



## SALISH BH-ASO POLICIES AND PROCEDURES

**Policy Name:** CONFIDENTIALITY, USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION **Policy Number:** PS902

**Effective Date:** 1/1/2020

**Revision Dates:**

**Reviewed Date:**

**Executive Board Approval Dates:** 5/22/2020

### PURPOSE

To establish standards for confidentiality, use, and disclosure of Protected Health Information (PHI).

### POLICY

The Salish Behavioral Health Administrative Services Organization (SBH-ASO) adheres to federal and state statutes, all requirements of the Health Insurance Portability and Accountability Act (HIPAA) confidentiality and use/disclosure of protected health information, and 42 CFR Part 2.

### PROCEDURE

#### Confidentiality

The SBH-ASO shall protect all personal information, records, and data from unauthorized disclosure in accordance with 42 CFR §431.300 through §431.307, RCW 70.02, 71.05, and 71.24, and for individuals receiving substance use disorder treatment services, in accordance with 42 CFR Part 2. The SBH-ASO shall have a process in place to ensure that all components of its provider network and system understand and comply with confidentiality requirements for publicly funded behavioral health services. This is also construed to include protected health information and records compiled, obtained, or maintained relating to complaint or grievance investigation as confidential and disclosed only as authorized or otherwise provided by law. Pursuant to 42 CFR §431.301 and §431.302, personal information concerning applicants and recipients may be disclosed for purposes directly connected with the administration of the HCA BH-ASO Contract. Such purposes include, but are not limited to:

- Establishing eligibility.

- Determining the amount of medical assistance.
- Providing services for recipients.
- Conducting or assisting in investigation, prosecution, or civil or criminal proceedings related to the administration of the State Medicaid Plan.
- Assuring compliance with Federal and State laws and regulations, and with terms and requirements of the Agreement.
- Improving quality.

SBH-ASO employees are responsible to use reasonable efforts to safeguard an individual's protected health information and maintain confidentiality of such information. Any document, record, or other written material containing individually identifiable health information is not left unattended and/or unsecured in the SBH-ASO office. All employees read and sign the SBH-ASO Confidentiality and Security Agreement.

If PHI must be transported to or from the SBH-ASO site, the following guidelines must be followed:

#### Transporting Paper PHI From/To Off-Site SBH-ASO site

1. Only transport the minimum amount of PHI necessary.
2. All PHI must be in a separate locked container and the container must be transported in the locked vehicle, preferably out of sight such as in the trunk.
3. Never leave PHI (including portable media devices) unattended, including in your vehicle.
4. Maintain a log of files or documents that are leaving the SBH-ASO site. When you arrive at the off-site clinic, immediately make sure all the files you listed on the log are in your possession. The log of files or documents must either remain with the locked PHI contents or must be listed without any identifiable PHI.

The SBH-ASO shall (and require its subcontractors and providers to do so) establish and implement procedures consistent with all confidentiality requirements of HIPAA (45 CFR §160 and §164) and 42 CFR Part 2 for medical records and any other health and enrollment information that identifies a particular individual.

In the event an individual's picture or personal story will be used, the SBH-ASO shall first obtain written consent from the individual.

The SBH-ASO shall prevent inappropriate access to confidential data and/or data systems used to hold confidential client information by taking, at a minimum, the following actions:

- Verify the identity or authenticate all of the system's human users before allowing them access to any confidential data or data system capabilities.
- Authorize all user access to client applications.
- Protect application data from unauthorized use when at rest.
- Keep any sensitive data or communications private from unauthorized individuals and programs.
- Notify [prism.admin@dshs.wa.gov](mailto:prism.admin@dshs.wa.gov) with a copy to [hcamcprograms@hca.wa.gov](mailto:hcamcprograms@hca.wa.gov) within five (5) business days whenever an authorized user with access rights leave employment or has a change of duties such that the user no longer requires access. If the removal of access is emergent, include that information

with the notification.

- In the event of a Breach of unsecured PHI or disclosure that compromises the privacy or security of PHI obtained from any state data system, the SBH-ASO shall comply with all requirements of the HIPAA Security and Privacy for Breach Notification and as otherwise required by state or federal law and applicable contract.
- The SBH-ASO takes steps to ensure a valid mailing address with all postal mail. Even so, the post office sometimes returns mail marked “undeliverable”, or unclaimed. This returned mail needs to be handled carefully. Reasonable efforts will be used to review and ensure the accuracy of the original address. If an error is found, or an updated address has been provided, the item will be re-sent as soon as possible using the corrected address. If there is no correction or updated address information is not available, the returned mail item will be submitted for record retention processing.

