Status **Active** PolicyStat ID **11121876**

Origination	02/2021
Last Approved	09/2022
Effective	09/2022
Last Revised	09/2022
Next Review	09/2023
Owner	Sheree Jackson
Policy Area	Compliance
References	164.308(a)(1)(ii)(C), 45 CFR §§ 164.400 – 164.414, 45 CFR §§ 164.530

Data Breach Notification Policy

POLICY

It is the policy of Detroit Wayne Integrated Health Network (DWIHN) to provide notification of any Breaches of Unsecured PHI in accordance with the requirements of the HIPAA rules and the federal HITECH Act.

PURPOSE

The purpose of this policy is to describe steps that must be taken in the event of a Breach of Unsecured PHI, including providing notification of such Breach to:

1. Each consumer whose Unsecured PHI has been, or is reasonably believed to have been, Breached;
2. The Secretary of the U.S. Department of Health and Human Services ("HHS"); and
3. Prominent media outlets serving the state or jurisdiction if the Breach involves more than 500 residents of such state or jurisdiction.

APPLICATION

1. The following groups are required to implement and adhere to this policy: DWIHN Board, DWIHN Staff, Contractual Staff, Direct Contracted Network Providers and their subcontractors, Access Center, Crisis Services Vendors, Credentialing Verification Organization (CVO)
2. This policy serves the following populations: Adults, Children, I/DD, SMI, SED, SUD, Autism
3. This policy impacts the following **contracts/service lines**: MI-HEALTH LINK, Medicaid, SUD, Autism, Grants, General Fund

KEYWORDS

For the purpose of this Policy, the following definitions shall apply:

1. **Breach** means the acquisition, access, use or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rules which compromises the security or privacy of the PHI, provided that the following shall not constitute a Breach:
    a. Any unintentional acquisition, access or use of PHI by a Workforce Member or agent of DWIHN if it was made in good faith, within the scope of such individual's authority and does not result in further unauthorized use or disclosure of the PHI;
    b. Any inadvertent disclosure by a person authorized to access PHI by DWIHN to another person authorized to access PHI within DWIHN or organized health care arrangement in which DWIHN participates, provided there is no further unauthorized use or disclosure of the PHI; and
    c. A disclosure of PHI in which DWIHN has a good faith belief that the unauthorized person to whom the disclosure was made would not reasonably have been able to retain the PHI.
2. **HIPAA** means the Health Insurance Portability and Accountability Act of 1996, and any subsequent amendments thereto.
3. **HIPAA Privacy Rules** means the Privacy of Individually Identifiable Health Information regulations promulgated pursuant to HIPAA.
4. **Personal Information** means an individual's first name or first initial and last name in combination with any one or more of the following data elements when not encrypted or redacted:
    a. Social Security number;
    b. Driver's license or State identification card number; or
    c. Account number or credit or debit card number, or an account number or credit card number in combination with any required code or password that would permit access to the individual's financial account.
5. Personal Information does not include publicly available information that is lawfully made available to the general public from federal, state or local government records.
6. **Personal identifying information** means a name, number, or other information that is used for the purpose of identifying a specific person or providing access to a person's financial accounts, including, but not limited to, a person's name, address, telephone number, driver license or state personal identification card number, social security number, place of employment, employee identification number, employer or taxpayer identification number, government passport number, health insurance identification number, mother's maiden name, demand deposit account number, savings account number, financial transaction device account number or the person's account password, any other account password in combination with sufficient information to identify and access the account, automated or electronic signature, biometrics, stock or other security certificate or account number, credit card number, vital record, or medical records or information.

7. P**rotected Health Information ("PHI")** means information, including demographic information, that:
    a. Is created or received by a health care provider, health plan, employer, or health care clearinghouse;
    b. Relates to the past, present or future physical or mental condition of a consumer, the provision of healthcare to a consumer, or the past, present or future payment for the provision of healthcare to a consumer; and
    c. Identifies the consumer (or there is a reasonable basis to believe the information can be used to identify the consumer).
8. **Unsecured PHI** means PHI, in any medium, that is not maintained in a form which has been identified by HHS as a method for rendering the PHI unusable, unreadable or indecipherable to unauthorized individuals through the use of a technology or methodology specified in guidance issued by HHS. As of the effective date of this Policy, PHI will be deemed unusable, unreadable, or indecipherable if the PHI is either:
    a. Encrypted using a process identified and tested by the National Institute of Standards and Technology ("NIST") to meet this standard. For data at rest, such process shall be consistent with NIST Special Publication 800-111. For data in motion, such process shall be consistent with NIST Special Publication 800-52, 800-77, or 800-113, or other processes which are Federal Information Processing Standards 140-2 validated; or
    b. Destroyed such that the PHI cannot be read or reconstructed. For PHI maintained in an electronic form, the PHI must be destroyed in a manner consistent with NIST Special Publication 800-88. (Note: Redaction is not an acceptable method for destroying PHI.)
9. **Workforce Member** means employees, volunteers, trainees, and any other persons whose conduct and performance of services for DWIHN is under the direct control of DWIHN, and includes physicians, whether or not the individual receives compensation from DWIHN for such services.

