May/June 2012 | Volume 8, Issue 3
www.mcdmag.com

MCD

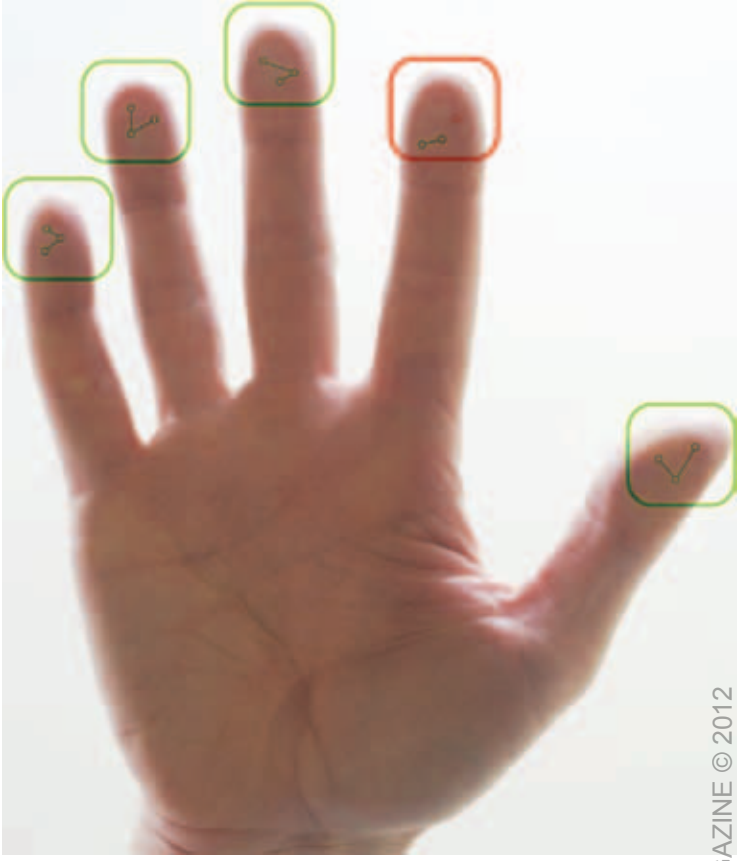
MEDICAL CONSTRUCTION & DESIGN®

THE SOURCE FOR CURRENT NEWS, TECHNOLOGY & METHODS

Susquehanna Health's $250-million redevelopment project serves community

RECREATING RURAL HEALTHCARE

FOCUS: HEALTHCARE INTERIORS | **SPOTLIGHT:** PATIENT SAFETY



Safe measures

Improved devices for patient, facility security

By Jim Otte

Hospitals would have to turn back the clock more than a decade to remember a time when the security and safety of patients was not nearly as important as caring for health. With the increase in both the number of security breaches in hospitals and the types of threats, patients' security is a major concern.

Complicating the problem is the fact that hospitals need to provide a high level of accessibility to the public almost around the clock. In addition, a wide variety of people make up the typical hospital environment — patients, staff, physicians, vendors and visitors — some of whom intend criminal activity. The hospital consists of many different rooms, types of spaces and entrances. Drugs are plentiful and many patients cannot walk unassisted or are vulnerable for other reasons. Unfortunately, security measures are often at odds with the popular trend toward making hospitals architecturally open, accessible and welcoming.

INTERNAL, EXTERNAL ACCESS CONTROL

One of the central issues in controlling access within a hospital is how to prohibit non-authorized individuals from entering a restricted area without impeding quick, easy access for hospital staff. A commonly used device has been the card reader. Each staff member carries a card or tag with credentials, which is swiped through a reader to gain access to an area. While this is an economical and easy-to-use solution, the fact that the cards can be lost, stolen or easily duplicated is problematic. If an unauthorized person has a card, the identity of the owner can be assumed, allowing movement throughout the facility.

In high-security areas, hand-recognition devices can be used in conjunction with card readers for dual authentication, however, both require physical contact and carry a risk of spreading germs.

If card readers are to be used, it is important encrypted smartcards are utilized with built-in authentication. This new generation of smart cards has challenge data bits communicated between the physical card or tag and the reader to verify the card is not cloned.

In high-security areas, dual-technology access control is recommended. In this case, the card reader is combined with another authorization device. Two options for the second device are key touchpads and hand-recognition devices. However, because both require physical contact, there is a risk of spreading germs. In addition, they are fairly easy to subvert.

The recommended technology to avoid these problems is a biometric iris recognition device. The individual looks into a camera that reads the pattern on the iris to verify identity. Without physical contact, it is difficult for diseases and bacteria to spread. However, the process is not instantaneous; it takes a few seconds to assume the correct position in relationship to the camera. Some hospital staff may feel this is a significant drawback because it lengthens the time it takes to respond to a patient in an emergency situation.

