Technology Upkeep Is Up to You

By **Fred Gebhart**, contributing writer

Pharmacies rely on technology for every aspect of their operations: patient profiles, drug utilization reviews, adjudication, dispensing, clinical services, point of sale, inventory management, wi-fi, phone systems, safety and security, alarms, refrigeration temperature monitoring, bookkeeping, payroll. The list can seem endless.

No matter what promises vendors make about automated upkeep and maintenance, technology does not take care of itself. Human intervention keeps pharmacy systems up to date, secure, and running optimally. And human intervention means pharmacist intervention.

"We have to take a role in technology upkeep," says Eric Bandy, RPh, owner of Bandy's Pharmacy and Medical Equipment in Salem, IL. "Our four pharmacies suffer if software is not upgraded successfully. And if there is a problem, the pharmacist always has a key role. We are not big enough to hire an IT guy, so I'm the go-to guy for all our technology housekeeping."

Vendors can help, Bandy says, and many do help with automated data backup and software updates, telephone support, user groups, and more. But vendors can't do it all.


Bandy

"Pharmacists and vendors both have roles," says Paul Carrig, vice president of technology for PioneerRx, a pharmacy software company. "Dividing up those responsibilities depends in part on what technology you use. We recommend steps for the pharmacist to take to protect their network, but ultimately it is their responsibility to keep their business safe and secure. Consequently, PioneerRx employs many best practices to ensure our users are protected against risks and vulnerabilities."

In the Workflow

The upkeep of your technology has three fronts:

1. A daily data backup.
2. Regular updates.
3. Security, both physical and virtual.

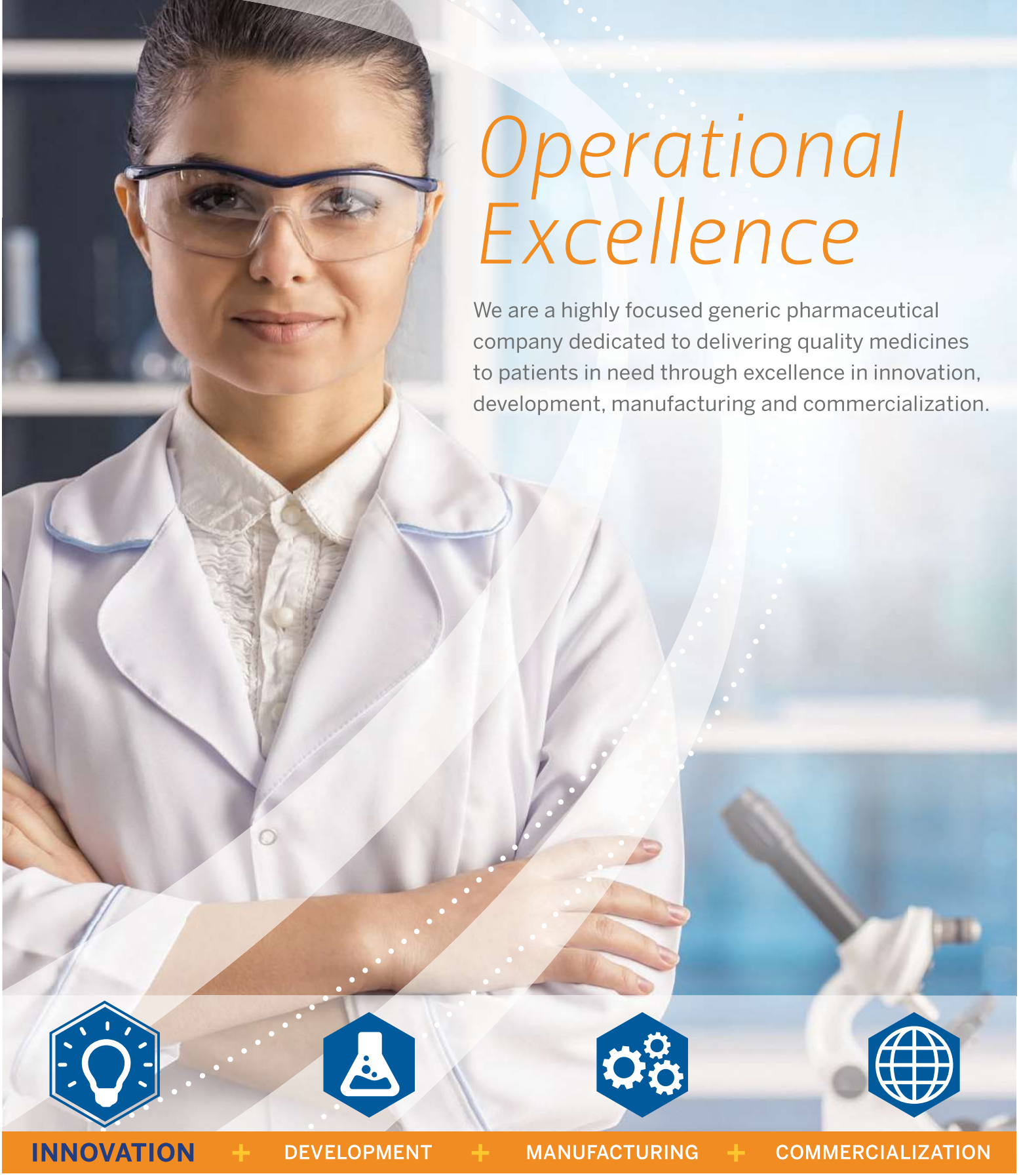
All three start with the pharmacist.

