

N.J. Medical Center Uses LF Tags to Protect Patient Records

Englewood Hospital requires staff to use RFID-enabled identity badges to access the institution's computers and applications.

By Beth Bacheldor

Nov. 14, 2007—A number of hospitals are starting to employ RFID to track medical devices and other assets. But Englewood Hospital and Medical Center (EHMC) is using the technology for another purpose: to protect patient data and control access to its clinical system and other critical applications.

In operation since 1890, the Englewood, N.J., hospital has 520 beds and more than 2,500 employees. The medical center is using an identity and access management (IAM) solution from Encentuate, based in Redwood City, Calif. The system combines low-frequency (LF) 125 kHz RFID proximity tags embedded in employee badges with single-sign-on (SSO) software, workflow and security management functions that nurses, doctors and other hospital employees can utilize to access the facility's computers and applications. SSO is a method of access control that enables a user to access multiple software applications after a single authentication.

EHMC was already using an RFID-enabled system from HID to control access to its computer rooms, employee entrances and pharmacy, says Gary Wilhelm, the hospital's business and financial systems manager overseeing the Encentuate RFID-based security rollout. After considering several options to secure access to its applications, it ultimately opted to use the same 125 kHz RFID proximity tags to not only control physical access to rooms, but also operational access to computers and software.

"I looked at quite a few," Wilhelm explains, such as USB keys, magnetic-stripe cards and fingerprint ID systems. "RFID seems to be easier to use. The magnetic stripes can go bad; the fingerprint readers are subject to oil on the device. With RFID systems, there seems to be less failure rates. And if the employee can't access a system because of a failure, that is very frustrating." Encentuate's system also allowed the hospital to use existing employee badges, which were RFID-enabled for the physical access security system already in place.

To date, EHMC has equipped 50 nursing computer stations (kiosks) and several dozen administrative computers with RFID interrogators and the Encentuate software. In mid-December, it plans to begin equipping an additional 100 PCs with RFID interrogators and security software.

To access the hospital's clinical system or other applications, a nurse or physician walks up to a kiosk and holds an RFID-enabled employee badge near its interrogator. The device reads the badge's unique tag ID number, which is correlated in Encentuate's database with that employee's information, including the specific applications that person is authorized to access. A user interface pops up on the kiosk's screen, prompting the user to enter a password. Once the correct password is entered, the user is presented with all applications he or she has permission to use.

A user who needs to walk away while working on a kiosk—for example, a nurse who is called to attend a patient down the hall—does not have to sign out before leaving the station. If the Encentuate software remains idle for two minutes, it will lock up the kiosk and a screensaver will appear on the screen. Then, if the user returns to the kiosk and no one else has used it in the interim, that person needs only hold his or her badge near the reader, and the system will automatically restore the previous session exactly where the user left off. If, however, another person walks up to the kiosk instead, that individual must hold his or her employee badge near the interrogator, then enter a password when prompted to initiate a new session.

"It used to be that when the IT team introduced a security system, things such as accessing applications would become a lot more difficult for users," says E.K. Koh, Encentuate's VP of products. "Now, this makes it much easier for users."

RELATED_ARTICLES In addition to providing secure access to applications within the hospital, Encentuate worked with EHMC to link the security system with the facility's virtual private network (VPN) secure remote access system. This enables doctors to log in via a Web browser from home or a private office to access the hospital's applications, and to still use the same password used on site (the remote access does not require an RFID-enabled badge, but users must key in their user name in addition to the password). Encentuate, which focuses primarily on the health-care market, has worked with other hospitals that also employ RFID to help secure their systems, though the company declines to specify how many.

According to Wilhelm, Encentuate has worked hard to meet the hospital's needs. "I find that they listen to what the institution has to say about what would make the product better," he states, "and so they are coming out with versions and releases that will take care of what I need. Whereas some of my concerns with the bigger [security] companies is that I was often told I would have to wait six months for a new release that would take care of the issue."

Copyright ©2005 RFID Journal, Inc. All Rights Reserved