STANDARDS

1. **REPORTING AN ACTUAL OR SUSPECTED UNAUTHORIZED USE OR DISCLOSURE OF PHI.** Any actual or suspected use or disclosure of PHI believed to be in violation of the HIPAA Privacy or Rules shall be immediately reported to the Privacy Officer. The suspected unauthorized use or disclosure shall be handled in the following manner:
    a. Workforce Member. In the event a suspected unauthorized use or disclosure is discovered by a Workforce Member, the Workforce Member shall immediately notify the Department Director, Manager or Administrative Director, as applicable, who shall report the incident to the Privacy Officer.
    b. Business Associate. In the event DWIHN receives notification of a suspected use or disclosure of PHI from a Business Associate, the Privacy Officer shall coordinate with the Business Associate to ensure that all necessary information regarding the incident and affected consumers is obtained.

c. Business Associate shall report to DWIHN any use or disclosure of PHI not provided for in the Business Associates Agreement of which it becomes aware, and/or any security incident of which it becomes aware, within ten (10) calendar days after discovery.

d. In addition, Business Associate shall undertake the following in connection with the breach notification requirements of HITECH.

    1. If Business Associate discovers a breach of unsecured PHI, as those terms are defined by 45 CFR 164.202, Business Associate shall notify DWIHN Privacy Officer without unreasonable delay and within five (5) calendar days after discovery. For this purpose, discovery means the first day on which the breach is known to Business Associate or by exercising reasonable diligence would have been known to Business Associate. Business Associate shall be deemed to have knowledge of a breach if the breach is known or by exercising reasonable diligence would have been known to any person, other than the person committing the breach, who is an employee, officer, subcontractor or other agent of Business Associate. The notification must include identification of each individual whose unsecured PHI has been, or it has reasonably believed to have been, breached and any other available information in Business Associate's possession which DWIHN or Business Associate is required to include in the individual notice contemplated by 45 CFR 164.

    2. Notwithstanding the immediately preceding paragraph, Business Associate shall assume the notice obligation specified in 45 CFR 164.404 on behalf of DWIHN where a breach of unsecured PHI was committed by Business Associate or its employee, officer, subcontractor or other agent of Business Associate or is within the unique knowledge of Business Associate as opposed to DWIHN. In such case, Business Associate will prepare the notice and shall provide it to the DWIHN Privacy Officer for review and approval at least five calendar days before it is required to be sent to the individual. The DWIHN Privacy Officer will promptly review the notice and will not unreasonably withhold its approval, but may in its sole discretion make a determination to amend the notice or assume responsibility for distribution of the notice. In the event, the DWIHN Privacy Officer does not provide a timely response, the Business Associate may proceed with distribution.

    3. If there is a breach involving the PHI of 500 or more Individuals committed by the Business Associate or its employee, officer, subcontractor or other agent, or is within the unique knowledge of Business Associate as opposed to DWIHN, Business Associate shall provide notice to the media pursuant to 45 CFR 164.406. Business Associate will prepare the notice and shall provide it to DWIHN Privacy Officer for review and approval at least five (5) calendar days before it is required to be sent to the media. The DWIHN Privacy Officer shall promptly review the notice and shall not unreasonably withhold its approval, but does retain discretion to amend the notice or assume control of media distributions. In the event, the DWIHN Privacy Officer does not provide a timely response, the Business

Associate may proceed with distribution.

4. Business Associate shall maintain a log of breaches of unsecured PHI with respect to DWIHN and shall submit the log to the DWIHN Privacy Officer within thirty (30) calendar days following the end of each calendar year so that the DWIHN Privacy Officer may report breaches to the Secretary in accordance with 45 CFR 164.408.

