Part B Insider (Multispecialty) Coding Alert

Patient Privacy: Discover These 3 Common Ways That Practices Violate HIPAA

Hint: You should train your temps if they aren't already hip to HIPAA.

Now that HIPAA is part of your practice's everyday operations, you may not focus as strongly on privacy training as you did a decade ago. However, HIPAA compliance is something that should be part of your daily operations, and letting just one aspect of privacy fall through the cracks could open you up to dozens of violations. Get to know these three ways that practices frequently violate the HIPAA privacy rules without realizing it.

1. Forgetting That HIPAA Rules Follow Charts That Leave the Office

Working in a medical office is like any other job in that employees tend to bring work home with them—and sometimes that translates into private employee information sitting on your kitchen table, where your family or other visitors can quickly see it. To avoid situations like this, which clearly violate patient privacy rules, you should establish a policy on taking charts home. Unless handled very carefully, you could violate HIPAA and face penalties even if you just misplace one superbill in your home.

While HIPAA certainly does not prohibit physicians from taking patient charts home, it's an issue to consider, and a decision each covered entity will have to make for itself. If you decide to allow physicians, coders, billers or other staff members to take charts out of the office, it's a good idea to implement a log-out system. That way, you'll know where each patient's information is, and there's some accountability.

You also should have a policy that says your staff members must safeguard any patient information when they remove it from the office, since the HIPAA laws protect the patient's privacy no matter where the chart happens to be.

2. Train Your Temps

Medical practices hire temporary employees from time to time, whether it's to fill in while you're hiring new staff members or to replace an employee who is out on maternity leave. And although it's not easy to offer HIPAA training to employees who will only be in your organization for a short period of time, failure to do so could open your practice up to enforcement scrutiny.

The reality is that temps must receive the same training as everyone else. If the temp hasn't already been trained through his or her placement organization, now is the time to nail down that training. You can either bring the temp in on group training if it's coming up soon, or you can perform one-to-one training followed by self training tools like a PowerPoint presentation with a quiz at the end or a security worksheet. All session documents and training materials are then kept in temporary employees' files.

3. Don't Let HIPAA Lapse After Patient Dies

If a patient passes away, that doesn't make his or her HIPAA agreement null and void. In fact, the HIPAA Privacy Rule protects a patient's individually identifiable health information for 50 years after the date of death, according to the

Department of Health and Human Services.

"During the 50-year period of protection, the personal representative of the decedent (i.e., the person under applicable law with authority to act on behalf of the decedent or the decedent's estate) has the ability to exercise the rights under the Privacy Rule with regard to the decedent's health information, such as authorizing certain uses and disclosures of, and gaining access to, the information," HHS says in 45 CFR 160.103 of the Privacy Rule.

Keep in mind that if a family member needs information about the decedent's health care specifically for the family member's own health care treatment, the practice "may disclose a decedent's protected health information, without authorization, to the health care provider who is treating the surviving relative," HHS says on its website in a separate question and answer.