Health Information Compliance Alert

Compliance Strategies: 6 Tips Streamline Your Accounting

Use this advice to ensure compliance during PHI leaks.

If you can't recognize an incidental disclosure of protected health information from a wrongful one, you could be in big trouble when it comes to compiling an accounting of disclosures.
Luckily, Eli's experts are here to help you pin down what information must go into an accounting of disclosures. Use these accounting guidelines to make sure you maintain only the data HIPAA mandates patients have a right to see.

1. List wrongful ��" not incidental ��" disclosures. An incidental disclosure is when PHI is shared inadvertently with unauthorized users during the performance of day-to-day operations, explains **Kelley Meeusen**, privacy officer for Harrison Hospital in Bremerton, WA.

A wrongful disclosure is when PHI is shared with unauthorized users outside of day-to-day operations.

2. Account for mandated disclosures. You must account for each state- or federally-required disclosure of patients' PHI you make. This is where public health oversight reporting comes in, notes **Susie Honeycutt**, privacy officer for Cardiovascular Associates in Kingsport, TN. Some of the disclosures patients can expect to find on their accounting include reporting for communicable diseases and suspected abuse.

3. Document paper and electronic disclosures. "The important word to remember is 'disclosure,'" stresses **Sue Miller** of Sue Miller's HIPAA and Healthcare Services in Concord, MA. Any information you disclose ---- whether it's through e-mail, a fax or a privacy or security breach -- that falls outside of incidental disclosures must be listed in the accounting of disclosures.

4. Be specific -- but not too specific -- about the disclosure. Any organization employee entering information into a disclosure log should be sure to give a "meaningful explanation of what was disclosed" without going overboard, Meeusen asserts.

Example: Harrison Hospital groups the information in its patients' medical records by episode of care. If a privacy breach or staff mistake led to a wrongful disclosure, staffers would note which episode of care was affected rather than all the information within that episode, Meeusen says.

Think of it this way: Apply the minimum necessary standard to your disclosure log, experts suggest. You should list the least amount of information needed for patients to understand what happened.

5. Remember to note disclosure dates. It's very important to log the date a disclosure was made, if you know it, Honeycutt assures. However, if you're recording a disclosure due to a privacy or security breach, you may not have the specific date. In those cases, you should note the date you discovered the disclosure along with some timeline of when the disclosure originated.

Example: Your system was inappropriately accessed in July, but your organization did not uncover the breach until late August. Your disclosure log should include both dates with a comment about why the exact disclosure date is unknown, Meeusen says.

6. Include your mitigation process. You don't have to write out exactly how you investigated and mitigated a wrongful disclosure, but you should note who led the investigation, the dates of the investigation and how you mitigated any fallout. Any relevant documentation -- such as a copy of the incident report -- should accompany the log.

This record can serve as another piece of evidence that you strove to protect your patients' PHI, Meeusen notes. And if

patients are upset about a certain disclosure, you can show them how your organization worked to ensure the disclosure did not lead to disaster for patients.

The Bottom Line: You must record all relevant information -- and only the relevant information -- in your disclosure tracking system so that those disclosures can be easily rounded up when a patient submits a request for an accounting of your PHI disclosures.