Status **Active** PolicyStat ID **10251278**

Origination	03/2018
Last Approved	06/2022
Effective	06/2022
Last Revised	06/2022
Next Review	06/2023
Owner	Michael Kinnell
Policy Area	Information Technology

Email Policy

POLICY

It is the policy of the Detroit Wayne Integrated Health Network (DWIHN) email services support the administrative activities of the organization and serve as a means of official communication by and between users and constituents. The purpose of this policy is to understand the appropriate use of electronic communications. At the same time, address how misuse of email can provide many legal, privacy, and security risks.

PURPOSE

The purpose of this email policy is to ensure the proper use of DWIHN email system and make users aware of what DWIHN deems as an acceptable and unacceptable use of its email system. This policy outlines the minimum requirements for use of email within DWIHN Network.

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

N/A

STANDARDS

1. All use of email must be consistent with DWIHN policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.
2. DWIHN email account should be used primarily for DWIHN business-related purposes; personal communication is permitted on a limited basis, but non-DWIHN related commercial uses are prohibited.
3. All DWIHN data contained within an email message or an attachment must be secured according to the Data Protection Standard.
4. Email should be retained only if it qualifies as a DWIHN business record. Email is a DWIHN business record if there exists a legitimate and ongoing business reason to preserve the information contained in the email.
5. Email that is identified as a DWIHN business record shall be retained according to DWIHN Record Retention Schedule.
6. The DWIHN email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any DWIHN employee should report the matter to their supervisor immediately.
7. Users are prohibited from automatically forwarding DWIHN email to a third party email system (noted in 8 below). Individual messages which are forwarded by the user must not contain DWIHN confidential or above information.
8. Users are prohibited from using **personal third-party account** email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct DWIHN business, to create or memorialize any binding transactions, or to store or retain email on behalf of DWIHN. Such communications and transactions should be conducted through proper channels using DWIHN-approved systems.
9. Using a reasonable amount of DWIHN resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from a DWIHN email account is prohibited.
10. DWIHN employees shall have no expectation of privacy in anything they store, send or receive on the company's email system.
11. DWIHN may monitor messages without prior notice. DWIHN is not obliged to monitor email messages.

QUALITY ASSURANCE/IMPROVEMENT

Compliance Measurement

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

N/A

LEGAL AUTHORITY

N/A

RELATED POLICIES

1. PHI Privacy and Confidentiality
2. Record Retention and Disposal Policy
3. Standards of Conduct

CLINICAL POLICY

N/A

INTERNAL/EXTERNAL POLICY

EXTERNAL

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