United States Department of Health & Human Services

Chief Technology Officer (CTO) Council

HHS Mobile Technology Strategy
January 19, 2012

Version 1.0

Table of Contents

Document Change History

Version Number	Release Date	Summary of Changes
0.1	06/09/2011	Formed Strawman Document for Review
0.2	06/14/2011	Populated document with input from OPDIVs
0.3	07/04/2011	Added security and privacy controls that are required for mobile technologies. Updated vision and background.
0.4	07/18/2011	Added additional controls and reformatted structure. Added new format for baseline configurations and necessary controls.
0.5	08/11/2011	Combined comments from NIH, CDC, CMS, and OCIO/Security. Restructured document according to comments and incorporated new sections as requested.
0.6	08/22/2011	Incorporated comments from CTO Council and added additional clarification for called out sections.
0.7	08/24/2011	Added in approved statements for CTO Council Review.
0.8	09/14/2011	Received 35 comments from workgroup, created comment matrix and added in additional material based on comments.
0.9	11/14/2011	Received 152 comments from CISO review, created comment matrix, and added incorporated comments into version 0.9.
0.10	11/28/2011	Received comments concerning document consistency from NIH and OCIO/Security, and added revised changes.
1.0	01/20/2012	Received CTO Council approval and made changes based on conditional approval statements.

1. Purpose

The purpose of the U.S. Department of Health and Human Services (HHS) Mobile Technology Strategy is to describe business drivers for use of mobile technologies within the HHS enterprise, identify the security requirements to adequately protect these devices and the information that they transmit and store, and offer recommendations selection and implementation of mobile technologies which meet or exceed these requirements.

This document is intended as guidance for use by HHS business and information technology leadership when implementing mobile technology and policies and solutions.

2. Background

Mobile devices (also known as handheld devices, smartphones, tablets, or personal digital assistants) have become indispensable tools for today's highly mobile workforce. Small and relatively inexpensive, these devices can be used not only for voice calls, but also for many functions previously handled by a desktop computer such as sending and receiving email, browsing the Web, storing and modifying documents, delivering presentations, and remotely accessing sensitive data. While these devices provide productivity benefits, they also pose new risks to the Department of Health and Human Services (HHS). As these devices become pervasive in daily use, pressure increases to include them in the enterprise. While mobile devices do have many benefits, such as increase availability and efficiency, the very nature of these devices represents challenges to traditional thinking in areas like network boundaries, information sharing and security controls selection.

HHS, in support of it mission to protect its people, resources, and information is developing this guidance to review existing security polices, examining the business needs for mobile devices and developing a position on the use of mobile devices within HHS.

3. HHS Mobile Technology Vision

The HHS Office of the Chief Information Officer (OCIO) understands the business value of mobile devices and is flexible in its strategy for securely integrating them into the HHS environment. While mobile devices have their limitations, they offer productivity and convenience in a compact form and are quickly becoming a necessity in today's business environment. In addition to standard workplace activities like email and Web browsing, mobile devices are increasingly supporting advanced health-related fieldwork such as inspection, infectious disease inventory, and health response. As such, the OCIO encourages the use of these devices to achieve and simplify mission objectives; and believes that the risk to the transport of data can be successfully mitigated with appropriate application of technology and training.

Due to the personal nature of mobile devices and the diversity in the mobile operating systems/platforms, the OCIO is planning to employ multiple risk mitigation strategies across the Department. While the OCIO is aware of the non-standard mobile devices with email connectivity that are currently deployed throughout HHS and Operating Divisions (OPDIVs), it is the position of the OCIO that such deployment without proper security controls introduces additional threat vector for unauthorized access to sensitive information.

In order to enable the workforce to use these devices, OCIO is focused on conducting the following activities:

- Identifying the user and business requirements for mobile technologies;
- Identifying the security and privacy requirements for mobile technologies;
- Developing configuration baselines for mobile technologies; and
- Providing recommendations on identified mobile technologies for implementation.

The acquisition and use of mobile technology devices is growing as the workforce itself grows increasingly mobile, the tech-savvy generation becomes integrated in the workforce, and the sophistication and functionality of mobile technology devices advances at an accelerating rate. Although the mobile technology risks persist, this increased desire for mobile technologies correlates with the increasing diversity of mobile device platforms including Apple iOS, Google Android, Microsoft Windows Phone, and Blackberry Tablet OS that are being requested for use.

