Smart Training on Privacy and Security

Save to myBoK

By Sandy Bacik, CISSP, ISSMP, CISM, CGEIT

ARRA's modifications to the HIPAA privacy and security rules are setting off a new round of training in facilities large and small. Trainers must fit the new training into existing schedules that already include organizational policies and procedures, HIPAA, and other regulations such as the Red Flags Rule.

Providing that training, however, can be a challenge. Much needs to be covered, and time and money are typically in short supply. Good planning allows trainers to design programs that combine training on these regulations for multiple groups. Scenarios can integrate training topics and help the lessons stick.

Looking for Crossover

Typically the first step in designing a training program is to assess and agree on what training is needed. Technical and management healthcare professionals require combined training to be effective and efficient in meeting security and privacy regulations as well as additional, internal topics within the enterprise policy architecture. All of these topics have three things in common: people, information, and technology.

People include staff members (including contractors, consultants, and volunteers), business associates, and patients or clients. This can be a big audience, but each category will not require the entire training. Training topics should be assigned for each staff category.

Take, for example, training that will cover security, privacy, and identity theft prevention. A possible table of priority training needs appears [below]. Below it appears a simple table that plots the training topics against the enterprise's policy architecture and federal regulations.

These tables help identify opportunities for consolidation: training for management and direct hires can be similar, as can training for business associates, contractors, consultants, and volunteers. Patients or clients have differing educational needs.

However, the topics will require some integration because, for example, information that is secured may not necessarily be private or protected from theft.

Identifying Opportunities for Consolidation

Training on privacy and security topics requires reaching a large audience on multiple regulations. Mapping the people who need training against the topics they need training on helps identify opportunities for consolidation. Mapping the regulations against the topics offers another look at potential for integration.

People	Security	Privacy	Theft Prevention
Business associates	x	x	x
Consultants	x	x	x
Contractors	x	x	x
Patients or clients		x	x
Direct hires	x	x	x
Management	x	x	x

People	**Security**	**Privacy**	**Theft Prevention**
Volunteers	x	x	x

Regulation	**Security**	**Privacy**	**Theft Prevention**	**Breach Reporting**
Enterprise policy architecture	x	x	x	x
HIPAA	x	x		x
ARRA	x	x		x
Red Flags Rule	x		x	x

Using Stories to Combine Topics

Identifying stories that combine the training topics will help integrate the training and reinforce its importance.

Those stories could come from the news or a situation within the organization. They could be fictional stories tailored to training needs. Examples that draw in security, privacy, and identity theft topics include:

- An employee returns from a vacation to find his home has been broken into and his laptop, which contains patient records, has been stolen
- An employee or business associate sells information about a clinic's patients
- A volunteer leaves a clinic computer logged in after hours and the contracted maintenance staff creates a new identity

Many of these situations could require that affected parties be individually notified under the new federal breach notification provisions, established in ARRA and added to HIPAA.

For Example…

Take, for example, a program with a goal of training in-house staff on the basics of HIPAA, ARRA, and the Red Flags Rule. The session must cover the following topics:

- Information types and policy architecture
- Information confidentiality, integrity, and availability
- Security and privacy provisions
- Identity theft prevention
- Breach notification

A slide deck could provide the definitions, references, and steps to follow when something happens. That may cover the bases, but it sounds boring. Staff will sit and listen and probably walk out not remembering a thing.

Making the topics relevant and real to the organization and the people in the room will make the training more interesting, keep the audience more attentive, and improve the likelihood that the information will be retained. It also will offer varied methods of delivery and communication. The trainer could:

- Relate why compliance is needed and how it affects the organization
- Relate how compliance works with the organization's policy architecture
- Provide examples for a home and work environment
- Give samples of the different information types involved
- Summarize recent relevant articles in the news
- Look at internal situations that have or almost happened
- Make some stories generic and relate to the organization
- Create a scenario of a potential incident and have audience members do some role playing

For example, a simple story like the following covers multiple topics in an engaging way:

> A patient data entry clerk is having trouble with a software application. Continually, the clerk must re-enter data because the application freezes or crashes. Someone approaches and says, "I see you are having problems. May I help?" The frustrated data entry clerk glances up and sees a badge, assumes the person is IT staff, and says, "Yes, sit down and I'll show you." The person with the badge inserts a USB drive into the computer, types a few commands, and says, "Try it again." The data entry clerk tries again, and everything appears to work. Within days, a news article appears that a famous person was treated at the clinic for cancer, and then a patient reports his identity has been stolen.

This simple scenario deals with security, privacy, and identity theft. It is sure to provoke discussion. Having the audience suggest solutions to prevent this from happening-and even role play to demonstrate-will enhance the training through active participation. This type of training can be easily adapted to train varying audiences.

Using recent events in ongoing training keeps things fresh-the same and yet different. Relating the information to real-life incidents at home and work helps ensure staff retain the situations and apply appropriate actions.

Sandy Bacik (sandy.bacik@enernex.com) is a principal consultant at EnerNex and a former chief security officer. A longer version of this article first appeared on the Journal of AHIMA *Web site at http://journal.ahima.org.*

Article citation:
Bacik, Sandy. "Smart Training on Privacy and Security" *Journal of AHIMA* 81, no.7 (July 2010): 42-43.