



Health care update

Crystal Run Healthcare considers itself ahead of the pack in putting its hospital management into the hands of private practitioners and setting more customer-centric standards.

In fact, it is one of the first private practices to achieve Joint Commission Hospital Accreditation (JCAHO). But when it comes to security and compliance, old problems of monitoring legacy systems and integrating them into overall security architectures are holding Crystal Run, and others like them, from realizing the competitive gains of today's rich customer applications.

"We have a lot of examples of very nice technologies serving patients, but their features make them unable to monitor or manage in any way," says Miguel Hernandez, director of IT for Crystal Run Healthcare, with 150 physicians and 900 employees in seven offices in New York's Hudson Valley and Catskills region. "This creates challenges in workflow, security and authentication because these applications can't even support basic functions like encryption or the use of RSA tokens."

Despite these problems, progress waits for no one. Experts say that those who want to be competitive in the future must not only update or replace unmanageable legacy systems, they must also prepare their infrastructures for competitive applications that will open their protected medical information to outside parties and mobile devices.

"In this country we have some of the best health care in the world, but our delivery system is broken," says Jackie Bassett, founder and CEO of BT Industrials, an IT business strategy consulting firm in the Washington, D.C. area. "Organizations are blocked from innovating because of regulations. Executives still see security as a roadblock. They need to see security as a business enabler of competitive technologies, such as e-medicine."

Out with the old...

In the health care industry, it's not uncommon to see hundreds of applications in a single enterprise that cannot be properly monitored, audited or authenticated, say experts. Windows 3.1 applications are still around, and users are plugging floppies into medical devices, then carrying them to records for manual data input at some hospitals, says Mark Rein, senior director of IT at Mercy Medical Center, a teaching hospital affiliated with the University of Maryland School of Medicine that has 6,000 end-users.

Because many of today's medical applications were designed to address a quick line of business, tasks such as logging, monitoring and data control, as well as audit and security controls, aren't even an after-thought, says Ansh Patnaik, product manager at ArcSight, a security information management vendor. Some may need to be retooled, some can be connected — using tools such as ArcSight's flex-connector that talks to the native device structure instead of the application — and some might have to be replaced, he says.

"Buyers don't know to ask their vendors what processes are in place to compensate for the vulnerabilities in their systems," adds Daniel Nutkis, CEO, Health Information Trust Alliance (HITRUST), a Dallas-based private company building a common security framework for health care organizations and stakeholders. "Specialty application vendors don't disclose vulnerabilities like Microsoft does. And these apps discourage the use of strong authentication and other controls."

Hernandez says that what's needed is a clear way for medical technology vendors to follow the 10 commandments of all things security when building their applications. This, he adds, would enable them to be audited for compliance and compensating controls.

Improvements are coming. The Certification Commission for Healthcare Information Technology has tested and certified more than 100 e-health care products in ambulatory and acute care hospitals, to be followed by other medical settings, such as mental health.

But to address the security deficiencies of networks and applications, HITRUST hopes to establish the bar on security in health care, then use best practices and standards in a common PCI-like security framework applied to medical systems. Over the next year, Cisco Systems, Highmark, Hospital Corporation of America, Humana, Johnson & Johnson and other health care stakeholders are working through HITRUST to develop this framework. The goal is for these standardized practices to grow with the advent of new health information technologies.

Moving forward, organizations should also be preparing their infrastructures for new forms of business, say experts.

Large national care groups, such as Kaiser Permanente, have set the bar for the delivery of personal health records through secure portals where patients can get lab results and confer with doctors over a closed email system. Data exchanges, such as that of the Healthcare Data Exchange, are being joined by regional medical centers and large membership organizations, including Blue Shield of California. Insurers are already discussing reimbursement schemes for virtual office visits, according to an October article in *Modern Health Care*. And telemedicine applications, like HealthPia's GlucoPhone, are using cell phone-based blood sugar testing units to send data about glucose levels back to the doctors of diabetes patients.

"Telemedicine facilitates the visual portion of the diagnostic that a doctor can't get with just a voice call," says Josee Morin, president and CEO of Myca, a Montreal-based telemedicine application company. Myca, which already hosts a telephone-based dietary consulting application, is in discussions with UCLA for a clinical study to diagnose strokes and connect neurosurgeons to emergency responders over ambulance-based cell phones.

...In with the new

Enabling new technologies that will save lives with early diagnosis is the wave of the future, says Bassett, who recently co-authored a book, *A Seat at the Table for CEOs and CSOs: Driving Profits, Corporate Performance & Business Agility* (AuthorHouse). She adds that such applications will also provide a competitive edge to large, streamlined organizations.

However, most medical establishments fall below the standard set by Kaiser. They are not ready to deploy futuristic applications like telemedicine, say experts. Many, like Lincoln County Medical Center in Troy, Mo., are just bringing their email into compliance.

"Employees have heard about HIPAA and are afraid of prosecution, so they weren't even using email to send communications internally because they were afraid of leaking regulated data," says Ben Miller, IT technician at Lincoln County Medical Center, which chose ProofPoint Messaging Security Gateway, an inline encryption/policy enforcement appliance.

Others considering e-health initiatives are taking their time evaluating the security and compliance implications before they begin deployments, many say.

"People will start to demand computing everywhere," says Mercy Medical Center's Rein, who hails from a financial IT background. "As in banking, we're moving beyond, 'I want to bank on a portal,' to 'I want to bank on my phone.' The health care industry is moving in that direction. And, some would say that health information is more sensitive than your bank account."

Looking ahead

As a Microsoft partner, Rein is watching to see what Microsoft does with its HealthVault service announced in October, before making any concrete plans for advanced customer-facing applications. He's also paying attention to authentication of doctor access to exchange networks before he rolls out systems like e-pharmacy and other apps linking outsiders to internal resources.

For now, he protects internal resources from a mobile user population through NAC-enabled controls on endpoint devices using ConSentry.

"For the longest time, the health care industry has been the last frontier," adds Hernandez. "Because of today's compliance requirements, people are moving forward slowly as they become more concerned about patient information, how it's distributed and how it hangs around."

From the March 2008 Issue of SCMagazine