Why the growth? “The key driver is patient safety and improving the quality of care,” Holland explains. By this benchmark, much independent research supports the argument that IT’s a good investment. One example: a comprehensive study published by Florida State University researchers in November 2007 showed that patients treated at hospitals using IT systems have better health outcomes. Though the benefits are clear, healthcare IT leaders know their operations have room to improve: 40 percent in a recent CDW-sponsored survey said their industry lags behind others in adoption of IT.

CIO Digest talked with three healthcare IT leaders about five areas where an IT checkup might be in order: (1) managing an ever-growing number of computers and special medical devices; (2) securing sprawling infrastructures; (3) storing the vast amount of data that the practice of medicine generates today; (4) complying with ever-changing internal rules, industry standards, and government regulations; and (5) managing the communication environment that glues together these sometimes far-flung enterprises.

Management: Minutes versus hours
In modern hospitals, PCs and mobile devices have replaced the patient chart at the foot of the bed. Healthcare asks a lot of these computers; they not only deliver Electronic Medical Records (EMRs) and radiology images, but they increasingly provide all manner of communications. “I look forward to a day when I have exactly one device on my desk with which I can do all my work, as well as handle conference calls, phone calls, and videoconferencing,” says Yeman Collier, CTO of Peoria, Illinois-based OSF Healthcare System, which operates seven acute-care facilities and more than 50 other sites.
But when you require more tasks from a single device, keeping that device secure becomes even more critical. To that end, Mercy Health Services of Baltimore adopted Altiris Client Management Suite from Symantec to support about 2,500 PCs spread among 30-plus sites, including the 235-bed Mercy Medical Center. When a computer fails, Mercy Health’s 75-member IT staff knows immediately, and they can often rebuild the system remotely over the hospital’s network. “We’re talking a matter of minutes versus a matter of hours for a machine to be back up and running,” says Jim Stalder, senior vice president and CIO of Mercy Health. This improves productivity for clinical personnel, keeps patient care humming, and frees up IT staff time for longer-term, strategic projects.

The Altiris solution has had another benefit at Mercy Health, where the IT group is also responsible for biomedical devices such as heart monitors and IV pumps. Preventive maintenance cycles for these devices are also managed by the Altiris Client Management Suite solution; the system pushes necessary tasks—as the devices’ maintenance schedules mandate—to technicians, along with needed checklists and documentation. “Before, all that was either in someone’s head or done manually on a piece of paper,” recalls Stalder. (For more on biomedical devices and services, see the “Integrating Biomedical Services onto the Network” sidebar on page 20.)

Security: Culture shock

Many healthcare organizations extend beyond hospitals to neighborhood clinics, home-health providers, and off-site services such as radiology interpretation and medical transcribers. In this dispersed environment, EMRs are always on the move, and the security of critical infrastructure—networks, PCs, servers, databases, and more—becomes more difficult. Reinoud Reynders, IT manager for Infrastructure & Operations at Universitaire Ziekenhuizen (UZ) Leuven, a 2,000-bed university medical center in Belgium, sums it up this way: “Privacy is very important, so security is very important. It’s at the same level of importance as in a financial bank.”

The difference between a bank and a healthcare organization is culture. The medical community has traditionally resembled an academic environment more than a business, open to collaboration and information sharing. But the diversity of staff roles in healthcare compounds the difference: a medical researcher has different information needs than a cook in a hospital kitchen—but both may want to know what a particular patient ate on a given day.

Because of this special cultural environment, security in healthcare requires a fine-tuned balance between technology and human elements. Standard practices and procedures, such as antivirus software and firewalls, are mandated, Stalder says, “as they would be for any IT organization.” Likewise, securing email systems against spam is as advisable as bed rest and chicken soup. Spam is a time-waster for employees and can provide an entry point onto networks for malicious code, but devices such as the Symantec Mail Security 8300 appliance used by UZ Leuven can reduce a spam flood to an easily managed drip.

But the healthcare environment presents security challenges different from those faced in the corporate world: Collier points out that popular biometric authentication solutions can be less viable to implement because protective masks, face shields, and latex gloves can hinder voice-, retina-, and fingerprint-recognition systems. Other challenges arise from the growing number and variety of wireless biomedical devices, such as EKG, heart rate, and blood pressure monitors used in modern medical settings. Problems with radio frequency interference, device compatibility, patient privacy and device security are expected to grow as wireless medical equipment becomes common. Automated, centralized security solutions and endpoint protection—with particular emphasis on portable devices and unmanaged points of data leakage such as CD writers and USB drives—are part of the cure for healthcare’s security headache. However, they need to
be flexible enough to adapt to an institution’s particular culture and needs. And they need to be non-intrusive, thereby not detracting from clinicians’ productivity.

**Storage: Growing pains**

The need for data storage in healthcare doubles every 18 months. For example, picture Archival and Communications Systems (PACS), which handle digital X-ray, CT, and MRI images and use significant storage. These systems are also ubiquitous, used in nearly 80 percent of healthcare organizations today.

Other numbers also tell the healthcare storage story: UZ Leuven had half a terabyte of storage in 2000 but has half a petabyte today; at OSF, storage needs grow by more than 20 terabytes annually. Why? “It often seems that we are required to keep everything,” admits Collier, partly due to regulatory pressures.

