Mobile Device Security and Storage Media Management

`2021.1`

MiCT recognizes that media containing sensitive data may be reused when appropriate steps are taken to ensure that all stored sensitive data has been effectively rendered inaccessible. Destruction/disposal of sensitive data shall be carried out in accordance with federal and state law. The schedule for destruction/disposal shall be suspended for sensitive data involved in any open investigation, audit, or litigation.

MiCT utilizes virtual storage repositories such as AWS EBS volumes and S3 buckets to store production data. Volumes and repositories utilized by MiCT and MiCT Customers are encrypted. MiCT does not use, own, or manage any mobile devices, removable storage media, or backup tapes that have access to sensitive data.

Policy Statements

MiCT policy requires that:

(a) All media, including mobile and removable media, storing MiCT company data must be encrypted.

(b) Critical data as defined in MiCT data classification model §data-management may not be stored on mobile devices or removable media such as USB flash drives.

(c) All destruction/disposal of sensitive data storage media will be done in accordance with federal and state laws and regulations and pursuant to the MiCT's written retention policy/schedule.

- Records that have satisfied the period of retention will be destroyed/disposed of in an appropriate manner.
- Records involved in any open investigation, audit or litigation should not be destroyed/disposed of.

(d) All sensitive data must rendered inaccessible in a forensically sound manner prior to media reuse or disposal.

(e) Mobile devices, including laptops, smart phones and tables, used in support of critical business operations shall be fully managed and/or audited by MiCT IT and Security.

Controls and Procedures

Media Disposal Process

IT and Security is responsible to ensure media containing critical / sensitive data is disposed securely in the following manner:

- The methods of destruction, disposal, and reuse are reassessed periodically, based on current technology, accepted practices, and availability of timely and cost-effective destruction, disposal, and reuse technologies and services. This may include
  - Secure wipe;
  - Physical destruction;
  - Destruction of encryption keys (if the data on the media is encrypted using a strong algorithm such as AES-256).
- If the records have been requested in the course of a judicial or administrative hearing, a qualified protective order will be obtained to ensure that the records are returned to the organization or properly destroyed/disposed of by the requesting party.
- All MiCT Subcontractors provide that, upon termination of the contract, they will return or destroy/dispose of all patient health information. In cases where the return or destruction/disposal is not feasible, the contract limits the use and disclosure of the information to the purposes that prevent its return or destruction/disposal.
- In the cases of a MiCT Customer terminating a contract with MiCT and no longer utilize MiCT Services, data will be returned or disposed per contract agreement or MiCT Platform use terms and conditions. In all cases it is solely the responsibility of the MiCT Customer to maintain the safeguards required of laws and regulations once the data is transmitted out of MiCT environments.

Use of USB Flash Drive and External Storage Device

Per MiCT corporate policy, confidential and critical data may not be stored on external devices such as USB flash drives. This includes and is not limited to ePHI. For definition of confidential and critical data, see MiCT Data Classification and Handling Policy.

Usage of USB flash drives for temporary transfer of confidential and critical data may be allowed on a case by case basis, when the following process is followed:

- Data is only allowed on encrypted flash devices approved by MiCT Security and the IT Manager (currently **IronKey**).
- The process starts with the submission of a ticket in Github. The ticket must be approved by IT and Security.

- Upon completion of data transfer all sensitive data on the device must be completely removed.
- The device is to be returned to the IT Manager to double check that the data has been removed.
- The IT Manager will check the drive back in.

Support and Management of BYOD Devices

MiCT provides company-issued laptops and workstations to all employees.

MiCT currently does not require or support employees bringing their own computing devices.

The end-user computing devices are self managed. Each MiCT employee is responsible to

- configure their laptop/workstation to meeting the configuration and management requirements; and
- ensure the latest security patches are installed or auto-update is enabled.

IT and Security provides automated scripts for end-user system configurations and/or technical assistance as needed. Such configurations are audited daily using **Jamf** centrally managed by the Security team.