

100-20**POLICY:**

All BIH Programs will establish and adhere to procedures to ensure and maintain the confidentiality of client exchange, records and electronic submissions.

- All BIH staff must accept and adhere to HIPAA (American Health Insurance Portability and Accountability Act of 1996) in order to ensure that all records and participant accounts meet nationally recognized standards in regards to documentation, handling and privacy.
- The HIPAA establishes standards for Personal Health Information (PHI) from disclosure and informs participants of how their information will be used.¹
- Requests for non-public BIH program information must be reviewed by MCAH, which is responsible for the BIH Program's overall evaluation and oversight.

PROGRAM STANDARD:

All BIH participants will have a signed Rights and Responsibilities and Release of Information/Consent form signed upon enrollment into the BIH Program and before personal and demographic information is obtained.

PROCEDURE:

1. Upon enrollment, all participants sign requisite Rights and Responsibilities and Release of Information/Consent forms.
2. All BIH Program staff will have knowledge regarding HIPAA confidentiality standards and will protect participant records and take proper precautions to maintain confidentiality of information.
3. All BIH Program staff must have on file a Confidentiality Agreement signed by each staff member who has the ability to view data, either by collecting the data or by viewing it after it has been recorded. The individual Confidentiality Agreements must be renewed annually.
4. All BIH Programs will establish and adhere to procedures to ensure and maintain the confidentiality of participant exchange, records and electronic submissions.

¹ BIH does not furnish, bill, or receive payment for health care and is therefore, according to standards established by the HIPAA Final Rule adopted in January 2013, not a HIPAA-covered program. Although BIH is not a HIPAA-covered program, these policies set minimum standards are designed to meet or exceed standards established by the U.S. Department of Health & Human Services for the maintenance and release of protected health information.

5. Participant information, written transactions and records, including copies, must be kept in a secure location that is inaccessible to unauthorized persons. Participant records include BIH data collection forms, consent and release of information forms, assessments, progress notes and other contacts with participants to be determined by the local agency. Appropriate safeguards include, but are not limited to:
 - a. Securing and maintaining all hard copy or other records containing PHI (such as CD-ROM, thumb-drives, diskettes, etc.) in a locked cabinet inaccessible to staff other than those directly involved with either the delivery of service to the participant, supervision of these direct-service delivery staff, or for data entry; and
 - b. Securing all electronic records in password protected encrypted files, with access only for staff directly involved in delivery of services to participants, supervision of these staff or data entry.

6. Each agency will establish a policy and maintain a system for the safe storage and retrieval of all participant records, as well as emergency and disaster procedures. Participants' records and copies must be kept in a secure location that is inaccessible to unauthorized persons. Original records are not removed from the program site unless the agency exceeds the storage limitations set by the agency. In this case, overflow closed cases may be stored in a secure offsite location.

7. Agency Incident Reports
 - a. The BIH Coordinator must notify the CDPH/MCAH Program Consultant and Contract Manager, by telephone and in writing, within 24 hours of any incident or occurrence that impairs or compromises the agency's ability to deliver services to participants. Notification should include the nature of the incident and a proposed plan for the continuation of services. Incidents or occurrences may include but not be limited to the following: (1) damage to the program site caused by fire, water, wind, earthquake or other destruction, and (2) legal action against the agency. Written documentation will be submitted to CDPH.MCAH-BIH via the transmittal process.

8. All BIH Programs must retain participant records for at least three years for purposes of potential audits and/or to reconcile with data from ETO.

9. All BIH Programs must have policies in place to ensure that confidential information's discarded through secure and confidential means (e.g. shredded, locked confidential destruction bins, pulverized).

- 10.** All BIH Programs must have a mechanism in place to ensure that removable media containing confidential, personal, or sensitive information is physically destroyed when no longer in use.
- 11.** Sending Confidential Information:
 - a. Prior to sending PHI or participant-related confidential information to MCAH-BIH, program staff must notify a member of the MCAH-BIH team;
 - b. When sending electronic PHI to MCAH-BIH, encrypt information by writing “[secure]” in the subject line of the email correspondence.
 - c. All BIH Program staff must add a confidentiality statement at the beginning or end of every fax or email that contains confidential, personal or sensitive information notifying persons receiving the fax or email in error to contact the sender and destroy the document.
- 12.** During the closure of an office or move, the LHJ must ensure that privacy and security of confidential, personal and sensitive information is maintained. If documents containing PHI must be transported to remote locations, these documents must be transported using a secure, bonded courier with a tracking system.
- 13.** Participant confidentiality and security of records are integral to BIH program integrity and success.
- 14.** Whenever possible, participants’ meetings with case managers should be conducted at the BIH office to ensure privacy and confidentiality for the participant.