

Your “Protected Health Information (PHI)”

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

- Your 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:

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

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

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

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

For Treatment: We may use protected health information about you to coordinate and manage your behavioral health care. Assuring that you receive the appropriate treatment in the right setting is one of our top priorities. For example, if you need to be admitted to the hospital, WBH collects information from your practitioner about your medical condition and your need to be in the hospital, and then authorizes your admission, if medically necessary. Whenever you visit a behavioral health practitioner for outpatient therapy sessions, your practitioner sends us updated information to let us know how you are progressing in treatment.

For Payment: We may use and disclose your protected health information for any activities that we undertake to reimburse your provider for health care services provided to you. Your provider provides information to WBH about services recommended for you in order to obtain prior approval or to determine whether the recommended treatment is covered by your Plan.

Your provider then sends us a treatment plan describing the services that he or she intends on providing.

For Health Care Operations: We may use and disclose protected health information about you 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 your protected health

information without your written consent or authorization in certain other circumstances. The following list outlines the types of uses and disclosures that may be made without your permission.

- When required by law: We may disclose information about you when federal, state, or local law requires us to do so.
- For public health activities. We may disclose information about you 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 you have been the victim of abuse, neglect, or domestic violence. We will only make this disclosure without your consent when we are required or authorized by law

Health Oversight Activities: We may disclose your 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 about you if you are 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 about you 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 you 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 about you 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 your 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 your protected health information when necessary to prevent or lessen a serious and imminent threat to your health or safety or the health or safety of another person or the public.
- Military and Veterans: If you are a member of the armed forces, we may release protected health information about you 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 about you for workers' compensation or similar programs that provide benefits for work-related injuries or illness.

- **Inmates:** If you are an inmate of a correctional institution or under the custody of a law enforcement official, we may release information about you to the correctional institution or law enforcement official. This release would be necessary (1) for the institution to provide you with care; (2) to protect your 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 your written permission. This permission is provided through a UPMC Health Plan authorization form. If you give the Health Plan/WBH permission to use or disclose information about you, you may revoke (cancel) that permission, in writing, at any time. If you revoke your permission, we will no longer use or disclose information about you for the reasons covered by your 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 your authorization or the authorization of your 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 an 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 either have the files securely deleted or, if this is not possible, the storage media must be destroyed.

Your Rights

With the exception of psychotherapy session notes, you have the right to access and amend your protected health information (PHI).

You can request a copy of your PHI, restrict the use of PHI, request confidential communication, request an account of any disclosures of your PHI other than for treatment, payment and health care operations purposes, and request amendments to your PHI. The process to exercise any of these rights is to put your request in writing. Please call the UPMC Health Plan’s Member Service Line at 1-888-876-2756 to obtain forms to do so.

On each of these forms, you need to follow the instructions, making sure that you fill in all the information requested, and sign and date your request. If you are unable to act on your own behalf, you can designate a personal representative. UPMC Health Plan can assist you in doing that.

If any of your requests concern your behavioral health information, UPMC Health Plan will review your request with WBH and will respond to you within the timeframe required by law. If your request is **granted**, a representative will help you review your PHI and will explain the process to you. Sometimes, UPMCHP and WBH can deny a request. If we are unable to grant your request, UPMC Health Plan will send you a letter describing:

- The decision
- The reason for the denial (why your request was not granted)
- How you can appeal (voice your disagreement if you do not agree with our decision) and the name or title and telephone number of a contact person for this step

Right to a Paper Copy of the Notice of Privacy Practices: You have the right to a paper copy of the UPMC Health Plan Notice of Privacy Practices, and you may ask UPMC Health Plan to give you a copy at any time. To obtain a paper copy of this document, please call the UPMC Health Plan’s Member Service Line at 1-888-876-2756. The Notice of Privacy Practices can also be found on the Health Plan’s Website at <http://www.upmchealthplan.com/home/hipaa.html>.

We will continue to keep UPMC Health Plan members and WBH providers informed of our policies and procedures about protected health information (PHI) through Health Plan communications and articles such as this.

Requests for confidential information may also be referred to your health care provider responsible for providing you with your medical information.

Effective Date

The effective date of this Notice is April 14, 2003.