

SECURITY FOR THE MIDMARKET

# A CIO's advice for implementing single sign-on solutions

By Linda Tucci, Senior News Writer

For a relatively small medical center, Good Samaritan Hospital is a sophisticated user of medical technology. The 247-bed community hospital based in Vincennes, Ind., has had bar-coded medication at the bedside for nearly a decade. But capital IT expenditures compete with equipment such as CT scanners and lab analyzers that actually generate revenue. So when CIO Chuck Christian looked into implementing single sign-on (SSO) solutions a few years ago, the argument that SSO was prudent security for a HIPAA-regulated institution was compelling but insufficient.

Christian doesn't have IT money to throw around, recession or no recession. The CIO of Good Samaritan hospital and medical center, which serves five counties in west central Indiana and southeastern Illinois, runs IT with a \$3 million annual budget, a staff of 27 and an all-hands-on-deck approach. "I have two managers and everybody works," said the aptly named Christian, who develops software as needed and is deeply involved in IT purchases.

With SSO, "We needed to find something that fit into our budget and was not cumbersome to operate and maintain," he said. Many of the high-profile single sign-on solutions in the marketplace came with a lot of add-ons and

the assumption that if you bought the one, you bought them all. He needed a solution that integrated with Microsoft's Active Directory and allowed users to log on to workstations one time to be given access to all the applications they would need.

"We didn't want the one thing plus everything else. I just wanted the truck," he said.

He and his business analysts came across an article about an enterprise single sign-on appliance that was easy to use from Imprivata Inc., then a startup company in Lexington, Mass. "You could call it dumb luck." But the claim that the appliance would basically run itself was met with skepticism. "I told them we live a little bit too close to Missouri [the Show-Me state] to believe you," Christian said.

Imprivata sent out a technician with an appliance so Christian could try it out for 30 days. The technician arrived in the morning and by the afternoon, seven applications used by the clinical staff were ready to go. Christian's staff rolled it out to the nursing unit the next day.

"Things that work great for the propeller heads in the IT department don't necessarily transplant well when you move them out to clinical staff. We wanted user feedback," he said.

“  
**We needed to find something that fit into our budget and was not cumbersome to operate and maintain.**

Chuck Christian, CIO  
Good Samaritan Hospital

”  
With the SSO appliance, a client is loaded on each of the hospital's workstations and made active on those where users are likely to need access to multiple applications throughout the day. (However, it is not active on all of them, Christian said. "It does not make sense if you have someone, for example, in accounting who is going to use one application all day long. The security built in to that application is sufficient.") According to the Imprivata website, the administrator console provides a Web-based interface that makes SSO easy to install, configure and deploy. Users can log on to applications as always. The system creates unique strong passwords behind the scenes to ensure compliance and patient data privacy.

One lesson learned in the month-long trial was to keep the look and feel of single sign-on solutions simple, especially for users who might log on to multiple applications during the workday.

"We were trying to be a little bit too flexible at first. You can leave the workstation in a variety of ways when you sign off, and it was creating frustration with our physicians. We are all creatures of habit. If they are walking up to eight, nine, 10 workstations in a given day, and they are all a different state, even though they are secure, it causes confusion."

"We re-implemented it and took away the choices," he said.

Christian said he did not do a formal ROI for what was essentially a must-have tool that, in his setting, can save lives if it helps busy physicians and nurses log on faster; the SSO solution has reduced help desk calls for passwords. Another form of ROI is hiring nurses who are already familiar with it. Good Samaritan exports its clinical applications, including SSO, to the nursing program at the local university. "When they walk in the door, they know how to use it, which helps with out training costs," he said.

In the four years since rolling out Imprivata OneSign, the appliance has not required a lot of care and feeding, Christian said, even through four upgrades. And

single sign-on has become not only standard practice but also a critical layer of the security defenses at Good Samaritan. The tool allows Christian, for example, to change employee access to applications quickly, including cutting them off entirely.

"We have had employees who left under less-than-friendly conditions. We're a healthcare organization. We take a dim view of people who look at things they shouldn't have looked at," Christian said.

In addition to worrying about people inappropriately accessing patient medical records, IT must keep vigilant watch for people who want to steal patient identities for financial gain. The SSO appliance generates audit trails, allowing IT to track who logs into what — a point Christian makes clear during his orientations for new hires.

"I basically tell them Big Brother lives and breathes at Good Samaritan hospital and he is standing right in front of them. I explain that I have audit trails on every one of the systems, and I can tell what they looked at, how long they looked at it and from there they looked at it," Christian said. "The last person they want to see walk in their director's office is me with the audit logs, because they next person they're going to see are the folks in HR, as they are being processed out of the building."

## ADVICE FOR IMPLEMENTING SINGLE SIGN-ON SOLUTIONS

**1. Where does secure sign-on (SSO) fit in an IT security strategy? SSO is one component of a complete identity management program. "SSO is one of the security features that we leverage in all the areas where the equipment is used by multiple staff members, for multiple application access," CIO Chuck Christian said. "The ability to lock a workstation with one key and then have all the application protected is a real plus and requirement. With the standard Windows functionality, locking the workstation will not (in all cases) lock access to the applications that may have been left open/running."**

**2. Look for a tool that is appropriately sized for your organization. SSO comes with lots of bells and whistles. Enterprise single sign-on solutions that integrate with your existing identity management systems — in Good Samaritan's case, Active Directory — will save money and maintenance.**

**3. Kick the tires. Though the IT team was impressed by how easy it was to implement the Imprivata enterprise single sign-on appliance, the team tested the appliance for 30 days to elicit user feedback.**

**4. Keep it simple. For organizations whose staff log on to multiple workstations during the day, keeping the look and feel of SSO solutions the same is important, cutting down on confusion.**

**5. Talk policy, not just machines. Good Samaritan's CIO discovered that soft-peddling security policy does not work. He tells new employees that Big Brother "lives and breathes" at the medical center and the last person they want to see is him walking into their bosses' offices with audit logs. — LT**