Version: 2.0	**POLICY:** Mobile Device Management Policy
Facility: All Inova **Applies To:** All Inova Personnel **Policy Manual:** Information Technology	**Key Words: BYOD***(Bring Your Own Device)*, **Mobile Device***(smartphones, tablets, iPads, etc.)*, **Airwatch**(Mobile device management monitoring application) **, CSL**(Inova Customer Support Line), **2-Factor Authentication, SARF**
Original Policy Date: 11/2015	**Revised Date(s):** 04/21/2016
Approved by: /s/ Chief Information Officer	**Approved by:**

I. Purpose

The Mobile Device Management Policy provides the standards and rules of behavior for the use of all "***Mobile Devices***"requiring access to Inova IT networks. This includes, personally-owned or ***BYOD*** (Bring Your Own Device) and Inova provided smart phones, tablets, and iPad devices. Inova employees requiring access to Inova network resources and/or services must adhere to the policy. Access to and continued use is granted on condition that each user reads, signs, respects, and follows the Inova's Information Technologies(IT) policies concerning the use of these resources and/or services.

➢ STATEMENT

This policy is intended to protect the security and integrity of Inova Health Systems' data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms. The referenced MDM/BYOD services, excluding the Inova Guest Wi-Fi Service, is strictly for the use of Inova employees only. This includes the "Airwatch" application which will be used to access Inova Email remotely on employee mobile devices (One licence per employee user).

➢ Expectation of Privacy

Inova will respect the privacy of your personal device and will only request access to the device by technicians to implement security controls or to respond to legitimate discovery requests arising out of administrative, civil, or criminal proceedings. This differs from policy for Inova provided equipment and/or services, where employees do not have the right, nor should they have the expectation, of privacy while using equipment and/or services.

II. Acceptable Use (any mobile device that is approved for access)

- Inova's IT Security defines acceptable business use as activities that directly or indirectly support the business of Inova Health Systems. Please reference the "Acceptable Use Policy", http://inovanet.net.inova.org/policies/view.aspx?id=2281&sid=1&categoryId=586
- Inova IT Security "Acceptable Use" policy defines acceptable personal use on company time as reasonable and limited personal communication or recreation, such as reading or game playing.
- Devices may not be used at any time to:
  - Store or transmit illicit materials
  - Store or transmit proprietary information
  - Harass others

- Engage in outside business activities

- Employees may use their mobile device to access the following company-owned resources:
  - Email
  - Calendars
  - Contacts
  - Documents

➢ Inova has a zero-tolerance policy for texting or emailing while driving and only hands-free talking while driving is permitted.

➢ Devices and Support

- The following devices are supported:
  - iPhone (iOS 8 and above; 5s or newer)
  - ipad (iOS 8 and above)
  - Android (5.1 or newer)

- Connectivity issues pertaining only to Inova network resources are supported by IT Customer Support Line (CSL); employees should contact the device manufacturer or their carrier for operating system or hardware-related issues.

- All Mobile Devices, Inova provided and personal (BYOD), requiring connectivity to the Inova network resources, *i.e.* Email, must be administered via a Mobile Device Management (MDM) System in order to comply with Inova IT Security standards to implement proper job provisioning and configuration of standard apps, such as Email, Browsers, Office Productivity Software, and Security Tools, in order that a user can access the Inova network securily. The current Inova IT approved MDM System is **AirWatch,** by VMWare.

➢ Security

- Password length and complexity should be in compliance with Inova IT Security Policy. Please reference ***"IT Access Control Policy" Section 2.2,*** http://inovanet.net.inova.org/policies/view.aspx?id=2281&sid=1&categoryId=586 .

