# Health Information Compliance Alert

## SECURITY: 3 PROVEN METHODS TO PUT THE BRAKES ON SECURITY BREACHES

**Train staff members to deal with violations before PHI winds up in the wrong hands**

A security violation could do more damage than just opening you up to the Centers for Medicare & Medicaid's scrutiny - it could wind up hurting your patients.

"Security breaches are particularly dangerous because hackers could use the information to steal patients' identities," says **Robert Markette**, an attorney with Gilliland & Caudill in Indianapolis. And identity theft is a hot button issue - almost 1 million people in the U.S. experienced the crime in the past year.

And the security rule is not the only legislation aimed at lessening the risk that patients' information turns into fake accounts for criminals. An increasing number of states are considering bills that would match California's strict laws for protecting the security of consumer and patient information, notes **Elisabeth Derwin,** Information Technology Specialist for Bennet Healthcare in San Francisco.

For example, California law requires its providers to contact each patient whose unencrypted personal information was or might have been accessed inappropriately - even if that access is minimally harmful. That means if you faxed patient information to the wrong provider's office and their staff immediately notifies you and shreds the document, you would still have to inform the patient.

That puts you squarely in the hot seat when it comes to unauthorized access to your patients' PHI - which could include Social Security numbers and other billing information. Here are some tips to help your personnel shine a light on security breaches before hackers and other criminals can use the information to their advantage.

### 1. Post Your Procedures In Employee Areas

"Make posters that list the common signs of security breaches and what steps to take if staffers notice those signs," advises **Betty Bundul**, HIPAA security compliance director with Allina Hospitals & Clinics in Minneapolis.

**Good idea:** Ask each department to come up with a list of its most common security concerns and whom to contact for each.

### 2. Outline Your Security Violation Reporting Routes

Your policies and procedures should clearly dictate whom employees should call if there's a suspected security breach, Markette says.

For example, if your staffers suspect their password has been compromised, they could call your tech support team. If they discover an office has been broken into, however, they'd want to call your security department.

**Best:** Establish and publicize an integrity line that employees can call for all work-related concerns, Bundul suggests. The integrity line staffers can then direct the calls to the proper person so that employees' don't have to.

### 3. Make Sure Staffers Know How To Use Their Tools

*CPT® 2023 American Medical Association. All rights reserved.*

Just creating security tools isn't enough - you have to teach your staffers how and when to use them. "Your security rule training should include each person in your organization, not just those who work with electronic PHI," Markette counsels.

That way, everyone from your maintenance staff to your medical records personnel will know how to deal with potential security breaches.

Coach your employees to contact your compliance expert whenever they are concerned that a breach might have occurred. The compliance expert can either explain to them why the issue is not a breach or give them the correct reporting route for alerting your organization of the problem.

**The Bottom Line**

While privacy breaches can cause extensive damage, security breaches have the potential to wreak havoc on every aspect of your patients' lives. "Security breaches are more likely to be the result of a purposeful, targeted search for information," Derwin says. But, by catching the problem early and plugging the holes that allowed the information to leak out, your staffers could save both your reputation and your patients' identities.

*CPT® 2023 American Medical Association. All rights reserved.*