



Origination 10/2019
Last Approved 01/2025
Effective 01/2025
Last Revised 01/2025
Next Review 01/2026

Owner Kara Glover: HIM and HIPAA/ Compliance Manager
Area Compliance

Confidentiality of Protected Health Information (PHI)

I. Purpose

The purpose of this policy is to establish general requirements for protecting the confidentiality of Protected Health Information (PHI) while allowing its necessary use, access, and disclosure for purposes of providing high quality care to the patients of Wellfound Behavioral Health Hospital (WBHH).

Additionally, the purpose of this policy is to establish standards for requesting, modifying, and terminating access to WBHH's information technology data.

II. Scope

This policy applies to all members of the WBHH workforce including, but not limited to: employees, medical staff, volunteers, students, administrative staff, contractors, and other persons performing work for or at WBHH.

III. Policy

All PHI, in any format (oral, written, or electronic), produced by or on behalf of WBHH is confidential and must not be shared by employees and/or agents of WBHH with other individuals and entities, including other WBHH employees and/or agents, unless necessary in order to enable the employee or agent to perform the duties within the scope of their employment. This policy is subject to limited exceptions as outlined below.

In general, all PHI, in any format, produced by or on behalf of WBHH is also subject to the Minimum Necessary Rule when said PHI is being accessed, used, or disclosed, unless the access, use, or disclosure falls under a limited set of exceptions as outlined below.

It is WBHH's policy to determine the need for access to and appropriate levels of security to protect the

confidentiality of data on our systems, including electronic Protected Health Information (ePHI). WBHH's personnel shall be identified and categorized by the degree of access and need for patient health information to perform their job's duties.

IV. Procedures/Guidelines

A. Confidentiality of PHI

1. To protect the confidentiality of PHI, individuals included within the scope of this policy should not access, discuss, or share PHI in public areas or with any individuals who do not have a need to know the information for purposes, such as treatment, payment, health care operations (TPO), or as otherwise required or permitted by law.

B. Special Categories of PHI with heightened protection

1. The following categories of PHI have heightened privacy protection:
 - i. HIV/AIDS PHI
 - ii. Mental health-related PHI
 - iii. Substance abuse (Drug and Alcohol) PHI
 - iv. Psychotherapy notes

C. Obligation to Sign Confidentiality of WBHH Information Attestation and Agree to Access and Confidentiality User Agreement

1. All individuals within the scope of this policy are required to sign the "Wellfound Confidentiality Statement".
2. Business Associates providing services on behalf of WBHH are required to sign a Business Associate Agreement (BAA). A review will be performed by the applicable service area leader or designee to confirm BAAs are in place as appropriate on a periodic basis.

D. Obligation of Department Directors

1. It is the responsibility of each department leader to evaluate the PHI generated and received within their department. It is then the responsibility of each department leader to develop and implement reasonable policies and procedures to safeguard all PHI and determine the categories of individuals within the department who must have access to PHI to accomplish their employment duties.
2. It is the responsibility of the department leader to ensure that only those necessary individuals attend medical education conferences in which PHI is discussed. At all such medical education conferences, any reference to the identity of patients shall be redacted from the case presentation. The case will be given a fictitious name or de-identified number that will be used throughout the discussion, but will not be associated with the patient's PHI in any way.

E. Access, Use, or Disclosure of PHI Permitted without an Authorization

1. WBHH is only permitted to access, use, or disclose an individual's PHI for treatment,

payment, or health care operations (TPO), unless a validly executed "Release of Information (ROI) Authorization to Use or Disclose" form has been provided or a specific regulatory exception applies.

2. An authorization to access, use, or disclose PHI is not required, but may be requested for record-keeping purposes, in the following circumstances:
 - i. The access, use, or disclosure involves the patient, the patient's personal representative, or a patient's family member or friend who, according to the health care provider's professional judgment, is acting in the best interest of the patient's care;
 - ii. The access, use, or disclosure involves a correctional institution or other law enforcement custodian who is overseeing the health care of an incarcerated patient, for purposes of caring for the patient, in addition to the others in the institution;
 - iii. Patient's will be given the option to allow individuals to know of their treatment at WBHH through the assignment of a passcode;
 - iv. The access, use, or disclosure is for purposes of emergencies, national security and intelligence activities, military or veteran's affairs activities, public health, regulatory oversight, or accreditation; is in accordance with a legally valid subpoena; or is permitted or required by law;
 - v. The access, use, or disclosure is to a medical examiner or funeral director for purposes of carrying out their scope of duties related to the patient;
 - vi. The access, use, or disclosure is for the purposes of cadaveric, eye, or tissue donation if that is consistent with the patient or patient's designated representative's intent; and/or
 - vii. The access, use, or disclosure is legally required by a program providing benefits to a patient for a work-related injury or illness.
3. Individuals have the right to request restrictions on the access, use, or disclosure of their PHI.

