KLAMATH BASIN BEHAVIORAL HEALTH
GROWTH • WELLNESS • COMMUNITY KBBH

POLICY:	KBBH Health Insurance Portability and Accountability Act (HIPAA) Disclosures Policy
DEPARTMENT:	Compliance
REVISION DATE:	May 2024

POLICY STATEMENT: It is the policy of Klamath Basin Behavioral Health when using or disclosing Protected Health Information (PHI) or when requesting PHI from another covered entity, to make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. As a rule, KBBH employees may not disclose or request an entire clinical record of a client unless the entire clinical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the disclosure or request.

Additionally, KBBH employees, interns and contractors will limit their review of any client's clinical record to those portions of the record required to accomplish their purpose, to limit the amount of PHI exposed to possible unauthorized disclosure or re-disclosure by establishing standards for various types of disclosures.

DEFINITIONS:

Minimum Necessary Information: Accessing or disclosing the minimum amount of PHI necessary to fulfill the goal.

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

Protected Health Information (PHI): Any information in the medical record or designated record set that can be used to identify an individual and that was created, used, or disclosed in the course of providing a health care service such as diagnosis or treatment.

PROTOCOL FOR USING, DISCLOSING OR REQUESTING MINIMUM NECESSARY INFORMATION:

KBBH's Compliance Manager shall identify persons (or classes of persons) within KBBH who need access to PHI to carry out their duties. For each person (or classes of persons) KBBH's Compliance Manager shall identify the category (or categories) of PHI to which access is needed and any conditions appropriate to such access. Once persons within KBBH who need access to PHI and categories of information are identified, KBBH will make reasonable efforts to limit access only to such identified persons and such uses or disclosures only in such identified categories.

For any type of disclosure or request, KBBH's Compliance Manager will develop criteria and train identified persons to limit the PHI disclosed to the amount reasonably necessary to accomplish the purpose of the disclosure or request; and have KBBH staff review requests for disclosure on an individual basis in accordance with provided criteria.

Release of Information (ROIs). KBBH employees will rely on the documents listed on an ROI as the minimum necessary for the stated purpose (if reliance is reasonable under the circumstances) in the following situations:

- When making disclosures to public officials under 45 CFR §164.512 if the requesting official represents that the information is the minimum necessary.
- When the information is requested by another covered entity.
- When the information is requested by a KBBH Professional, or is a business associate of KBBH, and the request is for the purpose of providing professional services to KBBH, or if the Professional represents that the information requested is the minimum necessary for the stated purpose(s).
- When the information is requested for research purposes and the person requesting the information has provided documentation or representations that comply with 45 CFR §164.512(l).

KBBH employees, interns and contractors shall use, disclose, or request the minimum necessary amount of PHI in all situations, except the following:

- Disclosures to or requests by a health care provider for treatment.
- Uses or disclosures made to the client: (1) as permitted or required under the Security Policy; or (2) pursuant to a valid patient authorization under the Release of Information Policy.
- Disclosures to the Secretary of Health and Human Services.
- Uses or disclosures relating to data elements specified in the implementation guides for HIPAA administration simplification standard transactions in the Transaction Rules. (§164.502(b) (2) (v).
- Uses or disclosures that are required by law.

Uses and Disclosures Required by Law CFR 164.512. KBBH may use or disclose PHI without the written consent or authorization of the client in the following situations:

- Disclosures required by law, which include:
- For minors and adults in protective status: Disclosures about victims of abuse, neglect or domestic violence when staff reasonably believes the client is a victim of one of the above and the information is disclosed to a social service or protective service staff of the governmental agency authorized to receive such reports.
- Disclosures for judicial or administrative proceedings in the form of a court or administrative tribunal order or in response to a discovery request, subpoena or other lawful process that is not accompanied by a court or tribunal order, as long as the requester can demonstrate that they have made reasonable efforts to inform the client whose PHI is being asked for about the request and the purpose of the request.
- Disclosures for Law Enforcement purposes as required by law. These may include court orders, warrants, summons, grand jury subpoena, or an administrative request. Provided that the specific and limited in scope to what is reasonable in light of the purpose for which the information is sought.
- Limited disclosure to law enforcement personnel for identification and location purposes when the law enforcement official is attempting to identify or locate a suspect, fugitive, material witness, or missing person. In this case, the information that may be disclosed is limited to:
    - Name and address
    - Date, place of birth, if known
    - Social Security number
    - Date and time of death, if known
    - Physical description including height, weight, gender, race, hair and eye color, presence or absence of facial hair, scars, tattoos or other distinguishing physical characteristics.
    - Limited disclosure to a law enforcement official when the client is the victim of a crime.
- If in doubt, contact the Compliance Manager to determine if a disclosure is permissible.

