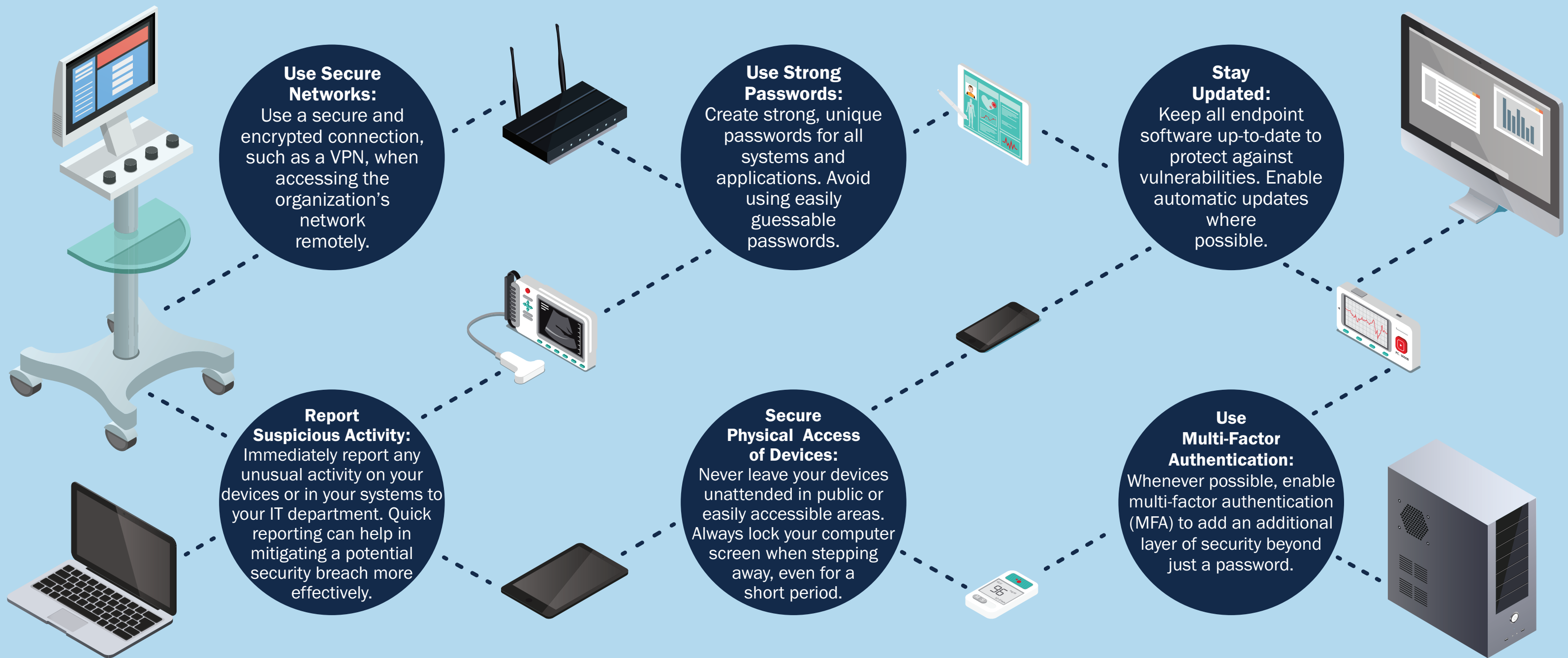# Protect Your Endpoints: A Safeguard for Healthcare

Healthcare Relies on Technology: Every day, healthcare settings use devices that connect to the internet to access and share medical records, communicate with patients, and manage sensitive data.

Endpoints are Gateways: Devices like computers, tablets, and mobile phones are gateways to your organization's network. Protecting these endpoints is crucial to prevent unauthorized access and cyberattacks.

Patient Safety and Privacy: Secure endpoints ensure the confidentiality, integrity, and availability of patient data, reducing the risk of data breaches that can compromise patient safety and privacy.

Use Secure Networks: Use a secure and encrypted connection, such as a VPN, when accessing the organization's network remotely.

Use Strong Passwords: Create strong, unique passwords for all systems and applications. Avoid using easily guessable passwords.

Stay Updated: Keep all endpoint software up-to-date to protect against vulnerabilities. Enable automatic updates where possible.

Report Suspicious Activity: Immediately report any unusual activity on your devices or in your systems to your IT department. Quick reporting can help in mitigating a potential security breach more effectively.

Secure Physical Access of Devices: Never leave your devices unattended in public or easily accessible areas. Always lock your computer screen when stepping away, even for a short period.

Use Multi-Factor Authentication: Whenever possible, enable multi-factor authentication (MFA) to add an additional layer of security beyond just a password.