EDGE
SOLUTIONS & CONSULTING

EDGE Cybersecurity Checklist for Regional Hospitals

A Practical Guide to Strengthening Your Cybersecurity Defenses

This checklist breaks down key cybersecurity steps that regional hospitals can immediately start using to improve their defenses. It covers areas such as technology, processes, staff training, and compliance with a focus on practical action.

❑ Address Insider Threats with Strong Access Controls

- **Challenge**: Insider threats (both malicious and unintentional) are a leading cause of breaches in hospitals.
- **Solution**: Implement **multi-factor authentication (MFA)** and **role-based access control (RBAC)** to restrict access to sensitive data, ensuring that healthcare workers only access what they need for their roles. Also apply and provide MFA for systems that patients log into.

❑ Train Staff to Prevent Phishing Attacks

- **Challenge**: Hospitals are prime targets for phishing attacks that could lead to ransomware.
- **Solution**: Conduct **ongoing cybersecurity training** focused on recognizing phishing emails and social engineering tactics and simulate attacks to test awareness.

❑ Secure Medical Devices Against Vulnerabilities

- **Challenge**: Many hospital medical devices and IoT systems are outdated and vulnerable to attacks. Some FDA approved systems cannot be updated as they were certified on a specific operating system.
- **Solution**: Regularly update device software, implement **strong encryption** for communication between devices, and isolate them on **segmented networks** to limit risk exposure.

❑ Encrypt Data to Mitigate Ransomware Threats

- **Challenge**: Hospitals are particularly vulnerable to ransomware, which encrypts sensitive patient data and demands payment for its release.
- **Solution**: Encrypt all sensitive data (both at rest and in transit) and ensure **regular backups** are stored offline or in a secure, off-site location. This can help in quick recovery without paying ransom. Purchase cybersecurity insurance. Many cybersecurity insurance providers also assist with ransomware payments and incident investigation and remediation through their partners.

EDGE
SOLUTIONS & CONSULTING

❑ Ensure Timely Software Updates and Patch Management

- **Challenge**: Legacy systems common in healthcare often run on outdated software with known vulnerabilities.
- **Solution**: Implement a strict **patch management process** to ensure all systems, including Electronic Health Record (EHR) platforms, are updated regularly, reducing exposure to cyber threats. Flex your patch management system with network segmentation controls to account for systems that cannot be patched for various reasons.

❑ Backup Critical Data to Minimize Impact of Attacks

- **Challenge**: Loss of patient data can halt operations and delay treatments, especially in a ransomware scenario.
- **Solution**: Implement frequent data backups and store them in **multiple, secure locations**. Regularly test restoration procedures to ensure backup integrity and availability in emergencies.

❑ Deploy Advanced Firewalls and Intrusion Detection Systems

- **Challenge**: Hospitals face advanced persistent threats (APT) and other cyberattacks aimed at breaching critical systems.
- **Solution**: Use **next-gen firewalls** and **Intrusion Detection/Prevention Systems (IDS/IPS)** to detect and prevent unauthorized access, malware, or suspicious traffic in real time.

❑ Segment Networks to Isolate Critical Systems

- **Challenge**: A breach in one part of the network can potentially compromise the entire hospital system.
- **Solution**: Implement **network segmentation**, keeping administrative systems, medical devices, and patient data on separate networks. This limits the scope of any breach, minimizing the impact on critical infrastructure.

❑ Develop and Test a Cyber Incident Response Plan

- **Challenge**: Many hospitals are unprepared for coordinated cyberattacks, which can cripple operations and leave patient care in jeopardy.
- **Solution**: Create and regularly update a **cyber incident response plan** specifically tailored for healthcare scenarios, like ransomware attacks or DDoS, and perform routine simulations to

ensure readiness. Apply the learnings and incrementally improve your incident response plan. Account for how-to maintain the integrity of patient care while systems are unavailable.

❑ Manage Third-Party Risk in Vendor Networks

- **Challenge**: Hospitals rely heavily on third-party vendors for software, equipment, and IT support, which increases exposure to security breaches.
- **Solution**: Conduct **vendor security audits** and ensure compliance with HIPAA and other healthcare regulations. Monitor third-party access to hospital systems and data and enforce strong cybersecurity practices with contractual obligations.

❑ Ensure Compliance with Healthcare Cybersecurity Practices (HICP)

- **Challenge**: Hospitals face increasing cybersecurity threats and must adhere to industry standards like HIPAA, HITECH, and the **Health Industry Cybersecurity Practices (HICP)**, which provide guidelines for managing cybersecurity risks specific to healthcare.
- **Solution**: Align your cybersecurity strategy with the **HICP framework**, which is designed to help healthcare organizations of all sizes manage key threats like ransomware, insider threats, and phishing. Conduct regular **HICP assessments** to ensure your hospital is following recommended practices, such as risk management, endpoint protection, and email security. By integrating **HICP guidelines** into your cybersecurity efforts, you ensure both regulatory compliance and alignment with healthcare security industry leading practices, minimizing the risk of breaches and ensuring patient data protection.

❑ Deploy Cloud Security Posture Management (CSPM)

- **Challenge**: Many healthcare organizations are moving to cloud-based systems for storing and managing patient data, but this introduces new risks if cloud security is not properly implemented. Misconfigurations or inadequate cloud security controls can lead to data exposure or breaches.
- **Solution**: Deploy CSPM tools to continuously scan cloud environments for misconfigurations. These tools automatically detect misconfigurations, providing recommendations to fix them before they can be exploited.