Detroit Wayne Integrated Health Network (DWIHN)
HIPAA Privacy Policies and Procedures
CONTENTS

General Administrative Policies and Procedures

Use and Disclosure of Protected Health Information

Notice of Privacy Practices

Business Associates and Patient Access

Complaints, Investigations and Compliance With Laws

Privacy Policies – DWIHN

P-1000 General Administrative Policies and Procedures

The policies in this section (P-1000) of the DWIHN HIPAA Privacy policy and procedure manual establishes the DWIHN's administrative policies and procedures for safeguarding the privacy of protected health information (PHI).

Regulations
45 CFR 164.530
Establishes requirements for administrative measurements to implement the policy standards.

Privacy Policies – DWIHN

P-1100 Workforce Responsibilities

The policies in the section establish the organizational responsibilities for compliance with the privacy standards and for overseeing the efforts of DWIHN to safeguard the privacy of patient information.

Regulation(s)
45 CFR 164.530(a)
Requires designation of Privacy Officer and contact person responsible for policy development and handling of privacy inquiries and complaints.

45 CFR 164.514(d)(2)
Requires identification of the categories of protected health information that each class or category of Workforce member may use or disclose.

P-1110 Designation of Privacy Officer

The Privacy Officer is responsible for the development and implementation of policies and procedures to safeguard the privacy of patients' health information consistent with federal and state laws and regulations.
The specific responsibilities of the Privacy Officer include:
• developing policies and procedures as provided in policy P-1500
• developing and conducting training programs on privacy policies and procedures
• responding to questions from Workforce and patients concerning privacy policies and procedures
• receiving complaints concerning the privacy practice described in the Notice of Privacy Practices (see policy P-3100)
• auditing compliance with privacy policies and procedures
• investigating and correcting violations of privacy policies and procedures
The Privacy Officer may assign any of these responsibilities to other Workforce members or contractors but continues to be responsible for making sure these responsibilities are carried out.

Regulation
45 CFR 164.530(a)(1)
Requires designation of Privacy Officer responsible for development and implementation of privacy policies and procedures, and a contact to whom requests for additional information and complaints can be directed.

P-1120 General Workforce Responsibilities

All Workforce members are responsible for safeguarding the privacy of patient/consumer health information. Specific Workforce responsibilities under these privacy policies and procedures will be listed in the Workforce member's job description.

All Workforce members must:

• use and disclose protected health information only as authorized in their job description or as authorized by a supervisor
• conduct oral discussions of personal health information with other Workforce or with patients and family members in a manner that limits the possibility of inadvertent disclosure
• complete privacy training (see policy P-1200)
• report suspected violations of a business associate's contractual obligations to safeguard protected health information (see policy P-1400)
• report suspected violations of the policies and procedures established in this manual by Workforce members as detailed in policy P-1500.

Regulations
45 CFR 164.514(d)(2)(ii)
Require reasonable efforts to limit access by medical practice Workforce members to the classes of information necessary to carry out their duties.

45 CFR 154.530(c)(2)(ii)
Requires reasonable efforts to limit incidental uses or disclosures of protected health information.

P-1130 Authority and Responsibility of Individual Workforce Members

The job descriptions of all Workforce members who require routine access to protected health information to perform their job-related duties must identify:
• the job functions that require the use of disclosure of protected health information
• the classes of protected health information the position will use or disclose
• any restrictions on the protected health information the position can use or disclose
• the procedures that must be followed to use or disclose protected health information not routinely available to the position.

These requirements may be satisfied by referring the standard job classes that the Privacy Officer may establish under policy P-2000 or define the positions authorized to routinely use or disclose standard categories of protected health information.

Regulation
45 CFR 164.514(d)(2)(ii)
Requires reasonable efforts to limit access by medical practice Workforce members to the classes of information necessary to carry out their duties.

P-1200 Workforce Training

This section establishes the responsibility for development and updating of Workforce training programs and materials on privacy policies and procedures. It also establishes the responsibility of all Workforce members to complete privacy training.

P-1210 Content of Privacy Training Program for Workforce

The Privacy Officer or a Workforce member designated by the Privacy Officer will develop a privacy policy orientation and training program.

The purpose of this program is to make sure that all Workforce members are familiar with the privacy policies and procedures adopted by DWIHN.

The training and orientation programs will cover:

- the definition and identification of protected health information
- providing the Notice of Privacy Practice to all patients and obtaining a written acknowledgment of receipt
- using and disclosing protected health information for treatment payment and healthcare operations
- obtaining authorization when required for use and disclosure of protected information
- procedures for handling suspected violations of privacy policies and procedures
- penalties for violations of privacy policies and procedures
- documentation required by the policies and procedures manual

Workforce members will:

- receive a summary of the medical practice's privacy policies and procedures
- have an opportunity to review the policies and procedures manual
- have an opportunity to ask questions about the privacy policies and procedures of DWIHN

Regulation
45 CFR 164.530(b)(1)
Requires training of all Workforce members on privacy policies and procedures.

P-1220 Initial Privacy Orientation and Training

All Workforce members must complete the privacy policy orientation and training program during their orientation period.

1. Completion of the privacy policy orientation and training program will be documented in the employee's personnel file by the Privacy Officer or the Workforce member who conducts the training.
2. Until Workforce members complete the privacy policy orientation and training program, their supervisors will closely monitor their use and disclosure of protected health information.
3. Prior to the orientation of a Workforce member, his or her supervisor should confirm that he or she has completed privacy training.
4. The employees who do not complete the privacy policy and training programs will not be eligible for benefits that would have become available after their first 90 days of employment.

Regulation
45 CFR 164.530(b)
Establish HIPAA requirements for Workforce training.

P-1230 Revised Policies and Procedures Training
The Privacy Officer or a Workforce member designated by the Privacy Officer will develop training materials on new or revised privacy policies and procedures.

Procedures
1. Workforce whose job responsibilities are affected by a change in privacy policies and procedures must complete training on the revised policies and procedures within thirty (30) days of their effective date.
2. Completion of training on revised policies and procedures will be documented in the employee's personnel file.

Regulation
45 CFR 164.530(b)(2)(ii)
Requires documentation of training.

P-1300 Workforce Compliance and Sanctions

The policies in this section of the privacy manual establish disciplinary procedures for employees whose actions are out of compliance with DWIHN's policies and procedures.

Regulation
45 CFR 164.530(e)
Requires covered entities to apply appropriate sanctions against Workforce members who violate its privacy policies and procedures.

P-1310 Reporting of Suspected Violations of Privacy Policies and Procedures
All Workforce members should report possible violations of privacy policies and procedures to their supervisor/team leader. If the supervisor determines that a violation occurred, or that the situation warrants further investigation, the possible violation should be reported to the Privacy Officer.

Under the following circumstances, potential violations should not be reported by a Workforce member to his or her supervisor:

- when the violation involves the Workforce member's supervisor, it should be reported directly to the Privacy Officer
- when the violation involves the Privacy Officer, it should be reported to the Executive Director/Board of Trustees. When the violation involves a member of the Executive Director or Board of Trustees, it should be reported to the Secretary of Health and Human Services (HHS)

Reportable offenses include use and disclosure of protected health information that may violate:

- the practices described in the Notice of Privacy Practice form
- a patient's authorization

Discussion of protected health information in public areas should be reported only if the discussion involves the disclosure of
protected health information and it would have been practical to conduct the discussion in a private area.

The Workforce member reporting violation should briefly describe the possible violation in writing, or should arrange a meeting with the Privacy Officer to discuss the possible violation.

P-1311 Sanctions and Penalties
There are two types of violations of privacy policies and procedures:

- technical violations that do not result in the use or disclosure of protected health information
- violations that do involve the use or disclosure of protected health information

There are two types of violations that involve the use or disclosure:

- unintentional or accidental uses or disclosures
- intentional and deliberate uses and disclosures

Incidental disclosures of information, such as disclosures that occur when a consumer asks a question in a public area, do not need to be reported, documented, or investigated. No sanction will be imposed for incidental disclosures of information. Workforce members should, nevertheless, make reasonable efforts to minimize incidental disclosures.

The severity of penalties varies with the type of violation. The most severe penalties apply to the intentional disclosure of protected health information in violation of policies and procedures. The least severe penalties apply to unintentional technical violations of policies that do not result in the disclosure of protected health information.

Examples of violations include:

- Technical violations. When obtaining an authorization, Workforce member fails to notice that the parties signed but did not date the authorization form.
- Accidental disclosure. Information on the wrong patient is accidentally sent to a third party payer.
- Intentional disclosure. A Workforce member provides a vendor representative a list of consumers with an identified medical condition without obtaining the consumer's (or the consumer's legally appointed representative) authorization for this disclosure.

The procedure and penalties that apply to each of these types of violations are defined in Policy P-1312 through P-1315.

Regulation
45 CFR 164.530(e)
Requires covered entities to apply appropriate sanctions against Workforce members who violate their privacy policies and procedures.

P-1312 Investigation of Potential Privacy Violations by Workforce Members
Upon being notified of a potential violation of privacy policies and procedures by a Workforce member or consumer (under policy P-5200), the Privacy Officer will:

- review any documentation
- meet with the Workforce member or patient who reported the possible violation
- meet with the Workforce member(s) who may have violated the policies and procedures
- determine what, if any, protected health information was used or disclosed
- determine whether the use or disclosure violated policies and procedures
- determine whether the violation was accidental or intentional
- recommend to the Workforce member's supervisor that disciplinary action, if any, should be taken
- document the findings of the investigation and action taken

Regulation

45 CFR 164.530(e)
Requires covered entities to apply appropriate sanctions against Workforce members who violate their privacy policies and procedures.

P-1313 Sanctions and Penalties for Technical Violations Not Involving Use of Disclosure

A Workforce member who commits a technical violation of privacy policies and procedures that does not result in any use or disclosure of protected health information will:

- meet with his or her supervisor to review the policies and procedures that were violated
- demonstrate to the satisfaction of the supervisor, that he or she understands the policies and procedures that should be followed in similar circumstances

The violation will be documented in the Workforce member's personnel file.

A pattern of reported technical violations, even if none result in the inappropriate use or disclosure of protected health information, may result in transfer to another position, suspension, or termination of the Workforce member.

Regulation
45 CFR 164.530(e)
Requires appropriate sanctions against medical practice Workforce members who violate privacy policies and procedures.

P-1314 Sanctions and Penalties for Unintentional Violations Involving Use and Disclosure

A Workforce member who unintentionally uses or discloses protected health information in violation of the privacy policies and procedures will:

- meet with his or her supervisor to review the use or disclosure of protected health information that violated the medical practice's policies and procedures or the Workforce member's authority to use or disclose information
- demonstrate to the satisfaction of the supervisor that he or she understands the uses and disclosures that he or she is authorized to make under DWIHN's policies and procedures

The violation will be documented in the Workforce member's personnel file.

A pattern of repeated unauthorized use or disclosure of protected health information will result in transfer to another position, suspension or termination of the Workforce member.

Regulation
45 CFR 164.530(e)
Requires appropriate sanctions against medical practice Workforce members who violate privacy policies and procedures.

P-1315 Sanction and Penalties for Intentional Violation Involving Use and Disclosure
The intentional violation of privacy policies and procedures may result in immediate suspension pending further investigation and termination.
Documentation of the investigation of the violation must show clear evidence that the disclosure of information was intentional and deliberate. That is, the Workforce member must have disclosed the information knowing that the disclosure violated the policies and procedures of DWIHN.

If the Workforce member has previously disclosed the same or similar type of information under the same or similar circumstances, it will be presented that the disclosure was intentional and deliberate.

Regulation
45 CFR 164.530(e)
Requires appropriate sanctions against medical practice Workforce members who violate privacy policies and procedures.

P-1316 Protection of Whistleblowers
No action shall be taken against a Workforce member who reports a violation of privacy standards to the Secretary of HHS or to any state or local law enforcement or oversight agencies.

Regulation
45 CFR 164.530(g)
Prohibits a covered entity from retaliation against individuals who report violations of the privacy standard.

P-1320 Documentation of Sanctions Brought Against Employees
The Privacy Officer shall establish and maintain files that document all actions taken to impose sanctions under policy P-1311 through P-1314. This information shall include:

- a description of, and documenting evidence for, the violation
- a statement clarifying the nature of the violation, specifically indicating whether it was technical or involved the use or disclosure of protected health information, and whether the violation of policies was accidental or intentional
- a description of the sanction that was imposed

An unproven or unsubstantiated allegation of a violation of privacy policies and procedures does not have to be documented.

Regulation
45 CFR 164.530(e)(2)
Requires covered entities to document sanctions that are applied.

DWIHN
Privacy/Security Officer Job Description
General Description:

The Privacy Officer ("PO") is responsible for the development and implementation of the policies and procedures of DWIHN relating to privacy issues. This includes the compliance with both federal and state laws. At various times, the Privacy Officer will be involved in diverse and miscellaneous aspects of the activities, including, but not limited to, development, implementation, maintenance of and adherence to Practice's policies and procedures relating to privacy issues and protected health information ("PHI").

