
TITLE: **INFORMATION SECURITY: DEVICE AND MEDIA CONTROLS**

POLICY:

Reasonable steps are taken to protect, account for, properly store, back up, encrypt and dispose of hardware, paper and electronic media.

PURPOSE:

Secure information stored on paper, disks, tapes, and other electronic media.

APPLICABILITY:

Hospital staff, employees, affiliates, owners, custodians, and users of information systems

PROCEDURE:

1. Types of hardware and media to which this policy applies include:
    - Computers (servers, desktops, laptops, tablets, other)
    - Smart phones
    - Portable storage media, USB drives, CD/DVD, Zip, memory cards, removable storage for cameras and smart phones
    - Tapes and external Hard drives
    - Paper records

2. Workforce members may not attempt to physically duplicate, copy or move information for which they have not been authorized by a Director-level (or above) person in their department or the department head. The Owner of an information system may establish additional limits for the Users and Custodians of the system. All institutional policies are applicable to any copies (paper or electronic) that are made. The department head and workforce member who makes the copies are responsible for the security of the information.

3. All computers connected to institutional networking resources are registered in the Hospital's Information Technology (IT) Service Management system in order to be authorized for access to institutional information (see *Asset Inventory Procedure*). Alternatively, institutional authentication methods that identify the

owner with a valid authorization to connect to the network to access resources, and create an appropriate audit log may be used for asset registration. Any computer that is not registered with either the Hospital or its affiliates' asset management is not authorized to connect to the institutional network.

4. **Servers**

All Hospital information systems servers, whether physical or virtual, follow these rules:

A. Servers are placed in IT approved data centers; or servers are in a hosted or cloud environment with appropriate Legal, IT Security and IT Operations approval.
B. Exceptions, with documentation, are permitted for certain servers which have physical placement restrictions for their operation (such as biomedical device servers), and they require appropriate physical and operational security checks under *Risk Analysis Procedure*.
C. Servers used for Hospital functions are managed by IT unless an exception is approved and documented in the IT Service Management system. This document requires approval from Hospital's operational Vice President, IT Operations and IT Security.

   If an Affiliate owns and manages servers/systems used for Hospital functions, the exception document includes explicit sign-off on Information Security and Operations risk analysis and monitoring from the Affiliate's Information Security Office.
D. Hospital departments are not permitted to purchase servers outside of rules stated above.
E. Personally owned and managed information servers are forbidden.

5. **Desktops**

All desktops physically connected to the network are authorized to access Hospital information systems and follow these rules:

A. Desktops are under active inventory and management of IT with full disk encryption and with active and current anti-virus protection (See *Asset Inventory Procedure* and ***Workstation Use and Security policy*** (#I230)); or Desktops are under the inventory and management of an Affiliate, are

encrypted and password protected, and are certified by the Affiliates' Information Security Office.

B. Personally owned desktops are not permitted to be physically connected to the network. (Also see Personal Endpoints below.)
C. Hospital departments are not permitted to purchase desktops to be placed on the Hospital network outside of rules stated above. Refer to the Infonet *Information Services Hardware Price Guide* for a list of appropriate desktop devices.

Certain exceptions are permitted in the case of biomedical devices and workstations, or for others on a case by case basis, and such exceptions are approved and documented by IT Operations and IT Security. Additional documented physical and technical security controls are specified and implemented for desktops with possible sensitive data to mitigate the risk of such exceptions.

6. **Hospital owned Mobile Endpoints (Laptops, Tablets, Smartphones)**

All Hospital owned endpoints follow these rules

A. IT identifies a set of endpoints to be the Hospital standard. Hospital departments may acquire only the Hospital standard equipment and coordinate with IT for distribution and use.
B. Before distribution and use, the endpoints are configured by IT for encryption and password protection. Users may not bypass these controls.
C. Hospital owned Tablets and Smartphones are configured by IT for Mobile Device Management (MDM) for a higher level of control of these devices, in addition to encryption and password protection. Users may not bypass these controls. Configuration changes are requested to IT for approval and documentation.
D. IT maintains the inventory based on the *Asset Inventory Procedure*.

