HABILITATION ASSISTANCE CORPORATION	Policy number: 064.1 Policy Title: Written Information Security Plan Category: General Information
Date Issued: 12/87 Date modified: 01/01/26	
Policy Description:	To provide a policy regarding the agency's comprehensive written information security program ("WISP")
Policy Scope:	All Employees.
Policy Guidelines:	**I. OBJECTIVE:** Habilitation Assistance Corporation's objective in developing and implementing this comprehensive written information security program ("WISP") is to create effective administrative, technical and physical safeguards for the protection of personal information of our members, customers and our employees, as well as to comply with our obligations under 201 CMR 17.00 (the "regulations"). The WISP sets forth our procedure for evaluating and addressing our electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting personal information. For purposes of this WISP, "personal information" is defined in the regulations as the following: *A Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.* **II. PURPOSE:** The purpose of the WISP is to better: (1) ensure the security and confidentiality of personal information; (2) protect against any reasonably anticipated threats or hazards to the security or integrity of such information; and (3) protect against unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft or fraud.

III. SCOPE:

In formulating and implementing the WISP, Habilitation Assistance Corporation has addressed and incorporated the following protocols:
(1) Identified reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information;
(2) Assessed the likelihood and potential damage of these threats, taking into consideration the sensitivity of the personal information;
(3) Evaluated the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risks;
(4) Designed and implemented a WISP that puts safeguards in place to minimize those risks, consistent with the requirements of 201 CMR 17.00; and
(5) Implemented regular monitoring of the effectiveness of those safeguards.

Habilitation Assistance has in place several documents and policies that support this WISP and are designed to protect personal information of our members, staff, and customers. These documents and policies include, but are not limited to:

- Code of Conduct/Code of Ethics (Policy #03)
- Confidentiality/HIPPA (Policy # 04)
- Employment Records (Policy # 011)
- Computer Use (Policy# 53.2)
- Visitor Policy (Policy # 63.1)
- Policy on Record Access
- Risk Management Plan
- Statement of Confidentiality
- Notice to Members regarding Privacy Rights
- Technology Plan
- Corporate Compliance Plan

IV. DATA SECURITY COORDINATOR:

Habilitation Assistance Corporation has designated its Corporate Compliance Committee to implement, supervise and maintain the WISP. This designated employee (the "Data Security Coordinator") will be responsible to oversee and monitor the following:

a. Implementation of the WISP
b. Training of all employees;
c. Regular testing of the WISP's safeguards;
d. Reviewing the scope of the security measures in the WISP at least annually or whenever there is a significant change in our business practices that may involve the security or integrity of records containing personal information;
e. Conducting an annual training session on the elements of the WISP for all owners, managers, and employees, including temporary and contract employees who have access to personal information. All attendees at such training sessions are required to certify their attendance at the training, and their familiarity with our requirements for ensuring the protection of personal information.

V. INTERNAL RISK MITIGATION POLICIES:

To guard against internal risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the following measures are in place:

1) We will only collect personal information of clients, customers or employees that is necessary to accomplish our legitimate business transactions or to comply with any and all federal, state or local regulations.
2) Access to records containing personal information shall be limited to those employees whose duties, relevant to their job description, have a legitimate need to access said records, and only for this legitimate job-related purpose.
3) Written and electronic records containing personal information shall be securely destroyed or deleted at the earliest opportunity consistent with business needs or legal retention requirements.

