

## **POLICY: 1.016 PERSONAL HEALTH INFORMATION (PHI)**

Access to and use of patients' PHI must be *protected* in accordance to HIPAA privacy regulations. PHI should only be accessed or used when "minimally necessary." Any PHI breach by law must be reported to the NYSDOH Privacy Office (caryl.shakshober@health.ny.gov) per the guidelines in the HIPAA Breach Notification Rule (<http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html>).

### **What is Personal Health Information (PHI)?**

The Office for Civil Rights enforces the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, which protects the privacy of individually identifiable health information; the HIPAA Security Rule, which sets national standards for the security of electronic protected health information; the HIPAA Breach Notification Rule, which requires covered entities and business associates to provide notification following a breach of unsecured protected health information; and, the confidentiality provisions of the Patient Safety Rule, which protect identifiable information being used to analyze patient safety events and improve patient safety.

For information related to HIPAA Privacy Rules, refer to The Office for Civil Rights at: <http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html>

HH are required by law to report any PHI breach as per the HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414 which can be accessed on the US Department of Health and Human Services website at: <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html>

Additionally, as per the Data Use Agreement (DUA), HHs are required to report any PHI breach involving a HH member that occurs within the HH or its network providers to the NYS DOH Bureau of Security and Privacy at: [doh.sm.Medicaid.Data.Exchange@health.ny.gov](mailto:doh.sm.Medicaid.Data.Exchange@health.ny.gov)

Enrolled members are to provided with information on where to file a complaint if s/he feels their PHI was used without their permission (refer to information contained within Health Home consent forms (DOH-5055, DOH-5058, DOH-5201, DOH-5202 and FAQ document). Members may contact 1. 855-201-9807; 2. Email [nyphealthhome@nyp.org](mailto:nyphealthhome@nyp.org); to report PHI related complaints. The Executive Director or Privacy officer are to be informed within 24 hours of the incident , an investigation is to occur and if it is determined a breach did occur the incident will be reported to the State Department of health.

### **PROCEDURES:**

Care Management Agencies must:

1. comply with all state and federal laws, DOH guidance documents, and HH policy related to consents to prevent unauthorized access and sharing of PHI;
2. use appropriate DOH-numbered form(s)

3. update consents when there are care team changes and upon annual reassessment and assure consent remains on file ;
4. address and document any limitations/restrictions set by the member regarding the sharing of PHI, and the use of agency-specific HIPAA compliant consent forms to document such limitations, where applicable. For example, if a member wants daughter listed as *emergency contact* but has not given her access to other specified information a CMA will;
  - Document limitations in a care plan activity note
  - Not add the collateral to the DOH consent if there are limitations to the data sharing, rather use a general HIPAA consent form and list the data you can share in the “other” line.
  - Document in the care plan activity note other patient details tab stating PHI restriction including a specific description of the information sharing restriction.

#### 4b. RHIO /PSYCKES Information Sharing Considerations

By completing this consent form, a member is agreeing to allow his/her health information to be accessed by the HH from the Regional Health Information Organization (RHIO) and PSYCKES (Psychiatric Services and Clinical Knowledge Enhancement System) systems.

If the member is allowing only limited access to/sharing of PHI with approved entities, the HHCM must assure an alternate HIPAA compliant consent form is used (not the DOH-5055), for example: *between* selected healthcare providers; for non-healthcare agencies/services; and, for the member’s ‘emergency contact’. This alternate form can be provided by the CMA or by the agency requesting the information. The document must clearly reflect the member’s choice, define the information to be accessed/shared, identify the purpose, indicate if time limited, etc. The process must include appropriate means of communicating limitations between entities as appropriate to the situation.

Care Management agencies also document any limitations posed by members to access information from the RHIO and/or PSYCKES to prevent unauthorized sharing with providers. If a member opts out of sharing information in any system, the Care Management agency must

- Document limitations in a care plan activity note
  - Inform the Health Home via email within 24 hours in the event Healthix alerts must be turned off for the member
5. assure member rights are addressed during the signing of consent. Individual(s) signing consent (member and/or designee) must fully understand the content and intended use: e.g., voluntary enrollment; the sharing of (PHI) to support the provision of HHCM services; the development of a plan of care and establishment of a care team (multidisciplinary team) approved by the member; ability to update consent information; etc. (For HHSC, the required FAQ and documentation that the FAQ was reviewed with the parent/guardian/legally authorized representative accomplishes ensuring the understanding of the signed consent forms);
  6. use forms in the language most suitable for the member with regard for limited English Proficiency (LEP), cultural competency, physical limitations, etc.;

7. offer and provide a copy of the completed and signed consent form(s) to the member;
8. maintain completed and signed consents in the member's record, or document why a required consent or parts of consent (e.g., HHSC, section 2 of the DOH 5201) were not completed;
9. ensure the workflow for the transfer of consent information into the MAPP-HHTS is operational and working correctly

The MAPP-HHTS must be used to document the presence of consent and sharing of information (PHI) accordingly upon enrollment, throughout the duration of enrollment (e.g., when a new consent is signed), and upon disenrollment. Information related to consent must be accessible via MAPP-HHTs at any time for auditing purposes. When a situation warrants that a member's segment in MAPP-HHTS ends the HH must correctly update consent information as appropriate. Consent information may be carried forward when a new segment is created if the initial consent has remained in place and is unchanged.

