Protecting Labs Against Cyber Threats

FIVE EXPERT TIPS

1. **Keeping systems up to date and free of any vulnerabilities** is at the top of the list to avoid security breaches, but is easier said than done. It requires constant monitoring of connected devices, operating systems, and programs for updates, patches, as well as unnecessary files or users.

2. **Enabling two-factor authentication** is something that comes up repeatedly in conversations about cybersecurity, and many hospitals have already jumped on board. But some smaller organizations still need to catch up. Two-factor authentication requires something in addition to a PIN or password to access data, such as a physical card or badge, or a user's voice or fingerprint.

3. **Setting up your system to be able to manage isolated breaches** is one way to avoid downtime in patient care. "You have to build processes into the design so that a single point of failure won't result in downtime," said David Robb, manager of laboratory information systems at Sutter Health in Palo Alto, California.

4. **Training end users is essential**, according to David Finn, the healthcare IT officer of Symantec. He suggested training lab workers who may not regularly interact with IT about what to look out for and how to alert IT about problems that could indicate security breaches. "End user training is the biggest bang for your buck when it comes to cybersecurity," he said.

5. When it comes to buying new lab equipment, **choosing devices carefully** also goes a long way, Robb noted. Red flags include vendors who use out-of-date software themselves, or vendors that rarely issue patches for security holes. "When you pick instruments, you should pick them as a package with redundancy and the operating system in mind," Robb said.