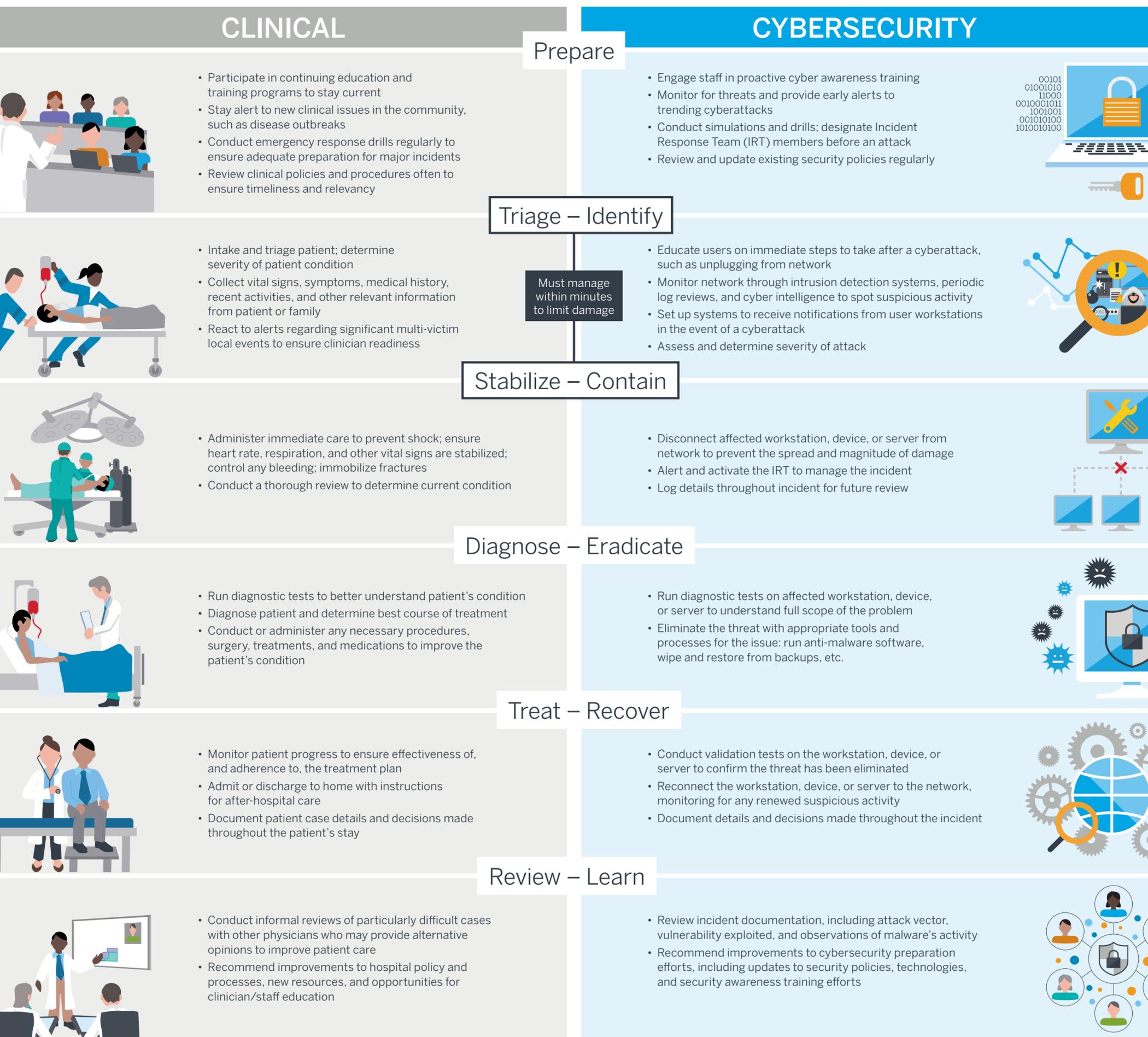


# When a Breach Occurs, the Whole Hospital Is Our Patient

Health care organizations are under attack. Vicious threats like ransomware can significantly disrupt or even shut down clinical and business operations at a moment's notice. While the implications of cyberattacks are often unknown to health care leaders, clinicians, and staff, they are used to handling critical incidents in patient care. Luckily, the process for handling a cyber incident is nearly the same.

This graphic details how the steps in responding to a clinical crisis mirror one of the most widely used cyber response methods, the SANS Institute's PICERL approach: preparation, identification, containment, eradication, recovery, lessons learned. By relating information security tactics to patient care, everyone can get on the same page and work together.



Must manage within minutes to limit damage

## How IT Staff Support a Healthy Cybersecurity Environment

- Conduct security awareness training, provide regular updates on the latest phishing techniques, and encourage good cyber hygiene.
- Ensure basic technical countermeasures are in place to defend against malicious emails and limit access to harmful websites.
- Maintain and test backups regularly, keeping them disconnected from the network as some ransomware variants target and encrypt or destroy backups.
- Review and adjust security policies regularly to ensure they address new and emerging threats and account for new technologies and systems within the organization.