Codify
BY AAPC

MDS Alert

HIPAA: Keep Business Associate Agreements Current

As covered entities that often engage with many outside vendors, nursing homes may risk noncompliance if contracts aren't reevaluated and updated.

The Health Information Portability and Accountability Act (HIPAA) Privacy Rule only applies to covered entities, but most facilities rely on many other businesses too in their daily functioning.

Because the Centers for Medicare and Medicaid Services (CMS) considers nursing homes as providers - and covered entities - nursing facilities can be held liable if they don't have proper policies in place to safeguard protected health information (PHI), especially when sharing or disclosing it to business associates.

The need to protect PHI is increasingly important as health records are stored electronically and are increasingly susceptible to new and varied attacks by cunning criminals and lax security practices.

One way nursing homes can shore up their HIPAA compliance is by regularly checking contracts (or "agreements") with business associates to make certain that all t's are crossed and i's are dotted.

Business Associates Exist in Many Forms

"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 **Department of Health and Human Services 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."

Many business associates aren't necessarily involved in patient care, nor do they interact with patients directly. Consider PHI access when you're evaluating who's a business associate - and think about the myriad ways someone may come into contact with PHI. Not only attorneys or accountants, but also the people responsible for computer repair, cleanliness around the facility, or a hired security service.

As a provider, your facility almost definitely works with at least one business associate, and probably many. Here are some examples, as provided 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."

Make These Precautions Standard

While "business associates" are technically exempt from HIPAA regulations, covered entities can only disclose protected PHI if "the providers 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 facility must have contracts with business associates. These contracts or "agreements" (BAAs) must specify the particular times and terms that the business associate can disclose, access, or otherwise utilize PHI. You can find a sample contract here: https://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 **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.

Be Careful With Cloud Storage of EHR

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

Hint: To remain compliant, it's crucial that you have a business associate agreement in place and signed before moving forward with cloud storage of electronic PHI (ePHI).

Your facility could get the blame for any PHI mishaps by business associates, so make sure your agreements are watertight.

"It's not uncommon for healthcare organizations 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 business associate agreement, 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.

Trust is paramount in the handling of such sensitive data.

"Transparency promotes trust," Elliot says. "If your CSP does have a compliance program, assure 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."

Beware: The HIPAA Privacy Rule covers PHI and other sensitive health data regardless of where it's stored. If your facility uses a CSP and are not sure whether the storage servers are located in the United States, it may be worth checking to make sure that the CSP's standard practices ensure HIPAA-compliant security, regardless of location.

Make Sure PHI is Secure Physically, Too

The MDS is a wellspring of sensitive information and PHI, and because of its ubiquity in facilities - and use by so many team members - staff may forget exactly how much sensitive data is included.

For example: Though CMS is moving to strike social security numbers from the MDS, there are still a few months to go with its common use in Section A of the MDS. Leaving a resident's MDS open on a computer screen or even printed out for use amongst other team members leaves that resident's SSN especially vulnerable. Several nursing home employees

have been charged with identity theft in recent years. Your BAAs may not currently address inadvertent access of PHI or ePHI - in which case, you should consider updating your contract standards.