Responsibilities of the Privacy Officer:

The Privacy Officer is also the contact person (PO) or office who is responsible for receiving complaints under this section, and the PO shall be able to provide further information about matters covered by the notice required by 164.520, specifically relating to the handling of complaints regarding alleged violations of privacy rights.

Other responsibilities of the Privacy Officer shall include, but not be limited to, the following:

- Development of privacy protection procedure
- Works with corporate compliance officer
- Implement formal security policy
- Assessment of privacy risks
- Advises legal counsel and management as to procedures for maintenance of forms, notices
- Assist in coordinating data back-up plan
- Oversees Workforce privacy training
- Monitors business associates as necessary
- Supervise maintenance personnel
- Establish procedures for tracking, coordinating and managing PHI
- Oversees and coordinates inspections, amendments and access to PHI
- Assists in investigations of possible breaches of security, and takes appropriate action where necessary
- Works to assure compliance by Practice's office personnel with HR policies, security personnel, administration and legal counsel as applicable
- Assists in formulating disaster recovery plan
- Creates and implements privacy awareness procedures
- Acts as liaison with information systems concerning security plans throughout Practice in order to coordinate security procedures and privacy concerns
- Coordinates release of PHI in compliance with DWIHN's policies, procedures, and legal specifications
- Advances knowledge and awareness of privacy laws and standards
- Attends continuing education courses relating to HIPAA and other privacy technology issues
- Cooperates with OCR and other governmental agents in compliance reviews and investigations

Qualifications:

- Knowledge of and experience in privacy laws, access, use and disclosure of protected health information, and release control technologies
- Organization, facilitation, communication and presentation skills

P-2000 Use and Disclosure of Protected health Information

Purpose:
To comply with applicable law regarding the use and disclosure of protected health information.

Definitions:
"Health Care Operations" means any of the following activities performed by DWIHN to the extent that the activities are related to covered functions:

(1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalized knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and consumers with information about treatment alternatives; and related functions that do not include Treatment;

(2) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;

(3) Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance);

(4) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;

(5) Business planning and development, such as conducting cost management and planning related analyses related to managing and operating the entity, including formulary development and administration, and development or improvement of methods of Payment or coverage policies; and

(6) Business management and general administrative activities of the entity, including, but not limited to:

(i) Management activities relating to implementation of and compliance with privacy policies and procedures;

(ii) Customer service;

(iii) Resolution of internal grievances;

(7) Creating de-identified health information or a limited data set and fundraising for the benefit of DWIHN

"Payment" means:

(1) The activities undertaken by:

• A health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or
• A covered health care provider or health plan to obtain or provide reimbursement for the provision of health care; and

(2) Activities such as those relating to:

• Determinations of eligibility or coverage and adjudication or subrogation of health benefit claims;
• Risk adjusting amounts due based on enrollee health status and demographic characteristics;
• Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;
• Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;
• Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and
• Disclosure to consumer reporting agencies of any of the following Protected Health Information relating to collection of premiums or reimbursement:

(A) Name and address;
(B) Date of birth;
(C) Social security number;
(D) Payment history;
(E) Account number; and
(F) Name and address of the health care provider and/or health plan.

"Protected Health Information" means individually identifiable health information transmitted by electronic media; or transmitted or maintained in any other form or medium. Protected Health Information excludes individually identifiable health information in:

(i) Education records covered by the Family Educational Rights and Privacy Act, as amended;

(ii) Records described in subsection (a) of the Family Educational Rights and Privacy Act, as amended; and

(iii) Employment records held by DWIHN in its role as employer.

"Treatment" means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

Policy:

It is the policy of DWIHN to use and disclose Protected Health Information only in compliance with state and federal laws and regulations. This policy should be read in conjunction with all other policies relating to the use or disclosure of patients' health information.

Procedure:
PERMITTED USES AND DISCLOSURES. DWIHN may use or disclose Protected Health Information as follows and in accordance with DWIHN's Notice of Privacy Practices:

- To the individual;
- For Treatment, Payment or Health Care Operations, as permitted by relevant DWIHN policies and the Privacy Regulations as outlined below;
- Incident to a use or disclosure otherwise permitted or required by this policy, other DWIHN policies, and/or the Privacy Regulations, provided that:
    - DWIHN complies with its policies relating to the minimum necessary requirements; and
    - DWIHN implements reasonable safeguards to limit incidental uses and disclosures and intentional or unintentional uses or disclosures that violate DWIHN policies and/or the Privacy Regulations.
    - Pursuant to and in compliance with a valid authorization;
    - Pursuant to an agreement by the individual; and
    - As permitted by and in compliance with this policy and other privacy policies or for fundraising purposes.

REQUIRED DISCLOSURES. DWIHN shall disclose Protected Health Information:

- To an individual, when access to records or an accounting of disclosures is requested, unless in the written judgment of DWIHN, the disclosure would be detrimental to the individual or others (the decision to withhold access to the record may be appealed by the consumer, parent or guardian); and
- When required by the Secretary of Health and Human Services to investigate or determine DWIHN's compliance with the Privacy Regulations.

USES AND DISCLOSURES FOR TREATMENT, PAYMENT AND HEALTH CARE OPERATIONS. DWIHN may disclose Protected Health Information:

- For its own Treatment, Payment, or Health Care Operations;
- For treatment activities of another health care provider;
- To another covered entity or a health care provider for the Payment activities of the entity that receives the information.

References:
45 CFR §§ 164.502(a); 164.506(c)

P-2010 Use and Disclosure of Protected Health Information to Patient/Consumer Surrogates

Purpose:
To comply with applicable law regarding the treatment of persons acting as personal representatives of a patient.

Definitions:
"Individual" means the person who is the subject of protected health information.

Policy:
Except in certain circumstances, described below, Michigan law allows a person (such as a parent, guardian or other person) with legal authority to act on behalf of the Individual (known as in loco parentis) when the Individual is a minor or does not have the mental capacity to make his or her own decisions. In these situations it is the policy of DWIHN to treat a person, who has the legal authority to act on behalf of a patient, as the Individual.

Procedure:
ADULTS, EMANCIPATED MINORS, OR UNEMANCIPATED MINORS
If a person is the parent, guardian or acting in loco parentis acting on behalf of an Individual who is an adult, an emancipated minor, or an unemancipated minor, DWIHN shall treat such person (patient/consumer surrogate) as the Individual. This policy shall be implemented in conjunction with DWIHN's policy regarding release of records regarding minors and parents' access to minors' records.
Exception: DWIHN shall not treat the personal representative of an unemancipated minor as the Individual, and the minor has authority to act as an Individual with respect to protected health information pertaining to a health care service if:

- The minor consents to such health care service; no other consent to such health care service is required by law, regardless of whether the consent of another person has also been obtained; and the minor has not requested that such person be treated as the personal representative;
- The minor lawfully obtains such health care service without the consent of a parent, guardian, or other person acting in loco parentis; and the minor, a court, or other person authorized by law consents to such health care services; or
- A parent, guardian, or other person acting in loco parentis consents to an agreement of confidentiality between a covered health provider and the minor with respect to such health care services.

DECEASED INDIVIDUAL OR ESTATE
EXECUTOR, ADMINISTRATOR OR PERSONAL REPRESENTATIVE: If an executor, administrator, personal representative, or other person has been appointed or otherwise has lawful authority under state law to act on behalf of a deceased Individual, or the Individual's

estate, DWIHN shall treat such person as a patient surrogate with respect to protected health information relevant to such personal representation.

CORONER OR MEDICAL EXAMINER: If a request is received from a coroner or medical examiner, 45 CFR§ 164.512(g) permits DWIHN to disclose protected health information of a decedent for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law. If DWIHN also performs the duties of a coroner or medical examiner, it may likewise use protected health information for those purposes.

FUNERAL DIRECTORS: DWIHN may disclose protected health information of a decedent to funeral directors prior to, in reasonable anticipation of, and following the death of an individual consistent with applicable law and as may be necessary to carry out their duties with respect to the decedent as permitted by 45 CFR§ 164.512(g).

DOMESTIC VIOLENCE, ABUSE, NEGLECT
DWIHN shall not treat a person as a patient surrogate of an Individual if:

- There is reason to believe that the Individual has been or may be subject to domestic violence, abuse, or neglect by such person; or treating such person as the personal representative could endanger the Individual; and
- In the exercise of professional judgment, it is decided that it is not in the best interest of the Individual to treat the person as the Individual's personal representative.

References:
45 CFR § 164.502(g)
HIPAA Privacy Brief - Uses and Disclosures for Which Consent, and Authorization, or Opportunity to Agree or Object is not Required
45 CFR § 164.512(g)

P-2020 Incidental Uses and Disclosures of Protected Health Information

Purpose:
To ensure compliance with federal regulations related to the incidental uses and disclosures of Protected Health Information.

Definitions:
"Incidental Use or Disclosure" is described as a secondary use or disclosure that cannot reasonably be prevented, is limited in nature, and that occurs as a by-product of an otherwise permitted use or disclosure under the Privacy Rule.

Policy:
It is the policy of DWIHN to comply with federal regulations related to the incidental use or disclosure of Protected Health Information

Procedure:
INCIDENTAL USE OR DISCLOSURE OF PROTECTED HEALTH INFORMATION
Incidental uses or disclosures of Protected Health Information are permitted only if DWIHN has complied with the minimum necessary and safeguard standards of the HIPAA Regulations.

Incidental uses or disclosures are not required to be included in an accounting of disclosures provided to an individual.

References:
HIPAA Privacy Brief Incidental Uses and Disclosures
45 CFR §§164.502(a), and 528(a)

P-2030 Reasonable Safeguards to Protect the Privacy of Protected Health Information

Purpose
To comply with applicable law regarding safeguards to protect the privacy of protected health information.

Policy
It is the policy of DWIHN to reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of HIPAA Privacy Regulations.

Procedure
Safeguards: DWIHN shall put in place appropriate administrative, technical and physical safeguards to protect the privacy of protected health information.
Documentation: DWIHN shall document the appropriate administrative, technical and physical safeguards that it puts in place to protect the privacy of protected health information.

References:
HIPAA Privacy Brief—Administrative Requirements
45 CFR § 164.530(c)

P-2040 Minimum Necessary Requirements for Uses and Disclosures of Protected Health Information

Purpose:
To ensure compliance with federal regulations regarding the minimum necessary requirements for requests for or the uses or disclosures of protected health information.

Policy:
It is the policy of DWIHN to impose limits on employees' access to protected health information, develop protocols for routine and recurring disclosures, and ensure that information used or disclosed is limited to the amount reasonably necessary to achieve the purpose for which the request was made, subject to federal regulations.

Procedure:
MINIMUM NECESSARY APPLIES
When using or disclosing protected health information or when requesting protected health information from another entity or facility, DWIHN shall make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure or request.

MINIMUM NECESSARY DOES NOT APPLY
This requirement does not apply to:

- Disclosures to or requests by a health care provider for treatment;
- Uses or disclosures made to the individual, or pursuant to an authorization;
- Disclosures made to the Secretary of Health and Human Services;
- Uses or disclosures required by law; or
- Uses or disclosures that are required for compliance with applicable privacy policies of DWIHN and/or the Privacy Regulations.

MINIMUM NECESSARY USES OF PROTECTED HEALTH INFORMATION

• Identify Class of Persons Needing Access to Protected Health Information. DWIHN shall identify the following: those persons or classes of persons, as appropriate, in its workforce who need access to protected health information to carry out their duties; and for such person or class of persons, the category or categories of protected health information to which access is needed and any conditions appropriate to such access.

• Limitations on Access. DWIHN must make reasonable efforts to limit the access of such persons or classes identified herein to protected health information consistent with this policy.

MINIMUM NECESSARY DISCLOSURES OF PROTECTED HEALTH INFORMATION

• Routine and Recurring Disclosures. For disclosures made on a routine and recurring basis, DWIHN shall implement policies and procedures (which may be standard protocols) that

limit the protected health information disclosed to the amount reasonably necessary to achieve the purpose of the disclosure.

• All Other Disclosures. For all other disclosures beyond those which are routine and recurring, DWIHN shall:

  • Develop criteria designed to limit the protected health information disclosed to the information reasonably necessary to accomplish the purpose for which the disclosure is sought; and

  • Review requests for disclosures on an individual basis in accordance with such criteria.

• Reliance on Disclosures as those which are Minimally Necessary: DWIHN may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when:

  • Making permissible disclosures to public officials, if the public official represents that the information requested is the minimum necessary for the stated purpose(s);

  • The information is requested by another health care provider;

  • The information is requested by a professional who is a member of its workforce or as a business associate of DWIHN for the purpose of providing professional services to DWIHN, if the professional represents that the information requested is the minimum necessary for the stated purpose(s); or

  • Documentation or representations that comply with the research regulations have been provided by a person requesting the information for research purposes.

MINIMUM NECESSARY REQUESTS FOR PROTECTED HEALTH INFORMATION

• DWIHN shall limit any request for protected health information to that which is reasonably necessary to accomplish the purpose for which the request is made, when requesting such information from other covered entities

• For requests made on a routine and recurring basis, DWIHN shall respond pursuant to policies and procedures (which may be standard protocols) that limit the protected health information requested to the amount reasonably necessary to accomplish the purpose for which the request is made.

