MDS Alert

Staffing and Training: Stay Alert to Minimize HIPAA Breaches

Untrained staff are a major source of privacy breaches.

As covered entities (CEs), nursing facilities are responsible for complying with the Health Information Portability and Accountability Act (HIPAA), including the various components of the Privacy and Security rules. Nursing facilities are at risk for incidental disclosures of resident protected health information (PHI).

Focusing on staff training and continuing education is the best defense against these incidental disclosures.

Define PHI Incidental Disclosure

Incidental disclosure is a disclosure of PHI to somebody who's not supposed to have it, but it's incidental to performing your day-to-day operations.

One of the most common examples of an incidental disclosure would be a facility visitor overhearing a PHI-laden conversation between a resident and nurse from a resident's room.

Caution: Although such incidental disclosures are permitted under HIPAA's Privacy Rule, you must meet two important conditions, according to the "Incidental Uses and Disclosures" part of the rule listed on the Department of Health and Human Services (HHS) website. These conditions are as follows:

- First, you have to comply with the minimum necessary requirement, which requires entities to have already made reasonable efforts to limit staffers to the minimum amount of PHI they need to perform their jobs.
- Second, you must have policies and procedures that seek to minimize incidental disclosures, which includes implementing reasonable safeguards to protect residents' confidential health data from incidental leaks.

Important: You must meet both of the above requirements to get a pass under the rule on incidental disclosures. Otherwise, it could constitute a violation.

To help your organization minimize incidental uses or disclosures - and the potential for privacy violations - look at these five steps you can take.

Step 1: Decide What Constitutes 'Reasonable'

A CE must have reasonable administrative, technical, and physical safeguards in place that will limit incidental uses and disclosures, according to the HHS Office for Civil Rights (OCR) guidance.

So, when it comes to preventing incidental leaks, the question for many CEs to ask will be "What constitutes a reasonable safeguard?" which includes reasonable use of PHI in the facility and in coordination with business associates (BAs).

OCR's privacy guidance also specifically states that entities need not implement safeguards that would create undue financial or administrative burdens. For example, you don't need to rebuild your facility to create private, soundproof rooms.

Note: What's deemed reasonable will largely going to depend upon the individual entity, the type of disclosure, and the context in which the disclosure is made.

"For example, a biller needs to know what are permissible ways of communicating with insurance companies and what

are not. An IT person needs to know how to properly transfer PHI from one system to another," says **Adam Kehler, CISSP**, principal consultant and healthcare practice lead with **Online Business Systems**. "These are topics that may not be in the general training but are critical for how workforce members handle PHI in their day-to-day activities."

What you can do: You should discuss what kinds of safeguards your organization considers reasonable and then document those decisions. This way, you should be able to produce a documented rationalization if any of your safeguards or policies are ever called into question.

Step 2: Boost Staff's HIPAA Knowledge

Use training time to orient your workforce with your organization's policies concerning PHI incidental uses and disclosures. Trainers could pose various kinds of examples and then have the staff talk it through and decide whether the use or disclosure would be deemed okay or not under the rule.

Residents' data is often impermissibly used and disclosed due to a lack of staff training and human error. "Consider your workforce's privacy knowledge" and train your employees accordingly, suggest healthcare counsel **Elizabeth Hodge**, and partner attorney **Carolyn Metnick**, with national law firm **Akerman LLP**.

Step 3: Make Privacy Part of Continuing Education

Just because you've already given your workforce members their one-time privacy training required by HIPAA doesn't mean you've completely catalogued and contained all incidental uses and disclosures in your facility. With the high turnover inherent to the long-term care industry, regular and continuing education is especially important.

Your organization should be able to establish that it has provided appropriate training to sensitize your staff about possible issues, as well as demonstrate that campaigns are done on a continual basis to update your workforce on new HIPAA requirements and concerns. These types of scenarios remind them about the potential dangers of incidental PHI disclosures and how best to avoid them.

Your primary aim should always be to protect residents while creating an environment that reinforces the appropriate handling of PHI, such that employees will always know better than to talk about PHI on social media, on the street, or any other inappropriate venue.

Communicate: You can also raise privacy and security awareness within your organization by providing regular updates on privacy matters, including email blasts, posters, and/or in-service lunch training sessions, Hodge and Metnick maintain. Centralize information about policies and procedures and helpful links and consider sending emails about opportunities for additional training and learning.

You should also keep track of news reports for real examples of privacy violations or inappropriate disclosures at other facilities. Then, bring those reports to department meetings where you can determine how such occurrences might be prevented within your own organization.

Ultimately, management needs to cultivate and support a privacy culture, and the privacy message should filter down into the workforce ranks.

Step 4: Make Breach Reporting Accessible

Any CE eager to keep tabs on its incidental uses and disclosures of PHI should implement - or already have in place - a mechanism for staff to identify and report any such incidents.

What's important for entities to keep in mind is that most unintended disclosures of PHI have more to do with bad training or lack of supervision than with a disgruntled employee who releases information. That's why it's essential that your staff feel comfortable reporting any mistakes or privacy breaches they may make or witness.

One way to both educate and involve your workforce when it comes to reporting incidental disclosures is to use staff discovery tools. These instruct employees to be on the lookout for issues and to record any incidental disclosures they

may spot - and allow you to continually monitor the effectiveness of your policies and procedures.

Tip 5: Self-Audit to Find Areas for Improvement

Incidental disclosures may be permitted under HIPAA, but is your organization constantly thinking of low-cost ways to minimize their occurrences?

For instance, anyone who visits a busy hospital unit is sure to see whole banks of electronic monitors labeled with patients' names. Anyone walking through that area might see heart rates, EKGs, and other respiratory monitoring output on virtually every patient on the unit.

And while the HIPAA regulations might allow for the incidental disclosure of PHI on these machines, simply by repositioning monitors out of public view, entities could avoid such disclosures altogether with minimal cost and effort.

Consider this: Does your organization leave resident charts in open areas, such as at a nursing station or outside the door of therapy offices? If so, then maybe you could flip the chart upside down and have it face the wall. Or simply take the charts off the top of the counter and put them below in a desk drawer. These are all low-cost, easy steps any entity could take to help minimize incidental disclosures.