This increased desire for mobile technology devices will not decrease in the future. Therefore, this guidance document will provide ways to utilize these devices and enable the HHS workforce to increase productivity, communication, and ease-of-use.

4. Business Drivers

As mobile devices increase in popularity and become more widely used, the respective user and business requirements will increase proportionally. Within HHS, numerous business requirements including field service and healthcare have resulted in the piloting and experimentation with mobile devices in the IT environment. In addition, emerging user requirements for mobile technologies has forced the analysis of widespread adoption within HHS. Section 4.1, Section 4.2, and Section 4.3 address current business drivers for the use of mobile technologies within HHS.

4.1 Field Service

Instances where mobile technologies can be used for field service:

- ***Mapping***: Multi-touch has made mobile technologies an ideal map-reading platform. A user can go from a global view down to a street-level view, and zoom out again.
- ***Schematics***: As with mapping, schematics on a mobile device can be zoomed to a full device view down to the individual component level and back again.
- ***Data Collection***: Mobile technologies allow users to capture visual data and enter manual data at the point of inspection that allows for efficient and documented inspections.
- ***Surveillance***: Surveillance on a mobile technology is an upcoming use due to the multi-touch features that aide multi-camera displays, Pan-Tilt-Zoom features, and full monitor displays.
- ***Help Desk***: Mobile technologies can be used by help desk and IT support staff to provide updates to service tickets, scheduling of service calls, access to product warranty records, and access to IT knowledge repository.

Any one of these capabilities is useful in field service applications. Future applications that combine them will provide even more functionality. For example, tapping a spot on a map might reveal the equipment at that location (along with the schematics). Furthermore, previous data gathered at that site can be referenced and compared to new data gathered at the future state.

4.2 Healthcare

Instances where mobile technologies can be used for healthcare:

- ***Waiting Rooms***: Whether waiting for a doctor or conducting clinical trials, patient information can be displayed on the mobile technology and interactively changed by the doctor or patient if proper security measures and protocols are in place for patient use.
- ***Clinical Material***: Mobile technologies can be used for recording diagnostic information and accessing clinical information systems, including but not limited to medical imagery, patient records, and scheduling information.

- ***Reference Material***: Mobile technologies can house the full "Physician's Desk Reference," medical texts, medical journals, and or interactive medical media.
- ***Electronic Communication***: After diagnosing a patient or conducting a clinical trial, the mobile technologies can be used to forward prescriptions to a pharmacy or transmit clinical trial results.

Continued strong interest from doctors and researchers has forced the analysis of mobile technologies within Healthcare. The ability for mobile technologies to interactively display information, provide reference material, and instantly transmit information can revolutionize the effectiveness and efficiency of doctors and researchers. However, security concerns surrounding patient data and concerns relating to the durability of these technologies (sanitation, significant use) have limited direct patient care use.

4.3 Productivity

Instances where mobile technologies can be used to increase productivity:

- ***Networking/Communication***: Mobile technology allows agencies to have an unprecedented level of connectivity between employees, users, and/or the public. Real-time communication with the office can be important in delivering business benefits, such as efficient use of staff time, improved customer service, and a greater range services delivered.
- ***Document Review/Storage***: Mobile technology allows the user to store paperless documents and the ability to review those documents at any time. Mobile technologies provide the user with an easy way to review documents in any setting.
- ***Ease of Use***: Mobile technologies are extremely portable and can be used at both home or at the office. Mobile technologies allow a user to access all necessary information without the unnecessary computing power provided by a notebook that lacks touch screen sensitivity.

Mobile technologies provide the user the necessary tools to stay in constant, real-time contact with co-workers, to review and store documents, and to maintain a high-level of use whether at home, the office, or at stationary locations in-between.

4.4 Green Sustainability

Instances where mobile technologies can be used to increase sustainability:

- ***Paper Reduction***: Mobile technology allows agencies to review and discuss documents, charts, graphs, and email without having to print the materials. Mobile technologies allow a user to display all necessary information without the unnecessary need for excessive printing.

5. Approved Implementations for Mobile Devices

The below statements have been approved for implementation Department-wide; however, these statements are recommendations that can be implemented at the discretion of the OPDIV CIO.

