**PATHWAYS CMH**

| | | |
|---|---|---|
| **POLICY TITLE:**<br>Social Security Number Privacy | **CATEGORY:**<br>Compliance | |
| **EFFECTIVE DATE:**<br>05/04/17 | **BOARD APPROVAL DATE:**<br>05/03/17 | |
| **REVIEWED DATE:**<br>NEW POLICY | **REVISION(S) TO POLICY STATEMENT:**<br>☒ **Yes** ☐ **No** | **OTHER REVISION(S):**<br>☒ **Yes** ☐ **No** |
| **RESPONSIBLE PARTY:**<br>Compliance Manager | **CEO APPROVAL:**<br>Mary Swift, CEO | |

**APPLIES TO:**
Pathways Personnel
Contract Providers

**POLICY:**
Pathways personnel will comply with the Social Security Number Privacy Act, MCL 454 of 2004 (Act). Social Security numbers collected in the normal course of business shall be used as allowed by the Act or by state or federal statute, rule regulation, by court order, or pursuant to legal discovery or process.

**PURPOSE:**
To ensure all Pathways personnel maintain the confidentiality, prohibit unlawful disclosure, limit access to, and to the extent practical dispose of documents appropriately that contain a Social Security number.

**DEFINITIONS:**
***Mailed*** means delivered by the United States mail or other delivery service that does not require the signature of recipient indicating actual receipt.

***Pathways Personnel*** means personnel assigned to Pathways on a full or part-time basis, students, volunteers, interns, and Board Members.

***Public Display*** means to exhibit, hold up, post, or make visible or set out for open view, including, but not limited to, open view on a computer device, computer network, website, or other electronic medium or device, to members of the public, or in a public manner.

**REFERENCES:**
MCL 454 of 2004, Social Security Number Privacy Act

**HISTORY:**
REVISION DATE: NEW POLICY
REVIEW DATE: 04/07/17
CEO APPROVAL DATE: 04/12/17
BOARD APPROVAL DATE: 05/03/17

**PROCEDURES:**

1. Except as authorized or required by state or federal statute, rule, or regulation, by court order or rule, or pursuant to legal discovery or process a person shall not intentionally do any of the following with Social Security number or any personnel, contractor, student, consumer, or individual:

   **A. PUBLIC DISPLAY:** Publically display all or more than four (4) sequential digits of the Social Security number; including visibly print all or more than four (4) sequential digits of the Social Security number on any identification badge, time card, pay voucher/timesheet, or any other materials that may be accessed by the public.

   **B. ACCOUNT NUMBERS:** Use all or more than four (4) sequential digits of the Social Security number as the primary account number for an individual.

   **C. COMPUTER TRANSMISSION:** Require an individual to transmit more than four (4) sequential digits of the Social Security number to use/gain access to the internet/intranet, computer system, or network unless the connection is secure, or password protected or the transmission is encrypted.

   **D. MAILED DOCUMENTS:** Send an individual an envelope or package if the Social Security number is visible on the envelope or package or, without manipulation, can be seen from outside the envelope or packaging. A mailing shall not include all or more than four (4) sequential digits of the Social Security numbers in/on any document or information mailed or otherwise sent to an individual, unless, state or federal law, rule, regulation, or court order/rule authorizes, permits, or requires that a Social Security number appears in the document. Exceptions may include where:

      1. The document is sent as part of an application, enrollment process, or is requested by the individual, parent or legal guardian.

      2. The document is sent to establish, confirm the status of, service, amend, or terminate an account, contract, policy, or employee or health insurance benefit or to confirm with the accuracy of a Social Security number of an individual who has an account, contract, policy, or employee or health insurance benefit. Additional exceptions may include where Pathways seeks to:

         a. Verify the identity of an individual or to perform similar administrative purposes related to a transaction, or employment.

         b. Investigate an individual's claim, credit, criminal or driving record.

         c. Detect, prevent, and deter identify theft.

         d. Enforce a person's legal rights, including debt collection.

         e. Investigate, collect, or enforce a child or spousal support obligation or tax liability.

         f. Administer a health insurance, retirement benefit, or investment program.

   E. **FREEDOM OF INFORMATION ACT:** Documents subject to the Freedom of Information Act (FOIA) request containing Social Security numbers will have the Social Security number redacted or removed/struck/covered from view. The information shall then be mailed in compliance with the FOIA. Social Security numbers are exempt from FOIA

disclosure unless it meets one of the stated exceptions indicated here or within the Social Security Number Privacy Act.

F. **STORAGE/DOCUMENT DESCRUCTION:** All documents containing Social Security numbers shall be stored in a physically secure manner. Personnel using records containing Social Security numbers must take appropriate steps to secure such records when not in immediate use. Social Security numbers shall not be visible on electronic devices that are not secure/password protected and/or encrypted. Documents containing Social Security numbers will be retained in accordance with the requirements of state and federal laws. At such time as documents containing Social Security numbers may be disposed of, that disposal shall be accomplished in a manner that protects the confidentially of the number, such as shredding, demagnetization, and/or eraser of electronic storage.

G. **UNAUTHORIZED USE OR DISCLOSURE OF SOCIAL SECURITY NUMBERS:** Access to Social Security numbers is limited to only those persons who have a need to know the information as indicated within the main body of this policy. Any personnel who knowingly obtain/use or disclose Social Security numbers for unlawful purposes or contrary to the requirements described above shall be subject to the HIPAA Offense and Sanctioning Guidelines for all personnel (up to and including discharge). Additionally, certain violations of the Act carry criminal and/or civil sanctions and will involve law enforcement where indicated. Documentation of violations shall be maintained by the Privacy Officer, Security Officer, and/or Human Resources Department, where indicated.