Mobile Devices

Intended Audience

- All ARIES Users
- Managers and Supervisors
- Administrative Agencies

Policy Background

Mobile computing has become an inherent part of doing business. Most mobile computing and removable storage devices have the capacity to store information. ARIES users shall ensure due diligence is taken to protect this information appropriately, and shall take reasonable precautions for both the security of their mobile computing and removable storage devices, and the information they contain regardless of whether or not the information is considered sensitive or confidential.

For the purposes of this Policy, a mobile computing device is defined as any portable device, such as a laptop, personal digital assistant (PDA), Blackberry, tablet PC, cell phones, or smartphones. A removable storage device includes, but is not limited to, a compact disc (CD), digital video disc (DVD), flash drive, diskette, or other device that has the ability to store information. This definition is applicable to any new mobile device technology as it is developed.

These guidelines do not alleviate the contractor's responsibilities for adhering to federal Health Insurance Portability and Accountability Act (HIPAA) regulations for electronic protected health information.

Procedures

Agencies must demonstrate accountability and due diligence in the use of mobile devices to conduct ARIES-related activities. The proper safeguarding of mobile devices is imperative. Agencies must ensure that:

- Mobile computing and removable storage devices shall not be left unattended at the worksite at any time. When taken off the worksite premises, these devices shall not be separated from employees at airports, automobiles, or hotel rooms.
- Laptops and tablet PCs used at an assigned workstation shall be cable-locked to an immovable surface, or removed from a docking station and placed in lockable storage whenever the user leaves the workstation.
- Users shall take precautions to ensure other persons cannot view on-screen data in public locations.
- The identification number of the mobile computing device shall be recorded and kept separately in a safe place. It shall not be stored with the mobile computing device or in the carrying case.

- Users sign an agreement through which they acknowledge their understanding of mobile device usage and responsibilities. These agreements must be kept up to date and available for review by the State Office of AIDS (OA) or an Administrative Agency (AA).

- Mobile devices used for ARIES-related business are available for inspection by OA or an AA, upon request.

- OA is notified immediately if a mobile device used in the performance of ARIES-related activities is lost or stolen (see ARIES Policy Notice No. B1 regarding Security Incident Reporting).

Security/Confidential Information – Information related to HIV/AIDS must be kept as secure as possible. Agencies must ensure that:

- Data files on mobile devices that contain confidential information (client-identifying information such as names, social security numbers, unique record number (URN), addresses, telephone numbers, e-mail addresses, medical record numbers, etc.) only if specifically authorized in writing by OA or an AA.

- Data encryption technology must be used to protect confidential information. Encryption can be implemented at the drive, folder, or file level.

- When applicable, a disk drive lock should be installed on the mobile device.

- Mobile devices are password protected and enable password protection after a preset amount of inactivity. Passwords must have a minimum of eight characters including the use of upper and lower case letters and numbers. Passwords must not be shared or written down and must be changed every 90 days.

- Mobile devices are protected by a power-on password.

Software – Many mobile devices utilize software products to provide functionality. Software flaws can leave mobile devices vulnerable to external threats. Agencies must ensure that:

- When applicable, all mobile devices have anti-virus software and security patches installed and updated on a regular (at least monthly) basis.

- Computer software is acquired from reputable sources that assure the integrity of the software.

- All commercial software installed on each device must have a valid license, and software license agreements, terms and conditions, and copyright laws must be strictly followed.

- Reasonable steps are taken to protect against the installation of unlicensed or malicious software.

Disposition – Mobile devices are often reassigned, replaced or decommissioned as staff and technology changes. The information contained in mobile devices needs to be properly disposed of when mobile devices are reused, recycled, or otherwise disposed of. Agencies must ensure that:

- Prior to disposal of any mobile devices, the data residing on any device must be sanitized to eliminate the recorded data.

- If the wiping process is not able to initiate (e.g., system will not boot or recognize the drive) or the process is not able to complete error free, the disk drive must be removed from the device and physically modified or destroyed in such a way as to make the data unrecoverable.

- Methods for sanitizing a mobile device do not allow for the retrieval of data using data recovering/salvaging software or services.

- Mobile devices that contain confidential information are sanitized or destroyed before being designated as excess or surplus, reassigned to other staff, or before being sent off-site for repair.

- Rapid advances in technology preclude development of a comprehensive policy that specifically identifies all types of storage media. Magnetic positions on specially coated Mylar are no longer the only method of digital storage. Storage devices other than magnetic presently exist and certainly new devices will be developed. Regardless, the intent is the same – do not dispose of devices or media that store data unless the information can be certified unrecoverable.

Additional Information

- OA contractors can consult the Business Associates Agreement in their Master Agreement for more information.

Related Policies

- ARIES Policy Notice No. B1 regarding Security Incident Reporting

- ARIES Policy Notice No. B3 regarding Computer Workstations