"We needed much more functional space and the ability to segment equipment, reduce noise and allow our dispatchers to focus on customers and provide the level of service required of a security operation of this size," Nerette says.

With such a large, functioning network of Intellex DVRs, Nerette and his staff worked with systems integrators Tesla Systems, (Georgetown, Mass.) and Team AVS (Westford, Mass.), to find a VMS solution that would allow the DVRs to be used in tandem with the new IP-based cameras and NVRs, as well as function as a platform for the future as the institute eventually migrates to a fully-IP-based solution.

Using the new victor unified video client and VideoEdge NVR from American Dynamics, all IP and Intellex DVRs' analog video streams from Dana-Farber's 500 cameras are seamlessly integrated into a single system and user interface. Instead of toggling between different applications on their monitors, dispatchers can be concerned only about the content of the video and fulfilling their regular duties — not which recording technology the video is being generated from. "This approach allowed the institute to extend the life of our existing Intellexes," Nerette explains. "Rather than rip-and-replace, we were able to focus our new investments on state-of-the-art IP technology as part of the Yawkey expansion. This let us strategically add IP cameras in additional key areas and save money."

The 200 new IP cameras at The Yawkey Center and a handful of other camera clusters are recorded on four VideoEdge NVRs from American Dynamics, with two NVRs for fail-over to ensure no interruptions in operation. On average, 30 days of video is stored per camera on the institute's 70TB of external iSCSI storage.

With dispatchers viewing some 60 cameras view up at any given time, those unified operations are crucial to the workflow of the command center, according to Robert O'Rourke, Account Executive, Tesla Systems. "One of the unique challenges of this project was to integrate the analog and IP video technologies to make them function seamlessly together," he says. "The command center has two 42-inch monitors and 14 other 20-inch screens, with video coming in from five remote locations, so there was a lot of complexity."

Another essential requirement of the system was the ability to easily share video with other users within Dana-Farber, all while safeguarding unauthorized views and exports of the footage. With victor's embedded policy management functions, Nerette is able to grant secure access to other users of the CCTV system — outside of the security and facilities maintenance divisions — to view video from specific live feeds or recorded video only from other areas of the facility from designated cameras. These groups also cannot export any video as part of the victor policy management deployment.

Security staff in the institute's command center will soon have even one less standalone system to monitor. With an upgrade to Software House's C•CURE 9000 security monitoring platform planned for sometime next year, Dana-Farber will be able to use the upcoming 2012 victor system as a single unified event and security management platform to integrate the card access functions, as well as fire and other building management functions, according to Tom Leonard, president of Team AVS. ▮

Security Leadership Solutions Executive Council

Medical Labs Could See Changes as a Result of Proposed HHS Rule

In September, Department of Health and Human Services (HSS) Secretary Kathleen Sebelius announced a proposed rule that could impact IT security and privacy requirements for medical laboratories.

Under existing Clinical Laboratory Improvement Amendments (CLIA) regulations, a lab may release patient test results directly to the patient only if the ordering physician expressly authorizes it or state law expressly allows for it. Twenty-six states do not have such laws, and 13 states prohibit patients from having direct access to lab results. Thus, most U.S. healthcare patients only have access to their lab results through the ordering provider.

While HIPAA privacy rules generally provide individuals the right to inspect and obtain a copy of their protected health information, in the case of labs they defer to CLIA exceptions and exemptions. The HHS proposes to amend the CLIA and HIPAA to preempt contrary state laws governing access to lab result reports, requiring labs covered by HIPAA to securely provide test results to patients or their personal representatives.

The proposal states that "covered entities, including CLIA and CLIA-exempt laboratories...must satisfy the verification requirement of § 164.514(h) before providing an individual with access. This requirement is consistent with the proposed change to the CLIA requirements, which would allow a laboratory to provide patients with access to test reports when the laboratory can authenticate that the test report pertains to the patient."

Authentication is one gray area some labs may see in the proposed rule. There is no guidance regarding authentication or verification in the proposed rule; in fact, the wording of the proposal seems to imply that existing lab authentication processes should be sufficient to authenticate patient requests for information. Whether or not this is the case has likely come up during the comment period, which ended November 14.