5.1 Government Furnished Devices

The CTO Council approves the use of the below devices for Government purchase and support if the devices are FIPS-validated, have a Security Authorization, and they meet the compensating controls found in this document:

- **Blackberry OS-based and QNX OS-based devices** including Blackberry Smartphones and Blackberry Playbook assuming the devices are registered with the OPDIV Central Blackberry Enterprise Service (BES) and the user has a Blackberry OS-based device with which to use the Blackberry Bridge.
- **Windows OS-based devices**, which can be managed using existing processes, including Federal Desktop Core Configuration (FDCC) controls and comprehensive patch and security management.
- **iOS-based devices** including the iPhone 4, the iPhone 4S and the iPad assuming that OPDIV directors accept the risk of a not having FIPS-validated encryption, but where compensating controls are put in place through the use of a Mobile Device Management (MDM)-solution.

Android-based devices have not been approved for Government use due to the variances in OSs based on the device manufacturer. In addition, Android devices are currently not FIPS 140-2 validated or in the process for FIPS 140-2 validation.

Any subsequent devices to be considered for addition to this list must be submitted to the CTO Council for review and approval, or simple rejection if the use of a particular device is not considered acceptable under a government purchase model.

The current process for Government support of these approved mobile devices is under development and any immediate deployment of Government-furnished equipment from the approved list above will be considered pilot in nature.

In addition, Government support relating to these devices will be provided on a “best effort” basis as the formal processes are developed. In the future, additional support processes and contracts will be updated to provide the support necessary to fully integrate these devices within the Department.

5.2 Personal Mobile Devices

The CTO Council approves the use of personal mobile devices outside of those approved for government purchase and support. The user must pay for the service and the added configurations that must be in place before the devices may be used to access the HHS network including device

technical support as government IT staffs are prevented by liability issues on servicing personally-owned devices. Personally-owned equipment can only be used in conjunction with explicit approval from the OPDIV CIO after the POE has been demonstrated to comply with the OPDIV's minimum baseline security requirements.

The OPDIV must pay for the software that must be in place before connecting to HHS networks, and ensure that policies support restrictions on non-government furnished equipment, and that the restrictions to "restrict the mixing of federal and personal data" explicitly apply to personally-owned devices. The OPDIV can examine stipends for users returning Government-furnished equipment to use personal mobile devices.

CTO Council approves the use of personal mobile devices as a replacement for government furnished equipment as long as there exists a FIPS 140-2 certified secure enclave / container that can be managed from a central location and can restrict the mixing of federal and personal data. The managed container must have similar management and security capabilities as iterated in previous sections of this document including, but not limited to:

- FIPS 140-2 validated encryption of all government data
- Exclusive linkage between a central management system and an individual device
- The ability to enforce complicated passwords, which must protect the container during loading and foregrounding
- The ability to remotely wipe and remove the government data

5.3 Alternative Computing Form Factors

The CTO Council approves the use of alternative computing form factors that are compliant with the existing encryption requirements and can be managed using existing workstation management tools.

6. Security and Privacy Requirements

The security of mobile devices, information stored on them, and information transmitted to them requires special consideration. In order to maintain adequate security controls, the following requirements shall be implemented for mobile devices. These requirements may be met through capabilities native to the mobile device, the mobile device platform, or through third-party tools. Although third-party tools cannot completely meet security and privacy requirements for information stored on the mobile device, the Department must examine these tools for possible solutions to meet the requirements listed below.

As mobile devices increase in popularity and become more widely used, the prevalence of use will continue to increase. In order to maintain network security and privacy, OPDIV-approved mobile devices must be capable of and enabled to support the OPDIV Mobile Device Standards. As an initial step to mitigate risk, HHS and OPDIV CIOs should validate that, at a minimum, the following controls are in place, as required by HHS policy:

6.1 Automated User and Device Inventory and Management

At a minimum, all mobile devices shall be capable of uniquely identifying the device and associated user to a centralized management system using approved methods that provide an acceptable level of trust that the device has not been modified, that the user being authenticated has permission to access the device, and use it to access HHS or OPDIV systems and data.

Government Furnished Devices

Mobile devices must be managed by the OPDIV Mobile Device Management (MDM) System. This means that they must be registered with the OPDIV Central Blackberry Enterprise Service (BES), the OPDIV Exchange ActiveSync (EAS) service, or third party MDM solution.

Likewise all mobile devices must accept policy configuration information that allows the centralized application of security and acceptable use policies. Failure to apply the required policies by a device must result in it preventing a link to OPDIV MDM System.

Personally Owned Devices

In addition to the requirements above, there must exist a secure enclave/container on the device that can be managed by the OPDIV in place of a MDM solution that does not meet the necessary baseline configurations.

6.2 User Authentication

At a minimum, all mobile devices shall be capable of applying a central policy for enforcing a complicated password compliant with Department standards before granting access to device data and services.

