

## **HIPAA Privacy Policy and Procedures** **Genesee Area Healthcare Plan**

The participating school districts in the Genesee Area Healthcare Plan sponsor a group health plan which includes a self-administered prescription plan (GAHP). Employees of the GAHP office may have access to the individually identifiable health information of Plan participants for administrative functions of the plan.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations restrict the Plans ability to use and disclose protected health information (PHI):

*Protected Health Information.* Protected health information means information that is created or received by the Plan and relates to the past, present, or future physical or mental health or condition of a participant; the provision of health care to a participant; or the past, present, or future payment for the provision of health care to a participant; and that identifies the participant or for which there is a reasonable basis to believe the information can be used to identify the participant. Protected health information includes information of persons living or deceased.

It is the Genesee Area Healthcare Plan's policy to comply fully with HIPAA's requirements. To that end, all members of the GAHP workforce who have access to PHI must comply with this Privacy Policy and Procedures. For purposes of this Policy and Procedures, the GAHP workforce includes the Executive Director, Program Assistant and Clerk-Typist.

No third party rights (including but not limited to rights of Plan participants, beneficiaries, covered dependents, or business associates) are intended to be created by this Policy and Procedures. GAHP reserves the right to amend or change this Policy and Procedures at any time (and even retroactively) without notice. To the extent this Policy and Procedures establishes requirements and obligations above and beyond those required by HIPAA, the Policy and Procedures shall be aspirational and shall not be binding upon GAHP. This Policy and Procedures do not address requirements under other federal laws or state laws.

### **Policy and Procedures on Use and Disclosure of PHI**

#### **I. Use and Disclosure Defined**

The Genesee Area Healthcare Plan Office will use and disclose PHI only as permitted under HIPAA. The terms "use" and "disclosure" are defined as follows:

*Use.* The sharing, utilization, examination, or analysis of individually identifiable health information by any person working for or within the Genesee Area Healthcare Plan Office, or by a Business Associate (defined below) of the Plan.

*Disclosure.* For information that is protected health information, disclosure means any release, transfer, provision of access to, or divulging in any other manner of individually identifiable health information to persons not employed or working within the Genesee Area Healthcare Plan Office.

#### **II. Workforce Must Comply With Plan's Policy and Procedures**

All members of the Genesee Area Healthcare Plan Office (described at the beginning of this Policy and referred to herein as "employees") must comply with this Policy and Procedures.

#### **III. Access to PHI is Limited to Certain Employees**

The following employees ("employees with access") have access to PHI:

- Genesee Area Healthcare Plan Executive Director who performs functions directly on behalf of the Plan; and
- Program Assistant and Clerk-Typist who have access to PHI on behalf of the Plan for use in plan administrative functions (e.g., enrollments).

The employees with access may use and disclose PHI for plan administrative functions, and they may disclose PHI to other employees with access for plan administrative functions (but the PHI disclosed must be limited to the minimum amount necessary to perform the plan administrative function). Employees with access may not disclose PHI to other persons (other than employees with access) unless an authorization is in place or the disclosure otherwise is in compliance with this Policy and Procedures.

#### **IV. Specific Uses and Disclosures**

##### **A. Payment and Health Care Operations**

PHI may be disclosed for the Plan's own *payment purposes*, and PHI may be disclosed to another covered entity for the payment purposes of that covered entity.

- *Payment.* Payment includes activities undertaken to obtain Plan contributions or to determine or fulfill the Plan's responsibility for provision of benefits under the Plan. Payment also includes obtaining payment under a contract for reinsurance (including stop-loss insurance and excess loss insurance).

PHI may be disclosed for purposes of the Plan's own *health care operations*. PHI may be disclosed to another covered entity for purposes of the other covered entity's quality assessment and improvement, case management, or health care fraud and abuse detection programs. If the other covered entity has (or had) a relationship with the participant and the PHI requested pertains to that relationship.

- *Health Care Operations.* Health care operations means any of the following activities to the extent that they are related to Plan administration:  
 Enrollments and enrollment changes  
 Conducting or arranging for legal services and auditing functions  
 Prescription overrides

##### **B. For Non-Health Plan Purposes**

PHI may not be used or disclosed for the payment or operation of a participating school district's "non-health" benefits (e.g., disability, workers' compensation, life insurance, etc.), unless the participant has provided an authorization form for such use or disclosure or such use or disclosure is required by applicable state law and particular requirements under HIPAA are met.