10. document and act upon any member-approved changes to the consent in a timely manner, and assure entities involved in the member's care team are notified;
11. communicate to the Health Home a member is enrolled/denied enrollment/disenrolled and issue a Notice of Determination.

Enrollment is communicated by creating an enrolled segment within 3 business days and uploading the Notice of Enrollment in the documents section of the electronic record. For denials, the CMA may scan and email the appropriate for to [nyphealthhome@nyp.org](mailto:nyphealthhome@nyp.org). Disenrollment is communicated by ending enrolled segment with an appropriate end reason code and uploading the notice of determination within 3 business days.

Notice of Denied Enrollment is to be communicated if a member does not agree with the Notice of Determination. This is to occur by emailing the Notice of Determination for Denial of Enrollment into the Health Home Program (DOH 5236) to the Operations Manager and Quality Director who will review the Determination.

Refer to: *Health Home Notices of Determination and Fair Hearing* policy #HH0004 at:

- [https://www.health.ny.gov/health\\_care/medicaid/program/medicaid\\_health\\_homes/policy/greater6.htm#general](https://www.health.ny.gov/health_care/medicaid/program/medicaid_health_homes/policy/greater6.htm#general) under: Eligibility

12. CM core services must not be billed without an appropriately completed and signed consent; and,
13. CMA must report a violation of PHI as per State and Federal laws, and HH policy by submitting an incident form to the HH within 24 hours of occurrence or discovery of occurrence. The lead Health Home will submit the incident form via the HCS secure transfer tool and via email to [doh.sm.Medicaid.Data.Exchange@health.ny.gov](mailto:doh.sm.Medicaid.Data.Exchange@health.ny.gov)

## Procedures Related to AOT clients

All of the above procedures are to be followed for AOT clients. If an AOT client does not agree to sign a consent form the CMA is to upload a copy of the AOT order to confirm that court mandated enrollment is occurring. The Care Manager is to educate the member regarding their court order and the importance of signing a consent include the care manager's ability to advocate on behalf of the member as needed. A note documenting the attempt to obtain consent must be included in the chart.

Sections A-C to follow identify the various Health Home consent forms and describe their use in relation to enrollment, continued enrollment, and disenrollment, as appropriate:

- A. Opt Out
- B. Health Home Enrollment/Continued Enrollment, which includes:
  - Updating Consents
- C. Disenrollment from the Health Home Program

### **A. Opt Out**

*Opt Out* occurs when an individual, identified as HH eligible is approached about HHCM services but chooses not to enroll in the Health Home Program. *The DOH- 5059 Opt Out* form is used to document an individual's choice not to enroll.

The DOH-5059 is *not* used to withdraw consent. If the individual has signed a consent for Health Home enrollment (such as: *DOH-5055*, or *FAQ, DOH-5200* and *DOH-5201*), then the appropriate form to *withdraw* consent must be used. The DOH-5059 is only for individuals who chose *not* to enroll in the Health Home Program and, therefore would not have signed consent.

**Note:** *For the Health Home Serving Children's (HHSC) program.* It is a Health Home standard that when the individual or their consenter declines to enroll in the Health Home program, the HHCM notifies the referral source of the decision.

Care Management Agencies must:

- a. Facilitate the completion of the DOH-5059 in ACD. The form may be completed by the individual (or person acting on behalf of the individual), or by the HHCM as indicated and must include the *reason* for opting out.
- b. Inform the individual of his/her right to reconsider enrollment in the Health Home program, and provided with instructions on how to request enrollment;
- c. Offer or provide a copy of the completed and signed DOH-5059 to the individual; and, end the outreach segment ended using the appropriate reason code, e.g. member opted-out (pre-consent only).

**B. Health Home Enrollment/Continued Enrollment**

When the HH/CMA confirms an individual meets all appropriate eligibility criteria for enrollment into the Health Home Program, and the individual chooses to enroll, appropriate consent must be obtained to complete the enrollment process. HHCMs must confirm the member's understanding of what they are consenting to, and that signing consent confirms the member's choice to enroll (DOH-5055 or DOH-5200) and approval to access/share PHI (DOH-5055 or DOH-5201) with entities approved by the member.

HHs must be sure that individuals understand that without a signed consent, *enrollment cannot occur or continue*.