"Keeping your pharmacy running smoothly starts with recognizing that your technology is as critical to your operations as your staff is," says Robyn Ambers, a consultant with software vendor PrescsribeWellness.

"Engaging in using your technology, training on it, monitoring, and managing it is how you keep it running smoothly," Ambers says. "You can't ignore your technology any more than you can ignore your staff and expect them to function optimally on their own. Technology upkeep has to be part of your routine workflow."

CONTINUED ON PAGE 34 >

SIKOV/STOCK.ADOBE.COM



Operational Excellence

We are a highly focused generic pharmaceutical company dedicated to delivering quality medicines to patients in need through excellence in innovation, development, manufacturing and commercialization.

INNOVATION + DEVELOPMENT + MANUFACTURING + COMMERCIALIZATION

Providing patients and customers with uncompromising quality and value for more than 40 years.

PARPHARM.COM

PAR PHARMACEUTICAL
an endo international company

Advice on Best Practices

Data backup is your most important insurance policy. Back up all your data every night to at least two different locations, both physically outside the pharmacy—Tim Tannert, RPh, President, Framework LTC.

Trust your vendor, but verify every update because vendors can make mistakes, too. Test updates on a computer that is not part of your primary pharmacy operating network before installing on your primary system—Shantanu Bhide, VP of Technology, Framework LTC.

Tweak workflows and automate routine tasks. Think about simple workflow tweaks, such as automating state and physician reporting of immunizations, medication safety reviews, electronic calendars for medication synchronization and secure two-way texting for better patient engagement and reduced phone call volume—Al Babbington, CEO, PrescribeWellness.

Most breaches are inside your firewall. Never use or allow shared passwords and review all log-in activity at least monthly. Remove passwords as part of the outboarding process for every employee who leaves the pharmacy for any reason. And review cell phone, email and nonwork-related computer use policies quarterly—Al Babbington.

Keep your technology off the floor and out of the basement. A broken water pipe or a sprinkler system gone awry can flood floors and basement storage areas just as deeply as a hurricane or a rampaging river—Melissa Krause, PharmD, consultant and partner, Pharmacy Healthcare Solutions, Inc.

< CONTINUED FROM PAGE 32

Data Backup

Watching data backup is about as interesting as watching paint dry. That's why most vendors offer automated backup solutions.

"Doing backups is critical," says Christopher Antypas, PharmD, president and chief operating officer of Asti's South Hills Pharmacy in Pittsburgh. "The processing and dispensing of medications is the primary piece of what we do. If we were to go down, it would be crippling for us and for our patients."

Antypas

Asti's is three pharmacies in one, a retail operation that does 800 to 1,000 scripts a day, a closed-door long-term-care pharmacy, and a specialty pharmacy that delivers most of its scripts. Antypas backs it all up every night locally and remotely through his vendor.

Other pharmacies use public cloud backup for businesses such as Amazon Web Services or Microsoft Azure Cloud. They send nightly data backups to the cloud, a generic term for servers owned by Amazon, Microsoft, or other vendors which typically store data in multiple locations to increase reliability.

Business-focused cloud vendors offer high data-transmission speeds for quick backup. More importantly, they can provide quick downloads to restore data and get the store up and running in hours. Consumer-focused cloud backup is far cheaper, but downloading to restore data can take days at the transmission rates for consumers.

Backing up only at the pharmacy is as bad as not backing up at all.

"If you make a physical backup on site, you have to physically remove it from the location," says Tim Tannert, RPh, president of software vendor Framework LTC. "We've had pharmacies store their backup in a safe in the store. And when the building caught fire and the safe got hot and the backup media melted, it didn't help them much."

Updates

Updating software and hardware is a must. Skipping updates can mean missing out on regulatory changes and falling out of compliance.

