Codify
BY AAPC

Health Information Compliance Alert

Compliance: Get the Facts on BA Agreements

Tip: Thoroughly investigate your CSP to ensure a record of HIPAA compliance.

The protection of practice data is fully outlined for covered entities (CEs) in the HIPAA Privacy Rule. However, most medical practices rely on other, nonhealthcare business associates (BAs) to successfully address and administer patient care. The compliance of those vendors is essential for a practice to stay out ofhot water.

Make sure your practice remains HIPAA-compliant in business by knowing what protected health information (PHI) can be disclosed, and to whom, and when. Brush up on these particulars concerning BAs and business associate agreements (BAAs).

Understand Who Qualifies As a Business Associate

"A 'business associate' is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity," says the HHS Office for Civil Rights (OCR). "A member of the covered entity's workforce is not a business associate. A covered health care provider, health plan, or health care clearinghouse can be a business associate of another covered entity."

Tip: Those who may have access to PHI include not only attorneys and accountants, but also computer and medical hardware repair businesses, EHR-software vendors, off-site billing and coding companies, and physical security providers.

Most practices almost definitely work with at least one BA - but probably, utilize many others, too. Here are some examples, as outlined by the OCR:

- "A third-party administrator who assists a health plan with claims processing.
- "A CPA firm whose accounting services to a health care provider involve access to protected health information.
- "An attorney whose legal services to a health plan involve access to protected health information.
- "A consultant who performs utilization reviews for a hospital.
- "A healthcare clearinghouse that translates a claim from a nonstandard format into a standard transaction on behalf of a health care provider and forwards the processed transaction to a payer.
- "An independent medical transcriptionist who provides transcription services to a physician.
- "A pharmacy benefits manager that manages a health plan's pharmacist network."

Take These Precautions

While BAs are technically exempt from HIPAA regulations, CEs can only disclose PHI if "theproviders or plans obtain satisfactory assurances that the business associate will use the information only for the purposes for which it was engaged by the covered entity, will safeguard the information from misuse, and will help the covered entity comply with some of the covered entity's duties under the Privacy Rule," the OCR says.

To remain compliant, in most cases, your practice musthave contracts with these partners. These contractsor BAAs must specify the particular times and terms that the BA can disclose, access, or otherwiseutilize PHI. You can find a sample contract here:
www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html.

"Covered entities who have business associate agreements already in place should have their business associate agreements reviewed so that the appropriate amendments can be made if necessary, and those covered entities without

business associate agreements in place should have such agreements drafted immediately," say attorneys **Mathew J. Levy, Esq.**, partner at Weiss Zarett Brofman Sonnenklar & Levy, PC, and **Stacey Lipitz Marder, Esq.**, associate at Weiss Zarett Brofman Sonnenklar & Levy, PC, in New Hyde Park, New York, in a blog post.

"In addition to having compliant business associate agreements in place, covered entities need to make certain that their privacy and security policies, as well as HIPAA authorization forms, are compliant, and that their staff is informed of such changes," Levy and Lipitz Marder add.

Beware of Tricky EHR Cloud Storage

Take extra precaution if your practice stores EHRs or other PHI on the cloud, through a cloud services provider (CSP).

Hint: To remain compliant, it's crucial that you have a BAA in place and signed before moving forward with the cloud storage of electronic PHI (ePHI). This is vital because your practice could get the blame for any ePHI mishaps by BAs, so make sure your agreements are airtight.

"It's not uncommon for healthcare organizations to go beyond HIPAA requirements in their BAAs, using the document as the basis for service level requirements, too. If your BAA is that comprehensive, check for language about how you want your partner to demonstrate compliance, as well as what cybersecurity requirements, if any, are specified," says **Grant Elliott**, CEO of Ostendio and co-founder and President of the Health Care Cloud Coalition (HC3).

Even if you've covered your bases with an initial BAA, it's time to reevaluate your contracts.

"If you've had the same standard contract for a while, review it," Elliot says. Check to see whether you can audit the security program, whether there have been any amendments since the contract was drawn up and signed, and consider whether the contract needs any updates as cyberattacks become increasingly clever and frequent, he recommends.

Expert advice: There's a reason why the OCR as well as the National Institute of Science and Technology (NIST) have stringently defined what a CSP is and what HIPAA protocols must be in place for dealings with cloud providers. "Not all cloud vendors are alike. It is more nuanced than that," says **Kurt J. Long**, founder and CEO of FairWarning, Inc in Clearwater, Florida. "Look for third-party evidence when choosing a cloud vendor for your EHR - a good-looking website does not equate to a mature product or adequate security."

Remember: Trust is paramount in the handling of such sensitive data. "Transparency promotes trust," Elliot says. "If your CSP does have a compliance program, ensure you have a system or process in place that allows you to easily keep an eye on their ongoing privacy and security actions. It's reassuring for both parties, and can make a difference when called on to officially demonstrate you're on top of privacy and security."

Reference: Check out the OCR's advice on HIPAA and cloud computing at www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html.