Penn Medicine's Responsibilities

Securing Products & Devices During Network Onboarding

Penn Medicine uses comprehensive strategies to secure data and ensure compliance, aiming to protect sensitive information and maintain operational integrity as devices and products are integrated into the Penn Medicine networks.

As a Penn Medicine Business Owner, you must ensure each device / product connecting to the Penn Medicine network meets these minimum technical controls:

- ✓ **Contracts:** Ensure detailed data sharing agreements are in place with clear security standards before exchanging information. Agreements should include at a minimum, protection measures (encryption, compliance), SLAs, support details (hours, contacts, escalation), disaster recovery, backup procedures, RPO/RTO, audit rights, and termination terms (notice, post-termination data handling).
- ✓ **Data Accuracy:** Verify that only accurate, reliable, legal, and clinically appropriate data is entered into or transmitted by the device on the network.
- ✓ **Data Relevance**: Only transmit or store necessary data from the device required for operations. Unnecessary data flows can introduce additional risks.
- ✓ **Data Encryption**: Ensure that all patient and/or operational data, both at rest and in transit between devices and systems, is protected using strong encryption protocols to prevent unauthorized access.
- ✓ **Data Protection**: Implement robust security measures to safeguard all information handled by the device. This includes encryption and physical protection to shield data during both storage and transmission.
- ✓ **Network Segmentation:** Place devices on dedicated network segments minimizing potential exposure to threats and limiting the impact of security incidents.
- ✓ **Access Control**: Restrict access to devices and the data they process to authorized personnel only by setting up precise roles and permissions on the device and within the network.
- ✓ **Authentication**: Require secure authentication methods, such as Single Sign-On (SSO) or multi-factor authentication, for users accessing the device, device management interfaces or data.
- ✓ **Integration with Supporting Systems**: When devices interface with Penn Medicine's core clinical or administrative systems (such as Epic or Cerner), ensure that permissions are managed and regularly reviewed for accuracy and security. Data shared across these integrations should be carefully monitored and protected.
- ✓ **Logging and Monitoring**: Establish comprehensive logging and real-time monitoring for devices and network connections, ensuring that all access and activity are tracked, audited, and reviewed regularly to detect and respond to security threats or unauthorized behavior.
- ✓ **Software Updates and Antivirus**: Ensure all devices are routinely updated with the latest operating system, application patches, and antivirus definitions to mitigate vulnerabilities and protect against malware and other security threats.
- ✓ **Incident Response Plan**: Develop and maintain a response plan for security incidents involving devices. Quickly address and mitigate breaches to minimize disruption and data exposure.
- ✓ **Business Continuity**: Establish a business continuity plan to ensure that essential device-supported operations can continue during network disruptions or device failures.

Work with your IT Owner or technical lead to ensure these controls are implemented *where feasible*. By following these guidelines, you help protect the integrity, availability, and confidentiality of data and the safe operation of networked devices.