• All other requests shall be reviewed on an individual basis to determine whether the protected health information sought is limited to the information reasonably necessary to accomplish the purpose for which the request is made.

Entire Medical Records limitation. For all uses, disclosures or requests to which the minimum necessary requirements apply, DWIHN shall not use, disclose or request an entire medical record, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure or request.

References:

45 CFR §§ 164.502(b) and 164.514(d).

P-2050 De-Identification of Protected Health Information

Purpose:
To ensure compliance with federal regulations regarding de-identification of protected health information.

Definitions:
• "Individually Identifiable Health Information" is a subset of health information, including demographic information collected from an individual, and:
- Is created or received by health care provider, health plan, employer, or health care clearinghouse; and
- Relates to the past, present, or future physical or mental health or condition of an individual, the provision to health care to an individual, or the past, present, or future payment for the provision of health care to an individual; and: (i) that identifies the individual; (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Policy:
It is the policy of DWIHN to de-identify protected health information when appropriate and practical; thus, rendering such information not subject to the Privacy Regulations.

Procedure:
USES AND DISCLOSURES TO CREATE DE-IDENTIFIED INFORMATION
DWIHN may use protected health information to create information that is not Individually Identifiable Health Information or disclose protected health information only to a business associate for such purpose, whether or not the de-identified information is to be used by DWIHN

USES AND DISCLOSURES OF DE-IDENTIFIED INFORMATION
Health information that meets the requirements for de-identification hereunder is not considered to be Individually Identifiable Health Information (i.e., de-identified). The Privacy Regulations do not apply to information that has been de-identified, provided that:
- Disclosure of a code or other means of record identification designed to enable coded or otherwise de-identified information to be re-identified constitutes disclosure of protected health information, and
- If de-identified information is re-identified, DWIHN may use or disclose such re-identified information only as permitted or required herein.

REQUIREMENTS FOR DE-IDENTIFICATION OF PROTECTED HEALTH INFORMATION
DWIHN may determine that health information is not Individually Identifiable only if:
- A person with appropriate knowledge of and experience with generally acceptable and statistical and scientific principles and methods for rendering information not individually

identifiable determines that the risk is very small that the information could be used alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is the subject of that information; and documents the methods and results of the analysis that justify such determination; or

• The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed:

- Names;
- All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census: the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000;
- All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
- Telephone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social security numbers;
- Medical record numbers;
- Health plan beneficiaries numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URL's);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints;
- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic, or code; EXCEPT information may be "re-identified" as provided below; AND

• DWIHN does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is subject of the information.

RE-IDENTIFICATION

DWIHN may assign a code or other means of record to allow information de identified to be re-identified by DWIHN, provided that:

• Derivation. The code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and

• Security. DWIHN does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.

References:
45 CFR §§ 164.502(d) and 164.514(a)-(c)

P-2100 Verification Requirements for Disclosures of Protected Health Information

Purpose:
To ensure compliance with applicable laws regarding the identity of those who receive protected health information.

Policy:
It is the policy of DWIHN to verify the identity and authority of a person requesting protected health information prior to any disclosure permitted by the HIPAA Privacy Regulations, if the identity or any such authority of such person is not known to DWIHN

Procedure:
PRIOR TO ANY DISCLOSURE
Prior to any disclosure of protected health information, DWIHN must:

- Except with respect to disclosures requiring an opportunity for the individual to agree or object, verify the identity of a person requesting protected health information and the authority of any such person to have access to protected health information if the identity or authority of such person is not known to DWIHN, and
- Obtain any documentation, statements, or representations, whether oral or written, from the person requesting the protected health information when such documentation, statement, or representation is a condition of the disclosure.

CONDITIONS ON DISCLOSURE
If a disclosure is conditioned on particular documentation, statements, or representations from the person requesting the protected health information, DWIHN may rely, if such reliance is reasonable under the circumstances, on documentation, statements, or representations that on their face meet the applicable requirements.

ADMINISTRATIVE REQUESTS, SUBPOENA OR SUMMONS
The conditions for an administrative request, subpoena or summons may be satisfied by the administrative subpoena or similar process or by a separate written statement that, on its face, demonstrates that the applicable requirements have been met.

WAIVER APPROVAL
Documentation required for waiver approval by an institutional review board or privacy board for research projects may be satisfied by one or more written statements, provided that each is appropriately dated and signed.

VERIFICATION OF THE IDENTITY AND AUTHORITY OF A PUBLIC OFFICIAL
DWIHN may rely, if such reliance is reasonable under the circumstances, on any of the following to verify identity or authority when the disclosure of protected health information is to a public official or person acting on behalf of the public official:

- If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status with corresponding government issued photo identification;
- If the request is in writing, the request is on the appropriate government letterhead; or
- If the disclosure is to a person acting on behalf of a public official, or written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.
- A written statement of the legal authority under which the information is requested, or, if the written statement would be impracticable, an oral statement of such legal authority;
- A request made pursuant to a legal process, warrant, subpoena, order or other legal process issued by a grand jury or traditional administrative tribunal is presumed to constitute legal authority.

Verification requirements of this policy are met if DWIHN relies on the exercise of professional judgment in making a use or disclosure to give the patient an opportunity to agree or object, or acts on a good faith belief in making a disclosure and averting a threat to health or safety.

References:
Privacy Standards Manual Section 8.6
HIPAA Privacy Brief - Verification Requirements
45 CFR §164.514(h)

P-2200 Uses and Disclosures or Protected Health Information to Avert a Serious Threat to Health or Safety

Purpose:
To ensure compliance with federal regulations regarding uses and disclosures of protected health information for purposes of averting a serious threat to health or safety.

Policy:
It is the policy of DWIHN to permit the use or disclosure of protected health information without a HIPAA consent or authorization to avert a serious threat to the health or safety of a person or the public.

Procedure:
PERMITTED DISCLOSURES:
DWIHN may, consistent with applicable law and standards of ethical conduct, use or disclose protected health information if, in good faith, it believes that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public, and the use or disclosure is to a person(s) reasonably able to prevent or lessen the threat, including the target of the threat. Or, such disclosure can be made if DWIHN believes: (i) it is necessary for law enforcement authorities to identify or apprehend an individual because of a statement made by the individual admitting participation in a violent crime that may have caused serious physical harm; or (ii) where it appears from all circumstances that the individual has escaped from a correctional institution or from lawful custody.

PROHIBITED USES AND DISCLOSURES:
Information Acquired During the Course of/Request for Treatment, Counseling or Therapy: A use or disclosure based on an individual's statement admitting participation in a violent crime that DWIHN reasonably believes may have caused serious physical harm to the victim may not be made if the information described by that individual:

- Has been learned by DWIHN in the course of treatment, counseling, or therapy to affect the propensity to commit the criminal conduct for the disclosure; or
- Is learned by DWIHN through a request by the individual to initiate or to be referred for treatment, counseling, or therapy.

LIMIT ON INFORMATION THAT MAY BE DISCLOSED:
A disclosure made to law enforcement based on the individual's statement admitting participation in a violent crime that DWIHN reasonably believes may have caused serious physical harm to the victim shall only contain the statement described therein and the following protected health information:

- Name and address;
- Date and place of birth;
- Social Security number;
- ABO blood type and RH factor;

- Type of injury;
- Date and time of treatment;
- Date and time of death, if applicable;
- A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or mustache), scars, and tattoos.

PRESUMPTION OF GOOD FAITH BELIEF:
DWIHN is presumed to have acted in good faith with regard to the belief, based upon its actual knowledge or in reliance on a credible representation by the person with apparent knowledge or authority, that any use or disclosure herein is:

- Necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public;
- To a person or persons reasonably able to prevent or lessen the threat, including the target of the threat;
- Necessary for law enforcement authorities to identify or apprehend an individual because of a statement by an individual admitting participation in a violent crime that the entity reasonably believes may have caused serious physical harm to the victim, or;
- Appearing from all the circumstances that the individual has escaped from a correctional institution or from lawful custody.

References:
Privacy Standards Manual Section 7.10
HIPAA Privacy Brief, Uses and Disclosures for Which Consent, and Authorization or Opportunity to Agree or Object is not Required
45 CFR § 164.512(j)

P-2300 Marketing and Fund Raising

Purpose:
To comply with federal regulations for the use or disclosure of protected health information for marketing and fund raising purposes.

Definitions:
"Marketing" means:

(1) To make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service, unless the communication is made:

(i) To describe a health related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, DWIHN making the communication, including communications about: the entities participating in a health care provider network; or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits.

(ii) For treatment of the Individual, or

(iii) For case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to that individual.

(2) An arrangement between DWIHN and any other entity whereby DWIHN discloses protected health information to the other entity, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service.

Policy:
It is the policy of DWIHN to prohibit the use or disclosure of protected health information for Marketing activities without a HIPAA authorization, unless one of the exceptions set forth in the "Procedure" section of this policy are met.

It is also the policy of DWIHN that it may use or disclose to a Business Associate with an appropriate Business Associate Agreement, or an institutionally related foundation protected health information regarding demographics or dates
of health care provided to an individual for the purpose or raising funds for its own benefit without an authorization. Such information may not be used or disclosed for fund raising purposes as otherwise permitted herein, unless a statement required by the Regulations is included in DWIHN's notice or privacy practices. It is further the policy of DWIHN that it must include in any fund raising materials sent to an individual pursuant to this policy, a description of how the individual may opt out of receiving further fund raising communications.

Finally, DWIHN must make reasonable efforts to ensure that individuals who decide to opt out of receiving future fund raising communications are not sent such communications.

Procedure:

GENERAL RULE FOR MARKETING

DWIHN shall not use or disclose protected health information for Marketing without a HIPAA authorization, unless the Marketing meets the exceptions contained herein.

If the Marketing involves remuneration to DWIHN from a third party, the authorization obtained must state that remuneration is involved.

EXCEPTIONS RELATED TO MARKETING: A HIPAA authorization is not required for uses or disclosures of protected health information to make a Marketing communication to an individual that:

- Occurs in a face-to-face encounter with the individual; or
- Contains a promotional gift of nominal value.

AUTHORIZATIONS RELATING TO MARKETING: If neither exception above applies to a contemplated use or disclosure for Marketing purposes, an authorization must be obtained from the individual. This policy shall be implemented in conjunction with DWIHN's policy on authorizations.

GENERAL RULES FOR FUND RAISING

USE OR DISCLOSURE TO A BUSINESS ASSOCIATION WITHOUT AN AUTHORIZATION: DWIHN may use or disclose to a Business Associate or to an institutionally related foundation, the following de-identified protected health information for the purpose of raising funds for its own benefit, without an authorization:

- Demographic information related to an individual; and
- Dates of health care provided to an individual.

LIMITATIONS ON USE OR DISCLOSURE: DWIHN may not use or disclose protected health information for fund raising purposes or as otherwise permitted herein unless a statement required by the Regulations is included in the DWIHN notice of privacy practices.

NOTICE TO INDIVIDUALS: DWIHN must include in any fund raising materials sent to an individual pursuant to this policy, a description of how the individual may opt out of receiving any further fund raising communications. DWIHN must make reasonable efforts to ensure that individuals who decide to opt out of receiving further fund raising communications are not sent such communications.

References:

45 CFR § 164.508(a)(3)
Privacy Standards Manual § 8.4
HIPAA Self-Assessment Tool Kit,
HIPAA Privacy Brief - Fund Raising
45 CFR § 164.514(f)

P-2400 Uses and Disclosures Related to Victims of Abuse, Neglect or Domestic Violence

Purpose:
To comply with federal requirements regarding uses and disclosures of protected health information related to victims of abuse, neglect, or domestic violence.

Policy:
It is the policy of DWIHN to permit the disclosure of protected health information about an individual whom it reasonably believes to be a victim of abuse, neglect, or domestic violence to a governmental authority, including a social services or protected services agency, authorized by law to receive reports of such abuse, neglect, or domestic violence. This policy is to be followed in conjunction with DWIHN's policies regarding the reporting requirements under state law of suspected abuse, neglect or domestic violence situations.

Procedure:
DISCLOSURES TO GOVERNMENTAL AUTHORITIES: Except for reports of child abuse or neglect permitted under allowable disclosures to public health authorities (see, Policy on Public Health Activities), DWIHN may disclose protected health information about an individual whom DWIHN reasonably believes to be a victim of abuse and neglect or domestic violence to a governmental authority. Such authority includes a social services or protected services agency authorized by law to receive reports of such abuse, neglect, or domestic violence, provided that:

- The disclosure is required by law and complies with and is limited to the relevant requirements of such law;
- The individual agrees to a disclosure; or
- The disclosure is expressly authorized (not required) by statute or regulations and DWIHN believes that disclosure is necessary to prevent serious harm to the individual or other potential victims; or the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the protected health information for which disclosure is sought is not intended to be used against the individual, and that an immediate enforcement activity that depends upon the disclosure will be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

INFORM THE INDIVIDUAL OF THE DISCLOSURE: If DWIHN makes a permissible disclosure about victims of abuse, neglect, or domestic violence, it must promptly inform the individual that such a report has been made or will be made, unless:

- DWIHN, in the exercise of professional judgment, believes that informing the individual will place that individual at risk of serious harm; or
- DWIHN would be informing a personal representative, and DWIHN reasonably believes that the personal representative is responsible for the abuse, neglect, or other

injury, and informing such person would not be in the best interest of the individual as determined by DWIHN in the exercise of professional judgment.

