Wireless lock technology, innovative locking mechanisms and multipurpose smart cards are just a few of the innovations bringing increased safety and security to facilities operations today. At the same time, Web-based solutions are allowing facilities to access and control their security systems from virtually any location that is connected to a hospital’s network.

This more integrated approach to managing security and access to facilities has given many hospitals greater control over their environments and made it easier to prevent security breaches. In addition, major changes in health care occurring with the Affordable Care Act have led many organizations to reassess their security strategies to handle potential increases in patient flow.

“In addition to requiring security technologies that comply with the newest legislation, the Affordable Care Act means that facilities and their security technologies must be highly integrated and able to provide quality of care and patient satisfaction to accommodate an increased flow of people into the system,” says Paul Baratta, global commercial leader, health care, Stanley Security, Indianapolis.

Hospitals now are required to quickly control and restrict access (lockdown) in one particular area or...
simultaneously throughout the entire facility in the event of a natural disaster or other emergency, according to Lisa B. Pryse, CHPA, CPP, president, ODS Healthcare Security Solutions, Richmond, Va. "The hospital must be able to manage access as well as identify persons who come in and out of their facility during this type of event."

**Impacting health care**

James McGowan, vice president of sales and marketing for CyberLock Inc., Corvalis, Ore., sees two access control trends impacting the health care arena:

- Multipurpose smart cards are being used to provide access control, ID, time and attendance functionality.
- There’s also a push for systems based on an open architecture, which provide a measure of future-proofing to ensure that new features and capabilities can be added to systems over time.

A growing number of applications for which credentials are used in health care facilities is another trend, says Ann Geissler Timme, health care marketing manager, Allegion, a spinoff of Ingersoll Rand, based in Carmel, Ind.

“To meet that need, the aptiQ smart credential allows employees to use the same card for various applications they encounter, which creates a more efficient and secure organization. Because of its open-architecture design and fast data transfer rates, the addition of applications beyond security is encouraged.”

Wireless integrated locksets that allow a single device to be installed at a door location and provide all of the functions of access control — such as a card reader, status switch, request to exit and locking hardware — are becoming more prevalent in hospitals, according to Shawn Hanrahan, security account manager, Schneider Electric, Dallas. Because these devices operate on a wireless network, they eliminate the need for costly infrastructure requirements such as cabling and electrical rough-in.

“'The most significant trends we see in
access control for hospitals are related more to software than hardware," says Fernando Pires, vice president, sales and marketing, Morse Watchmans, Oxford, Conn. "The locking devices have not changed as much as the means by which they are networked, managed and controlled. More access control solutions are striving to achieve some level of physical identity management and verification beyond simply allowing access and egress based on physical keys, traditional access cards or readers, or other forms of proximity devices.

These are areas where we are enhancing our key control software to accurately manage who has access to keys, what areas they have permission to access, and when keys are logged in and out of a KeyWatcher system. We also are seeing a rise in demand for biometric devices such as fingerprint readers to verify the identities of people requesting key access.”

Security integration is the main feature of new locking mechanisms available from Medeco Security Locks Inc., Salem, Va., says Joseph Kingma, vice president of the high security after market group. “The Medeco M100 and K100 with Aperio technology integrate into an existing or newly installed electronic access control system,” he notes. “The Aperio products communicate wirelessly to a hub, which connects to the access control system using RS485 or Wiegand wiring. Support for HID 125kHz proximity or 13.56 mHz iCLASS allows for integration into the majority of access control systems.”

Wireless solutions for closing and locking doors represent a trend, says Richard Nortier, marketing manager, Siemens Industry Inc., building technologies division, Buffalo Grove, Ill. “In the past, the cost to run cables and power to a door — especially one that is remote — proved challenging. Now, battery-powered, offline solutions provide improved security and audit trails for these doors and may prove more cost-effective over the long term than hiring security guards or maintaining keys and locks.”

**Wireless technology**

In the arena of access control, wireless technology, mobile devices and Web-based applications are gaining acceptance in health care, according to manufacturers that supply the nation’s hospitals. “Historically, wireless locking technology has taken longer to complete the necessary communication and subsequent locking actions,” says Pryse. “However, there now exist modular wireless locks that work on an active signal principle, checking for commands every few seconds, versus only upon a request that could take minutes to initiate.”

