

# Health Information Compliance Alert

## HIPAA: Pocket 6 Tips to Cut Your PHI Disclosure Risks

**Hint: Training employees on the Privacy Rule is a great place to start.**

The HIPAA Privacy Rule may seem pretty straightforward, but nuances exist. For many practices, incidental disclosures are a bit of a gray area, and confusion over what is considered the "reasonable use" of patients' protected health information (PHI) sometimes leads to a violation down the line.

A covered entity (CE) that fails to take appropriate steps to curb and manage any incidental uses and disclosures of PHI could easily find itself running into a brick wall of irate patients and potential HIPAA violations.

### Review the Background

So what is an incidental use or disclosure? In short, it's 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 one patient overhearing a PHI-laden conversation in an adjoining room between a physician and another patient.

**Two requirements:** Such incidental disclosures are permitted under HIPAA's Privacy Rule, but only if two very important conditions are met, according to the "Incidental Uses and Disclosures" part of the rule listed on the **Department of Health and Human Services** (HHS) website.

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 patients' confidential health data from incidental leaks.

You have to meet both of those requirements in order 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 - consider these quick HIPAA compliance tips.

### Tip 1: Determine What 'Reasonable' Means to Your Organization

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

So when it comes to reining in incidental leaks, the question for many CEs will be "What constitutes a reasonable safeguard?", and that includes reasonable use of PHI in the office 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. Therefore, you don't need to rebuild your office to create private, soundproof rooms, for example.

**Instead:** What's deemed reasonable is largely going to depend on 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," explains **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."

You should discuss what kinds of safeguards your practice 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.

### **Tip 2: Raise Your Staff's Awareness**

Use training time to orient your workforce with your organization's policies concerning 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.

Patients' 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**.

### **Tip 3: Don't Slack on Staff Privacy Training Updates**

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.

What you should be able to establish is that not only has appropriate training been done to sensitize your staff about possible issues - but 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 patients while creating an environment that reinforces the appropriate handling of PHI, such that employees will always know better than to talk about PHI in an elevator, on the street, or any other inappropriate venue.

**Ideas:** 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.

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

### **Tip 4: Make Breach Reporting Easy, Open, and Comfortable**

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 also allow you to continually monitor the effectiveness of your policies and procedures.

**Tip 5: Look for Areas of 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 that's up there.

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

**Consider this:** Does your organization leave patient charts in open areas, such as at a nursing station or outside the door of a doctor's office? 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.

**Tip 6: Don't Let Safeguards Impede Patient Care**

While it's necessary for CEs to employ reasonable safeguards to curtail incidental disclosures, it's also vital that your safeguards don't interfere with the efficient delivery of care.

The key is balancing incidental disclosures with the idea that we still have care to provide. You don't want to let HIPAA policies and procedures get in the way of providing care; but, you have to look at how information is used and how it might be disclosed in an incidental fashion - and find ways to decrease your risk factor.

**Resource:** Review HHS "Incidental Uses and Disclosures" guidance at [www.hhs.gov/hipaa/for-professionals/privacy/guidance/incidental-uses-and-disclosures/index.html](http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/incidental-uses-and-disclosures/index.html).