References:
Privacy Standards Manual Section 7.3
HIPAA Privacy Brief - Uses and Disclosures for Which Consent, and Authorization, or Opportunity to Agree or Object is not required
45 CFR § 164.512(c)

P-2500 Uses and Disclosures for Public Health Activities

Purpose:
To comply with federal regulations regarding uses and disclosures for public health activities for which a HIPAA consent, authorization, or opportunity to agree or object is not required.

Definitions:
"Public Health Authority" means an agency or authority of the United States, a state, a territory, a political subdivision of a state or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.

Policy:
It is the policy of DWIHN to permit the disclosure of protected health information for public health activities to a Public Health Authority, other government authority, a person subject to the jurisdiction of the Food and Drug Administration, a person who may have been exposed to a communicable disease or at risk of spreading or contracting the disease, or an employer in certain situations, without first obtaining a HIPAA consent, authorization or giving an individual an opportunity to agree. This policy shall be followed in conjunction with other policies of DWIHN pertaining to reporting requirements.

Procedure:
PUBLIC HEALTH AUTHORITY
DWIHN may disclose protected health information for public health activities to a Public Health Authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability. This includes, but is not limited to, the reporting of disease, injury, vital events, such as birth or death, in the conduct of public health surveillance, public health investigations, and public health interventions. At the direction of the public health authority, DWIHN may disclose protected health information for public health activities to an office of a foreign government agency that is acting in collaboration with the health authority.

DWIHN is permitted to disclose protected health information to a Public Health Authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect.

FOOD AND DRUG ADMINISTRATION
DWIHN is permitted to disclose protected health information to a person subject to the jurisdiction of the Food and Drug Administration to report adverse events, product defects or problems with biological product deviations, if the disclosure is made to the person required or directed to report such information to the Food and Drug Administration;

- To track products if the disclosure is made to a person required or directed by the Food and Drug Administration to track the product;

• To enable product recalls, repairs, or replacements; or
• To conduct post marketing surveillance to comply with requirements or at the direction of the Food and Drug Administration.

COMMUNICABLE DISEASES
DWIHN may disclose protected health information for public health activities to a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, if DWIHN or a Public Health Authority is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation.

EMPLOYER NOTIFICATION
DWIHN is permitted to disclose protected health information about an individual who is a member of the workforce of an employer to the employer if:

• DWIHN is a department of or its physicians are employed by such employer, or DWIHN provides health care to individuals at the request of the employer to conduct evaluations relating to medical surveillance of the workplace or to evaluate whether an individual has a work-related illness or injury.
• Any such disclosure of protected health information must consist of findings concerning a work-related illness or injury or workplace-related medical surveillance. The employer must require such findings in order to comply with its obligations under federal regulations or state law, to record such illness or injury, or to carry-out responsibilities for workplace medical surveillance.
• DWIHN must give written notice to the individual that protected health information relating to medical surveillance of the workplace and work-related illnesses and injuries will be disclosed to the employer. The notice requirement is met by giving a copy of the notice to the individual at the time the health care is provided, or if the health care is provided at the work site of the employer, such notice must be posted in a prominent place at the location where the health care is provided.

IMMUNIZATION NOTIFICATION
DWIHN is permitted to disclose protected health information to a school about an individual who is a student or prospective student of the school if the disclosure is limited to proof of immunization, if it is required by the State or other law for the school to have such proof of immunization. DWIHN must obtain and document the agreement to disclose such information.

References:

45 CFR § 164.512(b)

P-2510 Uses and Disclosures of Protected Health Information Required by Law

Purpose:
To comply with federal regulations regarding uses and disclosures of protected health information as Required by Law.

Definitions:
"Protected Health Information": means individually identifiable health information transmitted by electronic media; or transmitted or maintained in any other form or medium. Protected Health Information excludes individually identifiable health information in:

(i) Education records covered by the Family Educational Rights and Privacy Act, as amended;
(ii) Records described in subsection (a) of the Family Educational Rights and Privacy Act, as amended; and
(iii) Employment records held by DWIHN in its role as employer.

"Required By Law" means a mandate contained in law that compels a covered entity to make a use or disclosure of protected health information and that is enforceable in a court of law. Required By Law includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court (but not a private attorney, unless the patient has provided written permission), grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

Policy:
It is the policy of DWIHN to permit the use or disclosure of protected health information without the written authorization of the individual if such use or disclosure is Required By Law.

Procedure:
REQUIREMENTS FOR USE OR DISCLOSURE REQUIRED BY LAW: If a use or disclosure of protected health information by DWIHN is Required By Law, DWIHN shall make such use or disclosure without obtaining the written agreement of the individual; provided, however, if the use or disclosure is for the purposes described below, prior to use or disclosure, DWIHN must meet the requirements discussed in the following policies of DWIHN:

- Victims of Abuse, Neglect, or Domestic Violence.
- Disclosures for Judicial and Administrative Proceedings.
- Disclosures for Law Enforcement Purposes;
- Disclosures requested by a private attorney through a subpoena;
- Disclosures requiring the written permission of the individual whose protected health information is requested.

References:
Privacy Standards Manual Sections 7.1, 7.3, 7.5 and 7.6
HIPAA Privacy Brief - Use and Disclosure for Which Consent, And Authorization, or Opportunity to Agree or Object is not Required
45 CFR §§ 164.512(a), (c), (e) and (f)

P-2600 Uses and Disclosures for Involvement in an Individual's care; Notification Purposes

Purpose:
To ensure compliance with federal regulations regarding the uses and disclosures of protected health information to third parties who are involved in the care of a patient.

Policy:
DWIHN is permitted to disclose to third parties protected health information that is directly relevant to the third party's involvement with an individual's care or related to payment for the individual's care.

Procedure:
PERMITTED USES AND DISCLOSURES
Information Directly Related to a Third Party's Personal Involvement: DWIHN may disclose to a family member, other relative, close personal friend of the individual, or any other person identified by the individual, of protected health information directly relevant to such person's involvement with the individual's care, or payment related to the individual's health care.

Notification of Location, Condition or Death: DWIHN may use or disclose protected health information to notify or assist in the notification of an individual's location, general condition or death to the following: a family member; a personal representative; or another person responsible for the care of the individual. Any such use or disclosure of protected health information must be consistent with the other provisions of this policy.

Uses and Disclosures when the Individual is Present: If the individual is present for, or otherwise available prior to a use or disclosure and has the capacity to make health care decisions, DWIHN may use or disclose the protected health information if it:

- Obtains the individual's agreement;
- Provides the individual with the opportunity to object to the disclosure and the individual does not express such an objection; or
- Reasonably infers from the circumstances, based on the exercise of professional judgment that the individual does not object to the disclosure.

Limited Uses and Disclosures when the Individual is not Present: Where the individual is not present for, or the opportunity to agree or to object to the use or disclosure cannot practicably be provided because of the individual's incapacity or an emergency situation, DWIHN may in the exercise of professional judgment, determine whether disclosure is in the best interest of the individual. If DWIHN determines that such disclosure is in the best interest of the individual, it may disclose the protected health information that is directly relevant to the third party's involvement with the individual's health care. The best interest of the individual should be determined by DWIHN's professional judgment, experience, and common practice from which it may make a reasonable inference. Relevancy of third party involvement may be determined by

the individual allowing a third party to act on its behalf in picking up filled prescriptions, medical supplies, x-rays, or other similar forms of protected health information.

Use and Disclosures for Disaster Relief Purposes: DWIHN may use or disclose protected health information to a public or private entity authorized by law or by its charter to assist in disaster relief efforts for the purpose of coordinating uses or disclosures. The requirements set forth by this policy will apply to such uses and disclosures if DWIHN in the exercise of professional judgment, determines that the requirements do not interfere with the ability to respond to emergency circumstances.

References:
Privacy Standards Manual Section 6.2
HIPAA Privacy Brief - Involvement in the Individual's Care and Notification Purposes
45 CFR § 164.510

P-2700 Disclosures for Health Oversight Activities

Purpose:
To comply with federal regulations regarding disclosures of protected health information for health oversight activities.

Definitions
"Health Oversight Agency" means an agency or authority of the United States, a state, a territory, a political subdivision of a state or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

Policy:
It is the policy of the DWIHN to permit the disclosure of protected health information to a Health Oversight Agency for health oversight activities as authorized by law.

Procedure:
DISCLOSURE OF PROTECTED HEALTH INFORMATION TO HEALTH OVERSIGHT AGENCIES: DWIHN may disclose protected health information to a Health Oversight Agency for oversight activities authorized by law, including:

- Audits, civil, administrative, or criminal investigations; inspections, licensure or disciplinary actions.
- Civil, administrative, or criminal proceedings or actions, as well as other activities necessary for appropriate oversight of each of the following:
    - The health care system;
    - Government benefit programs for which health care information is relevant to beneficiary eligibility;
    - Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or
    - Entities subject to civil rights laws for which health information is necessary for determining compliance.

CLAIM FOR PUBLIC BENEFITS: If a health oversight activity or investigation is conducted in conjunction with an oversight activity or investigation relating to a claim for public benefits not related to health, the joint activity or investigation is considered a health oversight activity, and DWIHN is permitted to disclose protected health information in such case.

HEALTH OVERSIGHT ACTIVITY DOES NOT INCLUDE: an investigation or other activity in which the individual is the subject of the investigation or activity, and such investigation or other activity does not arise out of, and is not directly related to:

- Receipt of health care;
- A claim for public benefits related to health care;
- Qualification for, or receipt of, public benefits or services when a patient's health is integral to the claim for public benefits or services.

COVERED ENTITY IS A HEALTH OVERSIGHT AGENCY: If DWIHN is also a Health Oversight Agency, DWIHN may use protected health information for health oversight activities as herein permitted.

References:
Privacy Standards Manual Section 7.4
HIPAA Privacy Brief - Uses and Disclosures for its Consent, and Authorization, or Opportunity to Agree or Object is not Required
45 CFR § 164.512(d)

P-2710 Disclosures for Law Enforcement Purposes

Purpose:
To ensure compliance with federal regulations regarding the use and disclosure of protected health information for law enforcement purposes.

Policy:
It is the policy of DWIHN to permit the disclosure of protected health information for law enforcement purposes without first obtaining a HIPAA consent or authorization.

This policy shall be followed in conjunction with DWIHN's other policies regarding disclosure to law enforcement officials or for law enforcement purposes.

Procedure:
DISCLOSURES PURSUANT TO PROCESS AND AS REQUIRED BY LAW
DWIHN may disclose protected health information:

- As required by law, including laws that require reporting of certain types of wounds or other physical injuries (except public health disclosures regarding reports of child abuse, neglect, or government authority disclosures, which include social service or protected services agencies authorized by law to receive reports of abuse, neglect or domestic violence. See DWIHN's policies for reporting of abuse for guidance for these situations); or
- in compliance with and as limited by the relevant requirements of:
    - A court order or court-ordered warrant;
    - A subpoena or summons issued by a judicial officer;
    - A grand jury subpoena; or
    - An administrative request, including an administrative subpoena or summons, a civil or authorized investigative demand, or similar process authorized under law, provided that:
        - The information sought is relevant and material to a legitimate law enforcement inquiry;
        - The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and
        - De-identified information could not reasonably be used.

LIMITED INFORMATION FOR IDENTIFICATION AND LOCATION PURPOSES
DWIHN may disclose protected health information in response to a law enforcement official's request for information for the purpose of identifying or locating a suspect, fugitive, material witness or missing person. Such information must be limited to the following:

- Name and address;
- Date and place of birth;
- Social Security Number;
- ABO Blood Type and RH Factor;
- Type of injury;

• Date and time of treatment;
• Date and time of death, if applicable; and
• A description of distinguishing physical characteristics, including height, weight, gender, race, hair, and eye color, presence or absence of facial hair (beard or mustache), scars, and tattoos.

DWIHN may not disclose any other protected health information related to an individual's DNA or DNA analysis, dental records, or typing, samples, or analysis of body fluids or tissue to a law enforcement official for purposes of identification or location.

LAW ENFORCEMENT OFFICIAL'S REQUEST ABOUT A CRIME VICTIM (EXCLUDING ABUSE AND NEGLECT IN DOMESTIC VIOLENCE)
Unless the disclosure is required by law, DWIHN may disclose protected health information in response to a law enforcement official's request for such information about an individual who is suspected to be a victim of a crime if:

- The individual agrees to the disclosure;
- DWIHN is unable to obtain the individual's agreement because of incapacity or other emergency circumstances, provided that:
    - The law enforcement official represents that such information is needed to determine when a violation of law by a person other than the victim has occurred, and such information is not intended to be used against the victim;
    - The law enforcement official represents that immediate law enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; and
    - The disclosure is in the best interests of the individual as determined by DWIHN, in the exercise of professional judgment.

