

This story appeared on Network World at
<http://www.networkworld.com/news/2009/102909-novell-healthcare-organizations.html>

Healthcare organizations find security, privacy cures

Novell's single sign-on worked so well at Hartford Hospital, it scared some

By [Ellen Messmer](#), Network World

October 29, 2009 10:50 AM ET

Healthcare organizations are energetically seeking cures for managing identity and [security](#) in fast-paced hospital environments to help physicians and nurses do their jobs more easily -- and to keep patient data safe.

Sophisticated single sign-on systems are being deployed in hospitals to make it simpler for time-pressed physicians to find records, while encryption and data-loss prevention (DLP) technologies are being introduced as barriers to any chance of exposing sensitive patient data . That's more urgent than ever since a new federal law that's gone into effect, called "Health Information Technology for Economic and Clinical Health Act" ([HITECH Act](#)), forces healthcare organizations to make a public announcement through the media if they lose patient data that's not encrypted.

As such, the HITECH has become a driver propelling healthcare organizations into deploying new technologies, such as DLP, to try and make sure they're not among those forced into the harsh limelight of disclosing mishaps with patient data.

[Health privacy undermined: Worst breaches of 2009](#)

"We have two major systems being implemented right now because of the HITECH," says Ben Nathan, associate director for security and identity management at New York City-based Weill Cornell Medical College, affiliated with New York Presbyterian Hospital and other institutions. With HITECH in effect, "if we lose personal health information, the onus is on us to report it to everyone, and to the media."

The college is adopting a DLP system based on the [Symantec Vontu](#) product and is also deploying PGP Inc.'s encryption software on laptops. The medical college, which has 5,000 faculty and students, has already put in place an electronic- records monitoring system based on vendor [FairWarning's](#) surveillance and audit product that analyzes how individuals access data, with the goal of flagging suspicious activities.

"We want to know if someone who usually looks up 10 records a day is suddenly looking up 1,000," Nathan says. "Or if someone looks up data from another department. We at least need to know about it because maybe someone's account has been compromised."

Weill-Cornell Medical College is tying these data-security and [monitoring systems](#) back into its ArcSight security-event and information management system to centralize alerts and correlate information. It's the best method for understanding the risks and what's occurring, Nathan says.

It's not just the HITECH Act that's prompting healthcare organizations to usher in new risk-management controls.

Physicians and clinical support staff work in fast-paced environments, but getting into patient records and charts, where information is stored in various applications, is sometimes frustrating because it's necessary to remember a significant number of logins and passwords.

To meet that challenge and make life easier for medical staff, the Enloe Medical Center outside of Sacramento, Calif., has been putting in a single-sign on and provisioning system based on Novell's Role-based Provisioning and Identity Manager products.

Finding something better than multiple logins was "pushed by our physician community of 500 physicians," says CIO Jim Hauenstein.

But the complexity of putting in a full-fledged identity management and provisioning system -- which has run into the half million dollars and up range -- takes months, he says.

While the single sign-on piece was the first part of it to be put in place, allowing physicians to log on once to get access to many applications, there's still more work being done in what's known as application-context management. This lets physicians easily click from one page to another in separate applications to get information they need about a patient.

Complete identity management for automated provisioning and de-provisioning is yet another step. "It takes time and energy to build this," Hauenstein says, pointing out it's not a code-development issue but a process of designing templates and having software analysts create properly-coordinated systems.

But the benefit of the provisioning piece is that while it's usually necessary for someone to manually spend about seven hours setting up a new log-in for student nurses, for instance, the same process can take place in 30 minutes, and "de-provisioning is a quick process. We don't have to touch all the different applications," Hauenstein says.

Hauenstein cites openness for picking Novell for its [identity management](#) and provisioning project over [Encentuate](#) (now owned by IBM), Forward Advantage (specializing in healthcare-related IT) and [Sentillion](#).

"We wanted an open architecture that we could manage ourselves and we wouldn't have to hire experts for it," he says, noting the IT environment at Enloe is mostly Citrix and Microsoft software with HP hardware. "Novell fit into that world."

But ironically, it seems that advances in single sign-on and provisioning can have the unexpected impact of scaring those individuals that you would rather impress. That's what happened at Hartford Hospital, which also managed to set up single sign-on for physicians there using Novell's products.

After considerable effort establishing single sign-on, synchronizing Novell's e-Directory in Identity Manager with Microsoft Directory and setting up the right workflow, the demonstration of how it all worked for physicians at terminals ended up spooking some in the hospital's medical-records department, says Fernando Seguro, manager of systems engineering at the Hartford, Conn., hospital.

Seguro says some voiced concerns that doctors would walk away and not log off from applications exposing unified patient records, leading to a greater chance of patient data being compromised.

"So, we disabled the single sign-on six months ago," Seguro says. "It's a victim of its own success."

But he adds, "We can turn it back on at any time," and the hospital is pursuing the addition of other risk-management controls, such as proximity devices that will automatically log off systems based on detection of electronic badges, to allay any concerns about single sign-on.

[Read more about security](#) in Network World's Security section.