Android Enterprise Devices for Resident Use

A cost-effective, managed solution for residents at Oregon State Hospital

Definitions

- **Android Enterprise**: A Google-led initiative that enables organizations to deploy and manage Android devices securely and efficiently.
- **Enterprise Management**: The process of overseeing and controlling devices within an organization using tools such as MDM systems.
- **Mobile Device Management (MDM)**: Software used to remotely manage, monitor, and secure mobile devices, ensuring compliance with organizational policies.
- **Work Managed / Corporate-Owned Mode**: A configuration setting in Android Enterprise that restricts device functionality for security and compliance during use within an organization.
- **SIM Card**: A small card inserted into a mobile device that provides cellular connectivity; in this context, devices for residents will be provided without SIM cards to prevent unauthorized connectivity.
- **Bootloader Lock**: A security feature that inhibits unauthorized modifications to the device's operating system, thereby blocking factory resets that bypass management controls.
- **Segregated WiFi:** A network configuration that divides a single wireless network into isolated virtual segments, often implemented using VLAN technology, to ensure that traffic from different user groups (such as residents and staff) remains separated. This segregation enhances security by eliminating unauthorized access and allows for tailored network policies for each segment.
- **VLAN Technology:** A method that allows a single physical network to be divided into multiple isolated virtual networks. Each VLAN operates as an independent network segment, enhancing security, reducing unnecessary traffic, and enabling specific network policies for different user groups or functions. (This is already in use for the resident computers.)

Overview of the Concept

- The Resident buys a budget Android Device through the Market which is then enrolled in an enterprise management (EMM) solution during their hospital stay.

- Devices will be enrolled in a "corporate-owned" mode via a Mobile Device Management (MDM) system, following a process very similar to what IT currently uses for state work phones.

- Key features such as disabling the camera, restricting cellular connectivity (e.g., disabling 5G), and disabling app installations and uninstallations without damaging hardware to ensure enhanced security and compliance during the residents' stay.

Leveraging Android Enterprise Management

- **Restricting Network Connectivity:**
  - Disable the ability to change mobile network settings.
  - Force usage of a specified, hospital-approved Wi-Fi network (Filtered like the Chromebooks in Treatment Mall).
  - Guides for manual disabling (e.g., turning off 5G) are available at:
    - Mobile Guardian – Configuring Android EMM Restrictions
    - Android Onboarding: Part 1 - Setting Up Android Enterprise Mobility Management (EMM) with Google Workspace – Mobile Guardian
- **Other Restrictions:**
  - Prevent app installation/uninstallation, block USB file transfers, disable screen capture, etc.

Understanding Proposed Resident Segregated WiFi VLAN

What Is a VLAN?

- Virtual Local Area Network (VLAN): Think of it as a "virtual room" inside your WiFi network.

What Does "Segregated" Mean?

- It means separating the network into distinct sections.
- Each section (or "room") can have its own rules and access.

Imagine the Kirkbride building. Employees use one secure area. Residents have their own separate area inside the secure perimeter. Even though they are in the same building, the spaces are separated to protect sensitive areas.

Why Use a Segregated WiFi VLAN?

- **Security:** Keeps guest devices separate from private, internal systems.
- **Organization:** Manages different types of network traffic more effectively.
- **Control:** Allows administrators to apply specific rules for each section.

Risk: Unauthorized Device Reset

- **Risk Details:**
  - Residents might intentionally or inadvertently attempt to perform a factory reset to bypass the managed configuration and restrictions.
- **Mitigation Strategy:**
  - To mitigate risks from unauthorized device resets that could bypass managed restrictions, OSH should implement a multi-layered security approach. SIM cards will stay classified as a Tier 0 item, and will remain physically unavailable, ensuring that even if a device is reset, it cannot reconnect to the hospital resident filtered Wi-Fi (limiting its functionality to 911 calls only, as it loses access to 5G data without a SIM). Additionally, bootloader locking will be enabled to prevent device resets unless performed by the IT department with a standard computer capable of installing the Android Developer Kit. A capability which is not available on resident Chromebook or Supported Education computers. Residents will also be informed of the consequences and futility of attempting a factory reset, further reducing the risk of unauthorized use.

