

# IBM Systems

M A G A Z I N E

Aurora Health Care uses PKWARE's SecureZIP  
to ensure that sensitive healthcare information  
is kept safe from prying eyes

BY JIM UTSLER

# Healthy Security

**C**ustomer information is important in every industry, but it is of foremost importance in the medical industry. After all, it contains many personal aspects of patients' lives, including medical histories, current medical status and personal identifiers such as Social Security numbers.

Thanks to the Health Insurance Portability and Accountability Act (HIPAA) of 1996, healthcare providers have become acutely aware of the importance of keeping that information safe from prying eyes. But as the Internet increasingly becomes a primary vehicle for data transfer, the safe-data directives of HIPAA can become a sticky issue.

While much has been made lately of misplaced data tapes—some even missing from the backs of trucks—Web-data transfers can be similarly insecure, even when steps are taken to safeguard the transmissions. Thankfully, tools are available that address many of these issues, helping ensure that even if a

## UP CLOSE

**CUSTOMER:** Aurora Health Care

**HEADQUARTERS:** Milwaukee, Wisc.

**BUSINESS:** Healthcare provider

**HARDWARE:** IBM System z9 z900 and z890 servers, as well as a number of IBM System i and System p servers

**CHALLENGE:** Meeting HIPAA requirements by safeguarding sensitive medical data

**SOLUTION:** Using SecureZIP from PKWARE Inc. to both compress and encrypt Internet-based data transmissions

transmission is hijacked, it won't be readable.

One such tool is SecureZIP from Milwaukee-based PKWARE Inc., which has been adopted by Aurora Health Care. Since deploying the solution, Aurora now not only has the ability to compress data for Web delivery, but also securely encrypt it. As Robert Burgess, supervisor of systems software with the healthcare company, puts it, "We can address two critical issues at once."

### Keeping Up with the Press

Aurora, also based in Milwaukee, services much of eastern and central Wisconsin, having—between itself and its affiliated Aurora Medical Group—13 hospitals, more than 100 clinics and about 120 community pharmacies. Its staff of about 25,000 includes more than 3,400 physicians, of which more than 680 comprise Aurora Medical Group.

The not-for-profit Aurora has grown a great deal over the years, beginning in 1984, when St. Luke's Medical Center and Good Samaritan Medical Center merged. Since then, its growth has been the result of "the building of new hospitals in new locations wherever it's warranted," says Burgess.

Running in the background are a cornucopia of servers, including IBM\* System p\*, System i\* and System z\* platforms, as well as several HP systems. The former two types of IBM servers are used for a variety of purposes, including time-and-attendance applications, WebSphere\* Application Servers (WASs) and MySQL database servers, but much of its primary

production takes place on the System z servers, including a z900 and a z890. Aurora is considering upgrading its older AIX\* boxes to System p5\* models and older OS/400\* servers to System i5\* models, citing the partitioning capabilities of the newer POWER5\* chip technologies as the reasons why. The company is also entertaining the notion of running AIX on the System i platform.

The z900 hosts a variety of what Burgess calls "legacy applications," as well as general ledger and payroll-processing applications, and the z890 hosts other legacy applications that have been re-engineered as Web applications. As Burgess explains, "These are J2EE-compliant applications that we host on an IBM WAS using Apache HTTP servers. We also run our own portal on that machine, and if it ever has a problem, we failover to the z900, which makes us capable of providing 24-7 availability."

Availability—whether for around-the-clock operations or not—is one of the vital services Aurora offers its patients. Because the organization has such a large presence, it has to make patient data available wherever it's needed, including its many hospitals, clinics and pharmacies. Before it digitized much of this information, this wasn't always so simple.

"If a patient had to go to another one of our hospitals, his charts or enrollment forms didn't necessarily go with him," Burgess recalls. "So he would have to re-enroll, which takes awhile."

In addition, some HIPAA guidelines require that that information be made readily available. If healthcare organizations don't follow those and other rules, they won't be certified as HIPAA compliant.