##### **C. To Individual and DHHS**

A participant's PHI must be disclosed as required by HIPAA in two situations:  
 The disclosure is to the individual who is the subject of the information.  
 The disclosure is made to DHHS for purposes of enforcing HIPAA.

##### **D. For Legal and Public Policy Purposes**

PHI may be disclosed in the following situations without a participant's authorization, when specific requirements are satisfied. These requirements include prior approval of the GAHP Privacy Official. Disclosures without authorization are permitted:

- about victims of abuse, neglect or domestic violence;

- for judicial and administrative proceedings;
- for law enforcement purposes;
- for public health activities;
- for health oversight activities;
- about decedents;
- for cadaveric organ, eye or tissue donation purposes;
- for certain limited research purposes;
- to avert a serious threat to health or safety;
- for specialized government functions; and
- that relate to workers' compensation programs.

**E. Pursuant to an Authorization**

PHI may be disclosed for any purpose if an authorization that satisfies all of HIPAA's requirements for a valid authorization is provided by the participant. All uses and disclosures made pursuant to a signed authorization must be consistent with the terms and conditions of the authorization.

**F. To Spouses, Family Members, and Friends**

The GAHP employees will not disclose PHI to family and friends of an individual except as required or permitted by HIPAA. Generally, an authorization is required before another party, including spouse, family member or friend, will be able to access PHI. If an employee receives a request for disclosure of an individual's PHI from a spouse, family member or personal friend of an individual, and the spouse, family member, or personal friend is either (1) the parent of the individual and the individual is a minor child; or (2) the personal representative of the individual, then follow the procedure for "Verification of Identity of Those Requesting Protected Health Information."

**G. To Business Associates**

Employees may disclose PHI to the Plan's business associates and allow the Plan's business associates to create or receive PHI on its behalf. However, prior to doing so, the Plan must first obtain assurances from the business associate that it will appropriately safeguard the information. Before sharing PHI with outside consultants or contractors who meet the definition of a "business associate," employees must contact the Privacy Official and verify that a business associate contract is in place. Disclosures must be consistent with the terms of the business associate contract.

*Business Associate* is an entity or person who:

- Performs or assists in performing a Plan function or activity involving the use and disclosure of PHI (including claims processing or administration, data analysis, underwriting, etc.); or
- Provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation, or financial services, where the performance of such services involves giving the service provider access to PHI.

**H. De-Identified Information**

The Plan may freely use and disclose de-identified information. De-identified information is health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. Employees will obtain approval from Privacy Official for the disclosure. The Privacy Official will verify that the information is de-identified.

## **V. Minimum Necessary Standard and Disclosures**

The “minimum necessary” standard applies to disclosures described in IV(A), IV(B), IV(D), and IV(G).

This standard generally requires that when PHI is used or disclosed, the amount of information disclosed must be limited to the “minimum necessary” to accomplish the purpose of the use or disclosure.

### *Procedures for Disclosures and Requests for Protected Health Information*

- For recurring disclosures and requests (e.g., to business associates), and all other disclosures and requests, the Privacy Official will be consulted to ensure that the amount of information disclosed is the minimum amount necessary to accomplish the purpose of the request or disclosure.

### *Exceptions*

- The “minimum necessary” standard does not apply to any of the following:
  - Uses or disclosures made to the individual;
  - Uses or disclosures made pursuant to an individual authorization;
  - Disclosures made to DHHS;
  - Uses or disclosures required by law; and
  - Uses or disclosures required to comply with HIPAA

## **VI. Documentation of Disclosures**

Disclosures described in IV(A), IV(B), IV(C) *DHHS*, IV(D), IV(E), and IV(G), must be documented in accordance with the “Documentation Requirements”.

## **VII. Privacy Official Approval of Disclosures**

Requests for disclosures described in: IV(B), IV(D), and IV(G) shall be submitted in writing to the Privacy Official who will determine the appropriateness of the request based on applicable regulations, and if necessary, consultation with the Plan’s legal counsel.

## **VIII. Verification of Identity of Those Requesting Protected Health Information**

*Verifying Identity and Authority of Requesting Party.* Employees must take steps to verify the identity of individuals who request access to PHI. They must also verify the authority of any person to have access to PHI, if the identity or authority of such person is not known. Separate procedures are set forth below for verifying the identity and authority, depending on whether the request is made by the individual, a parent seeking access to the PHI of his or her minor child, a personal representative, or a public official seeking access.

*Request Made by Individual.* When an individual requests access to his or her own PHI, the following steps should be followed.

