Security Awareness: The Right Messages

Save to myBoK

by Margret Amatayakul, MBA, RHIA, CHPS, FHIMSS

How many of you have warned your e-mail users about "phishers"—e-mail that appears to come from a trusted source asking the recipient to click on a link to update personal details? But the site is really a fake, and the e-mail is a scam to steal personal information.

Reminding e-mail users to think about the likelihood that their bank would really be asking for personal information in this manner is one way to protect your staff and IT resources and comply with HIPAA.

Awareness Building

Awareness building is a key part of the HIPAA security awareness and training standard, section 164.308(5). While implementation specifications would have covered entities address security reminders, protection from malicious software, log-in monitoring, and password management, the standard itself requires the implementation of a "security awareness and training program for all members of [the] work force (including management)."

An awareness program should be a well-planned, coordinated set of activities, messages, and behaviors that support making information security a way of life. The program should be comprehensive, covering all aspects of HIPAA and any other measures the organization believes would contribute to its mission of caring for its patients and workers. The program should also be dynamic, with the flexibility to respond to new threats and breathe new life into old messages. Most of all, there must be commitment from executive leadership for the program. They must set the example, including using their own swipe cards for access to secure areas, memorizing their unique user IDs and passwords, and carrying out background investigations, sanctions, and mitigation policies consistently.

The Medium Is the Message...

When one thinks about building awareness, one often thinks of various methods to convey the message. Marshall McLuhan's famous assertion "the medium is the message" comes to mind.[1]

In January 2002 the "HIPAA on the Job" column provided guidance on HIPAA education, training, and awareness, offering suggestions on low-cost methods to help build awareness. In general, it is a good idea to use a variety of media for delivering the information security message. Using only one medium will likely be ignored over time. Since many of the messages to be conveyed must be delivered over and over, any new twist or spin is essential to their being observed again. After all, the first time this message was included in "HIPAA on the Job," it was in paragraph form with a description. This time, the chart "Awareness Media: Pros and Cons," below, provides a list of media with their corresponding pros and cons.

...But the Message Matters, Too

While the information security message can—and should— take many forms, the message is not just the medium. The message itself is as important as the medium. In general, the information security message should reflect a consistent theme. Some suggest having an information security motto so that it is clearly recognizable on any medium and with any specific content.

The security message will vary as much as, if not more than, the medium. The security message will also vary not only over time, but by target and location. While it is obvious that a reminder to send a fax cover sheet needs to be on a poster by the fax machine and is probably not very effective in an e-mail reminder, some messages are more universal than others.

Virtually every one of the HIPAA security rule standards could be an appropriate topic for a reminder. "What to Say? Awareness Message Suggestions," below, offers a summary.

Get with the Program

In addition to specific messages, many organizations also like to have general reminders or tips that raise security awareness in general. Much like advertising, it is difficult to determine the effectiveness of any one specific message or medium. More likely, an appropriate mix of messages and media is necessary.

Another easy way to raise awareness is to incorporate information security into other activities. For example, safety fairs, Joint Commission mock surveys, protective service rounds, general audits, and other inspections provide an opportunity to check on security. Not every aspect on information security needs to be addressed at every opportunity, but a carefully constructed plan should ensure that a variety of issues are addressed throughout the year in a variety of these activities. For this reason, awareness building should not be left to chance. Awareness building needs to be carefully designed so that all aspects are covered with neither too much "blitz" nor too little left to chance.

No amount of creatively designed and planned messages and media is effective if undermined by management disregard. It is definitely by design that HIPAA's security awareness and training standard admonishes covered entities to target management for awareness and training. Management must set the tone and be vigilant about following procedures and encouraging others to do so as well.

Awareness Media: Pros and Cons

Medium	Pros	Cons
Fliers or handouts	• Professional appearance • For stable messages • Good for waiting rooms to communicate with public	• Relatively expensive • One-time communication • Require balanced message of value without fear
Posters, including tent cards	• Instructional • Demonstrate commitment • Moderate to low cost	• Can be unsightly • Can be ignored if not changed frequently
Intranet	• Reference, especially for lengthy material • Ability to link to organizational policies and procedures	• Available only to work force members with intranet access
Banners and screen savers	• Continual learning • Direct presentation to users	• Can be ignored • Can slow access • Available only to work force members with workstation access
Newsletters	• Can describe newsworthy events • Flexible for each edition	• Tendency to sensationalize • Need to keep in mind that public may see
E-mail reminders	• Direct presentation to users • Can target specific groups of users or even specific users	• Can be deleted without review • Too many can become internal spam
Trinkets	• Judicial use of tasteful products can be handy reminders	• Can be relatively expensive • Can be ignored over time
Games, quizzes	• Depending on venue, can be a pleasant change of pace	• Can be time consuming and affect productivity
Meeting agenda items	• Good for complex topics where Q&A is important	• Message may vary by person

	• Can be reassuring • Can be part of ongoing compliance monitoring	
Report cards	• Can be effective part of ongoing compliance monitoring	• Can be embarrassing to individuals
Hotline	• Quick response to issues	• Can be costly • Must be linked to security incident management

What to Say? Awareness Message Suggestions		
Message	**Targets**	**Media**
Password construction	• Users	• Instructions on an intranet site • E-mail to specific users identified with weak passwords • Games (perhaps in a newsletter)
Password management	• Users • Supervisors	• Screensavers • Banners
Internet use	• Users	• Newsletters • E-mail to specific users • Meeting agendas
E-mail use	• Users	• Banners • Games, quizzes
Fax use	• Faxers	• Posters near fax machines
Telephone fraud	• All work force	• Posters, including tent cards • Banners • Newsletters
Social engineering	• All work force	• Newsletters • Meeting agenda items • Report cards
Building access	• All work force	• Posters
Portable device security	• All work force	• E-mail to device users • Posters
Portable media security	• All work force	• Banners
Paper disposal	• All work force	• Posters near printers
Identity and authority verification	• All work force • Visitors	• Posters
Malicious software	• Users • IT	• Banners • Intranet home page
Software licensing	• Users • IT	• Intranet • Newsletters
Downloading executable files	• Users • IT	• Intranet • Newsletters

Back-ups	• Targeted users	• E-mail reminders
What constitutes an incident	• All work force • Visitors	• Fliers or handouts • Banners and screen savers • Newsletters • Trinkets • Meeting agendas • Report cards
Incident reporting	• All work force • Visitors	• Intranet • Internet • Hotline
Suspicious persons	• All work force • Visitors	• Fliers or handouts • Newsletters • Hotline
Missing equipment	• All work force	• Posters • Banners • Hotline
Identity theft	• All work force	• Posters, including tent cards • Banners • Newsletters
© 2004, Margret\A Consulting, LLC		

Note

1. McLuhan, Marshall. *Understanding Media: The Extensions of Man*. New York: New American Library, 1964.

Margret Amatayakul *(margretcpr@aol.com) is president of Margret\A Consulting, LLC, an independent consulting firm based in Schaumburg, IL.*

Article citation:
Amatayakul, Margret. "Security Awareness: The Right Messages." *Journal of AHIMA* 75, no.4 (April 2004): 56-59.