• This WISP policy is reviewed by each current employee and to each new employee on the beginning date of their employment. It shall be the employee's responsibility to abide by its provisions. Employees are encouraged and invited to advise the WISP Data Security Coordinator of any activities or operations which appear to pose risks to the security of personal information. If the Data Security Coordinator is him or herself involved with these risks, employees are encouraged and invited to advise any other manager or supervisor or business owner,
• A training session for all current employees will be held annually to detail the provisions of the WISP.
All employees are required to comply with the provisions of the WISP and to prohibit any nonconforming use of personal data as defined by the WISP.
• Terminated employees must return all records containing personal data, in any form, in their possession at the time of termination. This includes all data stored on any portable device and any device owned directly by the terminated employee
• A terminated employee's physical and electronic access to records containing personal information shall be restricted at the time of termination. This shall include remote electronic access to personal records, voicemail, internet, and email access. All keys, keycards, access devices, badges, company IDs, business cards, and the like shall be surrendered at the time of termination.
• Disciplinary action will be applicable to violations of the WISP, irrespective of whether personal data was actually accessed or used without authorization.
• All security measures including the WISP shall be reviewed at least annually to ensure that the policies contained in the WISP are adequate to meet all applicable federal and state regulations.
• Should our business practices change in a way that impacts the collection, storage, and/or transportation of records containing personal information, the WISP will be reviewed to ensure that the policies contained in the WISP are adequate to meet all applicable federal and state regulations.
• The Data Security Coordinator or their designee shall be responsible for all review and modifications of the WISP and shall fully consult and apprise management of all reviews including any recommendations for improves security arising from the review.

	• The Data Security Coordinator or designee shall maintain a secured and confidential master list of all lock combinations, passwords, and keys. The list will identify which employee keys, keycards, or other access devices and that only approved employee has been provided access credentials. • Current employees' user IDs and passwords shall conform to accepted security standards. All passwords shall be changed at least annually or more often as needed • Employees are required to report suspicious or unauthorized use of personal information to a supervisor or the Data Security Coordinator • Whenever there is an incident that requires notification pursuant to the Security Breach Notifications of Massachusetts General Law Chapter 93H: "Security Breaches" (copy attached), the Data Security Coordinator shall host a mandatory post-incident review of events and actions taken, if any, in order to determine how to alter security practices to better safeguard personal information. **VI. EXTERNAL RISK MITIGATION POLICIES:** • Firewall protection, operating system security patches, and all software products shall be reasonably up-to-date and installed on any computer that stores or processes personal information • Personal information shall not be removed from the business premises in electronic or written form absent legitimate business need and use of reasonable security measures, as described in this policy • All system security software including, anti-virus, anti-malware, and internet security shall be reasonably up-to-date and installed on any computer that stores or processes personal information. • There shall be secure user authentication protocols in place that: ▪ Control user ID and other identifiers; ▪ Assigns passwords in a manner that conforms to accepted security standards, o or applies use of unique identifier technologies; ▪ Control passwords to ensure that password information is secure. **VII. OPERATIONAL PROTOCOL** This section of our WISP outlines our on-going efforts to minimize security risks to any computer system that processes or stores personal information, ensures that physical files containing personal information are reasonable secured and develops daily employee practices designed to minimize access and security risks to personal information of our clients and/or customers and employees. A. **Recordkeeping Protocol** • At the end of the day, all files containing personal information are to be returned to their assigned locked filing cabinets • Paper or electronically stored records containing personal information shall be disposed of in a manner that complies with M.G.L. c. 93I sec. 2 • Electronic records containing personal information shall not be stored or transported on any portable electronic device, sent or transmitted electronically to any portable device, or sent or transported electronically to any computer, portable or not, without being encrypted.

B. Access Control Protocol:

• All our computers shall restrict user access to those employees having an authorized and unique log-in ID

• All computers that have been inactive for 5 or more minutes shall require relog-in

• After 5 unsuccessful log-in attempts by any user ID, that user ID will be blocked from accessing any computer or file stored on any computer until access privileges are reestablished by the Data Security Coordinator or their designee

• Access to electronically stored records containing personal information shall be electronically limited to those employees having an authorized and unique login

• Visitors are required to sign-on and wear a visitor ID badge in a plainly visible location on their body, unless escorted at all times. Where practical, all visitors are restricted from areas where files containing personal information are stored. Alternatively, visitors must be escorted or accompanied by an approved employee in any area where files containing personal information are stored.