### **Restricted Uses and Disclosures as mandated by 42 CFR Part 2**

SBH-ASO recognizes the purpose and effect of 42 CFR Part 2 to ensure that a patient is not more vulnerable by reason of the availability of the record that the patient receives treatment for substance use disorder. Any treatment information, whether or not recorded, and any information which references the patient as having a substance use disorder cannot be disclosed unless expressly authorized by 42 CFR Part 2.

Consultation with SBH-ASO Privacy Officer is strongly encouraged.

### **42 CFR Part 2 Information/Substance Use Disorder Information**

Federal regulations governing the confidentiality of Part 2 Information generally are more restrictive than HIPAA and should be followed when any Part 2 Information is requested for use or disclosure. A fundamental concept of protecting Part 2 Information is not identifying the Individual as having a diagnosis or having received Treatment concerning substance use disorder (SUD). Part 2 applies to Part 2 Programs. SBH-ASO is not a Part 2 Program.

Individuals routinely authorize Part 2 Programs to disclose Part 2 Information to SBH-ASO for Payment, Health Care Operations and other purposes. As a result, SBH-ASO is a lawful holder of Part 2 Information, subject to various Part 2 requirements.

Therefore, SBH-ASO will comply with Part 2, as applicable. Workforce members must obtain a specific authorization for each disclosure of Part 2 Information concerning an Individual, EXCEPT:

**Internal Program Communication.** Workforce members may disclose Part 2 Information to other Workforce members or to an entity having direct administrative control over SBH-ASO, if the recipient needs the information in connection with the provision of substance abuse disorder diagnosis, Treatment, or referral for Treatment.

**Medical Emergencies.** Workforce members may disclose Part 2 Information to medical personnel who have a need for the Part 2 Information about an Individual for the purpose of treating a condition that poses an immediate threat to the health of any

person and requires immediate medical intervention. Workforce members may disclose Part 2 Information only to medical personnel and must limit the amount of Part 2 Information to that which is necessary to treat the emergency medical condition. Immediately following the disclosure, Workforce members must document the following in the Individual's records:

- The name and affiliation of the medical personnel to whom disclosure was made;
- The name of the individual making the disclosure;
- The date and time of the disclosure; and
- The nature of the emergency

**Court Order.** Before a court may issue an order authorizing disclosure of Part 2 Information, SBH-ASO and any Individual whose records are sought must be given notice of the request for the court order and an opportunity to make an oral or written statement to the court. Before issuing the order, the court must also find there is "good cause" for the disclosure. Court-ordered disclosures must be limited to the Part 2 Information essential to fulfill the purpose of the order and they must be restricted to those persons who need the Part 2 Information. Typically, court orders will state they are "protective orders," "qualified protective orders," or "orders under seal." Workforce shall obtain the advance approval of the Privacy Officer before disclosing Part 2 Information for these purposes. If the order is sought by an authorized Law Enforcement Official or prosecuting attorney, the following criteria must be met:

- The crime involved must be serious, such as one which causes or directly threatens loss of life or serious bodily injury including homicide, rape, kidnapping, armed robbery, assault with a deadly weapon, and child abuse and neglect.
- There is a reasonable likelihood that the records will disclose information of substantial value in the investigation or prosecution.
- Other ways of obtaining the information are not available or would not be effective.
- The potential injury to the patient, to the physician-patient relationship and to the ability of the part 2 program to provide services to other patients is outweighed by the public interest and the need for the disclosure.
- When law enforcement personnel seek the order, the Part 2 Program has had an opportunity to be represented by counsel.

**Subpoenas.** Workforce members are prohibited from disclosing PHI about Individuals in response to subpoenas unless:

- The Individual has signed a valid authorization for the disclosure of the PHI, specifically including Part 2 Information; or
- A court has ordered SBH-ASO to disclose or release the PHI after giving the Individual and SBH-ASO an opportunity to be heard and after making a "good cause" determination. Workforce shall obtain the advance approval of the Privacy Officer before disclosing Part 2 Information for these purposes.

