

# Health Information Compliance Alert

## Security Strategies: Keep Staff on Same HIPAA Page With Set Sanctions

Applying sanctions consistently when employees disclose PHI is most effective.

Suppose a staff member switches patients' information and winds up making an inappropriate disclosure of PHI. Your only mitigation duty is to retrieve the records, right?

Wrong. Your mitigation efforts must extend to the sanctions you levy on staffers who cause inappropriate PHI disclosures under HIPAA, regardless of their intent. Use these strategies to keep staff and patients cool-headed when disclosures occur.

1. Apply sanctions consistently. Your written sanctions policy is a great tool for calming angry patients after a privacy or security breach, says **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:** If you don't apply your policy across the board, you could give the impression that it only applies to certain staff members and, therefore, to particular disclosures. For example, if your patients discover that you suspended a billing clerk 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.

2. Separate your sanctions into levels. You can break your sanctions into levels or categories based on the amount of mitigation required, says **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 says.

**Example:** A biller accidentally mails patient encounter statistics to the wrong address. If the information contained no discernable patient data, a "green" sanction like retraining 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 home addresses and Social Security numbers, you could levy a "red" sanction such as unpaid suspension or termination.

Next step: Make sure your employees are fully aware of your sanctions policy and understand each sanction level so that affected staffers can't complain you're being unfair.