Phone and Text Message Communication. KBBH employees should use systems provided by KBBH for communicating work related information. These systems include work provided cellphones and Zoom (or currently used) software. It is not acceptable to use personal cellular devices to transmit PHI. If a KBBH employee does not have a work provided cell phone, but needs to transmit PHI telephonically, the employee should either install the Zoom app on their personal phone or use the Zoom app on their computer. They should not use

their personal phone text messaging system to do so. Texting PHI, even on a work provided cell phone is not acceptable, use the Zoom app to message.

Email Communication. KBBH employees must be cognizant of the risks involved in transmitting PHI through email. Sending PHI by email exposes the PHI to two risks:

- The email could be sent to the wrong person, usually because of a typing mistake or selecting the wrong name in an auto-fill list
- The email could be captured electronically en route.

HIPAA requires that we take reasonable steps to protect against these risks but acknowledges that a balance must be struck between the need to secure PHI and the need to ensure that clinicians can efficiently exchange important client care information. Emails containing PHI being sent to recipients outside of the agency must be encrypted according to current protocols described by the IT department. Emails containing PHI being sent to recipients within the KBBH IT infrastructure are reasonably protected with current security protocols. In addition, you must observe the following rules:

- Limit the information you include in an email to the minimum necessary for your clinical, compliance, or billing purpose.
- Whenever possible, avoid transmitting highly sensitive PHI by email.
- Never use global automatic forwarding to send emails from your kbbh.org email account to a non-kbbh.org account.
- Never send PHI by email unless you have verified the recipient's address and you have double-checked that you have entered that address correctly.
- Subject lines should not include identifying information, including Client IDs.
- Always include a privacy statement and providing a contact to whom a recipient can report a misdirected message.
    - Recommended Privacy statement: *The information contained in this message may be privileged and confidential. If you are NOT the intended recipient, please notify the sender immediately with a copy to compliance@kbbh.org and destroy this message.*

Users must immediately report violations of this policy to their supervisor and/or the Compliance manager.

Client's Personal Representative.

Under Oregon law, a parent of an unemancipated minor, a court appointed guardian, an attorney-in-fact appointed under a health care power of attorney, an unappointed health care representative with authority under the Oregon Health Care Decision Act, or an

executor of a deceased client's estate may have authority to act as a client's Personal Representative.

a) Determine Category of the client. Prior to allowing a person to act as a client's Personal Representative in connection with KBBH's use or disclosure of the client's PHI, KBBH must first determine if the client is:
    a. an adult or emancipated minor;
    b. an unemancipated minor;
    c. deceased;
    d. a victim of abuse, neglect or endangerment.

    After making this determination, staff must follow the procedures applicable to the category of the client as set forth below.
b) Verify Authority of Personal Representative. For all categories of clients (except unemancipated minors), KBBH must obtain written documentation of a person's authority under Oregon law to act as the client's Personal Representative before allowing the person to act as the Personal Representative. Written documentation must be sent to the Compliance Manager, or their designee, for verification and approval.
c) Documentation. KBBH shall maintain in the client's medical record the written documentation of a person's authority to act as the Personal Representative. This information includes the Personal Representative's name, address, telephone number and relationship to the client.
d) Deceased Client. If, under applicable Oregon law, an executor, administrator, or other person has authority to act on behalf of a deceased client or on behalf of the client's estate, KBBH will treat such person as the Personal Representative with respect to PHI relevant to such Personal Representation. As discussed above, KBBH must obtain written documentation of a person's authority under Oregon law to act as the client's Personal Representative before allowing the person to act on the client's behalf.
e) Victim of Abuse, Neglect or Endangerment. KBBH may elect not to treat a person as the Personal Representative of a client if KBBH has a reasonable belief that:
    a. The client has been or may be subjected to domestic violence, abuse, or neglect by such person; OR
    b. Treating such a person as the Personal Representative could endanger the client.