> **2.7 Mobile Device Account PIN (All mobile devices accessing Inova's network must be registered and approved and must use AirWatch, application to access limited Inova's resources. Currently, access is limited to remote email access only).**
>
> 1. Mobile devices must be configured for *2-factor Authentication* {user login network credentials (User ID and AD domain password) + a personal 6 (six) Digit (numeric) "Passcode" selected by the user} to access Inova network resources, i.e. Email;
> 2. Users will be prompted to change their AirWatch Passcodes every 90 days;
> 3. *First* of 2-factor authentication for AirWatch is the user's Inova Network password. Passwords should meet section 2.2 of this policy (**Password Management for Inova Networks);**
> 4. *Second* of 2-factor authentication is the AirWatch "Passcode". AirWatch passcode must be at least six (6) numeric digits;
> 5. Inova network access via Mobile devices is limited for Inova employees only;
> 6. History of the past 6 (six) passcodes is cached; New passcode must be different from the past 6 (six) passcodes cached in history;
> 7. AirWatch content will be "**Enterprise Wiped**" (removes the AirWatch application and email access via AirWatch only) **after 6 (six) incorrect login attempts**. User must contact the Inova Customer Support Line (CSL) before their 6th and final login attempt if they cannot remember their 6 digit "Passcode/PIN "or password. If mobile device is "Enterprise Wiped" User must re-enroll in AirWatch by re-installing the application and reconfiguring their credentials with a fresh install of the AirWatch application.

- Rooted (Android) or jailbroken (iOS) devices (*devices where the approved device or application configurations have been modified or tampered with and no longer meet Inova IT approved configuration)* are strictly forbidden from accessing the network.

- Smartphones and tablets that are not on the Inova's list of supported devices are not allowed to connect to the network.
- Smartphones and tablets belonging to employees that are for personal use only are not allowed to connect to the network without proper authorization from the IT Access Management. To request access, a **SARF** (*System Access Request Form*) must be completed and approved by the individuals supervisor if the employee is an exempt Inova employee. For non-exempt employees, an additional approval from HR is needed. SARF **must** be completed with the requested employee information, employee supervisor's signed approval for exempt employees and supervisor and HR acknowledgement/approval for non-exempt employees, and the required information with respect to the mobile device that will be used to access Inova email and any other available resources via AirWatch.
- Employees' access to company data is limited based on user profiles defined by IT and automatically enforced.

➢ **The employee's device may be remotely wiped of all Inova related data, if:**

- The device is lost or stolen.
- The employee terminates his or her employment.
  IT detects a data or policy breach, a virus or similar threat to the security of the company's data and technology infrastructure.
- After the 6 incorrect login attempts.

➢ **Risks/Liabilities/Disclaimers:**

- Inova's IT staff will take every precaution to prevent the employee's personal data from being lost in the event it must remote wipe a device. However, it is the employee's responsibility to take additional precautions, such as backing up email, contacts, etc.
- Inova reserves the right to disconnect devices or disable services without notification.
- All lost or stolen devices used and authorized to access Inova's network resources must be reported to the Inova CSL immediately (*703-889-2000 or CustomerSupportLine@inova.org*). In addition, employees are solely responsible for notifying their mobile carrier immediately upon loss of a device. In this case, the employee is responsible of remotely wiping of any personal data. Inova CSL support will only be provided for Inova provided mobile devices only, with the exception of AirWatch connectivity assistance.
- The employee is expected to use his or her devices in an ethical manner at all times and adhere to the company's acceptable use policy as outlined above.
- The employee is personally liable for all costs associated with his or her personal device.
- The employee assumes full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.
- Inova reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

IV. Applies to

This policy applies to all Inova-affiliated facilities including, but not limited to hospitals, ambulatory surgery centers, home health agencies, long-term care facilities and all corporate departments, groups and divisions that use or disclose electronic protected health information for any purposes. The MDM/BYOD remote access services (Airwatch) is restricted for employees use only, and therefore, the policy applies to all employees.

V. Enforcement

User Acknowledgment and Agreement

I acknowledge, understand and will comply with the above referenced security policy and rules of behavior, as applicable to my BYOD usage of Inova's network and services. I understand that business use may result in increases to my personal monthly service plan costs. I further understand that reimbursement of any business related data/voice plan usage of my personal device is not provided by Inova Health Systems.

Employee Name: _____

BYOD Device(s): _____

Employee Signature: _____ Date: _____

Any employee found to have violated any of Inova IT policies may be subject to disciplinary action, including termination of employment.