2. **DETERMINING WHETHER A BREACH OF UNSECURED PHI OCCURRED**
Upon receiving a report of any actual or suspected unauthorized use or disclosure of PHI as described in Section 1, the Privacy Officer shall immediately investigate the incident to determine if the incident resulted in a Breach of Unsecured PHI. This investigation shall include the following steps:

   a. Step 1. Determine whether the incident resulted in a violation of the HIPAA Privacy Rules. If yes, then proceed to Step 2. If no, then no Breach of Unsecured PHI occurred and no notification is required under this Policy.

   b. Step 2. Determine whether the incident involved "Unsecured PHI" (as defined in the Keywords). If yes, then proceed to Step 3. If no, then no Breach of Unsecured PHI occurred and no notification is required under this Policy.

   c. Step 3. Determine whether the incident is excluded from the definition of the term "Breach" (as defined in the Keywords). If yes, then proceed to Step 4. If no, then no Breach of Unsecured PHI occurred and no notification is required under this Policy.

   d. Step 4. Conduct a risk assessment to determine whether the incident demonstrates that there is a low probability that the protected health information has been compromised using the following factors:

      1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
      2. The unauthorized person who used the protected health information or to whom the disclosure was made;
      3. Whether the protected health information was actually acquired or viewed; and
      4. The extent to which the risk to the protected health information has been mitigated.
      If, based on the risk assessment, it is determined that the incident demonstrates that there is a low probability that the protected health information has been compromised, DWIHN, in consultation with legal counsel if appropriate, shall conclude that no Breach of Unsecured PHI has occurred and that no notification is required under this Policy.

   e. If, based on the risk assessment, it is determined that the incident demonstrates that there is a low probability that the protected health information has been compromised, DWIHN, in consultation with legal counsel if appropriate, shall conclude that no Breach of Unsecured PHI has occurred and that no notification is required under this Policy.

3. **PROCEDURE IF NO BREACH OF UNSECURED PHI OCCURRED**

If based on Steps 1through 4 above, the DWIHN Privacy Officer determines that the incident did not constitute a Breach of Unsecured PHI, the DWIHN Privacy Officer shall document such conclusion and the rationale for such conclusion and shall maintain such documentation and any additional supporting documents for a period of at least six (6) years from the determination.

4. **PROCEDURE IF A BREACH OF UNSECURED PHI OCCURRED**
If based on Steps 1-4 above, the DWIHN Privacy Officer determines that a Breach of Unsecured PHI occurred, the DWIHN Privacy Officer shall provide notice of the Breach and maintain documentation of such notice as follows:

    a. *NOTICE TO CONSUMER*. Unless contrary instructions from law enforcement are received (see Section 5(d) below), written notice of Breach shall be provided to each consumer whose Unsecured PHI has been Breached, or is reasonably believed to have been Breached, as follows:

        1. Timing of Notice. The notice shall be provided promptly and no later than sixty (60) days after DWIHN discovers the Breach. The Breach is considered to be discovered on the first day on which the Breach is known, or would have been known by exercising reasonable diligence to any person who is a Workforce Member or agent of DWIHN (other than the person committing the Breach).
        2. Manner of Notice. The notice shall be sent by first-class mail addressed to the consumer's last known address. Notice may be sent electronically if the consumer has agreed to receive electronic notice and the agreement has not been withdrawn. If DWIHN knows that the consumer is deceased, DWIHN shall provide written notice to the next-of-kin or personal representative of such consumer if DWIHN has the addresses of those individuals. Notice may be provided in one or more mailings as additional information becomes available.
        3. Content of Notice. The notice shall be written in plain language and shall contain the following information:
            i. a brief description of the incident, including the date of the Breach and the date of the discovery of the Breach if known,
            ii. a description of the types of Unsecured PHI involved in the Breach (rather than a description of the specific PHI),
            iii. any steps the consumer should take to protect himself or herself from harm resulting from the Breach,
            iv. (brief description of what DWIHN is doing to investigate the Breach, to mitigate the harm to the consumer and to protect against future occurrences, and
            v. contact procedures for the consumer to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, website or postal address.
        4. Substitute Notice. If there is insufficient or out-of-date contact information for a consumer that precludes written notice to such consumer, as soon

as reasonably possible after such determination, DWIHN shall provide notice reasonably calculated to reach the consumer as described below.

i. If there is insufficient or out-of-date contact information for fewer than ten (10) consumers, notice may be provided by e-mail, telephone or other means.

ii. If there is insufficient or out-of-date contact information for ten (10) or more consumers, notice shall (1) be in the form of either a conspicuous posting for ninety (90) days on DWIHN's website home page or conspicuous notice in major print or broadcast media in geographic areas where the affected consumers likely reside, and (2) include a toll-free number that remains active for at least ninety (90) days so that the consumer can learn whether his or her Unsecured PHI was included in the Breach.

iii. Substitute notice need not be provided if the affected consumer is deceased and DWIHN has insufficient or out-of-date contact information for the next of kin or personal representative of the consumer.

