HEALTHCARE SECURITY

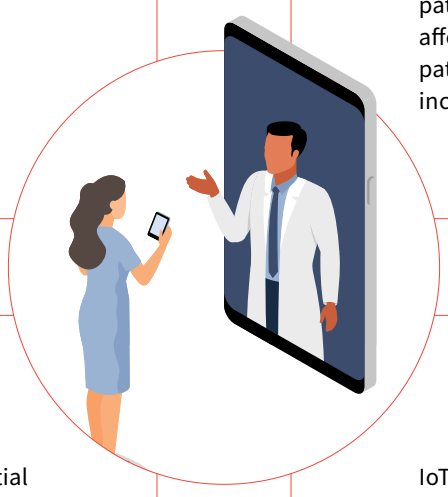
# Top 10 Ways to Improve Healthcare Security

## Don't be a defenseless target.

1

### Availability

Systems availability and reliable access to information are critical. Implement state-of-the art IT and cybersecurity tools and support to ensure life-saving data, devices and systems are reliable.



2

### Legacy applications

Software updates and patching are one of the most basic security measures you can take. Unfortunately, sometimes patching means losing support from a vendor, which can affect the regulatory status of devices and systems. When patching isn't possible, consider network segmentation and increased monitoring.

3

### Malware

Ransomware is one of your top threats, and has the potential to cause significant damage if critical systems and devices are affected. In addition to a strong backup and disaster recovery process, implement ongoing security awareness training to improve your defenses.

4

### The Internet of Things

IoT has introduced a plethora of network-connected medical devices, bringing both clinical benefits and security risks. Ensure your network can identify mobile devices as they connect and apply security policies dynamically.

5

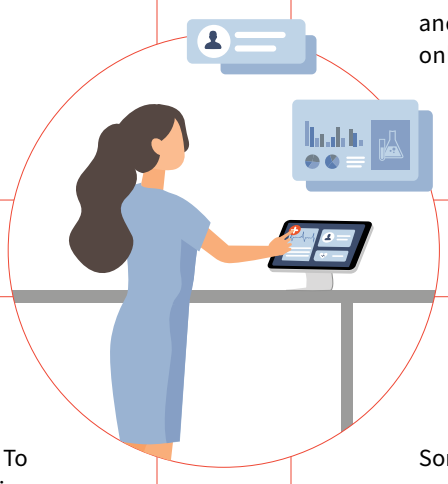
### Vendor risk management

As organizations merge or decentralize functions to improve efficiencies, different vendors enter the picture. Prepare for this shift by performing thorough security due diligence on key vendors and implementing business associate's agreements.

6

### Identity management

Identity management is one of your best defenses. It allows you to see not only who is trying to access your network, applications and data, but which geographic region that access request is coming from, at what time, on what device, and in what way. This information makes it easier to ensure only authorized people and devices have access.



7

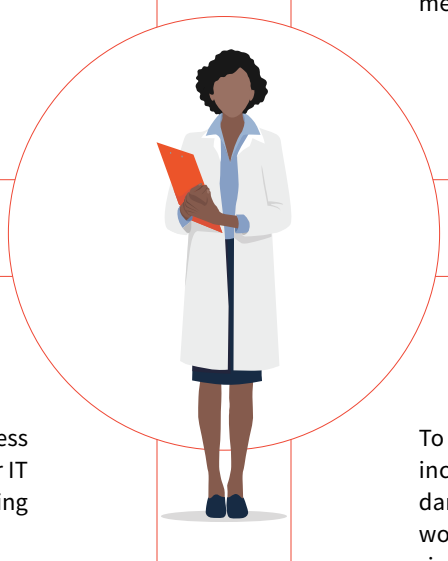
### Insider threats

60% of healthcare cybersecurity threats come from insiders. To protect Patient Health Information (PHI), implement preventive measures, such as disk encryption, regular review of PHI access logs, and an incident response plan.

8

### Cultural realities

Some security breaches are caused by people who use unofficial processes and technology in an attempt to get their work done faster. Instead of just blocking these behaviors, foster a culture of security and establish a secure means of meeting staff needs.



9

### Skills and capabilities

There is a shortage of skilled security professionals. To address this challenge, invest in cybersecurity skills training for your IT people. If training doesn't meet all your needs, consider hiring third-party experts to help.

10

### Executive leadership

To minimize the risk and impact of a cybersecurity breach—including loss of confidentiality, system downtime, reputation damage, and risk to users and patients—executives need to work together with their cybersecurity team to prioritize the right cybersecurity investments.

## Next Steps

Hire Experts to Help

Cybersecurity Audit

Cybersecurity Improvement Plan

Security Awareness Training