DISCLOSURE OF PROTECTED HEALTH INFORMATION ABOUT A DECEASED PERSON WHERE DEATH MAY HAVE RESULTED FROM CRIMINAL CONDUCT
DWIHN may disclose protected health information about an individual who has died to a law enforcement official for the purpose of alerting law enforcement of the death of the individual if DWIHN has a suspicion that such death may have resulted from criminal conduct.

CRIMINAL CONDUCT ON THE PREMISES OF DWIHN
DWIHN may disclose to a law enforcement official protected health information that DWIHN believes in good faith constitutes evidence of criminal conduct that occurred on the premises of DWIHN

References:
Privacy Standards Manual Section 7.6
HIPAA Privacy Brief - Uses and Disclosures for Which Consent, and Authorization, or Opportunity to Agree or Object is Not Required
45 CFR § 164.512(f)

P-2800 Disclosures of Protected Health Information for Workers' Compensation

Purpose:
To ensure compliance with federal regulations regarding the disclosure of protected health information for workers' compensation or similar programs providing benefits for work-related injuries without regard to fault.

Policy:
It is the policy of DWIHN to permit the disclosure of protected health information for workers' compensation purposes or any similar such program established by law in providing benefits for work-related injuries or illness without regard to fault.

Procedure:
DISCLOSURE RELATED TO WORKERS' COMPENSATION OR OTHER SIMILAR PROGRAMS:
DWIHN may disclose protected health information as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs established by law to provide benefits for work related injuries or illness without regard to fault.

References:
Privacy Standards Manual Section 7.12
HIPAA Privacy Brief - Uses and Disclosures for Which Consent, and Authorization, or Opportunity to Agree or Object is Not Required
45 CFR § 164.512(l)

P-2810 Disclosures for Judicial and Administrative Proceedings

Purpose:
To comply with federal regulations regarding disclosures of protected health information for judicial and administrative proceedings.

Definition:
"Qualified Protective Order" means an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that prohibits the parties from using or disclosing the protected health information for any purpose other than the litigation or proceeding for which such information was requested. It further requires the return to DWIHN or destruction of the protected health information at the end of the litigation proceeding.

Policy:
It is the policy of DWIHN to comply with court orders, subpoenas, discovery requests or other lawful process not accompanied by a court order or administrative tribunal order, provided that it complies with state and federal laws and regulations in disclosing protected health information in response to such requests.

Procedure:
DISCLOSURE OF PROTECTED HEALTH INFORMATION IN RESPONSE TO AN ORDER OF A COURT/ADMINISTRATIVE TRIBUNAL: DWIHN may disclose protected health information in response to an order of a court or administrative tribunal, provided it discloses only the protected health information expressly authorized by the order.

DISCLOSURE OF PROTECTED HEALTH INFORMATION IN RESPONSE TO A SUBPOENA, DISCOVERY REQUEST OR OTHER LAWFUL PROCESS: DWIHN may disclose protected health information in response to a subpoena, discovery request or other lawful process, provided it receives satisfactory assurance from the party seeking the information that reasonable efforts have been made by such party to ensure that the individual who is the subject of the protected health information that has been requested has been given notice of the request, or that the party has secured a Qualified Protected Order that meets the above requirements.

SATISFACTORY ASSURANCES: Satisfactory assurances are obtained if a party seeking protected health information provides to DWIHN a written statement and accompanying documentation demonstrating that:

- It has made a good faith attempt to provide written notice to the individual, or if the individual's location is unknown, to mail a notice to the individual's last known address.
- The notice included sufficient information about the litigation or proceeding in which protected health information is requested to permit the individual to raise an objection to the court or administrative tribunal; and

• The time for raising objections by the individual has elapsed and no objections were filed, or all objections filed by the individual have been resolved by the court or the administrative tribunal, and the disclosures sought are consistent with such resolution.

In the alternative, satisfactory assurances are demonstrated if the parties to the dispute giving rise to the request for information have agreed to a Qualified Protective Order and have presented it to the court or administrative tribunal with jurisdiction over the dispute, or requested a Qualified Protective Order from such court or administrative tribunal.

NO SATISFACTORY ASSURANCES REQUIRED: DWIHN may disclose protected health information in response to lawful process without receiving satisfactory assurances herein, if DWIHN makes reasonable efforts to provide sufficient notice to the individual or to seek a Qualified Protective Order. DWIHN is not required to take these actions, however, and can require the submission of satisfactory assurances at its option.

References:
Privacy Standards Manual Section 7.5
HIPAA Privacy Brief - Uses and Disclosures for Which Consent, and Authorization, or Opportunity to Agree or Object is Not Required
45 CFR § 164.512(e)

P-2900 Disclosure of Protected Health Information by Whistleblowers and Workforce Member Crime Victims

Purpose:
To comply with federal regulations regarding disclosures of protected health information by whistleblowers and Workforce member crime victims.

Definition:
"Workforce" means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for DWIHN, are under its direct control, whether or not they are paid by DWIHN

Policy:
It is the policy of DWIHN to permit Workforce members, business associates, or Workforce members who are victims of a crime to disclose protected health information if they have a good faith belief in the inappropriateness of conduct, or the disclosure is made to a health oversight agency, public health authority, health care accreditation agency, attorney or law enforcement official.

Procedure:
DISCLOSURE BY WHISTLEBLOWERS
DWIHN shall permit a Workforce member or business associate to disclose protected health information if:

- The Workforce member or business associate believes in good faith that DWIHN engaged in unlawful conduct or otherwise violated professional or clinical standards, OR that the care, services or conditions provided by DWIHN potentially endangered one or more patients, workers, or the public; AND
- The Workforce member or business associate makes a disclosure to a health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of DWIHN; or to an appropriate health care accreditation agency for the purpose of reporting the allegation of failure to meet professional standards or misconduct by DWIHN; or the disclosure is to an attorney retained by, or on behalf of, the Workforce member or business associate for the purpose of determining the legal options of the Workforce member or business associate with regard to the unlawful or unprofessional conduct.

DISCLOSURES BY VICTIMS OF CRIMINAL ACTS
If a member of DWIHN's Workforce is a victim of a criminal act, the member may disclose protected health information to a law enforcement official as long as:

- The suspected perpetrator is the subject of the protected health information; AND
- Protected health information disclosed is limited to the following information:

• Name and address;
• Date and place of birth;
• Social security number;
• ABO blood type and RH factor, type of injury, date and time of treatment, date and time of death, if applicable; and
• A description of the distinguishing physical characteristics, including height, weight, gender, race, hair, and eye color, presence or absence of facial hair (beard or mustache), scars, and tattoos.

References:
Privacy Standards Manual Section 2.11
45 CFR § 164.502(j)

P-3000 Notice Of Privacy Practices

Purpose:
To ensure compliance with applicable law regarding the creation, maintenance and distribution of DWIHN's Notice of Privacy Practices.

Policy:
It is the policy of DWIHN to create, maintain and distribute in accordance with applicable law a Notice of Privacy Practices.

Procedure:
Right to Notice. DWIHN shall provide all individuals with adequate notice of the uses and disclosures of their protected health information DWIHN shall inform individuals of their rights and DWIHN's legal duties with respect to protected health information.

Uses and Disclosures in Conformity With the Notice. DWIHN shall not use or disclose protected health information in a manner inconsistent with its Notice of Privacy Practices. DWIHN shall not use or disclose protected health information for any activities that are required to be included as a specific statement in its Notice unless the required statement is included in the Notice.

Revisions to the Notice. DWIHN shall promptly revise and distribute its Notice whenever there is a material change to uses or disclosures, individual's rights, DWIHN'S legal duties, or other privacy practices stated in the Notice. Except when required by law, a material change to any term of the Notice may not be implemented prior to the effective date of the Notice in which such material change is reflected.

Provision of Notice.
DWIHN shall:

- Provide the Notice no later than the date of the first service delivery, including service delivered electronically, to any individual after the first effective date of this policy;
- In an emergency treatment situation, DWIHN shall provide the Notice as soon as reasonably practicable after the emergency treatment situation;
- Except in an emergency treatment situation, DWIHN shall make a good faith effort to obtain from the patient written acknowledgment of receipt of the Notice, and if not obtained, DWIHN shall document its good faith efforts to obtain such acknowledgment and the reason why the acknowledgment was not obtained;
- Make the Notice available at all offices and other health delivery sites to individuals to request to take with them;
- Post the Notice in a clear and prominent location so that individuals seeking service are able to read the Notice; and
- Make revised Notices available upon request on or after the effective date of the revision.

Specific Requirements for Electronic Notice.

• DWIHN shall prominently post the Notice on its web site in a printable version, and make the Notice available electronically through the web site.
• DWIHN may provide the Notice to an individual by e-mail, if the individual agrees to electronic notice and such agreement has not been withdrawn. If DWIHN knows that the e-mail transmission has failed, a paper copy of the Notice must be provided to the individual. Provision of electronic notice by DWIHN will satisfy the provision requirements herein when timely made.
• If the first service delivery to an individual is delivered electronically, DWIHN shall provide an electronic notice automatically and contemporaneously in response to the individual's first request for service.
• Individuals that receive an electronic notice also have the right to obtain a paper copy of the Notice upon request.

Joint Notice by Separate Covered Entities. If DWIHN participates in organized health care arrangements with other covered entities, it may comply by a Joint Notice, provided that:

• The covered entities participating in the organized health care arrangement agree to abide by the terms of the Notice with respect to protected health information created or received by DWIHN as part of its participation in the organized health care arrangement;
• The Joint Notice meets the content of notice requirements, and reflects the fact that the Notice covers more than one DWIHN;
• The Notice describes with reasonable specificity the covered entities, or class of entities, to which the Joint Notice applies;
• The Notice describes with reasonable specificity the service delivery sites, or classes of service delivery sites, to which the Joint Notice applies; and
• State that the covered entities participating in the organized health care arrangement will share protected health information with each other, as necessary to carry out treatment, payment, or health care operations relating to the organized health care arrangement.
• The covered entities included in the Joint Notice must provide the Notice to individuals in accordance with the applicable provision of Notice specifications in this policy. Provision of the Joint Notice to an individual by any one of the covered entities included in the Joint Notice will satisfy the provision requirement herein with respect to all others covered by the Joint Notice.

Documentation. DWIHN shall retain copies of the Notice, and if applicable, any written acknowledgments of receipt of the Notice or documentation of good faith efforts to obtain such written acknowledgments, for at least six (6) years from the date the Notice or documentation was created or last in effect.

References:
45 CFR §§ 164.502(i) and 164.520

P-4000 Business Associate Relationships

Purpose
To ensure compliance with federal regulations regarding the use or disclosure of protected health information to Business Associates within the context of a contractual relationship.

Definitions
"Business Associate," with respect to DWIHN, is a person or organization who on behalf of DWIHN or an organized health care arrangement in which DWIHN participates, but other than in the capacity of a member of the workforce of such DWIHN or arrangement, performs or assists in the performance of: a function or activity involving the use, disclosure or maintaining of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or any other function or activity regulated by the Privacy Regulations. Or, the Business Associate provides, other than in the capacity of a member of the workforce of such DWIHN, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for DWIHN, or to or for an organized health care arrangement in which DWIHN participates, where the provision of the service involves the disclosure of individually identifiable health information from DWIHN, or arrangement, or from another Business Associate for DWIHN or arrangement, to the person.

Policy
DWIHN may disclose protected health information to a Business Associate and allow it to create or receive protected health information on its behalf provided DWIHN obtains satisfactory assurance that the Business Associate will appropriately safeguard the information.
Such assurance must be documented by DWIHN through a written contract, written agreement or arrangement with the Business Associate.

The requirement to obtain satisfactory assurances does not apply with respect to disclosures by DWIHN to a health care provider concerning the treatment of the individual.

If DWIHN knows of a pattern or activity or practice of the Business Associate that constitutes a material breach or violation of the Business Associate's obligation under the contract or other arrangements, DWIHN must take reasonable steps to cure the breach or end the violation. If such actions are unsuccessful, the contract or arrangement must be terminated, if feasible.
Alternatively, the problem must be reported to the Secretary of Health and Human Services.

Procedure
For those relationships that constitute "Business Associate" relationships, DWIHN shall enter into appropriate written agreements with the Business Associate.