**Crime on Premises.** Workforce members may disclose limited information to Law Enforcement Officials when a crime has been committed on the premises of a Part 2 Program or against Part 2 Program personnel. These disclosures must be directly related to crimes and threats to commit crimes on SBH-ASO premises or against SBH-ASO Workforce and must be limited to the circumstances of the incident and the Individual's status, name, address and last known whereabouts. Workforce shall obtain the advance approval of the Privacy Officer before disclosing Part 2 Information for these purposes.

**Research Purposes.** Under this exception, Workforce may disclose Part 2 Information to researchers the Privacy Officer determines are qualified. A qualified researcher must have adequate training and experience in the area of research to be conducted and must have a protocol that ensures Part 2 Information will be securely stored and not re-disclosed in violation of law. Workforce shall obtain the advance approval of the Privacy Officer before disclosing Part 2 Information for these purposes.

**Audits.** Workforce shall obtain the advance approval of the Privacy Officer before disclosing Part 2 Information for audit purposes and will follow protocol set out by the Privacy Officer with respect to the audit.

As long as Part 2 Information is **not** downloaded, copied, or removed from the premises or forwarded electronically to another electronic system or device, Workforce members and Part 2 Programs may disclose Part 2 Information in the course of record review on the premises to a government agency that funds or regulates a Part 2 Program, or other lawful holder, or a third-party payor, or a quality improvement organization (or its designated contractors) that request access to the records of a Part 2 Program or lawful holder.

Part 2 Information may be copied or removed from the premises or downloaded or forwarded electronically to another electronic system or device in the course of record review on the premises to a government agency that funds or regulates a Part 2 Program, or other lawful holder, or a third-party payor, or a quality improvement organization (or its designated contractors) that request access to the records of a Part 2 Program or lawful holder only if the auditor agrees in writing to:

- maintain and destroy the Part 2 Information in a manner consistent with Part 2;
- retain Part 2 Information in compliance with applicable federal, state, and local record retention laws;
- and comply with the Part 2 restrictions on use and disclosure of Part 2 Information.

Part 2 Information may be disclosed to a person or entity for the purpose of conducting a Medicare, Medicaid, or CHIP audit or evaluation.

**Abuse and Threats to Health and Safety.** Workforce members may and are encouraged to, disclose Part 2 Information when the Part 2 Program is reporting under State Law incidents of suspected child abuse and neglect to appropriate authorities. In this case, SBH-ASO may make only an initial report; SBH-ASO may not respond to follow-up requests for information or to subpoenas, unless the Individual has signed an Authorization, or a court has issued an order that complies with the Part 2 Rule. Additionally, SBH-ASO may report Part 2 Information to relevant authorities the abuse

of Vulnerable Adults on an anonymous basis if it determines it is important to report elder abuse, disabled person abuse, or a threat to someone's health or safety. Health Care Providers are mandatory reporters.

**Review of Part 2 Disclosures.** Any PHI disclosed without the consent and/or authorization of an Individual in a Part 2 Program may be made only in consultation with the Privacy Officer. If SBH-ASO receives a request for disclosure of an Individual's record that is not permitted under Part 2, SBH-ASO will refuse to make the disclosure and will make the refusal in a way that does not reveal or identify the Individual has ever been diagnosed or treated for SUD.

### Use and Disclosure: Valid Authorization Required

The fact of admission and all information and records compiled, obtained, or maintained in the course of providing behavioral health services by public or private agencies shall be confidential except as otherwise required or permitted by federal or state statute and regulations.

#### 1. Valid Authorization

Protected health information will be disclosed to other individuals designated in a valid authorization. To be valid, the authorization must include, but not limited to, the following elements:

- a. The name of the Individual
- b. The specific name(s) or general designations of the part 2 program(s), entity(ies), or individual(s) permitted to make the disclosure.
- c. The name(s) of the individual(s) to whom a disclosure is to be made; or
  - a. If the recipient entity has a treating provider relationship with the individual whose information is being disclosed, such as a hospital, a health care clinic, or a private practice, the name of that entity; or
  - b. If the recipient entity does not have a treating provider relationship with the individual whose information is being disclosed and is a third-party payer, the name of the entity;
- d. The purpose of the disclosure. In accordance with §2.13(a), the disclosure must be limited to that information which is necessary to carry out the stated purpose.
- e. A statement that the consent is subject to revocation at any time except to the extent that the part 2 program or other lawful holder of patient identifying information that is permitted to make the disclosure has already acted in reliance on it. Acting in reliance includes the provision of treatment services in reliance on a valid consent to disclose information to a third-party payer.
- f. The date, event, or condition upon which the consent will expire if not revoked before. This date, event, or condition must ensure that the consent will last no longer than reasonably necessary to serve the purpose for which it is provided.
- g. The signature of the patient and, when required for a patient who is a minor, the signature of an individual authorized to give consent under 42

CFR §2.14; or when required for a patient who is incompetent or deceased, the signature of an individual authorized to sign under 42 CFR §2.15. Electronic signatures are permitted to the extent that they are not prohibited by any applicable law.