The proposal states that "that there are a total of 22,671 laboratories which provide approximately 6.1 billion tests annually in the 39 States and territories impacted by this rule . . . If the proposals contained in this rule are finalized, most of these 22,671 laboratories will need to develop processes and procedures to provide direct patient access to test reports." Those responsible for HIPAA compliance at these facilities should follow the progress of this proposed rule to determine the impact on their procedures and organizations. To view the proposal's September 14 entry in the Federal Register, visit http://www.gpo.gov/fdsys/pkg/FR-2011-09-14/pdf/2011-23525.pdf.

The Security Executive Council (www.securityexecutivecouncil.com) is a leading problem-solving research and services organization focused on helping businesses effectively manage and mitigate risk. Drawing on the knowledge of a large community of security practitioners, subject matter experts, and strategic partners, the Council provides strategy, insight and proven practices. Our research, services, and tools work to help security leaders initiate, enhance or innovate security programs; build their leadership skills; and bring quantifiable value to their organizations.

Access Control Gets the Job Done

Blue Cross & Blue Shield of Rhode Island deploys multi-functional access control technology

Blue Cross & Blue Shield of Rhode Island (BCBSRI) has played a significant role in both the health and economy of the state of Rhode Island since 1939. The organization's mission is to provide its members with peace of mind and improved health by representing them in their pursuit of affordable, high-quality healthcare.

BCBSRI needed to upgrade its workplace to a more efficient, secure, effective and sustainable environment. An in-depth analysis compared the feasibility of renovating several older buildings to constructing a new building. A benefit for the new building was the opportunity to install a completely new state-of-the-art system to dramatically increase security. Having a secure work environment is a major issue for a health insurance company in meeting HIPAA requirements, and can involve access control, visitor management and video surveillance.

To meet both HIPAA requirements and to create a streamlined work environment, the company looked to deploy a multi-function, high-security and user-friendly solution that integrated easily with other cutting-edge systems in the new building.

Another goal in this transition was to create an environmentally friendly and sustainable workplace. One aspect of this was to install multi-function printers (MFPs), something BCBSRI had been considering for 10 years. It was critical to have a security system that enabled the move to MFPs.

The company also wanted a one-card solution that opens more than just the door. They wanted the same card to be enabled for use with services such as cashless vending in the cafeteria, as well as for access control in the company gym and parking structures. In addition, BCBSRI wanted an elevated level of security in restricted areas, so a system enabling biometrics was also desirable.

Eric Caruso, of security systems integrator Team AVS, presented HID Global technology — iCLASS R40 readers and iCLASS smart cards — as the core of the access-control solution. The integrator also recommended using HID Identity on Demand (IoD) services to produce the new badges, thus simplifying the re-badging project and reducing the strain on company resources during the move.

In the old buildings, BCBSRI employees had a separate card for the cashless vending system that is already compatible with HID's technology, which made the transition simple and successful.

Now, employees carry only one card for secure access and cashless vending.

That same card also works for parking, gym membership, and printing, copying and faxing using the MFPs. When an employee sends a job to print, it sits in the cloud until the person arrives at the printer, scans their HID multi-purpose smart card, and requests the specific job to output.

"If we didn't have the HID cards, we couldn't have had the multi-function printers," says Tom Bovis, assistant vice president of Corporate Real Estate/Administrative Services for the organization.

As required by HIPAA, the cards also display the employee's photo. For those needing access to restricted areas, including the data center and cash processing, their cards also contain biometrics.

"People are happy with the system," Bovis says.

Migrating employees to the new smart cards was easily accomplished with the Identity on Demand services (IoD). Although BCBSRI had its own badge printer that would work with iCLASS, officials instead used a dedicated IoD project-management team to gather the necessary information and handle card production. IoD was able to use the photos and information in BCBSRI's existing database for the new cards, and it created custom card designs for various populations, such as employees and contractors. ▮