• Cleaning personnel (or others on site after normal business hours and not also authorized to have access to personal information) are not to have access to areas where files containing personal information are stored unless all personal information is in locked cabinets.

• All computers with an internet connection or any computer that stores or processes personal information must have a reasonably up-to-date version of software providing virus, anti-spyware and anti-malware protection installed and active at all times.

• An inventory of all company computers and handhelds authorized for personal information storage shall be maintained

SMS/Text Messaging:

1. Consent to Receive Text Messages:

By providing your mobile phone number and opting in, you expressly consent to receiving text messages from the company regarding work-related issues such as program closures, benefit enrollments, special events, etc. Messages will be sent as needed and the frequency will vary depending on need.

2. Opt-Out Instructions:

You may opt out of receiving text messages at any time by replying STOP. After opting out, you will receive one final confirmation message. No further messages will be sent unless you re-opt in.

3. Data Collected: We may collect your mobile phone number, message content, timestamps, delivery status, and opt-in/opt-out records. We do not collect sensitive personal information via SMS.

4. How We Use Your Information

Information is used to deliver messages, comply with FCC/TCPA regulations, improve customer service, and maintain consent records.

5. Data Sharing & Third Parties
We do not sell or rent your mobile number. Information may be shared only with trusted messaging
service providers for delivery purposes and compliance.
6. Data Security
We implement reasonable safeguards to protect your information from unauthorized access or misuse.
7. Message & Data Rates
Message and data rates may apply depending on your carrier and plan.
8. Changes to This Policy
We may update this policy periodically. Updates will be posted with a revised effective date.

VIII. <u>Breach of Data Security Protocol</u>:
Should any employee know of a security breach at any of our facilities, or that any unencrypted personal information has been lost or stolen or accessed without authorization, or that encrypted personal information along with the access code or security key has been acquired by an unauthorized person or for an unauthorized purpose, the following protocol is to be followed:

1) Employees are to notify the Data Security Coordinator or department head in the event of a known or suspected security breach or unauthorized use of personal information.
2) The Data Security Coordinator or designee shall be responsible for drafting a security breach notification to be provided to the Massachusetts Office of Consumer Affairs and Business Regulation and the Massachusetts Attorney General's office. The security breach notification shall include the following:
    - A detailed description of the nature and circumstances of the security breach or unauthorized acquisition or use of personal information;
    - The number of Massachusetts residents affected at the time the notification is submitted;
    - The steps already taken relative to the incident;
    - Any steps intended to be taken relative to the incident subsequent to the filing of the notification; and
    - Information regarding whether law enforcement officials are engaged in investing the incident

M. G. L. c.931 sec. 2:
Section 2. When disposing of records, each agency or person shall meet the following minimum standards for proper disposal of records containing personal information:
(a) paper documents containing personal information shall be either redacted, burned, pulverized or shredded so that personal data cannot practicably be read or reconstructed;

	(b) electronic media and other non-paper media containing personal information shall be destroyed or erased so that personal information cannot practicably be read or reconstructed. Any agency or person disposing of personal information may contract with a third party to dispose of personal information in accordance with this chapter. Any third party hired to dispose of material containing personal information shall implement and monitor compliance with policies and procedures that prohibit unauthorized access to or acquisition of or use of personal information during the collection, transportation and disposal of personal information. Any agency or person who violates the provisions of this chapter shall be subject to a civil fine of not more than $100 per data subject affected, provided said fine shall not exceed $50,000 for each instance of improper disposal. The attorney general may file a civil action in the superior or district court in the name of the commonwealth to recover such penalties.
Related Policies:	Code of Conduct/Code of Ethics, Computer Usage, Confidentiality/HIPAA,, Corporate Compliance, Discharge, Employment Records, Lockdown, Management Rights and Responsibilities, Orientation and Training, Progressive Discipline, Resignation/Terminations, Social Media, Visitor Policy