5. Additional Notice in Urgent Situations. If DWIHN determines there is potential for imminent misuse of the Unsecured PHI in connection with a Breach, DWIHN may provide information regarding the Breach to consumers by telephone or other means, as appropriate, in addition to providing the required written notice as described above.

b. *NOTICE TO HHS.* Unless contrary instructions from law enforcement are received (see Section 5(d) below), in addition to notifying the consumer as described above, DWIHN also shall notify HHS of the Breach of Unsecured PHI. Such notification shall be provided as follows:

1. If the Breach involves 500 or more consumers, DWIHN shall notify HHS of the Breach contemporaneously with providing the notice to the consumer and in a manner specified by HHS on its website.

2. If the Breach involves less than 500 consumers, DWIHN shall maintain a log or similar documentation of the Breach and shall provide the required documentation to HHS no later than sixty (60) days after the end of each calendar year in the manner specified by HHS on its website.

c. *NOTICE TO MEDIA.* Unless contrary instructions from law enforcement are received (see Section 4(d) below), if a Breach involves more than 500 residents of a state or jurisdiction, in addition to notifying the consumer and HHS, DWIHN also shall notify prominent media outlets serving the state or jurisdiction. Such notice shall be provided promptly and in no case later than sixty (60) calendar days after discovery of the Breach. The notice shall contain the same information included in the notice to the consumer.

d. *LAW ENFORCEMENT DELAY*. If a law enforcement official informs DWIHN that the notice to consumers, HHS or the media described above would impede a criminal investigation or cause damage to national security, DWIHN shall:

1. If the statement is in writing and specifies the time for which a delay is required, delay the notification for the specified time; or
2. If the statement is made orally, document the statement, including the identity of the official, and delay the notification for no longer than thirty (30) days from the date of the oral statement, unless during that thirty (30) day time period, the official provides a written statement requiring a different notification time-frame.

e. NOTICE TO INTEGRATED CARE ORGANIZATION. Unless contrary instructions from law enforcement are received (see Section 5(d) above), if a Breach involves an individual that DWIHN serves under its contract with the integrated care organization (ICO) and DWIHN discovers a Breach of that individual's unsecured PHI, as those terms are defined by 45 CFR 164.02, DWIHN shall notify the integrated care organization without unreasonable delay within the timeframe specified by any applicable Business Associate Agreement between the parties. Where there is no controlling BAA, DWIHN shall notify the ICO within five (5) calendar days after discovery. For purposes of this subsection (e), discovery means the first day on which the Breach is known to DWIHN or by exercising reasonable diligence would have been known to DWIHN. The notification must include identification of each individual whose unsecured PHI has been, or is reasonably believed to have been breached and any other available information in DWIHN's possession which DWIHN is required to include in the individual notice contemplated by 45 CFR 164.

5. **DOCUMENTATION OF BREACH NOTICE**.
DWIHN shall maintain the documentation related to the provision of notice to consumers, HHS, the media, if applicable, and any communication from law enforcement related to the delayed notification, if applicable, for at least six (6) years from the date notice was provided.

6. **ANNUAL REVIEW OF POLICY.**
This Policy shall be reviewed and updated at least annually and on an as needed basis to incorporate any amendments to the HIPAA Rules or HITECH Act related to providing notices of Breach of Unsecured PHI and any guidance issued by HHS relevant to this Policy.