Integration and Lifecycle Management

- **Enrollment Process:**
  - Resident purchases device and it is enrolled in the hospital's Android Enterprise management system.
  - Policies applied: disable camera, restrict 5G/cellular, force approved Wi-Fi (filtered).
- **Unenrollment Process:**
  - Upon discharge, IT remotely removes the enterprise management profile and device returns to normal consumer status.
  - Android Enterprise supports a "work profile" wipe or full unenrollment to restore personal settings.

Benefits for OSH:

- **Reduced Behavioral Incidents:** Secure, restricted device usage will provide healthy distractions and minimizes potential triggers, leading to fewer behavioral issues.
- **Enhanced Coping Skills:** Curated therapeutic and educational content supports residents in developing healthier coping mechanisms.
- **Improved Safety & Compliance:** Remotely managed devices ensure adherence to hospital policies, reducing risks and administrative burdens.
- **Better Recovery Outcomes:** A controlled digital environment contributes to a more structured and supportive treatment experience.
- **Modeling Excellence:** Enables OSH to emulate best practices seen in state hospitals in the Northeast with robust and liberal electronic policies, demonstrating a modern, patient-centered approach while generating positive public relations with stakeholders.

Resident Benefits:
Enhanced Connectivity & Entertainment

- **Secure Entertainment:** Access to on-demand streaming of music, TV shows, and educational content in a controlled, safe environment.
- **Enhanced Communication:** Facilitates secure video calls and messaging with family, counselors, and peers.
- **Therapeutic Tools:** Provides curated self-help apps and stress-reduction programs to support emotional well-being.
- **Personal Growth:** Offers educational resources that bolster recovery and personal development.
- **Seamless Transition:** Ensures a smooth shift from a managed device during treatment to a fully functional personal device upon discharge.

Increase in Position Authority

- Increase in position authority to create a dedicated role for resident facing technology support:
    - Direct interaction with residents about technology issues.
    - Current system resembles a game of telephone: issues relayed through unit staff emailing IT who aren't allowed to talk to residents directly.
- Current State: Many issues remain unresolved due to communication breakdowns.
- Proposed solution: Establish a Resident Technology Liaison as an entry-level IT position (potentially at level 20).
- Expected outcome: Streamlined communication and reduced frustration for residents.

Potential Device and Mobile Device Management (MDM) Considerations

- **Device Selection:**
  - Choose affordable smartphones (e.g., Motorola Moto G series or Nokia models) and tablets (e.g., Lenovo Tab series) that support Android Enterprise (Android 10 or later).
- **MDM Solutions Options:**
  - Google's Android Management API for custom policy creation.
  - Third-party options like SOTI, AirDroid Business, or Mobile Guardian.
- **Cost Efficiency:**
  - Residents purchase the device, while the hospital focuses on deploying the management profile.
  - IT "pushes" the configuration to enrolled devices.

Summary

Cost-Effective, Secure Solution:

- Residents purchase affordable Android devices at the Market (smartphones/tablets) which will be enrolled in an enterprise management system run by the OSH IT Department.

Managed Configuration:

- Devices operate in "corporate-owned" mode via MDM, mirroring the current state work phone process.

Robust Security Measures:

- Restrict features (e.g., disable camera, enforce hospital-approved Wi-Fi, disable 5G/cellular settings).
- Prevent unauthorized resets through MDM policies, bootloader locks, and exclusion of SIM cards.

Seamless Transition:

- IT removes the management profile upon discharge, reverting devices to full personal use.

Therapeutic & Mental Health Benefits:

- Low-cost monthly fee (versus jail tablets costing up to $50 for 10 hours of video).
- On-demand streaming of music, podcasts, and videos for comfort and distraction.
- Curated, safe web access supports recovery-focused content and engagement.
- Enhances overall well-being by combining **modern connectivity** with robust privacy and **security**.
- This system will help residents feel more comfortable, add more coping skills and tools to their toolbox. **Reducing boredom and giving us something to do in our rooms!** While also reducing Code Greens and Seclusion Events.