Backbone of the Security Rule

Save to myBoK

by Meg Featheringham, assistant editor

For Gail Kraft, RHIA, CHPS, a patient's medical information is sacred. "For me, and I believe this is true for other health information professionals, we've always been passionate about protecting the privacy of our patients and their medical information," she says. As regional privacy and security officer for Kaiser Foundation Health Plan of Georgia in Atlanta, she practices her passion. "This was a natural way for me to take that interest in protecting privacy to a higher level."

Kraft began her career at Elmhurst Memorial Hospital in Elmhurst, IL, in various coding positions. It was her move to Georgia, however, that "really set my career on a different path than it would have been had I stayed at Elmhurst Memorial," she notes.

Kaiser offered Kraft a wealth of opportunities in the world of HIM, first as a medical record supervisor, followed by involvement with the organization's release of information. "When a position opened up in IT for a systems analyst, it seemed to be a good fit for me. I knew the business of the records, and so to take that knowledge and apply it to work with technology seemed like a logical fit," she says. From there she became the health information administrator, which led to her current role in the compliance department.

AMR Experience

Kraft's interest in IT and security stemmed from Kaiser Permanente Georgia's move to an automated medical record (AMR). That first attempt at an AMR was suspended, however, because of a Kaiser Permanente initiative for a national solution. "Of course that took longer to develop and implement because of the number of Kaiser regions involved," Kraft notes.

The Georgia region of Kaiser Permanente will implement Kaiser's national AMR solution in May. "The national development was accomplished collaboratively with all of the regions of Kaiser Permanente," she explains. As regional privacy and security officer, Kraft is now responsible for "creating, implementing, and maintaining our compliance program around privacy and security, which involves ensuring the organization has the appropriate policies and procedures in place and that the safeguards implemented are being used," she says.

"Kaiser's national compliance officer gave the directive that compliance must be a component of our electronic record to make certain that we complied with all applicable federal and state laws," Kraft says. She was part of a team that consisted of IT representatives, attorneys, managers, and other professionals in developing security policies and procedures for the organization.

Security Training

Kraft is accountable for training the work force on the security regulations. "In the past our compliance training, including HIPAA privacy, was leader-led," she says. "This year, we're going to Web-based training, and I'm very excited about this program," she explains. All of Kaiser Permanente Georgia's 2,500 employees and clinicians will log on to the company's intranet site to complete the security training. The system will track employee attendance and generate reports that verify that all employees receive the required security training.

Kraft says the elimination of the leader-led training and manual tracking will assist her immensely. "There can be inconsistencies in leader-led training since not everyone's instructional methods are the same. With online training, each employee is receiving the same message and in the same manner," she says.

Article citation:
Featheringham, Meg. "The Backbone of the Security Rule." *Journal of AHIMA* 76, no.3

(March 2005): 84.