- Request a form of identification from the individual. Employees may rely on a valid driver’s license, passport or other photo identification issued by a government agency.
- Make a copy of the identification provided by the individual and file it with the request.
- If the individual requests PHI over the telephone, the employee will ask for the individual’s subscriber identification number and home address for verification.

*Request Made by Parent Seeking PHI of Minor Child.* When a parent requests access to the PHI of the parent’s minor child, the following steps should be followed:

- Seek verification of the person’s relationship with the child. Such verification may take the form of confirming enrollment of the child in the parent’s plan as a dependent.

*Request Made by Personal Representative.* When a personal representative requests access to an individual’s PHI, the following steps should be followed:

- Require a copy of a valid power of attorney.
- Make a copy of the documentation provided and file it with the individual’s request.

*Request Made by Public Official.* If a public official requests access to PHI, and if the request is for one of the purposes set forth above in IV(C) or IV(D), the following steps should be followed to verify the official’s identity and authority:

- If the request is made in person, request presentation of an agency identification badge, other official credentials, or other proof of government status. Make a copy of the identification provided and file it with the individual’s request and records.
- If the request is in writing, verify that the request is on the appropriate government letterhead;
- Obtain approval for the disclosure from the Privacy Official.

**Questions about validity or authorization**

- Verify that the identification matches the identity of the individual requesting access to the PHI. If the employee has any doubts as to the validity or authenticity of the identification provided or the identity of the individual requesting access to the PHI, contact the Privacy Official.

**Documentation**

- Disclosures must be documented in accordance with the procedure for “Documentation Requirements.”

**IX. Mitigation of Inadvertent Disclosures of Protected Health Information**

HIPAA requires that a covered entity mitigate, to the extent possible, any harmful effects that become known to us of a use or disclosure of an individual’s PHI in violation of this Policy and Procedures. As a result, if GAHP employees or plan participants become aware of a disclosure of PHI, either by an employee of the GAHP Office or an outside consultant/contractor, that is not in compliance with this Policy and Procedures, the employee or participant will immediately contact the Privacy Official so that the appropriate steps to mitigate the harm to the individual can be taken.

**Policy and Procedures for Complying with Individual Rights**

**I. Access to Protected Health Information and Requests for Amendment**

HIPAA gives participants the right to access and obtain copies of their PHI that the Plan (or its business associates) maintains in designated record sets. HIPAA also provides that participants may request to have their PHI amended. GAHP will provide access to PHI and will consider requests for amendment that are submitted in writing by participants.

*Designated Record Set* is a group of records maintained by or for the GAHP that includes:

- The enrollment, payment, and claims adjudication record of an individual maintained by or for the Plan; or
- Other PHI used, in whole or in part, by or for GAHP to make coverage decisions about an individual.

*Procedure*

- Follow the procedures for verifying the identity of the individual (or parent or personal representative) set forth in the "Verification of Identity of Those Requesting PHI."
- Review the disclosure request to determine whether the PHI requested is held in the individuals designated record set. No request for access may be denied without approval from the Privacy Official.
- Respond to the request by providing the information or denying the request within 30 days (60 days if the information is maintained off-site). If the requested PHI cannot be accessed within the 30-day (or 60-day) period, the deadline may be extended for 30 days with written notice to the individual outlining the reasons for the extension and the date by which the Plan will respond.

## **II. Accounting**

An individual has the right to obtain an accounting of certain disclosures of his or her own PHI. This right to an accounting extends to disclosures made in the last six years, other than disclosures:

- to carry out treatment, payment or health care operations;
- to individuals about their own PHI;
- incident to an otherwise permitted use or disclosure;
- pursuant to an authorization;
- for purposes of creation of a facility directory or to persons involved in the patient's care or other notification purposes;
- as part of a limited data set; or
- for national security or law enforcement purposes.

*Procedure*

- Respond to the request within 60 days by providing the accounting or informing the individual that there have been no disclosures that must be included in an accounting. If the accounting cannot be provided within the 60-day period, the deadline may be extended for 30 days with written notice to the individual outlining the reasons for the extension and the date by which the Plan will respond.
- If any business associate of the Plan has the authority to disclose the individual's PHI, then GAHP employees will submit the individual's written request along with the appropriate HIPAA form completed.
- Accountings must be documented in accordance with the procedure for "Documentation Requirements".