- h. The date on which the consent was signed.
- i. In addition to the Core Elements listed above, the authorization must contain statements adequate to place the individual on notice of all of the following:
  - a. The ability or inability to condition treatment, payment, enrollment, or eligibility for benefits on the authorization.
  - b. The potential for information disclosed pursuant to the authorization to be subject to redisclosure

### Disclosures Not Requiring Authorization

#### 1. Required disclosures

SBH-ASO is required to disclose protected health information:

- a. To the Individual upon that Individuals request when requested.
- b. When required by the Secretary of the U.S. Department of Human and Health Services to investigate or determine the agency's compliance with federal law.

#### 2. **HIPAA Permitted Uses and Disclosures**

SBH-ASO is permitted to use or disclose protected health information, except 42 CFR Part 2 information for:

- a. Treatment, payment, and health care operations (TPO, see Policy PS901 for more information) of SBH-ASO as described:
  - *Treatment* activities may include, but not limited to, the provision, coordination, or management of mental health care and related services by one or more mental health care providers, including coordination or management activities with a third party; consultation between mental health providers; or referral of an Individual to another provider.
  - *Payment* activities may include, but not limited to, those undertaken by SBH-ASO to obtain premiums, or to determine or fulfill its responsibility for coverage and provisions of benefits or to obtain or provide reimbursement for the provision of care.
  - *Health Care Operations* may include, but not limited to, conducting quality assessment and improvement activities, reviewing competence of or qualifications of behavioral health professionals, evaluating provider and program performance, conducting or arranging for auditing functions, including fraud and abuse detection and compliance programs; business planning and development; business management and general administrative activities including,

but not limited to, customer service; and resolution of internal grievances.

- b. *Required by Law.* SBH-ASO may use and disclose Protected Health Information without individual authorization *as required by law* (including by statute, regulation, or court orders).
- c. *Public Health Activities.* SBH-ASO may disclose PHI to:
  - i. Public health authorities authorized by law to collect or receive such information for preventing or controlling disease, injury, or disability and to public health or other government authorities authorized to receive reports of child abuse and neglect;
  - ii. Entities subject to FDA regulation regarding FDA regulated products or activities;
  - iii. Individuals who may have contracted or been exposed to communicable disease when notification is authorized by law; and
  - iv. employers, regarding employees, when requested by employers, for information concerning a work-related illness or injury or workplace related medical surveillance, because such information is needed by the employer to comply with the Occupational Safety and Health Administration (OSHA), the Mine Safety and Health Administration (MSHA), or similar state law.
- d. *Victims of Abuse, Neglect or Domestic Violence.* Protected health information (PHI) may be disclosed about a mental health Individual that SBH-ASO staff or contracted providers reasonably believe to be a victim of abuse, neglect, or domestic violence to the appropriate government authority. Protected health information may be disclosed about a substance use disorder Individual that SBH-ASO staff or contracted providers reasonably believe to be a victim of child abuse or neglect.
- e. *Health Oversight Activities.* PHI, except 42 CFR Part 2 information, may be disclosed for purposes of health oversight activities such as audits, investigations, inspections, and licensure.
- f. *Judicial and Administrative Proceedings.* PHI may be disclosed to the courts as required for the administration of RCW 71.05, or pursuant to a valid authorization or court order authorizing the disclosure of information.
- g. *Law Enforcement Purposes.* SBH-ASO may disclose PHI to law enforcement officials for law enforcement purposes under the following six circumstances, and subject to specified conditions:
  - 1. As required by law;
    - a. To identify or locate a suspect, fugitive, material witness, or missing person;
    - b. In response to law enforcement official's request for