OSF employs a multi-part cure for these growing pains: carefully defined storage policies; a tiered storage environment with online, nearline, and offline storage; and storage virtualization. “The intelligent indexing of stored data is one key to making the whole strategy work,” Collier says. “Better indexing means more accurate and timely retrieval, which can mean the difference between success or failure for caregivers making on-the-spot decisions.” At Mercy Health, Stalder has been consolidating disparate systems onto a storage area network (SAN) for about a year, a process that sometimes entails overcoming resistance from healthcare systems vendors.

But improving the storage environment means more than simply adding better storage hardware. Centralized, standardized storage-management software, independent of hardware and able to manage the diverse, heterogeneous environments that exist in real-world data centers, is an important ingredient in the ideal storage prescription. All three of the organizations interviewed for this article use Symantec Enterprise Vault, which provides several benefits, including maximizing utilization of existing storage, improving backup and recovery performance, and classifying structured and unstructured data to improve archiving and retrieval.

This last benefit is of particular importance to clinicians, who need the right information at the right time. “Medical information systems generate enormous data sets,” says John Moore, managing director of healthcare industry analyst firm Chilmark Research. “How you deliver what’s most important to a physician who’s looking at a given patient is not a trivial question.”

**Compliance: Anticipating change**

Healthcare storage requirements are often intertwined with compliance issues. How long information must be retained, who can see it, and who can retrieve it are questions healthcare organizations wrestle with every day, because of both internally generated policies and government regulations.

Reynders says regulatory challenges are greater in the United States and the United Kingdom than in Belgium and other European Union (EU) countries today, but that the EU’s rules are growing progressively more strict. “The only thing we know is that we don’t know what we have to do,” he says with a chuckle, but his underlying point is clear: regulations change, and they rarely—if ever—get looser.

As in data security, healthcare compliance efforts often require balancing technology solutions against human factors—in part because even in environments with mature EMR systems, some information remains on paper, and technology can’t keep paper from going astray. “Making sure people realize that compliance is a personal responsibility, versus a technology responsibility, is something that we strive to educate them on,” says Stalder.

Still, technology plays a role because everything IT can do helps clinicians to focus their energies on patient care. Automated tools can monitor access to critical systems, and management tools can keep systems patched, compliant with policies, and consistent across the enterprise. Collier says adopting an anticipatory strategy can help: “Maybe what we do now is enhance our ability to automate surveillance and audit reporting functions...
to help drive greater preemptive response,” he explains. “And I suspect that in the future there will be far more emphasis on employing those capabilities.”

**Communication: Shifting burdens**

Email use in healthcare is driven in part by the industry’s collaborative culture, and in recent years has been pushed farther by patients’ desire to communicate electronically with their medical caregivers. But increased email use has also become a burden for many healthcare IT departments. Reynders says UZ Leuven’s email system hit a tipping point when volume reached about a million messages a month for 10,000 users: every user encountered a corrupted mailbox about three times a year, and about 15 percent of UZ Leuven’s internal helpdesk capacity provided email support. In addition, an internally developed spam reduction solution captured just three-fourths of the 70,000 daily spam emails UZ Leuven received.

UZ Leuven’s 110-person IT team adopted a two-part cure for its email ills: Symantec Enterprise Vault (coupled with Microsoft Exchange and Network Appliance storage virtualization) to centrally manage email archiving, and the Symantec Mail Security 8300 appliance for spam reduction. The former reduced email-related helpdesk calls to 1 percent of total and cut email restore times by 50 percent. And the latter increased the capture rate for spam and virus emails to 99 percent, even as email volume and spam percentage increased by more than 700 percent.

Another email-related burden that weighs on some healthcare IT departments is e-Discovery, the process of combing through data (including email) for content related to litigation. Automating e-Discovery lightened that burden for OSF’s 348-person IT team and helped contain related costs. “The amount of manpower required to go through these e-Discovery efforts was monumental,” Collier says, but using Symantec Enterprise Vault rather than an outsourced e-Discovery firm reduced the cost by nearly 65 percent.

Mercy Health is also implementing Enterprise Vault and expects it will make email archiving, management, and e-Discovery a non-issue for users. “The burden on the user to manage where their email is, and how it’s being stored and sorted and archived locally, is largely gone,” Stalder says. Shifting this task from users—particularly clinicians—to IT gives Mercy Health employees more time to focus on patient care.

**Into the future**

While device management, infrastructure security, data storage, compliance, and communication management are major challenges in healthcare IT today, they’re not isolated from each other or unique to the industry. What may be unique to healthcare is the direction in which IT will be asked to evolve.

Our experts think many of the challenges that lie ahead revolve around data integration and data standards, especially as patients and consumer-oriented companies such as Microsoft and Google get involved. “Unless everybody agrees on a common approach to how you manage data, it’s virtually impossible to share,” Stalder says.

Collier concurs: “If we don’t figure out novel ways to make medical data solutions more seamless and integrated, then we lose.” But the payoff for doing so can be great. By helping clinicians to collect, share, and access knowledge, IT can enable the ultimate goal of everyone in healthcare: to improve people’s lives.

“If you can leverage the knowledge that represents the cutting edge of the profession, you have the ability to enhance the quality of care that every practicing physician offers,” says IDC’s Holland. “Then you can improve the health of the overall population.”

*CDW Healthcare Vital STATs 2008,* www.cdwg.com/vitalstats

Fred Sandsmark (www.fredsandsmark.com) writes about technology from his home office in the San Francisco Bay Area.