Wireless locking is replacing traditional cipher locks, adds Baratta. “Stanley’s EL Series electronic lock provides a low-cost application for storage closets and other areas that do not require a wired lock, but...”
MULTIPURPOSE SMART CARDS are being used to provide access control, ID, time and attendance functionality.

still provides an audit trail for entry,” he explains. “Wi-Q is a wireless locking system that integrates with access control.”

Smart cards and multitechnology card readers are a positive addition to the hospital environment, experts agree. They allow for the integration of existing technology to multiple security access system technologies (e.g., biometrics and access control numbers), says Pryse. “Many existing facilities’ systems may be upgraded with the new output technology, which is now able to interface with nearly all access control systems.”

Shane Meenan, area general manager, advanced services, Tyco Integrated Security, Norristown, Pa., agrees that smart card technology is gaining broader acceptance in hospitals. “Multitechnology card readers have been widely accepted for some time now,” he notes. “Utilizing a single credential for multiple applications such as declining balance for POS, time and attendance, electronic security, logical security for clinical applications and single sign-on are all means of leveraging smart card and multitechnology credentials.”

Hanrahan agrees that smart cards and multitechnology readers are becoming an industry standard within health care facilities. “Specifically for health care, it is critical because doctors and staff members typically need access to multiple buildings that may not be tied into the same security system,” he explains. “A multitechnology reader allows [each] staff [member] to carry one access badge that will work on multiple systems.”

Because multitechnology readers work with magnetic strip, proximity and smart cards, hospital employees can use their current credentials while migrating to smart credentials at their own pace, says Geissler Timme. “When their switch to smart cards comes about, they will not have to reinstall their facilities’ readers, and the transition will be seamless to their user base.”

Wireless devices have gained widespread acceptance in health care environments, agrees John Piccininni, CSCIP, vice president of business development, Identive, Santa Ana, Calif., noting that many hospitals use smartphones as staff notification devices, and tablets as primary data I/O devices. “There is still some wariness about Web-based applications, due to the regulations that govern protection of patient data,” he notes, “but technology and IT staff are learning how to enhance data protection. For example, public key infrastructure, or PKI, smart cards can be used to provide strong, certificate-based authentication to mobile devices and Web applications, and to encrypt files, local drives and even email, securing data at rest and in transit.”

How do access control systems manage the data they collect? Access control systems typically store the information locally in a relational database, says Nortier. “However, it is important to realize that more than just collecting and managing the data is involved — it involves logging every event, time and date stamp, and user.” A better goal is to convert the data into actionable information and leverage it to run the facility more efficiently using analytics and reporting. This can help facilities managers to identify trends related to the flow of people into and out of the campus, he adds.

Biometric options

The area of voice and facial recognition systems is an intriguing one, but one that is still under development, experts agree. “Voice and facial recognition systems, though slowly entering the market, are not considered mainstream and tend to have an unacceptable level of false reads,” says Hanrahan. “As a result, most health care customers do not consider them viable at this time.”

In the area of biometrics, a number of offerings in facial and iris recognition systems are available, according to Nortier. “We see more interest in iris scanning, but not wide-scale deployments,” he says. “Biometrics come with a higher installed price and so are generally left for locations needing higher security such as research areas and data centers — areas that, if breached, could adversely affect the business continuity.”

Geissler Timme agrees that voice and facial recognition biometrics are not widely used in hospitals today. However, many health care facilities employ biometric hand geometry systems for time and attendance. For example, she says, one health management organization with more than 1,000 staff members is using eight Schlage HandPunch biometric terminals in conjunction with a Legiant Timecard system to provide time and attendance reporting. “The system saves this long-term care provider 30 hours each payroll period just in totaling time-cards and eliminates fraudulent ‘buddy-punching’ practices,” she notes.

Looking ahead

Peering into the future, real-time location systems (RTLS) will play a bigger role in hospital security, according to Baratta. “The future of health care security technologies lies in the installation of RTLS, which allows facilities managers and administrators to track patients, staff and assets using the facility’s WiFi network. RTLS also allows for emergency notification of staff with real-time location and alerts.”

The near future will see the replacement of traditional RFID with RTLS for infant protection, patient wandering and, in cases of behavioral and elopement threat patients, a tracking device to alert staff immediately of such incidents, he adds. HFM

Neal Lorenzi is a freelance health care writer based in Mundelein, Ill.