Identity and Access Management for Hospitals

Single sign-on and identity and access management software suites ease the administrative burden of changing employees and improves security and compliance.

You may think you've seen the last of a departed employee, but if your hospital doesn't have a comprehensive identity and access management plan, you may be vulnerable to a security breach.

"The disablement of user accounts during the employee termination process is a gaping flaw in most organizations' policy," said Kurt Johnson, vice president of corporate development, at Courion, a single sign-on and identity and access management software vendor.

Months and sometimes years after employees have left an organization, it's not unusual to see their names and personal information still floating around in various applications, he said. In some cases, former employees' accounts are still active, leaving a security hole.

"Access creep" can also happen as employees change jobs within the same organization, but retain access to applications and information that aren't appropriate for their new job roles, Johnson said. This is a huge security hole, he added, and one that many hospitals struggle to combat.

If an identity and access management policy is too lax, it opens up a hospital to data loss and security breaches since too many employees have access to sensitive patient data. However, if the policy is too strict, some employees who need access and do not have it will simply defy the policy.

"If doctors, nurses and caregivers aren't given access to critical care information, they are going to find a way to go around," said Johnson, in some cases by leaving one user logged into applications that contain sensitive patient data or by sharing passwords.

Eliminating "Post-it Note" Passwords

Johnson said Courion recognized that automating sign-on to applications and streamlining repetitive tasks like password resets, user provisioning and activation and deletion of accounts could strengthen identity and access controls and make it easier for hospitals to remain secure and HIPAA (Health Insurance Portability and Accountability Act) compliant.

Mark Jacobs, director of technology services, operations and security at WellSpan Health said Password Courier, which automates password reset and synchronization across health care enterprise systems, makes it easier for his physicians to manage their own passwords.

"Having a single password that can synchronize your access to multiple systems has definitely helped our organization," Jacobs said. In some cases, he said, patient data could be stored in as many as 15 to 20 different places, and remembering different passwords for each was a challenge.

The Courion SSO system garnered a lot of positive feedback from WellSpan clinicians, Jacobs said.

Rachel Heftler, director of client services and information systems group at Memorial Sloan Kettering Cancer Center, said Courion's Password Courier eliminated a huge security problem and made it simpler for personnel to follow security procedures.

"You don't see any more of those sticky notes with people's passwords on them," she said, adding that passwords can easily be reset by having the user answer "secret questions" online or over the phone.

Troy Hottovy, operations leader for technology management at Alegent Health, said that implementing Courion's Account Courier software helped take a huge administrative burden off the IT department. Account Courier automates account creation and management across health care IT applications.

With about 180 separate clinical, financial and administrative applications, adding personnel accounts and application access was tedious, and involved inputting information about a new hire by hand, which could take three to five days, Hottovy said. Even then, some personnel didn't have access to the applications they needed, and would often have to log in using a colleague's name and password while access was requested, cleared and granted.

"We can now provision applications right when Human Resources sets up a person for new hire orientation," said Hottovy. He said that Alegent is working on allowing application access based on an employees' role in the organization, as well as what floor the person is working on and what specific patients they need to see.

An oncologist, for instance, would be automatically granted access to a specific set of oncologic applications, resources and records. A charge nurse would have access to a different set of applications. Roles can be modified to fit the needs of individual hospitals, since personnel with the same title may perform slightly different functions at different care facilities.

Hottovy said implementing identity and access management software was a security process improvement, and that Alegent was also working towards physical access provisioning, or granting or denying access to certain areas of the hospital based on an employee's role and asset provisioning the hospital's laptops, smart phones and even cell phones.

Account Courier can also resolve security issues surrounding employee terminations that used to take days to disable a user's account. If an employee left the hospital, their accounts would have to be deleted one at a time, and information would have to be manually removed from each application.

"It's one thing if it takes time to get someone on board. But with terminations, you want that person off your systems as quickly as possible," said Heftler. Heftler said Sloan Kettering is in the process of implementing Account Courior, and she expects that there will be a much faster turnaround for access and account termination.

"With the Courion product, you delete that person in one place and it'll terminate their accounts in all the other systems," Heftler said.

No More "Who Did What and When?"

Identity and access management can also play a role in compliance issues. Heftler said Sloan Kettering is also working on implementing Compliance Courier to ensure security and privacy in the event of an audit.

"Until now all the audits we did involved the manual process of finding out who had access to what? Who authorized that access? When was it authorized? When was the last time they reset their password? Did they recertify their account access? When was the last time they recertified?" she said.

With Courion, Heftler said, security and privacy auditing will be much easier, since managers will have ready access to their personnel information, their roles and their access rights to information and applications.

"If a manager finds that somebody's got access they don't need, or doesn't have access they do need, it'll be a very simple to remove or add that access," she said.