7. **MICHIGAN PERSONAL IDENTIFYING INFORMATION BREACH REQUIREMENTS.**
This Policy sets forth notice requirements in the event of a Breach of Unsecured PHI as required by the HIPAA Rules and the HITECH Act. Michigan law also requires specific action in the event of a breach of the security of Personal Identifying Information maintained by DWIHN as computerized data. The Security Officer shall be notified immediately of any unauthorized acquisition of any electronic Personal Identifying Information maintained by DWIHN that compromises the security, confidentiality or integrity of the Personal Information. The Security Officer shall coordinate with the Privacy Officer to notify each individual whose Personal Identifying Information was involved in the breach without unreasonable delay and consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security and confidentiality of the system. Consistent with the Michigan Identity Theft Protection Act (MCL §§445.61, et seq.), notice shall be provided using one of the following four methods:

a. Written notice addressed to the individual(s) whose Personal Information was compromised;

b. Written notice sent electronically to the recipient if any of the following are met:
    1. The recipient has expressly consented to receive electronic notice.
    2. DWIHN has an existing business relationship with the recipient that includes periodic electronic mail communications and based on those communications DWIHN reasonably believes that it has the recipient's current electronic mail address.
    3. DWIHN conducts its business primarily through internet account transactions or on the internet, or

c. If not otherwise prohibited by state or federal law, notice given by telephone by an individual who represents the person or agency if all of the following are met:
    1. The notice is not given in whole or in part by use of a recorded message.
    2. The recipient has expressly consented to receive notice by telephone, or if the recipient has not expressly consented to receive notice by telephone, DWIHN also provides notice under subdivision (a) or (b) if the notice by telephone does not result in a live conversation between the individual representing DWIHN and the recipient within 3 business days after the initial attempt to provide telephonic notice.

d. Substitute notice, if DWIHN demonstrates that the cost of providing notice under subdivision (a), (b), or (c) will exceed $250,000 or the number of individuals who must receive notices exceeds 500,000 of this state. A person or agency provides substitute notice under this subdivision by doing all of the following:
    1. If DWIHN has electronic mail addresses for any of the residents of this state who are entitled to receive the notice, providing electronic notice to those residents.
    2. If DWIHN maintains a website, conspicuously posting the notice on that website.
    3. Notifying major statewide media. A notification under this subparagraph shall include a telephone number or a website address that a person may use to obtain additional assistance and information.
    The requirements of this Section apply to the breach of any individual's Personal Identifying Information in the possession of DWIHN even if such individual is not a member of the DWIHN. For example, these requirements would apply to any Personal Identifying Information of Workforce Members maintained by the Human Resources Department or other DWIHN departments and Personal Identifying Information of other individuals maintained by DWIHN for purposes such as fundraising. DWIHN shall consult with legal counsel as necessary to ensure compliance with the requirements of the Michigan Identity Theft Protection Act in the event of a breach of the security of Personal Information maintained by DWIHN as computerized data.

8. **COMPLIANCE WITH OTHER DWIHN POLICIES**
In the event of an alleged unauthorized use or disclosure of PHI or Personal Identifying

Information, DWIHN shall consider whether the breach triggers any actions that need to be taken by DWIHN under other DWIHN policies applicable to unauthorized uses of PHI or Personal Identifying Information, such as DWIHN's HIPAA Security policies and procedures or any Medical Identity Theft Policy adopted by DWIHN.

QUALITY ASSURANCE/IMPROVEMENT

DWIHN management and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the DWIHN IT Security Officer, DWIHN HIPAA Privacy Officer, and the Deputy Chief Legal Counsel.

DWIHN shall review and monitor contractor adherence to this policy as one element in its network management program, risk management program, and Quality Assessment/Performance Improvement Program (QAPIP) Work-plan..

The quality improvement programs of Network Providers must include measures for both the monitoring of and the continuous improvement of the programs or processes described in this policy.

COMPLIANCE WITH ALL APPLICABLE LAWS

DWIHN staff, Direct Contracted Network Providers, and their 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

1. Michigan Department of Health and Human Services Medicaid Provider Manual v January 1, 2020 (in effect, and as amended)
2. Medicaid Managed Specialty Supports and Services Concurrent 1915(b)/(c) Waiver Program (PIHP/CMHSP contracts 10/1/2021-9/30/2022 in effect, and as amended)
3. MCL Act 452
4. 45 CFR 164

RELATED POLICIES AND PROCEDURES

1. **Acceptable Use**
2. **Health Insurance Portability and Accountability Act (HIPAA) Security**
3. PHI Privacy and Confidentiality
4. **Credentialing File Security Procedure**
5. **Customer Service Medical Record Retrieval Procedure**
6. **Risk Management Policy**
7. **Password Protection Policy**
8. **UM Security Controls Procedure**

CLINICAL POLICY

NO

INTERNAL/EXTERNAL POLICY

EXTERNAL

Approval Signatures

Step Description	Approver	Date
Final Approval Policy	Eric Doeh: President and CEO	09/2022
Stakeholder Feedback	Allison Smith: Project Manager, PMP	08/2022