Government Furnished Devices

Specifically, mobile devices must require an 8character password which includes capitals, numbers and special characters to access the device and its contents. Mobile devices must support failed password limitations and be configured to automatically wipe its contents after six consecutive failed password attempts.

Personally Owned Devices

Specifically, mobile devices must require an 8 character password which includes capitals, numbers and special characters to access the device and its contents. Mobile devices must support failed password limitations and be configured to automatically wipe the contents of the secure enclave / container after six consecutive failed password attempts.

6.3 Two-Factor Authentication

Government Furnished Devices

Policy enforcement will remain a challenge without data loss prevention technology. Handling, storing, or accessing sensitive government information on a mobile device is not recommended. Information is considered sensitive if the loss of confidentiality, integrity, or availability could be expected to have a serious, severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. The OPDIV CIO may decide when two-factor authentication is necessary based on the intended usage of the device.

If remote access to sensitive government information is required, the mobile device must support OPDIV VPN plus two-factor authentication such as HHS Public Key Infrastructure (PKI) certificates, Personal Identification Verification (PIV) cards, hardware tokens or two-factor soft tokens. In addition, OPDIV CIO approval is required before any remote access is provided.

Any sensitive information stored on the device must be encrypted. In the event that mobile devices must store and/or transmit sensitive data, then a Federal Information Processing Standard (FIPS) 140-2 approved encryption method must be implemented. Encryption must have at least begun the FIPS validation process to be considered.

Refer to the Guide for Identifying and Handling Sensitive Information at the OPDIV for more information. Also refer to the Personally Identifiable Information web page.

Personally Owned Devices

Handling, storing, or accessing sensitive government information on a personal mobile device is not allowed and the storing and/or transmittal of sensitive data are prohibited. Sensitive government information can be stored in a FIPS 140-2 approved secure enclave / container which is managed by the Government and meets all compensating controls.

6.4 Session Timeout and Re-authentication

Government Furnished Devices

At a minimum, all mobile devices shall be capable of enforcing policy requirements for session timeout for inactivity and provide the capability to force re-authentication after a specified period of time or in response to specific events. Mobile devices must incorporate a maximum 15-minute inactivity timeout that requires password re-authentication to access the device.

These capabilities shall be configurable on a scheduled basis and through administrative tools on a case-by-case basis.

Personally Owned Devices

At a minimum, all mobile devices shall be capable of enforcing policy requirements for session timeout for inactivity and provide the capability to force re-authentication after a specified period of

time or in response to specific events. Mobile devices must incorporate a maximum 15-minute inactivity timeout that requires password re-authentication to access the device and the secure enclave / container.

6.5 Encryption

At a minimum, all mobile devices shall be capable of establishing encrypted communications channels between the device and other HHS systems, as appropriate. In addition, all mobile devices must enable encryption for internal and removable storage.

Government Furnished Devices

Furthermore, all mobile devices shall be capable of encrypting sensitive information stored on the device. Mobile device encryption technologies shall be FIPS 140-2 validated solutions and capable of implementing all HHS encryption policy requirements for production.

However, OPDIV CIOs may accept the risk of a not having FIPS-validated encryption for use in a pilot, but where compensating controls are put in place through the use of a MDM-solution. Encryption must have at least begun the FIPS validation process to be considered. However, the devices must be FIPS 140-2 validated for full implementation. The MDM-solution must enforce the compensating controls which are described in this document.

Personally Owned Devices

All personally-owned mobile devices shall be capable of encrypting sensitive information stored on the device or in the enclave/ secure container. Mobile device encryption technologies shall be FIPS 140-2 validated solutions and capable of implementing all HHS encryption policy requirements. If FIPS 140-2 validated solutions do not exist, there must exist a FIPS 140-2 secure enclave/container on the device that can be managed by the OPDIV in place of a more robust MDM solution for personally owned devices.

6.6 Jail-break / Alternative Firmware Prevention

At a minimum, all mobile devices shall provide the capability to determine the firmware version, operating system, patch level, and vendor.

Government Furnished Devices

All Government furnished mobile devices should have the capability to restrict the user from "jail-breaking" the device. Mobile devices must be under current security patch support by the device manufacturer and the OS developer of the device. Devices that are end-of-support or are only supported for patching by the carrier are not eligible for OPDIV-approved use.