CONTRACT REQUIREMENTS

A. A contract between DWIHN and the Business Associate:

- Must establish permitted and required uses and disclosures of protected health information by the Business Associate.
- May permit the Business Associate to use and disclose protected health information for the proper management and administration of the Business Associate or permit the Business Associate to provide data aggregation services relating to the health care operations of DWIHN

B. The contract must also provide that the Business Associate will:

- Not use or further disclose the information other than as permitted or required by the contract or as required by law;
- Use appropriate safeguards to prevent uses or disclosures of the information other than as provided for by its contract;
- Report to DWIHN any uses or disclosures of the information not provided for by its contract of which it becomes aware;
- Ensure that any agents, including a subcontractor, to whom it provides protected health information, received from, or created or received by, the Business Associate on behalf of DWIHN agrees to the same restrictions and conditions that apply to the Business Associate with respect to such information;
- Make available protected health information in accordance with the Privacy Regulations;
- Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with the Privacy Regulations;
- Make available the information required to provide an accounting of disclosures in accordance with the Privacy Regulations;
- Make its internal practices, books, and records relating to the use and disclosure of protected health information received from, created or received by the DWIHN available to the Secretary of Health and Human Services for purposes of determining the DWIHN's compliance with the Privacy Regulations;
- At the termination of the contract, if feasible, return or destroy all protected health information, and copies received from, created or received by the Business Associate on behalf of DWIHN that the Business Associate still maintains. If such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information not feasible.

C. The contract must authorize termination of the contract by DWIHN if DWIHN determines that the Business Associate has violated a material term of the contract.

OTHER REQUIREMENTS FOR CONTRACTS AND OTHER ARRANGEMENTS

A contract or other arrangement between DWIHN and the Business Associate may permit the Business Associate to use the information received by the Business Associate in its capacity as a Business Associate to DWIHN, if necessary:

- For the Business Associate's proper management or administration, or to carry out the legal responsibilities of the Business Associate;
- If the disclosure is required by law; **OR**

• The Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person; **AND**
• The person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

OTHER ARRANGEMENTS
Service, Function or Activity Performed by Business Associate for DWIHN: If the Business Associate is required by law to perform a function, activity or service described in the definition of Business Associate for DWIHN, DWIHN may disclose protected health information to the Business Associate to the extent necessary to comply with the legal mandate without the requirements of the Privacy Regulations. DWIHN must attempt in good faith to obtain satisfactory assurances as required by the Privacy Regulations. If the attempt fails, the reason for the failure and the fact that assurances could not be obtained must be documented.

Termination Authorization: DWIHN may omit the termination authorization, if such authorization is inconsistent with statutory obligations of DWIHN or its Business Associate.

References:
Privacy Standards Manual Sections 2.6 and 3.3
HIPAA Privacy Brief – Business Associates
45 CFR §§ 164.502(e)(1) and 164.504(e)

P-4100 HIPAA Requirements for Group Health Plans

Purpose
To comply with Federal Regulations regarding the use and disclosure of protected health information by group health plans.

Definitions
"Group Health Plan" means an employee welfare benefit plan, including insured and self-insured plans, to the extent that the plan provides medical care, including items and services paid for as medical care, to employees or their dependents directly, or through insurance, reimbursement, or otherwise, that: has 50 or more participants; or is administered by an entity other than the employer that established and maintains the plan.

"Designated Record Set" means a group of records maintained by or for DWIHN that are medical and billing records about individuals maintained by or for DWIHN; the enrollment, payment, claims adjudication maintained by or for a health plan; or used in whole or in part, by or for DWIHN to make decisions about individuals. For purposes of this paragraph, the term "record" means any item, collection or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for DWIHN.

Policy
It is the policy of the Group Health Plan of DWIHN to use and disclose participant's protected health information only as permitted by federal regulations.

Procedure
USES AND DISCLOSURES
General Requirements

- The Group Health Plan shall include a statement in its notice of privacy practices that states "DWIHN's Group Health Plan, or a health insurance insurer, or a HMO, with respect to the Group Health Plan, may disclose protected health information to the sponsor of the plan." Failure to include this statement in the notice will prohibit the Group Health Plan from disclosing protected health information to the plan sponsor.

- The Group Health Plan shall not disclose protected health information to a plan sponsor for the purpose of employment-related actions or decisions or in connection with any other benefit or employee benefit plan of the plan sponsor.

- The Group Health Plan may disclose protected health information to the plan sponsor to carry out plan administration functions that the plan sponsor performs pursuant to the plan documents, as amended.

Disclosures of Summary Health Information
The Group Health Plan may disclose summary health information to the plan sponsor, provided the plan documents restrict uses and disclosures by the sponsor to summary health information for the purpose of: obtaining premium bids from health plans for providing health insurance coverage under the Group Health Plan; or modifying, amending, or terminating the Group Health Plan.

Multiple Covered Functions
DWIHN may use or disclose the protected health information of individuals who receive either of DWIHN's health plan or health care provider services, but not both, only for purposes related to the appropriate function being performed.

REQUIREMENTS FOR PLAN DOCUMENTS: The Group Health Plan shall ensure that the plan documents incorporate the following provisions to:

- Establish the permitted and required uses and disclosures of protected health information by the plan sponsor;
- Provide that the Group Health Plan will disclose protected health information to the plan sponsor only upon a receipt of a certification by the plan sponsor that the plan documents have been amended to incorporate the following provisions, and that the plan sponsor agrees to:
    - Not use or further disclose the information other than as permitted or required by the plan documents, or as provided by law;
    - Ensure that any agents, including subcontractors, to whom it provides protected health information received from the Group Health Plan agree to the same restrictions and conditions that apply to the plan sponsor with respect to such information;
    - Not use or disclose the information for employment-related actions and decisions, or in connection with any other benefit or employee benefit plan of the plan sponsor;
    - Report to the Group Health Plan any use or disclosure of information that is inconsistent with the uses or disclosures provided of which it becomes aware;
    - Make available protected health information to individuals for inspection and copying;
    - Make available protected health information for amendments and as required to provide an accounting of disclosures;
    - Make its internal practices, books, and records relating to the use and disclosure of protected health information received from the Group Plan available to the Secretary of Health and Human Services for purposes of determining compliance by the Group Health Plan;
    - Return or destroy all protected health information received from the Group Health Plan that the plan sponsor still maintains and retain no copies of such information when no longer needed, if feasible;
    - Ensure that adequate separation between the Group Health Plan and the plan sponsor is established by describing in the plan documents those employees or classes of employees or other persons under the control of the plan sponsor to be given access to the protected health information to be disclosed, provided that any

employee or person who receives protected health information relating to payment under, health care operations of, or other matters pertaining to the Group Health Plan in the ordinary course of business must be included in such description;
• Restrict the access to and use by such employees and other persons described above to the plan administration functions that the plan sponsor performs for the Group Health Plan; and
• Provide an effective mechanism for resolving any issues of noncompliance by employees under the control of the plan sponsor, who have access to the protected health information.

References:
Privacy Standards Manual Sections 3.4 and 3.5
45 CFR §§ 164.504(f) and (g)

P-4200 Limited Data Set; Uses and Disclosures

Purpose
To ensure compliance with federal regulations regarding uses and disclosures of protected health information contained within a limited data set.

Definitions
"Limited Data Set" is protected health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:

(i) Names;
(ii) Postal address information, other than town or city, State, and zip code;
(iii) Telephone numbers;
(iv) Fax numbers;
(v) Electronic mail addresses;
(vi) Social Security numbers'
(vii) Medical record numbers
(viii) Health plan beneficiary numbers;
(ix) Account numbers;
(x) Certificate/license numbers;
(xi) Vehicle identifiers and serial numbers;
(xii) Web Universal Resource Locators (URLs)
(xiii) Internet Protocol (IP) address numbers;
(xiv) Biometric identifiers, including finger and voice prints; and
(xv) Full face photographic images and any comparable images.

Policy
It is the policy of DWIHN to comply with federal regulations related to the use and disclosure of protected health information contained within a data set.

Procedure
PERMITTED USES AND DISCLOSURES
DWIHN may use or disclose a limited data set under this policy only for the purposes of research, public health, or health care operations.

DWIHN may use protected health information to create a limited data set that meets the requirements of this policy, or disclose protected health information only to a business associate with an appropriate Data Use Agreement for such purpose, whether or not the limited data set is to be used by DWIHN.

DATA USE AGREEMENT: DWIHN may use or disclose a limited data set only if it obtains satisfactory assurance, in the form of a data use agreement that meets the requirements of this policy, that the limited data set recipient will only use or disclose the protected health information for limited purposes.

DATA USE AGREEMENTS - REQUIREMENTS

A data use agreement between DWIHN and the limited data set recipient must:

- Establish the permitted uses and disclosures of such information by the limited data set recipient, consistent with this policy. The data use agreement may not authorize the limited data set recipient to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by DWIHN;
- Establish who is permitted to use or receive the limited data set; and
- Provide that the limited data set recipient will:
    - Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law;
    - Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement;
    - Report to DWIHN any use or disclosure of the information not provided for by its data use agreement of which it becomes aware;
    - Ensure that any agents, including a subcontractor, to whom it provides the limited data set agrees to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and
    - Not identify the information or contact the individuals.

COMPLIANCE

DWIHN is not in compliance with the standards in this policy if it knew of a pattern of activity or practice of the limited data set recipient that constituted a material breach or violation of the data use agreement, unless it took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful:

- Discontinue disclosure of protected health information to the recipient; and
- Report the problem to the Secretary.

If DWIHN is a limited data set recipient and violates a data use agreement, it will be in noncompliance with the standards, implementation specifications, and requirements of this policy

References:

Privacy Standards Manual Section 8.3
HIPAA Privacy Brief Limited Data Set
45 CFR § 164.514

P-4300 Confidential Communications

Purpose
To ensure compliance with applicable law regarding confidential communications by DWIHN

Policy
It is the policy of DWIHN to accommodate reasonable requests by consumers/patients to receive confidential communications of protected health information from DWIHN by alternative means or at alternative locations.

Procedure
Patient/Consumers shall make the request for a confidential communication in writing. The provision of a reasonable accommodation shall be conditioned on:

- When appropriate, information as to how payment, if any, will be handled; and
- Specification of an alternative address or other method of contact.

A patient/consumer, may request to restrict the disclosure of protected health information to the individual's health plan, if the patient/consumer's services are not being reimbursed by a federal payment program (i.e., Medicaid, Medicare). If a patient/consumer makes such a request, the request must be agreed to by DWIHN, but only if the patient/consumer has paid for the health care service in full.

It shall not be required that the patient provide an explanation as to the basis for the request as a condition of providing communications on a confidential basis.

References:
Privacy Standards Manual Section 10.2
HIPAA Privacy Brief – Confidential Communications
45 CFR §164.522(b)

P-4400 Patient Access to Protected Health Information

Purpose
To ensure compliance with applicable law regarding patient right of access to protected health information.

Definitions
"Designated Record Set" means:
A group of records maintained by or for DWIHN that is:

- The medical records and billing records about individuals maintained by or for DWIHN;
- Used, in whole or in part, by or for DWIHN to make decisions about individuals.

For purposes of this policy, the term "record" means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for DWIHN

Policy
It is the policy of DWIHN to permit patients with access to inspect and obtain copies of their protected health information in accordance herein.

Procedure
RIGHT OF ACCESS
A patient has a right of access to inspect and obtain a copy of protected health information about the individual in a Designated Record Set, for as long as the protected health information is maintained in the Designated Record Set. Exceptions to this policy are:

- Psychotherapy notes;
- Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceedings; and
- Protected health information maintained by DWIHN that is:
    - Subject to the Clinical Laboratory Improvements Act of 1988, to the extent the provision of access to the patient would be prohibited by law; or
    - Exempt from the Clinical Laboratory Improvements Amendments of 1988.

UNREVIEWABLE GROUNDS FOR DENIAL
DWIHN may deny a patient access without providing an opportunity for review if the protected health information is excepted from the right of access.

If DWIHN is acting under the direction of a correctional institution, it may deny, in whole or in part, an inmate's request to obtain a copy of protected health information, if obtaining such information would jeopardize the health, safety, security, custody, or rehabilitation of the patient or other inmates, or the safety of any officer, employee, or other person at the correctional institution, or responsible for the transporting of the inmate.

Patient access to protected health information created or obtained by DWIHN in the course of research that includes treatment may be temporarily suspended for as long as the research is in progress, provided that the patient has agreed to the denial of access when consenting to participate in the research that includes treatment, and DWIHN has informed the patient that the right of access will be reinstated upon completion of the research.

Patient access to protected health information may also be denied if it is:

- Contained in the records that are subject to the Privacy Act (5 U.S.C. 552(a));
- If the protected health information was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

Access may be denied to a patient, provided that the patient is given a right to have such denials reviewed, in the following circumstances:

- A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the patient or another person;
- The protected health information makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or
- The request for access is made by the patient's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the patient or another person.

REVIEW OF A DENIAL OF ACCESS

If access is denied, the patient has the right to have the denial reviewed by a licensed health care professional who is designated by DWIHN to act as a reviewing official and who did not participate in the original decision to deny. DWIHN must provide or deny access in accordance with the determination of the reviewing official.

REQUESTS FOR ACCESS AND TIMELY ACTION

DWIHN must permit a patient to request access to inspect or to obtain a copy of the protected health information about the patient that is maintained in a Designated Record Set. DWIHN may require patients to make requests for access in writing, provided that it informs patients of such a requirement. Once the request is received, DWIHN must act no later than thirty (30) days after the receipt of the request as follows:

- If DWIHN grants a request, in whole or in part, it must inform the patient of the acceptance of the request and provide the access requested;
- If DWIHN denies the request, in whole or in part, it must provide the patient with a written denial;
- If the request for access is for protected health information that is not maintained or accessible to DWIHN on-site, DWIHN must take action on the request no later than sixty (60) days from receipt of such a request.