- c. information about a victim or suspected victim of a crime;
  - d. To alert law enforcement of a person's death, if the SBH-ASO suspects that criminal activity caused the death
  - e. When the SBH-ASO believes that PHI is evidence of a crime that occurred on its premises; and
  - f. By a covered health care provider in a medical emergency not occurring on its premises when necessary to inform law enforcement about the commission and nature of a crime, the location of the crime or crime victims, and the perpetrator of the crime.
- h. *Research*: PHI may be disclosed to an individual, organization or agency as necessary for management or financial audits, or program monitoring and evaluation.
- i. *Serious Threat to Health or Safety*. SBH-ASO may disclose PHI that is believed necessary to prevent or lessen a serious and imminent threat to a person or the public, when such disclosure is made to someone they believe can prevent or lessen the threat.
- j. *Essential Government Functions*. An authorization is not required to use or disclose PHI for certain essential government functions. Such functions include: assuring proper execution of a military mission, conducting intelligence and national security activities that are authorized by law, providing protective services to the President, making medical suitability determinations for U.S. State Department employees, protecting the health and safety of inmates or employees in a correctional institution, and determining eligibility for or conducting enrollment in certain government benefit programs.
- k. *Workers' Compensation*. PHI may be disclosed as authorized by, and to comply with, workers' compensation laws and other similar programs providing benefits for work-related injuries or illnesses.

### Minimum Necessary

Uses and disclosures of protected health information are to consist of only the minimum necessary information required to fulfill the request and/or purpose of the use or disclosure.

1. "Minimum Necessary" applies:

When using or disclosing protected health information, or, when requesting protected health information from another covered entity, SBH-ASO must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

2. "Minimum Necessary" *does not* apply to:

- a. Disclosures to or requests by a health care provider for treatment.

- b. Uses or disclosures made to the individual.
- c. Disclosures pursuant to a properly formatted authorization for release of information.
- d. Uses or disclosures required for compliance with HIPAA Administrative Simplification Rules
- e. Disclosures made to the Secretary of Department of Health and Human Services is required under the Privacy Rule for enforcement purposes.
- f. Uses or disclosures that are required by other law

### Other Uses and Disclosures

Additionally, SBH-ASO may use and disclose protected health information for the following purposes and as allowed:

1. De-Identified Protected Health Information

SBH-ASO may use protected health information to create information that is not individually identifiable health information (see Policy PS901 for more information) or disclose protected health information only to a business associate for such purpose, whether or not the de-identified information is to be used by SBH-ASO. Health information that meets the standard and implementation specifications for de-identification under this policy is considered not to be individually identifiable health information, i.e., de-identified.

2. Business Associates

(a) For information related to mental health services: The SBH-ASO may disclose protected health information to a business associate and may allow a business associate to create or receive protected health information on its behalf, if SBH-ASO obtains satisfactory assurance that the business associate will appropriately safeguard the information. SBH-ASO must document, through a written contract or other written agreement or arrangement, the satisfactory assurances that a business associate meets the standards of this policy with respect to protection of identifiable health information. This standard does not apply with respect to disclosures by SBH-ASO to a health care provider concerning the treatment of the individual.

**Expanded Part 2 Content Requirements.** When a Business Associate, which is providing Payment or Health Care Operations services SBH-ASO, will create, receive, maintain, or transmit Part 2 Information, the BAA also must provide the Business Associate:

- (a) Is fully bound by the provisions of Part 2 upon receipt of Part 2 Information; and
- (b) Receives from SBH-ASO one (1) of the two (2) following notices:

(1) This information has been disclosed to you from records protected by federal confidentiality rules (42 CFR part 2). The federal rules prohibit you from making any further disclosure of information in this record that identifies a patient as having or having had a substance use disorder (SUD) either directly, by reference to publicly available information or through verification of such identification by another person unless further disclosure is expressly permitted by the written consent of the individual whose information is being disclosed or as otherwise permitted by 42 CFR Part 2. A general authorization for the release of medical or other information is NOT sufficient for this purpose (see § 2.31). The federal rules restrict any use of the information to investigate or prosecute with regard to a crime any patient with SUD, except as provided at §§ 2.12(c)(5) and 2.65;

or

(2) 42 CFR Part 2 prohibits unauthorized disclosure of these records.

(c) Implements appropriate safeguards to prevent unauthorized uses and disclosures of Part 2 Information;

(d) Report any unauthorized uses, disclosures, or breaches of Part 2 Information to SBH-ASO; and

(e) Not re-disclose Part 2 Information to a third-party unless the third-party is a contract agent of the Business Associate helping the Business Associate provide services described in the services agreement and only if the agent only further discloses the Part 2 Information back to the Business Associate or to SBH-ASO.