Personally Owned Devices

In addition to the requirements above, mobile devices may not be "jail-broken" and will be prevented to connect to HHS networks if determined to be "jail-broken". Mobile device administrative tools shall be configured to prevent connections to mobile devices with unapproved configurations.

Network attachment restrictions may be enforced on mobile devices on a permanent or temporary basis commensurate with the risk assessment of a vulnerability or possible malware exposure performed by the OPDIV CIO or designee.

6.7 Remote Wipe

Government Furnished Devices

At a minimum, all mobile devices shall be capable of being remotely erased or otherwise placed in a state where the information on the device is not recoverable as defined by HHS policy.

Personally Owned Devices

At a minimum, all personally owned devices shall have a secure enclave/ container that is capable of being remotely erased or otherwise placed in a state where the information on the device is not recoverable as defined by HHS policy. In addition, access to Government resources will be revoked when the secure enclave / container is wiped.

6.8 Application Whitelisting

At a minimum, all mobile devices shall be capable of enforcing limits on what applications may be installed and used on the mobile devices as defined by HHS or OPDIV policy, approved device use, and user roles and responsibilities.

Government Furnished Devices

All Government furnished equipment, mobile devices or otherwise, should be managed uniformly across each OPDIV and adhere to Department guidelines. Approved software deployments should continue to be managed according to OPDIV guidelines and mobile devices should conform to the service model.

App store applications cannot be scanned or evaluated for approval by OCISO security personnel and will not be allowed. Functional requirements are to be met by applications developed within HHS or developed for use by HHS.

Personally Owned Devices

For personally-owned devices, the use of a secure enclave/container will restrict the mixing of Federal and personal data and applications. App store applications cannot be scanned or evaluated for approval by OCISO security personnel and will not be allowed in the secure enclave / container. Within the secure enclave/container, only applications developed within HHS or developed for use by HHS will be approved.

6.9 Additional Considerations

Additional work will be needed in a number of areas that may impact the security of mobile devices and the risk state of HHS and OPDIV. These areas include, but are not limited to:

- Required policy for each OPDIV regarding mobile devices
- OPDIV-specific determination on where are the backups and how are the managed (where are they scattered on desktops, cloud backup services etc.)

- Establishing information flow enforcement requirements and controls.
- How to address device, operating system and vendor diversity
- Development of standardized methods, procedures, and capabilities for mobile device data encryption, key recovery, and disposition
- Identifying approved uses of mobile devices within HHS
- Development of mobile device enforcement and monitoring programs and capabilities

For additional information on recommended Device Policies and Organizational Policies, please refer to Appendix A.

7. Recommendations

The following recommendations support the HHS strategy for mobile devices and balance security with business needs. HHS should take a concurrent two-pilot approach to the implementation of mobile devices. In the first pilot, HHS should institute a pilot program to test the use of Government furnished mobile devices in a controlled and managed environment. In the second pilot, HHS should institute a pilot program to test the use of personally owned mobile devices with a FIPS 140-2 certified secure enclave / container that can restrict the mixing of federal and personal data. The following steps should be taken to institute a pilot program to begin the first pilot of Government furnished mobile device implementation:

- Initiate a test program that allows mobile devices to connect to HHS email and other systems as long as minimum security requirements are met in order to gather information and support planning efforts. Conduct a pilot of government employees using government furnished mobile devices that meet minimal password, time-out, and encryption requirements to determine how they may be used in the current operating environment.
- Connect mobile devices in the pilot program to HHS email using the Active sync control mechanisms of the HHS Enterprise Email System.
- Ask a select group of users to approve review of their usage patterns by authorized individuals on a pilot basis. Review the pilot data to determine use patterns and expected risks of a wider deployment.
- Obtain samples of representative mobile devices (e.g. iPad, other tablets) and conduct control testing.
- Refine use cases based on collected usage data and mobile device testing results.
- Review and update the business requirements for mobile devices within the HHS enterprise
- Identify the available in-place protective measures and the configuration requirements for their effective use. (what tools exist in the enterprise and at OPDIVS to support requirements)
- Refine acceptable uses and contexts for mobile devices (i.e. approved use cases for personally owned and government furnished equipment)
- Identify deficiencies in HHS capabilities and available industry solutions in support of enterprise-planning activities.
- Based on information collected from these efforts, develop a plan to mitigate risks, develop policies, finalize requirements, and begin implementation planning.
- Initiate a pilot program to test and validate technologies, develop standard procedures for mobile device usage, begin developing communication plans and training programs, finalize implementation plans and begin procurement planning.