1), (e)(1).

17. Office for Civil Rights. Fact sheet: Ransomware and HIPAA. U.S. Department of Health and Human Services website. https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf. July 11, 2016. Accessed February 2, 2018.

18. U.S. Department of Health and Human Services. Definitions. 45 CFR. §164.402.

19. U.S. Department of Health and Human Services. Modifications to the HIPAA privacy, security, and enforcement rules under the Health Information Technology for Economic and Clinical Health Act. *Fed Regist*. 2010;75(134):40868, 40874. Codified at 45 CFR §160 and §164.