BERRIEN MENTAL HEALTH AUTHORITY
PROCEDURE

| | |
|---|---|
| SUBJECT: Social Security Number Collection & Privacy Policy | SECTION: 07-50-06<br>Page 1 of 2 |
| EFFECTIVE DATE: March 2016<br><br>REVISED: 4/17, 3/18, 3/19, 2/2021, 5/2021, 2/2026 | REQUIRED BY:<br>SSN Privacy Act, MCL 454.81 et seq |

**PURPOSE:** To set forth a policy/procedure to protect the privacy and security when collecting and maintaining the social security numbers of Berrien Mental Health Authority's (BMHA) employees and contractual providers who receive payment with Federal funding, and to comply with the Social Security Number Privacy Act set forth in MCL 454.81 et seq.

**POLICY:** It is the policy of BMHA to follow all Federal and State requirements concerning the collection of sensitive information from employees and contractual providers in compliance with 42 CFR 445, disclosure of screen person information and MCL 454.81 Social Security Number Privacy Act. Numbers will be obtained, retained, and used only for legitimate business purposes within the Internal MCO Department. BMHA will cooperate with Southwest Michigan Behavioral Health (SWMBH) in collecting the numbers and maintaining their privacy only for the purpose of screening them through the Office of Inspector General System for Award Management and the Michigan Sanctioned Provider List. Further, BMHA will cooperate with all law enforcement or administrative agencies in the apprehension and prosecution of any individual who obtains, uses, or discloses Social Security numbers for unlawful reasons.

**STANDARDS and GUIDELINES:**

A. 42 CFR 445.104 requires the collection of social security numbers for individuals with an ownership, control or management function within an agency doing business with BMHA.

B. Collection will take place yearly in conjunction with the contract cycle and when changes within the Provider's business management/ownership structure takes place.

C. The Internal MCO Department will implement the following security measures to limit the access of social security numbers to only those who require access for work-related purposes:
    1. Social security numbers are stored at BMHA on an encrypted storage server which is a FEMA 361 structure that is tornado and vandalism secure. Security compliance adheres to AICPA SSAE 16 audited type 1 and 2 coverage with the HIPAA compliant standard granted to the site where the data is housed.
    2. The Director of Provider Network and the MCO Team Supervisor have been given the responsibility of obtaining all required social security numbers, storing them and arranging for them to be delivered to SWMBH. Both are prohibited from disclosing Social Security numbers to other employees within BMHA and SWMBH who do not have a work role related or need to know this information.
    3. Internal MCO Department will scan disclosure documents mailed directly to the Director of Provider Network or to the MCO Team Supervisor. Whether the document comes via email or mail, the document will be immediately saved to the dedicated secure drive and double

deleted from email. This process will be done immediately upon receipt. All paper documentation, once scanned, will be destroyed in a crosscut shredder which will render the information unreadable and unusable to unauthorized users. Transfer of information to SWMBH will take place in either of the following ways:

a) An encrypted thumb drive will be used to copy social security information for transfer to SWMBH
    1. The CEO, member of the executive team or the MCO Team Supervisor may transport the encrypted thumb drive to SWMBH's Compliance Specialist who is in charge of maintaining the official list of OIG and SAM information including social security numbers.
    2. The MCO Team Supervisor will provide SWMBH's Compliance Specialist with the password via encrypted email. The thumb drive and password will never be transported together or
b) An electronic transfer will be made through a secure file transfer portal directly to SWMBH. SWMBH Compliance will be notified prior to transfer when it will be completed, and it will be saved it a folder clearly marked for SWMBH Compliance.

4. Upon return to BMHA, the information on the thumb drive will be deleted and a new password will be created by the Information Systems Department.

D. Any BMHA staff who violates this policy will be subject to discipline consistent with the discipline standards set forth in any related compliance policy, up to and including termination. Staff may also be subject to any and all criminal and civil penalties associated with the misuse of this information.

**DEFINITIONS:** None

**FORMS:** None

**Reviewer:** Director of Provider Network
**Reviewed:** 2/17, 4/17, 3/18, 3/19, 6/2020, 2/2021, 5/2021, 2/2022, 2/2023, 2/2024, 6/2025, 2/2026