Client's Right to Request PHI. Clients may request to receive a copy of their own confidential PHI by submitting a request in writing to the Compliance Manager. This request may be made at the time of admission, at a regular visit, during the course of the client's care, or at any time whilst KBBH maintains records for that client. The request must include:

- The manner in which the client wishes to receive confidential communications from KBBH.
- The information, or type of information, to be communicated in the confidential manner requested (this may be limited to a particular illness or treatment or to all exchanges of PHI).
- If applicable, the time period to which the request applies.
- If confidential handling of billing matters is also requested, the manner in which payment for treatment will be made.

KBBH reserves the right to withhold PHI if it is defined as psychotherapy notes or information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding. See 45 CFR 164.524(a)(1)(ii).

Clients may request a receipt of their PHI disclosures at any time by submitting a written request to the Compliance Manager. KBBH is responsible for providing the client with a receipt of PHI disclosures for the six-year period immediately prior to the date of the request within 60 days of the initial request. KBBH is not required to provide information regarding the disclosure of any PHI as protected by state or federal law.

Client's Right to Amend PHI. A client must make a request for an amendment in writing. All requests must be submitted on KBBH's Request for Amendment Form and provide a reason to support the requested amendment. All requests shall be directed to KBBH's Compliance Manager. If a client makes an oral request for amendment, the staff shall inform them that such requests must be made in writing and offer the client the correct form. Staff may also assist the client to complete the form if needed. KBBH may refuse an oral request for amendment on the basis that such request is oral and not written.

Timing of Response. KBBH shall act on a client's request no later than sixty (60) days after its receipt of the request. KBBH may extend the time for action one time and by no more than thirty (30) days provided that it provides the client with a written statement (within the sixty (60) day period) of the reasons for the delay and the date by which KBBH will complete its action on the request.

Determination Procedure. KBBH may accept or deny the requested amendment. Determinations of whether to accept or deny the request for the amendment will be made by the Privacy Officer following a review of the relevant record and Designated Record Set, consultation with the treating physician or other staff, evaluation of the client's request, and to the extent appropriate, other health professionals familiar with the client's course of treatment.

If the amendment is accepted, KBBH will inform the client in a timely manner, in writing that the amendment has been accepted and obtain the client's identification of, and agreement to have KBBH notify the relevant persons with which the amendment needs to be shared. If the amendment is denied, KBBH will provide the client who requested the amendment with a written denial within sixty (60) days after receipt of the request for amendment. The written denial will include the basis for the denial, statement of the client's right to submit a written statement disagreeing with the denial, and a description of how the client may submit a formal complaint to the Compliance Manager.

UNAUTHORIZED DISCLOSURE: SUBMISSION, REVIEW, AND RESOLUTION.

Information regarding any Unauthorized Disclosure by KBBH or any of its Business Associates discovered by any employee of KBBH shall be reported promptly to the Compliance Manager or designee.

The Compliance Manager, in response to any report of or information about an unauthorized disclosure by KBBH or any of its Business Associates, including self-disclosures made by Business Associates pursuant to the terms of each Business Associate's contract or other agreement with KBBH, shall develop and implement a plan as soon as reasonably practicable to mitigate any known or reasonably anticipated harmful effects from such disclosure (the "Mitigation Plan"). The Mitigation Plan shall be tailored to the circumstances of each case, but may include as appropriate, the following elements:

- Identifying the source(s) of the disclosure and taking appropriate corrective action.
- Contact the recipient of the information that was the subject of the Unauthorized Disclosure and request that such recipient either destroy or return the information.
- Instruct such recipient to make no further disclosures of such information.
- Notify the client whose PHI was the subject of the Unauthorized Disclosure.
- Review, and correct where appropriate, any policy or procedure of KBBH that directly caused or contributed to the Unauthorized Disclosure.