Future technologies will provide portable devices similar to handheld phones that will hold encrypted confidential patient information and will be used in place of access cards and tags. These devices, when placed adjacent to the card reader, will allow access. If dual authentication is required, the portable unit will display a touchpad. Entering the correct numeric value will unlock the respective door. The advantage is, unlike a wall-mounted touchpad, an observer will not be able to see the handheld portable display. This system uses challenge phrases and will also be used as a means to receive and transmit data from the patients and staff.

CCTV CAMERAS

Cameras have historically been used to detect intrusion in various areas of the hospital. This was accomplished by having a security officer watch banks of CCTV monitors and was not very effective. Advancements in technology enable cameras to monitor the field of view by themselves and detect unauthorized individuals, unauthorized activities and confirm all individuals have left an area. New CCTV cameras are able to create zones or areas in the field of view, including a virtual

fence that when crossed or penetrated causes an alarm. New pan/tilt/zoom cameras are able to change fields of view and can follow individuals and automatically hand off surveillance to the next camera. CCTV cameras also now have facial detection. Within a few years, facial recognition will be able to detect specific individuals that have threatened patients.

LOCKING MECHANISMS

One important aspect of access control is having secure and durable locking mechanisms. The amount of security provided, durability and cost vary. Electric-strike locks provide the lowest level of security and require the most maintenance, but do offer the benefit of low cost. Magnetic locks provide better security and longevity, but are more expensive and require additional safeguards. Electrified hardware offers the highest level of security and durability, and is also the most expensive option.

State-of-the-art card readers can be wirelessly integrated into the doorknob. In the future, cameras will be integrated into the locks as well.

ADVANCED SECURITY FOR INFANTS

The most vulnerable patient population from a security standpoint is infants. The circumstances of a hospital stay only complicate the safety measures required for protection. Maternity wards attract a great number of visitors. Because infants spend time in either the nursery or the mothers' rooms, it is more difficult to keep track of them.

Attaching a tracking bracelet, or tag, to an infant's ankle is a reliable way to know exactly where the infant is. Advancements in technology are adding intelligence to the infant tags and continuously monitor the infant's temperature, heartbeat and stress levels. Technology is now available that displays a floorplan in the mother's room, or other location, that shows the location of the baby and his or her current condition. The tag also transmits an alert to the nurses' station when an infant is moved when not scheduled. It will even detect if an infant is in a patient room other than the mother's. Any attempt to remove the tag or the infant from the maternity ward will trigger an alarm and engage locks on the doors. Hospitals are also giving family members tags as a means of controlling who is allowed to visit patients in the maternity area. The infant tags have the ability to transmit and will set off a local alarm if it senses there is no tagged nurse or family member present.

NEW GENERATION OF CALL BUTTONS

Hospitals are providing a wide range of patients with wireless call buttons. This provides a sense of security to patients who are able to move around without assistance, but might need help at a moment's notice.

Technologies are being implemented that enable patients' call buttons to be equipped with hi-tech digital functionality and two-way voice. When a patient presses the call button, the nurse receives a signal at the nurses' station and on their portable device. The patient information and exact location is displayed on a hospital floorplan so staff can quickly respond. Once a nurse approaches the patient, the call is automatically canceled and a list of responses and follow-up action items are displayed on the nurse's portable device.

These devices measure the amount of time that expires between the patient's call and the nurse's response. The system offers insurance companies, healthcare systems, hospitals, patients and contract staffing agencies performance reports. The goal is to make hospitals and nursing contract agencies aware of response times so improvements can be made if necessary. On any given shift, if response is poor, the supervisor is notified.

MASS NOTIFICATION SYSTEMS

Thanks to technological developments, hospital mass notification systems far surpass basic buzzer or chime alerts. These systems now inform the population via voice message the nature of the problem and the action needed to take. For example, the message may tell people a tornado has been sighted in the area and direct them to specific places to take shelter. Installations must pass an electronic intelligibility test to verify the message is clear and understandable. Future technology will allow the mass notification system to instantaneously detect if any individuals are still in evacuated areas or have not entered a protected shelter or muster area.

Several government agencies are advocating that first responder communication systems be installed in certain settings, hospitals for one. A distributed antennae system solves the problem of faulty two-way radio performance that can occur when communicating in large buildings or in areas with a significant amount of electronic interference. The result will be clearer communications both inside and outside the hospital, helping expedite the response to an emergency situation. Funding is available to offset the cost of these systems.

In deciding what measures to take to assure patient security, hospitals have to balance the priorities of various groups. While the CFO needs to scrutinize how these expenditures impact the hospital's budget, the security director will likely be an advocate for the highest level of security regardless of cost. Hospital medical staff and employees, on the other hand, may resist measures they feel could compromise patient care or timely response. With technology's pace of change, it is important hospitals partner with a firm that stays abreast of the pros and cons of leading technologies.

Jim Otte, NICET IV, is a data/fire/security specialist at SSOE Group. With more than 25 years of experience, he specializes in the engineering and design of complex data, fire, security, sound and telecommunications networks. He can be reached in SSOE's Toledo, Ohio office at 419-255-3830 or by email at Jim.Otte@ssoe.com.