

Health Information Compliance Alert

Mitigation Tips: STOP, DROP AND ROLL TO EXTINGUISH PRIVACY FIRES

Taking the time to develop procedures for staff to follow when they make a mistake and mishandle protected health information could help prevent disasters down the road.

Providers should include in mitigation policies the following steps to eliminate or alleviate damage when an accidental PHI leak occurs and should make sure staff receive training in these procedures, attorneys counsel:

1. Report suspected violations immediately to the privacy officer, advises attorney **Robyn Meinhardt** with **Foley & Lardner** in Denver.
2. Investigate the violation promptly. The privacy officer should speak to the person who submitted the report and other people identified by that reporter, says Meinhardt. Its up to the privacy officer to examine all of the systems to determine why the accident happened.
3. Decide what the mitigation should be. This should be done by the privacy officer in consultation with the organizations legal counsel, advises Meinhardt. There should be some sort of disciplinary review of the employee who is responsible for the privacy breach, she notes.

If the accident occurred via e-mail, recall an e-mail if it can be recalled, send out another e-mail specifically directing all the recipients to destroy the message and not to forward, and if they make use of the information, they would be subject to legal penalties, suggests attorney **William Sarraile** with **Arent Fox** in Washington.

4. Document the violation. Make sure you establish a good record that youve acted on this, taken it seriously, and done everything reasonable under the circumstances, advises Sarraile.

The privacy officer should keep a log that contains the following information: written documentation of the concern, who reported it, the identity of the subject of the PHI, what was done about the mistake and a description of how youre going to prevent it in the future, counsels attorney **Phyllis Granade** with **Epstein Becker & Green** in Atlanta.

5. Take steps to fix the problems so they dont occur again. "Once the organizations privacy officials have decided what mitigation is practicable, theyre still not done because they have to go back and analyze what went wrong to fix their internal processes," explains Meinhardt. "This isnt a HIPAA requirement. It just makes good business sense," she notes.

Often the problem goes back to staff indifference about privacy issues, so strategies to prevent future violations should include clear directions to staff on the importance of being vigilant about the way they handle PHI, adds Granade. Its a good idea to develop a condensed checklist of PHI dos and donts to post near their telephones or computer terminals for quick reference.