Part of this involves the transfer of data. Not only did Aurora want to make sure that its patients' records followed them, but also that it wouldn't have to rely on tapes to share data with other organizations—including insurance companies, banks, Medicaid and the state. And as anyone in the IT industry knows—if they've been keeping up with the industry press—tapes can be lost or stolen.

**Aurora undertook an effort to digitize most of its records to meet HIPAA guidelines, reduce its reliance on tape and, most importantly, make sure its patients had the records they need when visiting an Aurora-affiliated facility.**

## Avoiding the Headlines

Aurora undertook an effort to digitize most of its records to meet HIPAA guidelines, reduce its reliance on tape and, most importantly, make sure its patients had the records they need when visiting an Aurora-affiliated facility.

“We wanted a computerized patient record, so no matter which clinic or hospital they visited, the most current record would be available at the time of the visit,” says Burgess. “All patients have to do is present an ID card.”

That information is shared via a secure portal, making it largely safe from tampering or interception—but there was still the issue of the tapes that were sent offsite to other organizations. Wanting to avoid making the headlines, Aurora decided it might be better to share data via the Internet. Of course, the files are somewhat large, so it needed a way to compress them. Simultaneously, the organization also wanted to help ensure that if the information was intercepted in transmission that no one could access it.

To address this issue, the organization explored several options, including pretty good privacy (PGP) and PKWARE’s SecureZIP, which would compress and encrypt the data. Before deciding, however, Aurora brought what Burgess calls “all of the players” together to review their requirements. These players included Aurora staff working with clinical applications, general ledger and payroll. As Burgess explains, “We have to send information to the federal government, to the state for taxing purposes, and sometimes to the bank that provides that information to a state or government agency.”

Aurora also had to make sure the solution would work in its heterogeneous environment. So rather than having a tool for each individual platform, it would have one that would handle all of its compression and encryption needs from a centralized server. In this case, that turned out to be the z900, on which SecureZIP (the solution Aurora finally decided upon) runs. Aurora had already been using PKWARE’s PKZIP for more than a year before moving to SecureZIP about a year ago.

Now, the organization has a centralized tool that allows users of other servers to FTP their files to a z900 and have them compressed, encrypted and transmitted.

“We’re actually using the System z platform to host SecureZIP. So the other platforms basically FTP their information to the server. They can then choose to compress it, secure it or compress and secure it,” Burgess says. The


process of installing and configuring SecureZIP took only about a day to complete.

The z900 was chosen to host SecureZIP because it also has scheduling software running on it. When FTPs are received on the System z platform from the other servers, an automated action is initiated to send the file where it needs to go and then monitor it to ensure that the transmission was successful.

“They know when a file will be finished FTPing to the SecureZIP server, which gives them an approximate time when they’d like to send something off,” Burgess says. “So they tell us that time, we schedule it and the job runs for when they want it to. If there are no files there at the scheduled time, they would receive a notification that someone may want to look into why the process failed.”

Today, many of its previously shipped data tapes have been replaced with electronic transmissions. However, there are always holdouts when big technological and cultural shifts like this happen—but Aurora is hoping that they’ll jump on board soon, thereby reducing its reliance on tapes and couriers entirely. It currently has one data recipient that still requests tapes. To hopefully avoid the headline-making issue of misplaced tapes, Aurora has contracted with a courier company for dedicated, door-to-door runs. It’s also looking into the hardware-encryption capabilities of the System z platform to further secure the data on the tapes.

## Another Layer of Security

Aurora realizes that fewer bits of data are more sensitive than those of its patients. That’s why it’s taken the steps it has to ensure that the information is kept safe, no matter the form of delivery. Of course, because it has digitized so much of its operations (thanks in part to its desire to gain HIPAA-compliance certification), it only made sense to the company to look into Internet-based data transmissions. And thanks to SecureZIP, it can now not only compress files, but also encrypt them, adding yet another level of security to its operations. And as far as Burgess is concerned, “I’d like to see us exploit it more.” 



**Jim Utsler**, *IBM Systems Magazine* senior writer, has been covering the technology for nearly a decade. Jim can be reached at [jutsler@msptech-media.com](mailto:jutsler@msptech-media.com).