should be kept to a minimum and each should have a card reader to allow access only to authorized employees.

The access control system will provide an audit trail of who entered the pharmacy and when. Video surveillance is also essential and may deter abuses of pharmacy resources. Cameras should be mounted to monitor the work areas and entries. In addition to standard access control and security technologies, advanced inventory management applications are available to not only restrict access to controlled substances but also provide patient accounting and medical records management.

Other critical areas that require video surveillance are elevator banks, waiting rooms, hallways in public areas, nurses' stations on each floor and entries to areas such as surgical suites and the nursery. All video should be transmitted to a central security station, where it will be recorded for investigative purposes. The station should be staffed at all times in order to respond immediately to alarm situations. By monitoring live video during a crisis, the attendant can help direct fellow security and law enforcement officers during the emergency.

Protecting Patient Information

A host of state and federal laws and regulations now require careful protection of private patient information. Data centers and record rooms should be treated much like a pharmacy — with limited entries, access control and cameras mounted to see who comes and goes. There are numerous regulatory and technology initiatives to convert hard copy patient information to data, making the convergence of physical and logical (data and network) security not only desirable, but a necessity. The "file room" of days gone by will become the computer workstation or handheld computer in the future, making data more readily accessible and making security and protection of medical records a united effort of both security and IT professionals.

Integrated Access Control

All employees, doctors and long-term contractors should be issued an access credential that they are required to display at all times, with the credential also serving as a visual photo identification badge. In addition to the previously mentioned use in pharmacies and patient record areas, an access control system can be deployed throughout the facility for control and management purposes. Each user should have customized access only to those areas required for them to complete their current assignment. For instance, doctors may be allowed to access elevators to surgical suites and any other patient care areas, while a maintenance worker's card may not allow entry to the data center. The system should allow access to be coded not only for individual location, but also by day and shift, job classification, certification currency, etc. The system may also be integrated with time-and-attendance functions, parking access and logical access functions for computer sign-on.

A highly integrated access system may help to track the movement of employees or other vital medical personnel. In an emergency, it would be helpful to know if a doctor had arrived at the hospital and in what department he or she is currently working. RFID-based tracking systems are also helpful for monitoring wandering patients, infants and portable equipment.

Stories of newborn babies being taken from a nursery make national news. That is

Compliance Scorecard

Security Leadership Solutions Executive Council

Stimulus Bill Tightens HIPAA Privacy Requirements

By Marleah Blades

Early this year, the healthcare industry watched closely as the U.S. House and Senate debated and passed the Federal economic stimulus bill, the American Recovery and Reinvestment Act of 2009 (ARRA). The bill, which was signed into law on Feb. 17, allocated nearly $30 billion for the improvement of the U.S. healthcare system, much of that coming in the form of grants and incentives to encourage the development and adoption of healthcare IT for digitized health records.

Clearly, implementing an industry-wide system of electronic health records will require even tighter security and privacy protections than those set forth by the Health Insurance Portability and Accountability Act (HIPAA). That's why Title XIII of the new law, called the Health Information Technology for Economic and Clinical Health Act or HITECH for short, amends HIPAA and adds new privacy and security stipulations.

Under HIPAA, the business associates of covered entities had to be contractually obligated to protect PHI (protected health information) to HIPAA standards, but these business associates were not directly subject to HIPAA themselves. This meant that if a business associate violated HIPAA privacy and security requirements, they would be liable for breach of contract but not subject to regulatory fines and penalties. HITECH changes this, placing the business associates of covered entities directly under HIPAA privacy and security rules, as well as the related enforcement mechanisms and penalties for non-compliance.

HITECH requires covered entities to notify individuals if their PHI is compromised in a data breach. No federal requirement for data breach notification previously existed in the area of healthcare information. The Department of Health and Human Services (HHS) is still developing final regulations for this requirement, but as of this writing, breaches will all need to be reported to HHS (the deadlines for reporting vary based on size of breach) and large-scale data compromise will be posted on the HHS Web site for the public to view.

Until now, the Department of Health and Human Services was authorized but not required to audit for HIPAA privacy and security compliance. HITECH mandates periodic audits.

HIPAA set down civil monetary penalties for fraud and abuse violations. HITECH requires formal investigation and penalties for "willful neglect" and amends HIPAA to include a tiered penalty structure based on the severity of the violation.

These are the provisions garnering the most attention; other changes are included as well. These new requirements are scheduled to take effect on Feb. 17, 2010 — giving covered entities and their associates one year from the law's inception to comply.

Marleah Blades is senior editor for the Security Executive Council (SEC). The SEC maintains a large and growing list of laws, regulations, standards and guidelines that impact security (https://www.securityexecutivecouncil.com/public/lrvc). Help the Council fill out the list and receive a selected complimentary metric slide from our store.