• If DWIHN is unable to take action on the request within the time limits provided herein, DWIHN may exceed the time for such action by no more than (30) days provided that:
    • DWIHN, within the applicable required time limit, provides the patient with a written statement of the reasons for the delay and the date by which DWIHN will complete its action on the request;
    • DWIHN may have only one such extension of time for action on a request for access.

PROVISION OF ACCESS

If access to protected health information is provided by DWIHN to a patient, DWIHN must comply with the following requirements:

• DWIHN must provide the access requested by patients, including inspection or obtaining a copy, or both, of protected health information about them in Designated Record Sets. If the same information requested is maintained in more than one Designated Record Set, or at more than one location, DWIHN need only produce the protected health information once in response to a request;
• DWIHN must provide the patient with access to the protected health information in the form or format requested by the patient, if it is readily producible in such form or format; or if not, in a readable hard copy form or such other form or format as agreed to by DWIHN and the patient;
• DWIHN may provide the patient with a summary of the protected health information requested, in lieu of providing access to the protected health information, or may provide an explanation, if:
    • Patient agrees in advance to such a summary or explanation; and
    • The patient agrees in advance to the fees imposed, if any, by DWIHN for such summary or explanation.

TIME AND MANNER OF ACCESS

Access must be provided as requested by the patient on a timely manner, including arranging with the patient for a convenient time and place to inspect or obtain a copy of the protected health information, or mailing a copy to the patient if requested. DWIHN may discuss the scope, format, and other aspects of the request for access with the patient as necessary to facilitate the timely provision of access.

FEES

DWIHN may impose a reasonable, cost based fee, provided that the fee includes only the cost of:

• Copying, including the cost of supplies for and labor of copying,
• Postage, when the patient has requested the copy, or the summary or explanation be mailed; and
• Preparing an explanation or summary of the protected health information, if agreed to by the patient.

If any State of Michigan law imposes a fee structure governing the fees that may be charged, or prohibits that a fee may be charged due to a patient/consumer's income level, for the copying, supplies, labor, postage, etc. of a patient's protected health information and/or medical record, DWIHN shall adhere to those applicable state laws. (See Medical Record

Access Act, MCL 333.26261, et seq., Effective April 1, 2004, and amendments, if any).

DENIALS

If DWIHN denies access, in whole or in part, to protected health information, DWIHN will comply with the following requirements:

- DWIHN must, to the extent possible, give the patient access to any other protected health information requested, for which it does not have a ground to deny access;
- DWIHN must provide a timely, written denial to the patient. The denial must be a plain language and contain the following:
    - The basis for the denial;
    - If applicable, the statement of the patient's review rights, including a description of how the patient may exercise such review rights; and
    - A description of how the patient may complain to DWIHN pursuant to DWIHN complaint procedures or to the Secretary of Health and Human Services. A description must include the name or title and telephone number of the contact person or office.
- If DWIHN does not maintain the protected health information that is the subject to the patient's request for access, and DWIHN knows where the request information is maintained, DWIHN must inform the patient where to direct the request.
- If a patient has requested a review of a denial, DWIHN must designate a licensed health care professional who is not directly involved in the denial to review the decision to deny access. DWIHN must promptly refer a request for review to such designated reviewing official. The reviewing official must determine, within a reasonable period of time, whether or not to deny the access. Thereupon, the DWIHN must promptly provide written notice to the patient of the reviewing official's determination.

DWIHN must document the following and retain the documentation for a period of six (6) years:

- Designated Record Sets that are subject to access by patients; and
- The titles of the persons or offices responsible for receiving and processing requests for access.

References:

Privacy Standards Manual Section 11.0
HIPAA Privacy Brief – Access of Patients to Protected Health Information
45 CFR § 164.524
MCL 333.26261, et seq.

P-4500 Amendments of Protected Health Information

Purpose
To ensure compliance with applicable law allowing patients to amend their medical records.

Definitions
"Designated Record Set" means:
A group of records maintained by or for DWIHN that is:

- The medical records and billing records about individuals maintained by or for DWIHN;
- Used, in whole or in part, by or for DWIHN to make decisions about individuals.

For purposes of this policy, the term "record" means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for DWIHN

Policy
It is the policy of DWIHN to permit patients/consumers the right to have DWIHN amend protected health information as provided herein.

Procedure

RIGHT TO AMEND
DWIHN shall permit patients/consumers to have DWIHN amend their protected health information or a record about the patient in a Designated Record Set, for as long as the protected health information is maintained in the Designated Record Set.

DENIAL OF REQUEST FOR AMENDMENT
DWIHN may deny a patient's request for amendment, if a determination is made that the protected health information or record that is the subject of the request:

- Was not created by DWIHN unless the patient provides a reasonable basis to believe that the originator of protected health information is no longer available to act on the requested amendment;
- Is not part of the Designated Record Set;
- Would not be available for inspection under DWIHN's policy on access to records; or
- Is accurate and complete.

REQUESTS FOR AMENDMENT
DWIHN must permit a patient/consumer to request that DWIHN amend the protected health information maintained in the Designated Record Set. DWIHN may require patients to make requests for amendment in writing and to provide a reason to support a requested amendment, provided patients are made aware of the policy.

TIME LIMITS

DWIHN must process the patient/consumer's request for an amendment no later than sixty (60) days after receiving the request by either taking action to respond to the request, or to deny the request, in whole or in part, by providing a written denial to the individual.

If DWIHN is unable to act on the amendment request within sixty (60) days after receipt of request, DWIHN shall extend the time for such action by no later than thirty (30) days, provided that:

- DWIHN, within thirty (30) days after receipt of the request, provides the patient with a written statement of the reasons for the delay and the date by which DWIHN will complete its action on the request; and
- DWIHN may have only one such extension of time on action on a request for an amendment

ACCEPTING THE AMENDMENT

If DWIHN agrees to the amendment request, in whole or in part, DWIHN must comply with the following requirements:

- Make the appropriate amendment to the protected health information or record that is the subject of the request for amendment by, at a minimum, identifying the records in the Designated Record Set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment;
- Inform the patient that the amendment has been accepted and obtain the individual's identification of an agreement to have the DWIHN notify the relevant persons with which the amendment needs to be shared;
- Make reasonable efforts to inform and provide the amendment within a reasonable time to:
    - Persons identified by the patient having received protected health information about the individual and needing the amendment; and
    - Persons, including business associates, that DWIHN knows have the protected health information that is the subject of the amendment and that may have relied, or could foreseeable rely on such information to the detriment of the patient.

DENYING THE AMENDMENT

Should the requested amendment be denied, in whole or in part, DWIHN must comply with the following requirements:

- Provide the patient with a timely, written denial. The denial shall be written in plain language and contain the following:
    - Basis for the denial;
    - Patient's right to submit a written statement disagreeing with the denial and how the patient may file such a statement;
    - A statement informing the patient if he/she does not submit a statement of disagreement, the patient may request that DWIHN provide his/her request for amendment in the denial with any future disclosures of the protected health information that is the subject of the amendment; and
    - A description of how the patient may complain to DWIHN pursuant to its complaint procedures or to the Secretary of Health and Human Services. The

description must include the name, title, and telephone number of the contact person or office.

STATEMENT OF DISAGREEMENT AND REBUTTAL
DWIHN shall permit the patient to submit a written statement disagreeing with the denial of all or part of the requested amendment and the basis of such disagreement. The length of the statement of disagreement shall be no longer than a page typewritten. DWIHN may prepare a written rebuttal to the individual's statement of disagreement. Whenever such a rebuttal is prepared, DWIHN must provide a copy to the patient who submitted the statement of disagreement. DWIHN must, as appropriate, identify the record of protected health information of the Designated Record Set that is the subject of the disputed amendment and append, or otherwise link the individual's request for an amendment, DWIHN's denial of the request, the individual's statement of disagreement, if any, and DWIHN's rebuttal, if any, to the Designated Record Set.

FUTURE DISCLOSURES
If a statement of disagreement has been submitted by the patient, DWIHN must include the material appended in accordance with the paragraph above, or, an accurate summary of any such information, with any subsequent disclosure of the protected health information to which the disagreement relates.

If the patient did not submit a written statement of disagreement, DWIHN shall include the patient's request for amendment in its denial, or an accurate summary of such information, with any subsequent disclosure of the protected health information, only if the patient has requested such action.

When a subsequent disclosure is made using a standard transaction under the HIPAA Transactions Regulations that does not permit the additional material to be included with the disclosure, DWIHN may separately transmit the material required above, as applicable, to the recipient of the standard transaction.

NOTICES OF AMENDMENT
If DWIHN is informed by another provider or facility of an amendment, it must amend the protected health information in its Designated Record Set.

Records shall be kept documenting who was responsible for receiving and processing requests for amendments by patients. Such documentation shall be retained for a period of six (6) years.

References:
Privacy Standards Manual Section 12.0
HIPAA Privacy Brief – Amendments of Protected Health Information
45 CFR §164.526

P-4600 Accounting of Disclosures

Purpose
To ensure compliance with applicable law regarding accountings of disclosures of protected health information provided to patients.

Policy
It is the policy of DWIHN to provide individuals with a right to receive an accounting of disclosures of protected health information made by DWIHN in the six (6) years prior to the date in which the accounting is requested.

Procedure
RIGHT TO AN ACCOUNTING
DWIHN shall provide individuals with an accounting of disclosures of protected health information made by DWIHN six (6) years prior to the date in which the accounting is requested, or a shorter period at the request of the individual, including disclosures to or by business associates of DWIHN.

EXCEPTIONS TO RIGHT OF ACCOUNTING
If patient requests an accounting of disclosures of protected health information made by DWIHN in the six (6) years prior to the date in which the accounting is requested, DWIHN must comply except for disclosures:

- To carry out treatment, payment, and health care operations;
- To individuals of protected health information about them;
- Incident to a use or disclosure otherwise permitted or required by the Privacy Regulations;
- To persons involved in the individual's care, or other notification purposes;
- For the facility's directory (If applicable);
- That occurred pursuant to an authorization;
- For national security or intelligence purposes;
- To correctional institutions or law enforcement officials;
- As part of a limited data set; and
- That occurred prior to the first effective date of this policy.

REQUIREMENTS OF WRITTEN ACCOUNTING
Each accounting shall include:

- Date of the disclosure;
- Name of the entity or person who received the protected health information, and, if known, the address of such entity or person;
- Brief description of the protected health information disclosed; and
- A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure; or in lieu of such statement, a copy of a written request for disclosure, if any.

If during the period covered by the accounting DWIHN has made multiple disclosures of protected health information to the same person or entity for a single purpose, the accounting may, with respect to such multiple disclosures, provide:

- The core elements required to be in all accountings as described above for the first disclosure during the accounting period;
- The frequency, periodicity, or number of the disclosures made during the accounting period; and
- The date of the last such disclosure during the accounting period.

If, during the period covered by the accounting, DWIHN has made disclosures of protected health information for a particular research purpose for 50 or more individuals, the accounting may, with respect to such disclosures for which the protected health information about the individual may have been included, provide:

- The name of the protocol or other research activity;
- A description, in plain language, of the research protocol or other research activity, including the purpose of the research and the criteria for selecting particular records;
- A brief description of the type of protected health information disclosed;
- The date, or period of time during which such disclosures occurred, or may have occurred, including the date of the last such disclosure during the accounting period;
- The name, address, and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed; and
- A statement that the protected health information of the individual may or may not have been disclosed for a particular protocol or other research activity.

If DWIHN provides an accounting for research disclosures, and if it is reasonably likely that the protected health information of the individual was disclosed for such research protocol or activity, DWIHN shall, at the request of the individual, assist in contacting the entity that sponsored the research and the researcher.

TEMPORARY SUSPENSION OF A PATIENT'S RIGHT TO RECEIVE ACCOUNTING

DWIHN will temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official for the time specified by such agency or official, if:

- Such agency or official provides DWIHN with a written statement that an accounting to the individual would be reasonably likely to impede the agency's activities; and
- Such agency or official specifies the time for which such a suspension is required.

If the agency or official statement referenced in the preceding paragraph is made orally, DWIHN shall:

- Document the statement, including the identity of the agency or official making the statement;
- Temporarily suspend the individual's right to an accounting of disclosures subject to the statement;
- Limit the temporary suspension to no longer than thirty (30) days from the date of the oral statement unless the agency's or official's written statement is submitted during that time.

TIME LIMITS FOR PROVIDING OF ACCOUNTING
DWIHN shall act on an individual's request for an accounting no later than sixty (60) days after receipt of such a request as follows:

- DWIHN must provide the patient with the accounting requested; or
- If DWIHN is unable to provide the accounting within the time required herein, a thirty (30) day extension to respond is permissible per request, provided that:
- DWIHN, within the sixty (60) day period, provides the individual with a written statement for the reasons for the delay and the date the request for the accounting will be completed.
- DWIHN may have only one such extension of time for action on request for accounting.