F. The Minimum Necessary Rule

1. In general, when permissibly accessing, using, or disclosing PHI, WBHH must limit such access, use, or disclosure to the minimum necessary to accomplish the intended purpose of the access, use, or disclosure.
2. For guidance on determining the minimum necessary amount of information to accomplish an intended purpose in any particular case, please contact the facility's Privacy Officer.
3. The Minimum Necessary Rule (standard) does not apply in the following circumstances:
 - i. The PHI is for use by, or a disclosure to, a healthcare provider for treatment purposes;
 - ii. The disclosure is to the patient or the patient's legally authorized representative (this is limited to the extent that such individual is

- authorized to receive such information);
- iii. The disclosure is pursuant to a valid authorization, in which case, the disclosure will be limited to the PHI specified on the authorization;
 - iv. The disclosure is to the Secretary of United States Department of Health and Human Services; or
 - v. The disclosure is required by law.
4. Statement of Purpose Requirement for All Disclosures to which Minimum Necessary Rule Applies
- i. For all disclosures to which this "minimum necessary" requirement applies, when a request is made for access to, the use or disclosure of PHI, WBHH shall determine whether the request includes a statement of purpose. If the request does include a statement of purpose, WBHH shall release only the minimum amount of information necessary to meet the stated purpose of the request. If the request does not include a statement of purpose, WBHH shall contact the requester to obtain the purpose for the request, document the contact with the requester, and take the appropriate action.
5. Routine Disclosures (e.g. Workers' Compensation, Third Party Payors)
- i. WBHH may disclose PHI on a routine, recurring basis to third parties, such as ambulance companies, revenue recovery agencies, or insurance payors (including but not limited to Medicaid, Medicare, private insurers, and workers' compensation insurers or administrative agencies) without authorization, for the purposes of obtaining payment for health care and to the extent necessary to comply with applicable laws.
 - ii. The first time that WBHH receives a request for PHI from an insurance payor or other third party, and each time that the request is modified thereafter, the facility or department shall review the request to ensure that the type and amount of PHI that is disclosed is limited to what is necessary in order to achieve the third party's purpose.
 - iii. For guidance on routine disclosures, please contact the facility's Privacy Officer.
6. Non-Routine Disclosures
- i. Non-routine disclosures and requests (e.g. to law enforcement or to a judicial body) will be limited to only the minimum amount of PHI necessary to accomplish the purpose of the disclosure or request. Non-routine disclosures and requests will be reviewed by the facility on an individual basis and limited accordingly. Questions regarding the minimum necessary standard requirements should be directed to the facility's Privacy Officer and to the Legal Department where appropriate.
7. Requests from WBHH to Other Entities
- i. WBHH must also limit its requests for PHI held by other entities to the

minimum necessary to accomplish the intended purpose of the request.

G. Training

1. Workforce members will be provided Health Insurance Portability and Accountability Act (HIPAA) training on, at least, an annual basis and as needed for any updates.

H. Sanctions

1. In compliance with the HIPAA Privacy and Security Rules, violations of this policy will be subject to disciplinary action as outlined in the Human Resources (HR) Policies and in the Bylaws, Rules, and Regulations of the Medical Staff.

I. Document Retention

1. Any documentation generated in compliance with this policy will be retained for a minimum of 6 years (plus current year) from the date of its creation.

- J. Questions related to access, use, or disclosure of PHI should be directed to the facility's Privacy Officer.

V. Definitions

Authorization: An individual's signed permission that allows a covered entity to use or disclose the individual's PHI for the purpose(s), and to the recipient(s), as stated in the Authorization.

Business Associate: An entity that performs, or assists in the performance of, a function or activity involving the access, use or disclosure of PHI, including, but not limited to, claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, or re-pricing.

Covered Entity: A facility that conducts Health Care Operations involving the creation and transmission of PHI. Each facility in Wellfound Behavioral Health Hospital which conducts Health Care Operations is its own Covered Entity. These Covered Entities are collectively considered an Organized Health Care Arrangement which allows each of the included Covered Entities to share PHI for Treatment, Payment and Health Care Operations.

Department Director: The person with managerial responsibility for an identified WBHH Department.

Disclosure: The release, transfer, access to, or divulging of information in any other manner outside the entity holding the information.

Health Care Operations: Activities of WBHH as they relate to covered functions, including, but not limited to, quality assessment and improvement activities, reviewing the competence or qualifications of health care professionals, activities related to contracting for health insurance or health benefits, conducting or arranging for medical review, legal review, or auditing functions, business planning and development, and business management and administrative activities.

Protected Health Information (PHI): Any oral, written, or electronic individually identifiable health information collected or stored by a facility. Individually identifiable health information includes demographic information and any information that relates to the past, present, or future physical or

mental condition of an individual.

HIPAA details eighteen items that render PHI identifiable:

1. Names;
2. 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 in certain situations;
3. All elements of date (except year) for dates directly related to an individual, including birth date, discharge date, date of death; and all ages over 89 and all elements of dates indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
4. Telephone numbers;
5. Fax numbers;
6. Electronic mail addresses;
7. Social security numbers;
8. Medical record numbers;
9. Health plan beneficiary numbers;
10. Account numbers;
11. Certificate/license numbers;
12. Vehicle identifiers and serial numbers;
13. Medical Device Identifiers;
14. Web Universal Resource Locators (URLs);
15. Internet Protocol (IP) address numbers;
16. Biometric identifiers, including finger and voice prints;
17. Full face photographic images and any comparable images; and
18. Any other unique identifying number, characteristic, or code.

Payment: The actions taken by a health care provider or health plan to obtain or provide reimbursement for the provision of health care.

Treatment: 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.

Minimum Necessary: The minimum necessary standard, a key protection of the HIPAA Privacy Rule, is derived from confidentiality codes and practices in common use today. It is based on sound current practice that protected health information should not be used or disclosed when it is not necessary to satisfy a particular purpose or carry out a function. The Privacy Rule's requirements for minimum necessary are designed to be sufficiently flexible to accommodate the various circumstances of any

covered entity.

VI. References

Health Insurance Portability and Accountability Act, 45 CFR Parts 160 and 164
Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A
and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No.
111-5 (Feb. 17, 2009)

Approval Signatures

Step Description	Approver	Date
Policy Committee	Cat Kintu: Director, Quality [KG]	01/2025
HIM and HIPAA/Compliance Manager	Kara Glover: HIM and HIPAA/ Compliance Manager	01/2025
Owner	Kara Glover: HIM and HIPAA/ Compliance Manager	01/2025

