Health Information Compliance Alert

HIPAA: Bolster HIPAA Understanding With These Fundamentals

Tip: Train staff on regulations to boost compliance efforts.

You may discuss HIPAA with your employees and the importance of protecting patients' data and think you're covered for compliance. Think again: You may only be offering a cursory knowledge of the rules, which can lead to staff errors, and ultimately, violations and fines.

For example: Take incident response, a crucial tool for HIPAA-covered entities to educate staff on because the quicker your team responds to a breach, the better. But unfortunately, employees are often nervous to verify breaches or tell practice management about their hunches. "Train [employees] in incident management, top to bottom," advises **Jim Sheldon-Dean,** principal and director of compliance services for Lewis Creek Systems, LLC, in Charlotte, Vermont. "Staff need to feel like they are empowered to report their suspicions of information security incidents. The handling of incidents needs to be clearly defined, and top management needs to understand the impacts of incidents and the necessity to prevent them as reasonably practicable."

Reminder: The Health Insurance Portability and Accountability Act of 1996 - or HIPAA for short - is most commonly associated with safeguarding patients' protected health information (PHI), but originally it was enacted to help workers with insurance issues between jobs. The feds also hoped to utilize the regulation to cut fraud, abuse, and waste in the industry while simplifying the transactionality of healthcare.

Compliance is important, and there are certain HIPAA-related terms that you may want your workers to understand. Here is a list of nine critical definitions to add to your training materials:

Covered entity: Believe it or not, there are still covered entities (CEs) that don't realize that they are CEs and must comply with the HIPAA Privacy, Security, and Breach Notification Rules. In fact, the Centers for Medicare & Medicaid Services (CMS) even offers those confused about their status a decision tool to determine if they are indeed a CE. In short, a CE is involved in the transmission of patients' PHI, and includes covered healthcare providers, health plans, and healthcare clearinghouses. Review the CMS tool at www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.

2. Business associate: A BA "is any person or entity that performs a function or activity on behalf of the practice involving the use and/or disclosure of protected health information (PHI) that is not a part of the practice's staff," says **Kent Moore,** senior strategist for physician payment at the American Academy of Family Physicians.

3. PHI: Protected health information, and its digital equivalent electronic PHI (ePHI), are best defined as "all 'individually identifiable health information' held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral," HHS Office for Civil Rights (OCR) guidance indicates. Under the HIPAA Privacy Rule, OCR lists the following 18 PHI identifiers:

1. Name
2. Address
3. Birthdate and other corresponding dates of admission, discharge, death, etc.
4. Landline and cellphone numbers
5. Fax numbers
6. Email addresses

7. Social Security Number
8. Medical record number
9. Health plan beneficiary number (i.e. Medicare Beneficiary Identifier)
10. Account number
11. State identification or license number
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. URLs
15. IP addresses
16. Biometric identifiers like finger or voice prints
17. Photo or image of patient, specifically the face
18. Any other unique code, characteristic, image, or number that identifies the individual

4. De-identified data: When data no longer can be used to identify an individual it's considered de-identified, according to OCR. "De-identified health information neither identifies nor provides a reasonable basis to identify an individual," and it's often passed two major HIPAA hurdles. First, a "qualified statistician" has verified the data; and second, all "specified identifiers" have been removed, including employer and family information, and CE determines the material stripped of identifiable PHI, indicates OCR.

5. Limited data set: The LDS is used for research or public health purposes and refers to partially-deidentified information that can be shared without prior authorization from the patient. However, if you're a CE and plan on sharing LDS files, you will need a data use agreement (DUA).

6. Designated record set: Not to be confused with the LDS, PHI, or other data-centered HIPAA acronyms, the DRS includes the record of patients' clinical, medical, and billing information. This data is maintained by CEs, and patients have the right to access the DRS upon request. "Designated record sets include medical records, billing records, payment and claims records, health plan enrollment records, case management records, as well as other records used, in whole or in part, by or for a covered entity to make decisions about individuals," OCR clarifies.

7. Minimum necessary: According to the HIPAA Privacy Rule standard, CEs should make "reasonable efforts to limit use, disclosure of, and requests for protected health information to the minimum necessary to accomplish the intended purpose," OCR advises. That means that you should always ensure that only PHI that is absolutely necessary to conduct business is shared.

8. Breach: When PHI is impermissibly used or disclosed compromising the security or privacy of PHI or ePHI, a breach has occurred.

9. HIPAA authorization: Sometimes a CE may need to use a patient's PHI for use or disclosure that's not covered under the HIPAA Privacy rule and for which voluntary consent will not suffice. That's where the HIPAA authorization comes into play. "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," explains OCR.