Health Information Compliance Alert

Privacy: Don't Rely on Aliases to Protect Your Patients' PHI

You can protect your patients' information without changing their names.

Picture it: Brad Pitt is rushed in after suffering a heat stroke on the set of his latest film, or President Clinton calls your office after experiencing heart palpitations.

You may be tempted to assign pseudonyms to your patients to ensure their information isn't leaked outside your organization, but coming up a with a fake name may cause more problems than it solves.

Whether you're guarding famous clients from the paparazzi or not-so-famous clients who simply want to remain anonymous, the draw of using an alias is understandable, says **Jason Levine**, a consultant with Murer Consultants in Joliet, IL.

"I can see it being especially useful in an outpatient setting where a patient might not want their name called out or written down on a sign-in sheet in full view," Levine explains. And many providers have a history of using aliases, he notes.

Direct Your Patients To The Directory

The privacy and security rules should eliminate your need to use fake names, points out **Adam Kaufman**, compliance analyst with Mercy Medical Center in Baltimore. HIPAA gives patients the option of being included -- or left out -- of any facility directories. If patients opt out, then their information will be masked from public view whether they are President of the U.S. or the cleaning lady.

Case in point: Mercy Medical Center often accommodates government officials who demand a high level of privacy and security. The center used to rely on aliases to ensure that those dignitaries remained anonymous; however, that eventually created chaos in their systems.

"We would change the patient's name in three different systems. Then we had to coordinate the name changes with our accounting offices so that they could match up the real name before submitting claims -- and then they had to switch back to the aliases after the claims were submitted," Kaufman says.

This process not only sucked up valuable time and energy, it also wasn't foolproof. Patients admitted under aliases ran the risk of a staffer forgetting the pseudonym or failing to attach crucial medical information to the record because of the different names, Kaufman warns.

Now Mercy avoids using fake names and instead relies on its privacy policies to protect its patients. "If a patient opts out of our directory, it's as if he never existed," Kaufman explains. Good idea: You should make sure patients understand what opting out really means. "We warn patients that they may not get flowers or phone calls" so they can make an informed decision, he says.

You can also institute across-the-board procedures that protect all patients, says **Robert Markette**, an attorney with Gilliland & Caudill in Indianapolis. Example: Ask patients who opt out of the directory to distribute their room's telephone number. Then instruct your staff members never to transfer calls to patients' rooms.

Track Your Staff Members' Access

Often, blame for exposing a famous person's location to the press falls on her spokesperson, but when it comes to nuts and bolts PHI, leaks are probably an inside job, Markette says.

Remember: You have a reliable tool for catching employees who are spying on relatives and neighbors or high-profile clients: your audit controls.

"Access into records is on a need-to-know basis for work-related functions only," Kaufman asserts. If your auditing and tracking turns up an employee who is accessing records outside of what he needs to perform his duties, you may have found the source of a potential privacy breach. By catching the problem early, you head off any leaks -- and the need for an alias.

The Bottom Line

"If your goal in using an alias is to protect patients' privacy, an alias may not be the way to go," Markette posits. If an employee is bragging about a famous person staying in your facility, it won't matter if the person is using a fake name or not.

Best bet: Create policies and procedures that ensure the equal protection of all your patients' information. Then educate and train your staff members to follow those procedures without blabbing any confidential information to unauthorized ears.