Navigating HIPAA, Breaches of Protected Health Information, and Privacy Laws in Louisiana

Q&A from May 31, 2023 Webinar

Q: Are hospitals required to comply with BAAs when engaged in referral agreements/MOUs?

A; If the referral agreements/MOUs involve the hospital acting as a business associate by performing administrative services that involves access to protected health information, then yes, compliance with a BAA is required. If there are no such administrative services being performed or PHI being accessed and shared, then a BAA is not necessary.

Q: Does a subpoena for medical records require a signature from the patient? Or does subpoena supersede consent?

A: The short answer is generally yes, a subpoena supersedes a patient's consent. A covered entity may disclose a patient's PHI in the course of any judicial or administrative proceeding in response to a subpoena if the covered entity receives satisfactory assurance from the party seeking the information that reasonable efforts have been made to:

a. Ensure that the individual who is the subject to the PHI has been given notice of the request, OR
b. Secure a qualified protective order. See 45 CFR 164.512(e)(1)(ii).

Regarding subpoenas for law enforcement purposes, a covered entity may disclose a patient's PHI without their consent in compliance with and as limited by the relevant requirements of a court-ordered, grand jury, or administrative subpoena. See 45 CFR 164.512(f)(1).

Q: Does the BAA have to be executed each year or can we include language allowing the BAA to be continuous and would end after a notice of 90 days?

A: A BAA does not need to be executed each year. The BAA can include term and termination language that allows it to be continuous until certain conditions are met, or the underlying agreement is terminated.

Q: What are requirements regarding mental and behavioral health records release when medical records requests are made?

A: HIPAA serves as the baseline for privacy and security requirements for PHI. If stricter state laws exist that provide greater protection for patient information, like mental health information, then those state laws preempt HIPAA and must be followed. If the mental and behavioral health records involve substance use disorder and treatment, there are additional limitations on how and when you can share that information under 42 CFR Part 2.

Q: We are a small independent RHC with limited space. Because of the limited space, some breach of HIPAA may occur while responding to a phone call with other patients around, although our employees try very hard to refrain from using patient names. Is this considered a breach requiring notification?

A: The HIPAA Privacy Rule explicitly permits the incidental disclosures that may result from certain practices, for example, when other patients in a waiting room hear the identity of the person whose name is called. However, these incidental disclosures are permitted only when the covered entity has implemented reasonable safeguards and the minimum necessary standard, where appropriate. Phone calls should not include the individuals name as well as a discussion of their medical conditions in front of other patients. As long as a name is not used, this would not be considered a breach requiring notification. See 45 CFR 164.502(a)(1)(iii).

Q: Our patients must give consent for disclosure of HIPAA protected information and give us the name of the person and the relationship. What is our exposure if the patient has not updated the list to whom we may disclose HIPAA protected information, and we inadvertently disclose such information? Should we protect ourselves by mandating that a patient complete a HIPAA release form? Where can we find a free sample of such a form?

A: The Privacy Rule permits, but does not require, a covered entity to voluntarily obtain a patient's consent for uses and disclosures of PHI for treatment, payment, and health care operations. Covered entities that do so have complete discretion to design a process that best suits their needs.

"By contrast, an 'authorization' is required by the Privacy Rule for uses and disclosures of protected health information not otherwise allowed by the Rule. Where the Privacy Rule requires patient authorization, voluntary consent is not sufficient to permit a use or disclosure of protected health information unless it also satisfies the requirements of a valid authorization. An authorization is a detailed document that gives covered entities permission to use protected health information for specified purposes, which are generally other than treatment, payment, or health care operations, or to disclose protected health information to a third party specified by the individual.

An authorization must specify a number of elements, including a description of the protected health information to be used and disclosed, the person authorized to make the use or disclosure, the person to whom the covered entity may make the disclosure, an expiration date, and, in some cases, the purpose for which the information may be used or disclosed. With limited exceptions, covered entities may not condition treatment or coverage on the individual providing an authorization." See the following link: https://www.hhs.gov/hipaa/for-professionals/faq/264/what-is-the-difference-between-consent-and-authorization/index.html.

If PHI is inadvertently and impermissibly disclosed without a patient's authorization, then that is considered a breach requiring notification to the patient. Best practice is to always have patients complete HIPAA release forms during intake. Free sample forms can be found online.

Q: All of our health information vendors (EHR, billing service, virtual fax, telemedicine platform) claim to be HIPAA compliant. As a provider, I depend on those companies to be able to provide a true HIPAA compliant service, so as part of the security risk analysis for my company, we indicate that those companies are HIPAA compliant. Do I still need to have an actual BAA with each of those companies?

A: Yes, covered entities must have a BAA with all health information vendors that perform functions or provides certain services to the covered entity that involve access by the business associate to protected health information. This is regardless of whether or not the vendor claims to be HIPAA compliant – a BAA is still required.