## **III. Requests for Alternative Communication Means or Locations**

Participants may request to receive communications regarding their PHI by alternative means or at alternative locations. For example, participants may ask to be called only at work rather than at home. Such requests may be honored if, in the sole discretion of Genesee Area Healthcare Plan, the requests are reasonable. Genesee Area Healthcare Plan employees shall accommodate such a request if the participant clearly provides information that the disclosures of all or part of that information could endanger the participant. The Privacy Official has responsibility for administering requests for confidential communications.

## **IV. Requests for Restrictions on Uses and Disclosures of Protected Health Information**

A participant may request restrictions on the use and disclosure of the participant's PHI. It is Genesee Area Healthcare Plan's policy to attempt to honor such requests, if, in the sole discretion of GAHP, the requests are reasonable.

## Other Policy and Procedures

### **I. Privacy Official and Contact Person**

The Genesee Area Healthcare Plan Executive Director will be the Privacy Official for the Plan. The Privacy Official will be responsible for the development and implementation of policies and procedures relating to privacy, including but not limited to this Privacy Policy and Procedures. The Privacy Official will also serve as the contact person for participants who have questions, concerns, or complaints about the privacy of their PHI.

### **II. Workforce Training**

It is GAHP policy to train all members of its workforce on its Privacy policy and Procedures. The Privacy Official is charged with developing training programs so that all workforce members receive the training necessary and appropriate to permit them to carry out their functions within the healthcare office.

### **III. Technical and Physical Safeguards**

The Genesee Area Healthcare Plan will establish appropriate technical and physical safeguards to prevent PHI from intentionally or unintentionally being used or disclosed in violation of HIPAA's requirements. Technical safeguards include obtaining digital certification for electronic access to prescription information. Physical safeguards include locking doors and filing cabinets.

### **IV. Privacy Notice**

The Privacy Official is responsible for developing and maintaining a notice of the Plan's privacy practices. The privacy notice will inform participants that the GAHP office will have access to PHI in connection with its plan administrative functions. The privacy notice will also provide a description of the Plan's complaint procedures, the name and telephone number of the contact person for further information, and the date of the notice.

The notice of privacy practices will be individually delivered to all participants. The Plan will also provide notice of availability of the privacy notice at least once every three years.

### **V. Documentation Requirement**

GAHP staff will document certain events and actions (including authorizations, requests for information, sanctions, and complaints) relating to an individual's privacy rights.

The documentation of any policies and procedures, actions, activities and designations may be maintained in either written or electronic form.

*Documentation.* GAHP will maintain copies of all of the following items for a period of at least six years from the date the documents were created or were last in effect, whichever is later:

- "Notices of Privacy Practices" that are issued to participants.
- When a disclosure of PHI is made:
  - the date of the disclosure;
  - the name of the entity or person who received the PHI and, if known, the address of such entity or person;
  - a brief description of the PHI disclosed; and
  - any other documentation required under these Use and Disclosure Policy and Procedures.

- Individual Authorizations.
- Requests for Amendments.
- Accounting of Disclosures.
- Requests for Restrictions on Uses and Disclosures of PHI.

Policies and procedures will be changed as necessary or appropriate to comply with changes in the law, standards, requirements and implementation specifications (including changes and modifications in regulations). Any changes in policies or procedures will be promptly documented.

If a change in law impacts the privacy notice the Privacy Policy and Procedures will promptly be revised and made available to participants. Such change is effective only with respect to PHI created or received after the effective date of the notice.

#### **VI. Plan Document**

The Plan document shall include provisions to describe the permitted and required uses and disclosures of PHI by the Genesee Area Healthcare Plan for administrative purposes.

#### **VII. Complaints**

The Genesee Area Healthcare Plan Executive Director, 585-344-7564, will be the Plan's contact person for receiving complaints.

The Privacy Official is responsible for creating a process for individuals to lodge complaints about the GAHP's Privacy Policy and Procedures and for creating a system for handling such complaints. A copy of the complaint procedure shall be provided to any participant upon request.

#### **VIII. Sanctions for Violations of Privacy Policy**

Sanctions for using or disclosing PHI in violation of this Privacy Policy and Procedures will be imposed in accordance with applicable law, collective bargaining agreements and policies, up to and including termination.

#### **IX. No Intimidating or Retaliatory Acts; No Waiver of HIPAA Privacy**

No employee may intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals for exercising their rights, filing a complaint, participating in an investigation, or opposing any improper practice under HIPAA.

No individual shall be required to waive his or her privacy rights under HIPAA as a condition of treatment, payment, enrollment or eligibility.