NYSPI Mobile Device Security Standard Bulletin

To address state and local compliance needs and to ensure the privacy and security of NYSPI data and systems, portable devices including smartphones, tablets and other mobile peripherals must be carefully managed. Details are including in the NYSPI System Management Procedures, which further references the NYS Account Management and Access Control Standard (http://on.ny.gov/2b3D288), which provides guidance on creating and managing access to data, and the NYS Authentication Token Standard (http://on.ny.gov/2bq4myp) which provides password requirements.

To this end, all mobile devices managed by a NYSPI-hosted system or system serving or storing NYSPI-data must comply with these standards. Mobile devices are computing devices in a small form factor that have at least one network connection interface, non-removable and/or removable storage, and is portable (i.e., non-stationary). These devices come in the forms such as: smartphones, PDAs, smart watches, tablets, laptops, and wearable devices.
Specifically, mobile devices must follow all requirements and meet the following criteria.

- Mobile devices must follow all requirements of the NYS Information Security Policy.
- As per the state Encryption Standard, all mobile devices that access or contain any NYSPI-data information must be encrypted.
- For NYSPI issued mobile devices or personal mobile devices with direct access to NYSPI-managed networks (**see NYSPI Bring Your Own Device Standard**), only those applications, which are approved by NYSPI, may be installed and or run on the mobile devices. Applications must be restricted through the use of whitelisting (preferable) or blacklisting. Applications must be digitally signed to ensure that only applications from trusted entities are installed on the device and that code has not been modified.
- NYSPI information must be removed or rendered inaccessible from mobile devices after no more than 10 incorrect authentication attempts.
- Mobile devices must automatically lock after being idle for a period not to exceed 10 minutes.
- Mobile devices which directly connect to NYSPI-managed private networks, virtually connect to NYSPI-managed private networks in a manner consistent with a directly connected device, or which contain or could contain NYSPI-data information, including

e-mail data, must be managed by a Mobile Device Management (MDM) or other centralized management solution.

- Use of synchronization services, such as backups, for mobile devices (e.g., local device synchronization, remote synchronization services, and websites) must be controlled by NYSPI through an MDM or other centralized management solution.
- Mobile devices may not access NYSPI private networks unless their operating environment integrity is verified (including whether the device has been rooted/jailbroken).
- NYSPI must manage all mobile devices by:
  a. Implementing device policies and configurations as appropriate to the use of the device.
  b. Developing and implementing processes which check for upgrades and patches to the software components, and for appropriately acquiring, testing, and deploying the updates to NYSPI issued devices.
  c. Reconfiguring access control features as needed based on factors such as policy changes, technology changes, audit findings, and new security needs.
  d. Detecting and documenting anomalies, which may indicate malicious activity or deviations from policy and procedures. Anomalies should be reported to other systems' administrators as appropriate.
  e. Providing training and awareness activities for mobile device users on threats and recommended security practices, which can be incorporated into the NYSPI security and awareness training.

Questions or requests for exceptions should be sent via a service desk ticket or by e-mail to PsyIT-Admin@nyspi.columbia.edu.