FEES
DWIHN shall provide the first accounting to an individual in any twelve (12) month period without charge. However, all subsequent accountings within the twelve (12) month period shall be provided for a reasonable fee, if allowable under state law (See Michigan Medical Records Access Act, MCL 333.26261, et seq., Effective April 1, 2004, and amendments, if any). DWIHN shall inform the patient in advance of the fee, if applicable, and provide the individual with an opportunity to withdraw or modify the request for a subsequent accounting.

RETENTION AND DOCUMENTATION
DWIHN shall document the following and retain the documentation as follows:

- The information required to be included in an accounting for disclosures of protected health information that is subject to an accounting hereunder;
- The written accounting that is provided to the individual hereunder; and
- Titles of the person or offices responsible for receiving and processing requests for an accounting by individuals.

Such documentation shall be retained for at least six (6) years.

Reference:
45 CFR § 164.528
MCL 333.26261, et seq.

P-5000 Investigation of Complaints by Secretary

Purpose:
To ensure compliance with federal regulations regarding the investigation of complaints filed under HIPAA regulations.

Definitions:
"Person" or "Individuals" means any person who has testified, assisted, or participated in an investigation, compliance review, proceeding or hearing with respect to carrying out the purpose and intent of the HIPAA Privacy Regulations.

"Secretary" means the Secretary of Health and Human Services or any other officer or employee of HHS to whom the authority involved has been delegated.

Policy:
It is the policy of DWIHN to cooperate with the Secretary, as necessary, in the investigation of complaints filed against DWIHN, including allowing a review of policies, procedures, practices and circumstances regarding alleged acts or omissions.

It is the policy of DWIHN to refrain from taking from any action that may intimidate, threaten, coerce, or discriminate against any Person or Individual who acts in good faith in filing a complaint against DWIHN or with the Secretary regarding DWIHN's privacy policies or practices.

DWIHN shall not require any Individual to waive his or her right to file a complaint with the Secretary as a condition of providing treatment.

Procedure:
DWIHN shall retain all such documents that may be necessary to support or defend the propriety of its privacy policies and procedures.

In the event any member of the DWIHN workforce receives notice from the Secretary of an investigation of a complaint against DWIHN, the member shall immediately notify the Privacy Official or designee.

DWIHN must permit access by the Secretary during normal business hours to its facilities, books, records, accounts and other sources of information that are pertinent to ascertaining compliance with the Privacy Regulations. If the Secretary requires documents or information that is in the exclusive possession of another office, agency, institution or person, and DWIHN cannot obtain such information, DWIHN must certify to the Secretary this fact, including the efforts made to obtain the information.

References:
Privacy Standards Manual Section 1.3
HIPAA Privacy Brief - Administrative Requirements
45 CFR §§ 160.300 through 160.306, 160.310, 160.312, and 164.530

P-5100 Compliance Reviews; Reports; Remedial Action

Purpose:
To ensure compliance with federal regulations regarding compliance reviews of privacy issues conducted by the Secretary of Health and Human Services.

Policy:
It is the policy of DWIHN to cooperate with the Secretary with respect to the compliance reviews that it undertakes to determine DWIHN's compliance with federal privacy regulations.

Procedure:
GENERAL
DWIHN shall keep records and submit compliance reports at such time and manner as the Secretary may determine necessary.

NON COMPLIANCE - REMEDIAL ACTION
Upon review of the Secretary's formal or informal action in response to a compliance review indicating non-compliance, DWIHN will review such action and determine if remedial action is warranted. If such remedial action is warranted, DWIHN shall implement it within a reasonable time frame if no time frame is indicated by the Secretary.

References:
Privacy Standards Manual Section 1.3
45 CFR §§ 160.308, 160.310, and 160.312

P-5200 Complaint Process

Purpose
To ensure compliance with applicable law regarding DWIHN's complaint process.

Policy
It is the policy of DWIHN to have sufficient processes in place to take complaints of individuals.

Procedure
DWIHN must provide a process for individuals to make complaints concerning DWIHN's privacy policies and procedures or its compliance with such policies and procedures.

DWIHN must document all complaints received and their disposition, if any, and retain such documentation for six (6) years from the date of its creation or the date when it was last in effect, whichever is later.

References:
Privacy Standards Manual Section 14.4
HIPAA Privacy Brief-Administrative Requirements
45 CFR §164.530(d)

P-5300 Mitigation of Any Harmful Effects

Purpose
To ensure compliance with the mitigation of harmful effects caused by violations of privacy policies.

Policy

It is the policy of DWIHN to mitigate, to the extent practicable, any harmful effect that is known to DWIHN of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of HIPAA Privacy Regulations by the DWIHN or its business associates.

References:
Privacy Standards Manual Section 14.6
HIPAA Privacy Brief – Administrative Requirements
45 CFR § 164.530(f)

P-5400 Refraining from Retaliatory or Intimidating Acts

Purpose
To ensure that individuals are free to exercise their rights designated under HIPAA Privacy Regulations without intimidation or coercion.

Policy
DWIHN may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by the individual of any right under, or for participation by the individual in any process established by HIPAA Privacy Regulations, including the filing of a complaint.

Procedure
DWIHN may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against not only the individual but also, against that individual or another person for:

- Filing of a complaint with the Secretary of Health and Human Services;
- Testifying, assisting, or participating in an investigation, compliance review, proceeding or hearing; or
- Opposing any act or practice made unlawful by HIPAA Privacy Regulations, provided the individual or person has a good faith belief that the practice proposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of protected health information in violation of the regulations.

References:
Privacy Standards Manual Section 14.7
HIPAA Privacy Brief – Administrative Requirements
45 CFR § 164.530(g)

P-5500 Implementing and Changing Policies and Procedures

Purpose
To ensure compliance with applicable law when new laws or changes in the law are implemented.

Policy
It is the policy of DWIHN to adopt policies and procedures with respect to protected health information that are compliant with applicable law.

Procedure

POLICIES AND PROCEDURES
Policies and procedures regarding protected health information must be reasonably designed, taking into account the size of and type of activities that relate to protected health information undertaken by DWIHN to ensure such compliance. This policy should not be construed to permit or excuse an action that violates any other requirement of DWIHN.

CHANGES TO PRIVACY PRACTICES
DWIHN shall change its policies and procedures as necessary and appropriate to comply with changes in the law. When DWIHN changes a privacy practice that is stated in the notice of privacy practices, and makes corresponding changes to its policies and procedures, the changes will be effective for protected health information that was created or received prior to the effective date of the notice revision if it is included in the notice a statement reserving the right to make such a change in the notice of privacy practices.

CHANGES TO POLICIES AND PROCEDURES
DWIHN may make any other changes to policies and procedures at any time, provided that the policy or procedure, as revised, complies with applicable law; and prior to the effective date of the change, the policy or procedure, as revised, is documented and retained for at least six (6) years.

CHANGES IN LAW
Whenever there is a change of law that necessitates a change to DWIHN’s polices or procedures, DWIHN will promptly document and implement the revised policy or procedure. If the change in law materially affects the content of DWIHN's notice of privacy practices, DWIHN must promptly make the appropriate revisions.

CHANGES TO PRIVACY PRACTICES STATED IN NOTICE
To implement a change in DWIHN's privacy notice, DWIHN shall:

- Ensure that the policy or procedure as revised to reflect a change in DWIHN’s privacy practice as stated in its notice, complies with applicable law;

- Document the policy or procedure, as revised, and retain it for at least six (6) years; and
- Revise the notice to state the changed practice and make the revised notice available. DWIHN may not implement a change to a policy or procedure prior to effective date of the revised notice.

NO RESERVATION OF RIGHT TO CHANGE PRIVACY PRACTICE

If the right to change a privacy practice that is stated in DWIHN's notice has not been reserved, DWIHN is bound by the privacy practices as stated in the notice with respect to protected health information created or received while such notice is in effect. DWIHN may change a privacy practice that is stated in the notice, and the related policies and procedures, without having reserved the right to do so, provided that:

- Such changes meets the implementation requirements provided above; and
- Such changes are effective only with respect to protected health information created or received after the effective date of the notice.

CHANGES

DWIHN may change, at any time, a policy or procedure that does not materially affect the content of the notice, provided that:

- The policy or procedure, as revised, complies with HIPAA Privacy Regulations; and
- Prior to the effective date of the change, the policy or procedure, as revised, is documented and retained for at least six (6) years.

References:

Privacy Standards Manual Sections 14.9 and 14.10
HIPAA Privacy Brief – Changes to Policies and Procedures
45 CFR § 164.530(i)

P-5600 Documentation and Retention of Records

Purpose
To ensure compliance with federal regulations regarding the retention of writings.

Policy
DWIHN shall document and retain documents as required by law. This policy shall be followed in conjunction with DWIHN's other policies regarding retention of records.

Procedure:
POLICIES AND PROCEDURES
DWIHN shall maintain in written or electronic format all policies and procedures implemented with respect to protected health information.

COMMUNICATIONS
If a communication is required by DWIHN to be in writing, DWIHN shall maintain such writing, or an electronic copy, as documentation.

WRITTEN OR ELECTRONIC RECORD
If an action, activity, or designation is required to be documented, DWIHN will maintain a written or electronic record of the action, activity or designation.

LENGTH OF DOCUMENT RETENTION
DWIHN will retain any documentation required by its policies for a period of six (6) years (or longer, if required by the DWIHN Record Retention Policy) from the date of its creation, or the date when it was last in effect, whichever is later.

References:
Privacy Standards Manual Section 14.11
HIPAA Privacy Brief – Documentation Procedures
45 CFR § 164.530(j)

P-5700 Waiver of Rights

Purpose
To ensure compliance with the federal regulations regarding an individual's waiver of rights.

Policy
DWIHN may not require individuals to waive their rights under HIPAA Privacy Regulations as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

References:
Privacy Standards Manual Section 14.8
HIPAA Privacy Brief – Administrative Requirements
45 CFR § 164.530(h)

P-5800 Preemption of State Law by Federal Law; Exceptions

Purpose
To ensure compliance with federal regulations that require preemption of State Law if it is contrary to federal laws or regulations.

Definitions
"More Stringent" means in the context of a comparison of a provision of state law and a standard, requirement, or implementation specification adopted under the Privacy Regulations, a state law that meets one or more of the following criteria:

(1) With respect to a use or disclosure, the law prohibits or restricts a use or disclosure in circumstances under which such use or disclosure otherwise would be permitted under the Privacy Regulations, except if the disclosure is:

(i) Required by the Secretary of Health and Human Services in connection with determining whether a DWIHN is in compliance with the Privacy Regulations; or
(ii) To the individual who is the subject of the individually identifiable health information.

(2) With respect to the rights of an individual who is the subject of the individually identifiable health information, regarding access to or amendment of individually identifiable health information, permits greater rights of access or amendment, as applicable; provided that, nothing in the Privacy Regulations may be construed to preempt any state law to the extent that it authorizes or prohibits disclosure of protected health information about a minor to a parent, guardian, or person acting in loco parentis of such minor.

(3) With respect to information to be provided to an individual who is the subject of the individually identifiable health information about a use, a disclosure, rights, and remedies, provides the greater amount of information.

(4) With respect to the form, substance, or the need for express legal permission from an individual, who is the subject of the individually identifiable health information, for use or disclosure of individually identifiable health information, provides requirements that narrow the scope or duration, increase the privacy protections afforded (such as by expanding the criteria for), or reduce the coercive effect of the circumstances surrounding the express legal permission, as applicable.

(5) With respect to recordkeeping or requirements relating to accounting of disclosures, provides for the retention or reporting of more detailed information or for a longer duration.

(6) With respect to any other matter, provides greater privacy protection for the individual who is the subject of the individually identifiable health information.

"State Law" means a constitution, statute, regulation, rule, common law, or other state action having the force and effect of law.

Policy
It is the policy of DWIHN to comply with those State Laws pertaining to privacy that are not preempted by HIPAA, and to otherwise comply with the HIPAA Privacy Regulations.

Procedure:

GENERAL PREEMPTION
If a standard under HIPAA is contrary to a provision of State Law, it preempts the provision of State Law unless:

A. The Secretary of Health and Human Services determines that the provision of State Law is necessary for each of the following reasons:

1. To prevent fraud and abuse related to the provision of or payment for health care;
2. To ensure lawful state regulation of insurance and health plans;
3. For state reporting on health care delivery or costs;
4. For purposes of serving a compelling need related to public health, safety, or welfare. Additionally, the Secretary must determine that the intrusion into privacy is warranted when balanced against the need to be served;

B. State Law is More Stringent than the Privacy Regulations;

C. State Law provides for the reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance, investigation, or intervention; OR

D. State Law requires a health plan to report or provide access to information for the purpose of management audits, financial audits, program monitoring and evaluation, or the licensure or certification of facilities or individuals.

DWIHN will obtain assistance from legal counsel if a question exists regarding whether or not a specific State Law is preempted.

Reference:
45 CFR §§ 160.201 – 160.205