7. **Personal Endpoints**

A. Personal desktops and laptops are not permitted to connect physically to the Hospital network (See Desktops above).

B. Workforce members accessing the Hospital information systems remotely using a personal desktop or laptop implement standards specified in the

policy. Specifically:

a. Managers request remote access privilege for a workforce member to IT Service Desk in order to document the need for remote access.
b. Workforce members attest to understanding of the security requirements on their behavior and management of their devices.
c. Full disk encryption, password protection and active and current anti-virus protection are required on all endpoints.
d. Regular security patching and upgrades of all software including operating system and other third party applications is required.
e. Use of such devices by the workforce member and other family members is highly discouraged for general Internet surfing, program downloading, gaming, and other family recreational activities.
f. Workforce members employ secure configuration of their home networks and routers with strong passwords.
g. IT may monitor these devices when they connect to the Hospital networks and systems, and may require appropriate patches and other security controls and restrictions in order to protect Hospital information resources.

C. Personal Tablets and Smartphones of Hospital employees and workforce requiring access to the Hospital information systems are permitted only with documentation of management approval and configured to be managed by the Hospital MDM by IT (see *Access Authorization for non-NYP Issued Devices Procedure*).

D. Personal Tablets and Smartphones of affiliated staff requiring access to the Hospital information systems are permitted only if they are configured to be managed by the Affiliate's MDM solution equivalent to the Hospital MDM.

E. All users are required to attest to the adherence to the remote and personal device access policies and procedures during training. The users understand that the Hospital MDM will alter configuration on their personal device, and impose password and encryption requirements of Hospital policy, and will continue to add other configuration changes and restrictions in future in order to protect Hospital information resources. (see *Access Authorization for non-NYP Issued Devices Procedure*).

F. In rare cases involving patient care scenarios and other important business reasons, exceptions may be granted with IT Operations and IT Security approval and documentation.

8. **Storage devices**

A. All external mobile storage devices (USB drives, flash cards, removable disk drives, Zip drives) must be encrypted and password protected for storage of sensitive information including EPHI. The Hospital has identified a list of fully encrypted USB drives for Hospital use by the workforce and affiliates in the Infonet *Information Services Hardware Price Guide*.
B. This list of USB drives are permitted to be connected to Hospital desktops. If a different USB drive, fully encrypted or otherwise, is used with Hospital desktops, a Data Loss Prevention (DLP) software may block or warn the user, or seek attestation from the user, when data is attempted to be copied to the USB drive. Refer to the *Data Loss Prevention Standard* for more information.
C. DLP may take the same action when data is copied to a CD/DVD or other drives.

9. **Disposal of Devices and Media**

Disposal of Hospital issued devices and media is performed in accordance with the *Disposal of Decommissioned Computer Equipment Procedure*.

A. Onboard storage media and hard drives are removed from computers, appliances and servers for destruction.
B. In rare cases where removal and destruction is prohibited by a contractual agreement, exceptions may be granted by requesting IT Service Desk for approval and documentation. In such cases, sensitive hospital information is removed from the storage media and hard drives through a magnetic erasure process or a industry standard disk overwrite technique.
C. Removable media is destroyed when no longer in use or for certain media types, users deposit media directly into Hospital's shredder containers for destruction (Refer to container label for supported media types).
D. Smartphones are remotely wiped through MDM to remove Hospital information.

Disposal of personal devices and media is performed in accordance with the *Access Authorization of non-NYP Issued Devices Procedure*.

E. Upon termination of employment, the device is remotely wiped of Hospital information by MDM for registered personally owned endpoint.
F. Upon upgrade of a registered personally owned device, the old device is remotely wiped of Hospital information and the new device is registered with the MDM.
G. When no longer in use, a personal storage device is either destroyed or sensitive hospital information is manually removed. Users deposit supported media types directly into Hospital shredder containers for destruction (Refer to container label for supported media types).

10. **Backup of Information**

Custodians make exact and retrievable backup copies of information (including sensitive data) on an ongoing basis to guard against system failures and data corruption. (Also see ***Information security: Disaster contingency and recovery plan policy*** (# I250).) Custodians take reasonable steps to ensure that information that is backed up in connection with movement of equipment can be recovered following a disaster or other emergency, or a failure of the equipment.

11. Owners and custodians ensure that all backup copies that are transported to any remote location are encrypted. If there are reasons that preclude encryption, then these reasons are approved and documented by IT Operations and IT Security.

12. Owners and custodians may arrange to store backup copies in a secure, remote location. Remote storage is required to have appropriate physical and environmental protection. The ability to retrieve the backup copies in a timely manner is also required.