(f) For information related to SUD services: The SBH-ASO must not disclose any identifying information about patients unless appropriate release of information is complete or exception is specified within 42 CFR Part 2.

### 3. Deceased Individuals

SBH-ASO must comply with the requirements of this policy, HIPAA, and 42 CFR Part 2 with respect to the protected health information of a deceased individual. If under applicable law, an executor, administrator, or other person has authority to act on behalf of a deceased individual or of the individual's estate, SBH-ASO must treat such person as a personal representative under this policy, with respect to protected health information relevant to such personal representation.

### 4. Personal Representatives

As represented under HIPAA and 42 CFR Part 2, the SBH-ASO must treat a personal representative as the individual for purposes of this policy.

- a. Adults and Emancipated Minors: If under applicable law, a person has authority to act on behalf of an individual who is an adult or an emancipated minor in making decisions related to health care, SBH-ASO must treat such person as a personal representative under this policy, with respect to protected health information relevant to such personal representation.

- b. Unemancipated Minors: If under applicable law a parent, guardian, or other person acting *in loco parentis* has authority to act on behalf of an individual who is an unemancipated minor in making decisions related to health care, SBH-ASO must treat such person as a personal representative under this policy, with respect to protected health information relevant to such personal representation, except that such person may not be a personal representative of an unemancipated minor, and the minor has the authority to act as an individual, with respect to protected health information pertaining to a health care service, if:
- The minor consents to such health care service; no other consent to such health care service is required by law, regardless of whether the consent of another person has also been obtained; and the minor has not requested that such person be treated as the personal representative;
  - The minor may lawfully obtain such health care service without the consent of a parent, guardian, or other person acting *in loco parentis*, and the minor, a court, or another person authorized by law consents to such health care service; or
  - A parent, guardian, or other person acting *in loco parentis* assents to an agreement of confidentiality between a covered health care provider and the minor with respect to such health care service.
- c. Abuse, Neglect, Endangerment Situations: Notwithstanding a state or federal law or any requirement of this paragraph to the contrary, SBH-ASO may elect not to treat a person as the personal representative of an Individual if SBH-ASO has reasonable belief that:
- The Individual has been or may be subjected to domestic violence, abuse, or neglect by such person; or
  - Treating such person as the personal representative could endanger the individual and, SBH-ASO, in the exercise of professional judgment, decides that it is not in the best interest of the Individual to treat the person as the Individual's personal representative.
5. Consistent with Privacy Notice
- SBH-ASO is required by HIPAA regulation to have a notice in public view and available to Individuals that it may not use or disclose protected health information in a manner inconsistent with established regulation and policy.
6. HIPAA Disclosures by Whistleblowers and Workforce Member Crime Victims
- a. Disclosures by Whistleblowers: SBH-ASO is not considered to have violated the requirements of this policy if a member of its workforce or a business associate discloses protected health information, provided that:
- The workforce member or business associate believes in good faith that SBH-ASO has engaged in conduct that is unlawful or otherwise

violates professional or clinical standards, or that the care, services, or conditions provided by the covered entity potentially endangers one or more Individuals, workers, or the public; and the disclosure is to:

- A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of SBH-ASO or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the covered entity; or
  - An attorney retained by or on behalf of the workforce member or business associate for the purpose of determining the legal options of the workforce member or business associate with regard to the conduct described above.
- b. Disclosures by Workforce Members Who Are Victims of a Crime: SBH-ASO is not considered to have violated the requirements of this policy if a member of its workforce who is the victim of a criminal act discloses protected health information to a law enforcement official, provided that:
- The protected health information disclosed is about the suspected perpetrator of the criminal act; and
  - The protected health information disclosed is limited to the information listed in this policy as minimum necessary information.

#### Authority to Disclose Information

When questions arise concerning the authority to disclose information or the type of information to be disclosed, staff shall first consult with and obtain approval of the SBH-ASO Privacy Officer before releasing information.

#### Authentication of Requester

Prior to disclosure of any protected health information, even with authorization, authenticity of the requester must be established by means reasonably certain of verifying the authenticity of the requestor.

When presented with a valid authorization, check a document to verify the signature is similar to the Individual's signature. The requester will be required to present picture identification to ensure information is given to the person intended.

#### Accounting of Disclosures

When any disclosure of information or records is made, an entry must be promptly entered into the record to include the date and circumstances under which the disclosure was made, the names and relationships to the individual or agency receiving the information, the information disclosed, identification, and signature of the staff disclosing the information.