Codify
BY AAPC

Health Information Compliance Alert

Compliance Strategies: Rely On Your Sanctions Policy To Mitigate PHI Leaks

The sanctions you impose could determine your patients' reactions to inappropriate disclosures.

Scenario: A staff member switches patients' information and winds up making an inappropriate disclosure. Your only mitigation duty is to retrieve the records, right?

Wrong. Your mitigation efforts extend to the sanctions you levy on staffers who cause inappropriate disclosures, regardless of their intent. Use these strategies to align your sanctions policy with your mitigation efforts.

Apply Sanctions Consistently

Your sanctions policy is a great tool for calming angry patients after a privacy or security breach, notes **John Parmigiani**, senior VP of consulting services for Quick Compliance in Avon, CT. Your sanction efforts prove to patients that you respect their privacy and that you are working to ensure the mistake doesn't happen again.

Problem: Inconsistent application of your sanctions policy could alarm both patients and staff. Otherwise, it could seem that your policies only apply to certain staff members and, therefore, to particular disclosures.

For example, if your patients discover that a billing clerk was suspended without pay for the same violation that landed a doctor with a slap on the wrist, your mitigation efforts could seem insincere -- leading patients to file a complaint or take their business elsewhere.

Separate Your Sanctions Into Levels

You can break your sanctions into levels or categories based on the amount of mitigation required, offers **Frank Ruelas**, compliance officer for the Gila River Hospital System in Sacaton, AZ.

Try it this way: Sort sanctions into categories like green, yellow and red with green representing basic sanctions for violations without the potential for great harm and red representing severe sanctions for violations that could seriously harm your patients, Ruelas recommends.

Examples: A staff member accidentally mails patient encounter statistics to the wrong address. If the information contained no discernable patient data, a "green" sanction like re-training would apply. If the statistics included patients' names, you could use a "yellow" sanction (such as a written warning). However, if the statistics listed patients' names along with their home addresses and Social Security numbers, you could levy a "red" sanction like unpaid suspension or termination.

Next step: Make sure your employees are fully aware of your sanctions policy and understand each level of sanction, Ruelas says. That way, affected staffers won't complain that you are treating them too harshly.

Keep Your Documentation Together

Your documentation on privacy and security breaches may seem thorough, but if your mitigation records don't detail what sanctions you levied and why you chose them, your investigation file is incomplete, says **Susie Honeycutt**, a privacy officer with Cardiovascular Associates in Kingsport, TN.

Your incident report -- and all the documentation that comes after it -- is your best record of the events leading up to and following a breach of patient information. While your human resources department might be responsible for carrying out

your sanctions policy, all information relating to the breach should be stored together in case the investigation documents are called upon down the road.

The bottom line: Accidents happen, experts and providers agree. But how you handle accidents could determine the success of your organization. By using your sanctions policy as a mitigation tool, you not only prove to patients that you are truly committed to protecting their privacy, but you also show your workforce members that you will not ignore behavior that jeopardizes your compliance.