# NYSPI Bring Your Own Device (BYOD) Standard Bulletin

To address state and local compliance needs and to ensure the privacy and security of NYSPI data and systems, BYOD devices including computers, smartphones, tablets and other devices running a mobile operating system, including but not limited to Android, BlackBerry OS, iOS, Linux, Mac OS X, Windows and Windows Mobile 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.

The purpose of this technical standard is to normalize the management and administration of personal devices accessing NYSPI resources. This standard applies to all administrators of BYOD programs.

This standard identifies four methods of accessing state data and the level of management required:

**Viewer-based Access**
Users can access NYSPI managed data via a web, virtual desktop, or other interface. The data in this level does not reside on the device; no state management of the device is required. (Example, a home PC logging into a NYSPI website to obtain information, either public or personally accessible to the user.)

**Application Access**
In the application model, all access to NYSPI data from the BYOD device is delivered via applications, which securely isolate NYSPI data from personal data on the device. Examples include virtual desktop infrastructure (VDI) or terminal clients that do not store State data, web browsers, or applications that encrypt data stored on the BYOD devices. (Example, a worker accesses a NYSPI managed desktop (physical or virtual) with an SSL VPN client. NYSPI manages the device and access method.)

Applications used in this manner must have the following capabilities:

1. Applications must not store plaintext NYSPI data on the BYOD device. Any NYSPI data stored on the device must be stored in a manner consistent with relevant security policies and encryption standards.

2. Applications must disallow access to NYSPI data to other applications on the device, unless access is secured in a manner consistent with relevant security policies and encryption standards.
3. The application or platform must have the ability to detect "jail broken" or "rooted" devices or similar mechanisms that bypass the platform security model and perform remediation.

**Native Messaging and Calendar Access**
In the messaging access model, end users are authorized to connect BYOD devices to NYSPI messaging platforms, using protocols such as Exchange ActiveSync or Outlook Web Access (OWA).

To allow this type of connectivity, BYOD devices must have the following capabilities:
1. Owners of the BYOD device must agree to allow NYSPI to take intrusive measures to manage and protect NYSPI data, including the installation of software for device management. Device management software includes password policy; usage monitoring and remote wipe capability. These measures will impact personal data on the device
2. The BYOD device must encrypt all NYSPI data in a manner consistent with relevant security policies and encryption standards.
3. Owners of the BYOD device must agree to be responsible for the use of the device, and to not allow others to use it without direct supervision.

**Managed Device Access**
In the managed device model, for cases where direct access to NYSPI-managed networks is required, BYOD devices are authorized to connect to NYSPI networks. Authorized devices will be managed in a manner identical to a NYSPI-owned device.
1. All devices must be compliant with enterprise baseline security requirements, and optional additional security controls specific to NYSPI that the device is assigned to.
2. Personal devices of this type must be managed in a manner consistent with the NYSPI Mobile Device Security Standard.

If compliance with this standard is not feasible or technically possible, or if deviation from this standard is necessary to support a business function, NYSPI shall obtain written authorization of the Chief Technology Officer and Chief Information Security Officer.

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