Health Information Compliance Alert

Security: Guard Against Internet Scams with These Expert Strategies

Keep your staffers on their toes with regular procedure updates and e-mail reminders.

If you aren't certain that your staffers know how to handle a suspicious e-mail attachment, you could be setting your organization up for failure.

Don't wait for an Internet scam to dupe your employee into handing over confidential information. Follow our experts' advice for designing a policy and procedure (P&P) to protect your staffers and patients' PHI from even the trickiest Internet scams.

Get Your So In The Game

Your organization's security officer (SO) must be aware of what scams are circulating the Internet, says **William Hubbartt**, president of Hubbartt & Associates, a privacy and security consulting practice in St. Charles, IL.

For example, your SO should spend a certain amount of time visiting security Web sites and reading up on how the newest viruses or scams can be detected and prevented. An important part of this process is constantly checking for software and anti-virus updates, Hubbartt stresses.

And, as your SO develops new ways to fend off e-mail and Internet attacks, she should update your P&Ps to reflect all new approaches. Similarly, if your SO amends your P&Ps in the face of a virus or Internet scam, that amendment should be documented.

Good idea: Ask your staff members to alert your SO or another designated security professional when they read about a new scam, recommends **Elisabeth Derwin**, an information technology specialist with Bennet Health System in San Francisco. Tip: Stress to staffers that they should always send news about scams to designated recipients and never to others in your organization.

School Employees & Patients

Your best laid plans will be foiled if just one staff member fails to follow your rules, points out **Chad Markham**, information security officer for Mercy Medical Center in Sioux City, Iowa.

Markham sets up regular security training sessions with his staffers to remind them about Mercy Medical Center's P&Ps. He also uses this time to educate his personnel on the latest happenings in e-mail and Internet hoaxes.

Priority: You can target more specific, in-depth training for employees who spend the majority of their time using e-mail or the Internet, Hubbartt advises. You can scale back your training for those in your organization least likely to need e-mail or the Internet.

Between training sessions, Markham uses in-house newsletters and e-mail reminders to keep his staff members on their toes about the dangers of e-mail and the Internet.

Here are two example reminders you could send out to your staffers:

1) "Immediately delete an e-mail if the subject line, punctuation or attachment extension looks suspicious. Some examples of this are: !HATNow!!, iloveyou, or File.mp3.exe. If you are unsure about an attachment, send it to the IT team without opening it."

2) "Never respond to an e-mail asking you for financial, medical or other confidential information. If the sender looks familiar to you (such as an e-mail from the medical center's or your bank's domain), pick up the phone and call to verify that they need the information-then give it to them over the phone. However, in 99.9 percent of these cases, the e-mail is a scam."

Patients also appreciate your willingness to go the extra mile to help them avoid falling victim to a virus or hoax. And though "it's not your responsibility to inform your patients about these scams, your proactive stance is a great customer relations boost," Hubbartt notes.

Send the tip sheet, located in the following article to all your patients who request that you send them e-mails in lieu of telephone calls. And, if you've experienced Internet security problems in the past, attach the sheet to your notice of privacy practices.