PURPOSE

The purpose is to establish the policy and procedure for the Michigan Department of Health and Human Services (MDHHS) to uniquely identify and track one workforce member from all others, for the purpose of access control to all networks, systems and applications that contain Electronic Protected Health Information (ePHI) and the monitoring of access to the aforementioned networks, systems and applications.

REVISION HISTORY

Reviewed: 01/01/2024.
Next Review: 01/01/2025.

DEFINITIONS

ePHI is the acronym for Electronic Protected Health Information. It is Protected Health Information that is transmitted or maintained in electronic form.

PHI is the acronym for Protected Health Information. It is information that can identify a person and contains health related data pertaining to that person.

Workforce Member means employees, volunteers and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity. This includes full and part time employees, affiliates, associates, students, volunteers and staff from third party entities who provide service to the covered entity.

POLICY

It is the policy of the MDHHS to provide all workforce members who require access to any MDHHS network, system or application that accesses, transmits or stores ePHI a unique user identification (user ID) string.

PROCEDURE

Workforce Member

Supply user ID in conjunction with a secure password when requesting access to any network, system or application that accesses, transmits or stores ePHI.

Not allow any other user to use their unique user ID or password.

ADMINISTRATIVE POLICY LEGAL **STATE OF MICHIGAN**

DEPARTMENT OF HEALTH & HUMAN SERVICES

Ensure user ID is not documented, written or otherwise exposed in an insecure manner.

Ensure assigned user ID is appropriately protected and only used for legitimate access to networks, systems, or applications. Report a security incident to the MDHHS security officer in a timely manner if believed their user ID has been compromised.

REFERENCES

45 CFR 164.312(a)(1)

CONTACT

For additional information concerning this policy and procedure, contact the MDHHS Compliance and Data Governance Bureau at MDHHSPrivacySecurity@michigan.gov.