PRIVACY COMPLAINTS

All Privacy Complaints shall be forwarded to the Compliance Manager at 2210 N Eldorado Blvd., Klamath Falls, OR 97601, (541) 883-1030, Fax # (541) 884-2338, E-mail compliance@kbbh.org. Individuals may use the Complaint Form to initiate the complaint process. Other written formats and oral complaints will also be accepted.

Privacy Complaint Log. The Compliance Manager (or their designee) shall document the following with respect to each Privacy Complaint received:

- the date the Privacy Complaint was received.

- a copy of the written Privacy Complaint, if any, or a general description of the verbal Privacy Complaint.
- a copy of the written statement provided to the person making the Privacy Complaint.

Responsible Party to Investigate and Resolve Complaint. The Compliance Manager (or their designee) will investigate the complaint and document the outcome of the investigation. Based on the results of the investigation, and the need for staff training and/or procedural changes or other follow up he/she will present the results of the investigation to the Director of Continuous Improvement and additional relevant KBBH Leadership for follow up with staff. If the Compliance Manager's investigation is inconclusive or in any other way ambiguous, he/she will forward the complaint and investigation information to appropriate KBBH Leadership for review and feedback about how to proceed in addressing the complaint.

Time Frame for Resolution. Investigation. Within [5] working days after the Compliance Manager receives a Privacy Complaint, the Compliance Manager must complete their investigation of the complaint or request more info or time from the individual. Resolution. Within [30] calendar days after the Compliance Manager receives a Privacy Complaint, the Compliance Manager must provide a written response (for written complaints) or verbal response (for verbal complaints) to the complainant which includes the following information:

- a name of a contact person at KBBH who will answer questions relating to the investigation and resolution of the Privacy Complaint.
- a general description of the steps taken to investigate the Privacy Complaint.
- an explanation of KBBH's resolution regarding the Privacy Complaint.
- the date of completion of the investigation of the Privacy Complaint.

KBBH shall retain copies of the documentation for a period of six (6) years from the date that the response was made to the Privacy Complaint. The Compliance Manager (with assistance from an automated report managed by Business Intelligence) will provide a monthly report of Privacy complaints to Cascade Health Alliance (CHA) regarding CHA Member complaints.

PREVENTING HIPAA BREACHES

KBBH employees are personally responsible for understanding HIPAA laws. KBBH provides training on HIPAA at onboarding and an ongoing basis. Employees are responsible for making sure that they receive this training on an annual basis at minimum. This training may be provided live or through the Relias Learning Management System. The best way to prevent breaches is to be familiar with the Security Rule and the Privacy Rule. Always use the Minimum Necessary concept. Avoid giving in to curiosity and never access records that you are not authorized to view.

As per KBBH processes, employees who are also clients of KBBH should never access their own PHI through our EHR, instead they should request their records the same way that a typical client does.

SANCTIONS AGAINST EMPLOYEES WHO VIOLATE HIPAA

KBBH has a progressive discipline policy under which sanctions become more severe for repeated infractions. At the discretion of KBBH Leadership KBBH may terminate an employee for the first breach of the agency's security policy or other individual policies and standards if the seriousness of the offense warrants such action. An employee could expect to lose their job for willful or grossly negligent breach of confidentiality, willful or grossly negligent destruction of computer equipment and data or knowing or grossly negligent violation of HIPAA standards, its implementing regulations, or any other federal or state law protecting the integrity and confidentiality of client information.

For less serious breaches, KBBH Leadership may impose a lesser sanction, such as a verbal or written warning, loss of access, suspension without pay, demotion, or other sanction. In addition, KBBH will include such violations by contractors and interns as grounds for termination of the contract or internship and/or imposition of contract penalties.
Violation of the agency's HIPAA policy may constitute a criminal offense under HIPAA, other federal laws, such as the Federal Computer Fraud and Abuse Act of 1986, 18 U.S.C. ' 1030, or state laws. Any employee or contractor who violates such a criminal law may expect that KBBH will provide information concerning the violation to appropriate law enforcement personnel and will cooperate with any law enforcement investigation or prosecution.
Further, violations of HIPAA may constitute violations of professional ethics and may be grounds for professional discipline. Any individual subject to professional ethics guidelines and/or professional discipline should expect KBBH to report such violations to appropriate licensure/accreditation boards and to cooperate with any professional investigation or disciplinary proceedings.