The top priority of software vendors is updating their systems and apps to comply with new regulatory requirements, notes Shelly Spiro, executive director of the Pharmacy HIT Collaborative. The group develops health information technology standards that are used throughout the industry.

Skipping updates is also a good way to open your system to attack. Security patches are among the most common software updates. IT security is a cat-and-mouse game with would-be hackers searching for vulnerabilities that open doors into systems. If your system has gotten old enough, vendors stop updating them, which may be a signal that you need to upgrade to a new system.

Pharmacies provide two good targets, warns Shantanu Bhide, vice president of technology for SoftWriters Inc. One is your business and financial information. Hacking into your point of sale system, ordering, adjudication, payroll, or other areas can reap healthy profits for the computer criminal.

Personal health information (PHI) has also become a valuable commodity and pharmacies store vast amounts of PHI, the protection of which is governed by HIPAA regulations. A break in—either virtual or physical—can result in a loss of data, which hurts the pharmacy's reputation, future business, and bottom line. The fines imposed for

"We've had pharmacies store their backup in a safe in the store. And when the building caught fire and the safe got hot and the backup media melted, it didn't help them much." TIM TANNERT, RPH

failing HIPAA data protection requirements can be painful.

Accept your vendor's updates, Bhide advised. And verify them. "We have seen customers accept a patch, maybe a firewall update to make the system more secure, and it changes access all over the system," he cautions. "Installing patches is a good thing, but check it out on a test system first to be sure it is not affecting your workflows. Push patches out to your production system only after verification."

Security

For all the attention focused on hacking and data theft, the reality is that most security breaches are inside jobs; employees or former employees, who steal data or who inadvertently open the way for someone else to hack in. Creating a secure environment starts on the inside, too.

The Ohio State Board of Pharmacy, like many state boards, requires positive identification of the responsible pharmacist on every prescription, notes Randy Myers, PharmD, owner of Harry's Pharmacy, an independent pharmacy that was founded by his grandfather in Carey, OH.

How to verify identity is up to the pharmacy. "In our system, everybody has a logon and a password," Myers explains. "I give out the logons, but employees choose their own passwords. Everyone has a specific security level based on their duties. I have friends who have gone biometric with fingerprint scanners. You can scan a badge and type in a password, there are a variety of approaches."

Staff education is a key element. Tricking or fast-talking someone into revealing confidential information, a practice called phishing, remains among the most successful attacks, Carrig says. Phishing, via web or email, is responsible for most data breaches today, he says. There are numerous email and web filtering tools to help reduce risk from phishing attacks.

"Installing patches is a good thing, but check it out on a test system first to be sure it is not affecting your workflows. Push patches out to your production system only after verification." SHANTANU BHIDE

"Nobody legitimate should unexpectedly be asking to provide sensitive information in person or electronically, or ask to install software on your network," he says. "If in doubt, always contact the requester directly to confirm the outreach is genuine. We encourage pharmacies to prohibit allowing staff to perform personal activities or download unapproved software on pharmacy networks. Everybody is better protected that way."

Not sure if you're ready to take on technology upkeep? Then you should start learning.

"We didn't go to pharmacy school to learn computer systems," Myers says. "But our businesses and our patients depend on those systems. Managing technology is every bit as important as managing staff." ■

Tech Upkeep in Chain and Health System Pharmacy

Technology upkeep typically falls to the owner in independent pharmacy, but life is different in the chain and health system worlds.


Krause

Chain pharmacists have it easier, at least in this area. They aren't allowed to do much except maintain the physical operating environment. "Chains are generally handling the technology, updates, and maintenance at the headquarters level," says technology consultant Melissa Krause, PharmD, Consultant and Partner, Pharmacy Healthcare Solutions, Inc. "The technology is pretty much locked down. Chains rely on the pharmacist to literally keep things clean, well ventilated, away from temperature extremes, and protected from environmental hazards."

Life is more complicated for health system pharmacists. Ideally the hospital or health system has an IT department with help on call, but don't count on IT people to know much about pharmacy operations needs or pharmacy technology without help. Health system pharmacy must proactively take a seat at the IT table so that its specialized needs will be met.

"ASHP's statement on the pharmacist's role in clinical informatics calls for pharmacy informaticists to lead as well as manage the risks and changes associated with the implementation and continuous improvement of clinical information systems," says Amey Hugg, PharmD, director of the Section of Pharmacy Informatics and Technology at ASHP. "It's about how you communicate with the nonclinicians in IT.

"Medications touch everyone regardless of the department. It is a multidisciplinary effort to create and maintain a successful medication use cycle. Our role in pharmacy and pharmacy informatics is to help IT care as much about pharmacy technology as we do," says Hugg. ■