Status **Active** PolicyStat ID **10742803**

Origination	06/2018	Owner	Michael Kinnell
Last Approved	06/2022	Policy Area	Information Technology
Effective	06/2022		
Last Revised	06/2022		
Next Review	06/2023		

Clean Desk Policy

POLICY

It is the policy of the Detroit Wayne Integrated Health Network (DWIHN) to maintain a clean desk to ensure that all sensitive/confidential materials are removed from an end user workspace and locked away when the items are not in use or when an employee leaves his/her workstation. This policy reduces the risk of security breaches at DWIHN and increases employee's awareness about protecting sensitive information.

PURPOSE

The purpose for this policy is to establish the minimum requirements for maintaining a "clean desk" – where sensitive/critical information about our members, employees, intellectual property, customers, and vendors is secure in locked areas and out of site. A Clean Desk policy is not only ISO 27001/17799 compliant, but it is also part of standard basic privacy controls.

APPLICATION

1. The following groups are required to implement and adhere to this policy: DWIHN Board, DWIHN Staff, Contractual Staff, Access Center, Network Providers, Crisis services vendor, Credentialing Verification Organization (CVO) and agents operating on behalf of DWIHN.
2. This policy serves the following populations: Not Applicable.
3. This policy impacts the following contracts/service lines: Not Applicable.

KEYWORDS

1. Protected health information (PHI) under US law is any information about health status, provision of health care, or payment for health care that is created or collected by a Covered

Entity (or a Business Associate of a Covered Entity), and can be linked to a specific individual.

2. Personally Identifiable Information (PII) is information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, including any other personal information which is linked or linkable to a specified individual.

STANDARDS

1. Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.
2. Computer workstations must be locked when the workspace is unoccupied.
3. Computer workstations must be shut completely down at the end of the workday.
4. Any employees with physical possession of documents containing Personally Identifiable Information (PII) or Protected Health Information (PHI) information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the workday.
5. File cabinets containing Personally Identifiable Information (PII) or Protected Health Information (PHI) must be kept closed and locked when not in use or when not attended.
6. Keys used for access to Personally Identifiable Information (PII) or Protected Health Information (PHI) must not be left at an unattended desk.
7. Portable computing devices such as laptops and tablets must be either locked with a locking cable or locked away in a drawer.
8. Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
9. Printouts containing Personally Identifiable Information (PII) or Protected Health Information (PHI) or any other confidential information should be immediately removed from the printer.
10. Upon disposal, Personally Identifiable Information (PII) or Protected Health Information (PHI) documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins.
11. Whiteboards containing Personally Identifiable Information (PII) or Protected Health Information (PHI) or any other confidential information should be erased.
12. Treat mass storage devices such as CDROM, DVD, or USB drives as sensitive and secure them in a locked drawer.
13. All printers and fax machines should be cleared of papers as soon as they are printed; this helps ensure that sensitive documents are not left in printer trays for the wrong person to pick up.

QUALITY ASSURANCE/IMPROVEMENT

Compliance Measurement

1. The Information Technology team in conjunction with the Compliance Officer will verify compliance to this policy through various methods, including but not limited to, periodic walk-

thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

1. Any exception to the policy must be approved by the Information Technology team and the Compliance Officer team in advance.

Non-Compliance

1. An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

COMPLIANCE WITH ALL APPLICABLE LAWS

DWIHN staff, contractors, and subcontractors are bound by all applicable local, state and federal laws, rules, regulations and policies, all federal waiver requirements, state and county contractual requirements, policies, and administrative directives, as amended.

LEGAL AUTHORITY

N/A

RELATED POLICIES

N/A

CLINICAL POLICY

No

INTERNAL/EXTERNAL POLICY

INTERNAL

Approval Signatures

Step Description	Approver	Date
Final Approval Policy	Eric Doeh: President and CEO	06/2022
Stakeholder Feedback	Allison Smith: Project Manager, PMP	05/2022
Director Committee Review	Yolanda Turner: Legal Counsel	05/2022