13. Owners and custodians are responsible to ensure that before media (tapes, disks, storage cards, etc.) are re-used, the information (including sensitive data) on the media is completely and irreversibly removed using appropriate erasure tools. Hardware and media on which information is stored may be physically destroyed if the hardware and media are to be disposed of permanently.

14. Paper Documents Containing Sensitive Data

Creation of paper documents containing sensitive data is prohibited unless *absolutely* necessary to accommodate clinical needs or business and regulatory requirements.

Examples of applicable documents include:

- Printed documents, labels, prescriptions, etc.
- Hand-written notes and memos

- Faxed documents
- Duplicate (copied) documents

A. In general, do not create copies of paper documents unless *absolutely* necessary.
B. Any documents, whether printed inside or outside of the Hospital premises, are handled in accordance with this policy.

15. Distribution and delivery of paper documents containing sensitive data is prohibited unless necessary to accommodate clinical needs or business and regulatory requirements.
   A. If paper documents are used in meetings or rounds, they are collected back from recipients at the conclusion of meetings or rounds or safely destroyed (see below) unless necessary to accommodate clinical needs or business and regulatory requirements.
   B. Delivery of paper documents containing sensitive data are made person to person only, whenever possible.

16. Storage of paper documents containing sensitive data is prohibited unless necessary to accommodate clinical needs or business and regulatory requirements.
   A. Do not print sensitive data to an unattended printer or fax machine.
   B. Do not leave extra pages, paper jam sheets, etc. in unsecured areas.
   C. Store documents in a secure location under lock and key except where the document is part of the official medical record where access is restricted to a secure location.
   D. Do not store paper documents in an unauthorized off-campus location (such as at home or in car).
   E. Paper documents used for matters conducted off campus are returned to campus at the conclusion of business or safely destroyed as below.

17. Transportation of paper documents containing sensitive data is prohibited unless necessary to accommodate clinical needs or business and regulatory requirements.
   A. Transportation of paper documents containing sensitive data to off-campus locations is prohibited unless necessary to accommodate clinical needs or business and regulatory requirements.
   B. Documents are transported in a physically secured and private manner so that no data is visible.
   C. Transportation of documents between Hospital locations are done:
      1. In the possession of a Hospital workforce member, or;
      2. Via Hospital shuttle service with person to person drop-off/pickup, or;
      3. Via a professional messenger service.

18. If retention of paper documents containing sensitive data is necessary, retention must conform to hospital policy.
    A. Each Vice President or his/her designee (departmental administrator) for a department is responsible for retention of paper documents in accordance with Hospital policies ***Medical Record Retention and Storage policy*** (# H125), ***Record Retention policy*** (# R140), etc.
    B. Original documents containing sensitive data should be destroyed when obsolete unless retention is required in accordance with Hospital policy ***Record Retention policy*** (# R140).
    C. Duplicate documents containing sensitive data are destroyed in accordance with this policy.

19. When no longer necessary, paper documents containing sensitive data are destroyed in a private and secure manner:
    A. Deposit paper into a Hospital provided secure, locked shredding container, or;
    B. Render paper un-readable via shredding or cutting each sheet.

20. Loss or theft of device or media

    If any device or media used for access or storage of Hospital information, whether institutional or personal, is misplaced, lost or stolen, workforce members immediately report the incident to the Privacy Office or the Information Security Office through direct contact or through the IT Service Desk (See ***Information Security Incident Procedure policy*** (#I255)).

RESPONSIBILITY:

Information Security Office

REFERENCES:

All information security policies
Access Authorization for non-NYP Issued Devices Procedure (IT-CS-003)
Asset Inventory Procedure (IT-CS-004)
Disposal of Decommissioned Computer Equipment Procedure (IT-DS-005)
Information Services Hardware Price Guide (IT-DS-001-S1)
Information Security Standard IS-Std-004 Data Loss Prevention (IT-SEC-STD-004)
Risk Analysis Procedure (IT-SEC-001)
Health Insurance Portability and Accountability Act of 1996, 45 CFR 164.310(d)(1),

164.310(d)(2)(i), 164.310(d)(2)(ii),
164.310(d)(2)(iii), 164.310(d)(2)(iv)

REVIEW/REVISION DATE:

March 2005
June 2009
June 2011
Revised: June 2013; **March 2015**