Consent must include, *at a minimum*, the following:

- the name of the CMA, and
- member's Medicaid Managed Care Plan (MMCP) if applicable, and
- primary care physician and/or healthcare provider from whom the member receives the majority of care (e.g. mental health, substance use, etc.). This includes the healthcare professional treating the chronic condition(s) identified for enrollment of the member into the HH if such professional is someone other than the primary care physician.

Consent guides the process for establishing and maintaining the member's care team and identifies, to what extent each entity may be given access to sharing member PHI. As a 'living document', consent may change over time to include new healthcare providers, service agencies, family and supports, etc. The member must be informed about the importance of including additional providers, services, supports and others to provide a greater level of care and support to the member in meeting his/her goals. Evidence of such changes must be documented in the member's consent, minimizing the potential for misuse of PHI.

Forms used for enrollment/continued enrollment are as follows:

**1. DOH-5055 Health Home Patient Information Sharing Consent**

The DOH-5055 is used to enroll/maintain enrollment for HH members who are adult, children/adolescent 18 years of age or older, or child/adolescent under age 18 if they are a parent, pregnant or married and able to self- consent.

When completing the form, page 3 is used to list healthcare providers, family/supports and other entities approved by the member and given full access to PHI, and integrated into all aspects of the member's plan of care.

*If using pre-listed HH network partners on page 3:*

In addition to listing the CMA, member's MMCP, and the member's primary care physician or healthcare provider from whom the member receives the majority of care reflective of the chronic condition for which the member was enrolled in a Health Home (e.g. mental health, substance use, etc.), the HHCM must clearly identify entities approved by the member as follows:

- place a check mark ( ✓ ) next to every entity approved by the member;  
OR,
- uncheck all entities except those that the member has approved

**IMPORTANT:**

Member cannot be asked to approve an entire pre-filled network list *in anticipation of* an entity possibly being needed in the future. Consent must clearly identify *only* those entities approved by the member directly involved in the member's care team/plan of care at the time of signing and updating consent to align with member choice and protect the member's PHI.

Health Homes *must* continuously monitor and assure proper protocols are being followed to complete the DOH 5055 and address any issues identified to prevent potential for misuse of member PHI.

Documentation

1. A Data Exchange Application and Agreement (DEAA) must be signed and submitted to NYPHH during contracting.
2. A signed consent form must be scanned and uploaded into ACD for each patient actively enrolled in the HH program.
3. Any time PHI is accessed or used there must be clear documentation regarding why that information was accessed or used, in what capacity, and with whom it was shared (if applicable) in the patient's Care Plan Activity Note on ACD.

## APPENDIX N. Examples of Administrative, Physical and Technical Safeguards for PHI.

### ➤ **Administrative Safeguards**

Measures related to administrative actions, policies and procedures for protecting personal health information.

- Assigning an officer to develop, implement and monitor compliance to policies and procedures for protecting PHI
- Training all personnel on and complying with HIPAA privacy regulations for protecting PHI
- Having a protocol in place for reporting noncompliance to policies and procedures for protecting PHI
- Applying appropriate consequences for personnel who are not compliant to policies and procedures for protecting PHI
- Limiting access to PHI as necessary for personnel to do their jobs
- Clearly identifying the individuals who may access PHI based on job responsibilities
- Verifying the identities of persons requesting PHI
- Obtain a combination of patient's demographic information (e.g., address, SS#, DOB, maiden name) to confirm patient's identity before releasing any other PHI when requested
- Performing periodic assessments to determine how well PHI are being protected

### ➤ **Physical Safeguards**

Measures to protect the structures/spaces/areas that house/contain/store personal health information from unauthorized use.

- Locking any cabinets or rooms containing PHI
- Marking all documents containing PHI as confidential
- Verifying the identity of persons requesting PHI
- Authorizing only essential personnel to access PHI based on job responsibilities
- Avoiding the sharing or use of PHI while in public spaces; this applies to face-to-face communication and communication via technology conferencing tools (e.g., audio, video, web)
- Speaking quietly in spaces with unauthorized PHI users
- Workstation and Device Security:
  - Locking workstation when stepping away from the desk
  - Protecting your user ID
  - Creating strong passwords and changing them frequently
  - Not sharing passwords with others or write them down
  - Not letting others use your account
  - Limiting the storage of PHI on hard drives
  - Using anti-virus software on PCs, laptops, etc...

### ➤ **Technical Safeguards**

Measures that protect data related to personal health information and the access to such data, including on handheld devices and flash drives.

- Creating unique user identifications (usernames and passwords) for each personnel that can be tracked
- Authorizing personnel access to PHI only as needed for performing job functions
- Password protecting files that contain PHI
- Encrypting files containing PHI that are sent electronically
- Encrypting emails that contain PHI
- Setting workstations to logoff automatically after a reasonable amount of time of inactivity
- For any faxes that contain PHI, including a confidentiality statement and writing the correct name of the receiver on the cover letter