

Member “Protected Health Information (PHI)”

Protected Health Information (PHI) is information about a member’s health. PHI means any health records that contain items that can be used to link to or identify a member, and these identifiers include such items as:

- Name, social security number, address, and phone numbers
- Date of birth, date of treatment
- A medical record number

The purpose of this article is to provide you with the following information about PHI:

- Routine uses and disclosure of PHI by Western Behavioral Health (WBH),
- The use of authorizations and the member’s ability to give authorization
- Protection of information disclosed to plan sponsor or employers
- WBH’s internal protection of oral, written, and electronic PHI
- The member’s right to access PHI
- The member’s right to amend PHI
- The member’s right to an accounting of PHI disclosures
- The member’s right to request restrictions on the use or disclosures of PHI
- The member’s right to request confidential communication

The Notice of Privacy Practices is distributed to all members by the UPMC Health Plan, which provides full details of rights regarding PHI.

How We May Use and Disclose Information For Treatment, Payment and Health Care Operations

WBH may use and disclose protected health information for a variety of reasons. The law provides that we are permitted to make certain uses/disclosures without member consent or authorization for treatment, payment and the operations of WBH. The list below describes the different ways information may be used for these purposes and gives examples of those uses.

For Treatment: We may use protected health information to coordinate and manage behavioral health care. Assuring that the member receives the appropriate treatment in the right setting is one of our top priorities. For example, if a member needs to be admitted to the hospital, WBH collects information from the practitioner about the member’s medical condition and need to be in the hospital, and then authorizes admission, if medically necessary.

For Payment: We may use and disclose protected health information for any activities that we undertake to reimburse for health care services provided. The practitioner must provide information to WBH about services recommended in order to obtain prior approval or to determine whether the recommended treatment is covered.

For Health Care Operations: We may use and disclose protected health information about members for basic business activities that are necessary to operate our business. These uses and disclosures are necessary to run WBH. These activities may include, but are not limited to, conducting compliance audits, accreditation surveys, and ongoing monitoring of the quality of provider services in order to assure that members are receiving quality care.

Other Uses and Disclosures Not Requiring Consent or Authorization: In addition to the disclosures for treatment, payment and health care operations described above, the law provides that we may use/disclose protected health information without the member’s written consent or authorization in certain other circumstances. The following list outlines the types of uses and disclosures that may be made without permission.

- **When required by law:** We may disclose information when federal, state, or local law requires us to do so.

- For public health activities. We may disclose information to authorities for public health purposes. These activities generally include the following:
 - To report child abuse or neglect
 - To report reactions to medications or problems with products
 - To notify the appropriate government authority if we believe the member has been the victim of abuse, neglect, or domestic violence. We will only make this disclosure without consent when we are required or authorized by law.

Health Oversight Activities: We may disclose protected health information to federal, state, or county agencies that oversee our activities. Health oversight activities are necessary for government agencies such as the Pennsylvania Department of Health and the Pennsylvania Insurance Department to monitor the health care system, provision of required (mandated) benefits, and compliance with civil rights laws. These activities include audits and other investigations.

- Lawsuits and Disputes: We may disclose protected health information if the member is involved in a lawsuit or dispute and we must respond to a court or administrative order. Only the information expressly authorized by the order will be disclosed. Information may also be disclosed in response to a subpoena, discovery request, or other lawful process initiated by someone else involved in the dispute, but only if efforts have been made to tell the member about the request or to obtain an order protecting the information requested.
- For Law Enforcement or Specific Government Functions: We may disclose protected health information in response to a request by a law enforcement official made through a court order, subpoena, warrant, summons or similar process. We may disclose PHI to federal officials for intelligence, counterintelligence, and other national security activities authorized by law.
- Coroners, Medical Examiners, Funeral Directors, and Organ Donation: We are permitted to release protected health information to a coroner, medical examiner or funeral director. This disclosure may be necessary, for example, in determining the cause of death. Although WBH does not generally have information pertaining to organ donation, if we do possess such information, disclosure is permitted.
- Serious Threats to Health or Safety: As permitted by applicable law and standards of ethical conduct, we may use or disclose protected health information when necessary to prevent or lessen a serious and imminent threat to the member's health or safety or the health or safety of another person or the public.
- Military and Veterans: If the member is affiliated with the armed forces, we may release protected health information as required by military command authorities. We may also release information about foreign military personnel to the appropriate foreign military authority.
- Workers Compensation: We may release PHI for workers' compensation or similar programs that provide benefits for work-related injuries or illness.
- Inmates: If the member is an inmate of a correctional institution or under the custody of a law enforcement official, we may release information to the correctional institution or law enforcement official. This release would be necessary (1) for the institution to provide the member with care; (2) to protect the member's health and safety or the health and safety of others; or (3) for the safety and security of the correctional institution.

Your Authorization in Certain Circumstances

Some uses and disclosures of information, other than as identified above, specifically require the member's written permission. This permission is provided through a UPMC Health Plan authorization form. If the member gives the Health Plan/WBH permission to use or disclose information, the member may revoke (cancel) that permission, in writing, at any time. If the member revokes permission, we will no longer use or disclose information for the reasons covered by written permission. We would be unable to take back any disclosures, however, that we already made with the original authorization.

The Protection of Information Disclosed to Employers or Plan Sponsors

WBH does not share member-identifiable data or information with employers without the member's authorization or the authorization of a legally authorized representative. WBH works with UPMC Health Plan on any request from an employer concerning group data or information. Under no circumstances would WBH share member-identifiable data or information with an employer without the member's authorization or the authorization of the member's personal representative. When an employer requests member-identifiable information from UPMC Health Plan, if the inquiry concerns behavioral health issues, the Health Plan will review the request with WBH to attempt to meet the information need with data and information that are not member-identifiable, for example, aggregated (general) data or information. In the event that the employer required member-identifiable data or information, the member would be contacted for his/her authorization.

In all instances, WBH discloses only that minimum information necessary to accomplish the purpose of the disclosure.

WBH's Internal Protection of Oral, Written, and Electronic PHI

WBH uses appropriate safeguards to ensure confidentiality. If we use information for reasons other than those described above, we change or remove any portions of the information that could allow someone to identify a member or we contact the member to obtain authorization.

WBH has designated a Privacy Officer (Director of Compliance) to oversee company policies and procedures regarding Confidentiality and Privacy and the internal protection of oral, written, and electronic information across the organization.

All WBH employees are required to sign a Statement of Confidentiality, which indicates that any employee having access to sensitive and confidential information, has agreed not to access information from any source(s) that is not needed to perform his or her job duties. Another part of the Statement of Confidentiality is that only the minimum information necessary is used by any employee at WBH to perform his or her job duties. WBH's expectations are that only the minimum amount of information needed by our employees is used. WBH's Compliance and Information Systems Departments will oversee and monitor employees' access to member-confidential data.

WBH also maintains an array of security provisions to protect confidential data and information. These include:

- Restricted access based on job responsibilities to information maintained in WBH's information system
- Physical lock and key arrangements
- Electronic security systems
- Mandatory compliance with WBH's Statement of Confidentiality

All physical media, including but not limited to paper, magnetic, and optical, used to store confidential data and information must be stored under a double lock system. All desks or secured storage areas must be in areas with keyed entry, maintaining a minimum of a dual-key system. All electronic media containing confidential information must be password protected.

Confidential data and information—no longer required for legitimate business purposes—must be destroyed in a secure manner. Paper records must be thoroughly shredded. Magnetic files must be deleted in a manner that does not permit the files to be undeleted; for example, by reformatting a floppy disk using the "secure" format option. Optical storage media must

