Written Information Security Program (WISP)

STANDARD:
Old Colony Hospice has established this written information security program (WISP) policy in order to assure our employees, volunteers, Board of Directors members, patients & families, donors and others who may be affiliated with Old Colony Hospice of our firm commitment to protecting any personal information or other data collected in accordance with any legitimate business or employment need.

POLICY:
- Old Colony Hospice is committed to ensuring security of information gathered for business or employment purposes. To prevent unauthorized access or disclosure, we have put into place appropriate physical, electronic and managerial procedures to safeguard and secure the information we collect.
- Personal information includes 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 public.
- Record or records is any material upon which written, drawn, spoken, visual or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics.
- Service Provider is any person that receives, stores, maintains, processes, or otherwise is permitted access to personal information through its provision of services directly to a person that is subject to this written information security program.

PROCEDURE:

Old Colony Hospice has taken the following steps to protect and secure sensitive information:
- Inventory of equipment (desktop and laptop computers, blackberries/cell phones and any other communication device) and all locations (filing cabinets, websites, storage, computer applications, etc.) holding or recording information that may determined to be sensitive whether electronic or in paper form
- Assuring that we retain only that information that is necessary for the conduct of daily business
- Assuring that sensitive information is encrypted, locked or otherwise inaccessible to any but those with legitimate need
- Assuring that sensitive information is properly disposed of according to any state or federal requirement
- Establishing a plan to respond in the event of any security breach or incident

- Collecting privacy and security policies from all vendors and others who may request, submit or otherwise have access to sensitive business or employee data
- IT backup and storage is encrypted, password protected; and anti-virus, SPAM and other safeguards are up-to-date on the computer server and systems
- Employees are encouraged to protect information that they may be working with and guard against leaving sensitive papers out on their desks or other work areas when they are away from their work area
- Personnel Information: Old Colony Hospice does not use employee Social Security Numbers for identification or other purposes; a records retention guide has been established to identify what information must be kept, how secure it is, how long it must be kept and how it will be disposed of when no longer needed. All personnel paper files are kept in the human resource manager's office in locked cabinets with access limited to only those with legal or legitimate need for access. All computerized records are held in password protected files.
- Volunteer Information is maintained in a locked cabinet by the Volunteer Coordinator and also by the Human Resources Manager. All of the information regarding volunteers' personal information has limited access to only those with legal or legitimate need for access.
- Business Information – sensitive business data will be kept as long as there is a business reason to do so. Once that business need is over, the information will be disposed of properly.
- Old Colony Hospice will seek security assurance from third-party vendors or service providers that any information they collect that may fall within the guidelines of this policy is secure and protected. Copies of these security assurances will be kept with the human resources manager or other administrative personnel, as may be applicable.
- All records that are being destroyed because they are outdated, no longer needed or for one reason or another must be shredded—no patient records or employee information should be simply put in the trash to be collected and disposed of by cleaning crew.
- Terminating employees will be required to return any and all equipment and paperwork immediately.
- Passwords and other protections
    1. Employees must: use passwords to protect sensitive information; not share or post passwords near workstation; use passwords that are complex (a combination of letters and numbers and that are not easily recognized); lock their computers when leaving their workstations by pressing ctrl, alt, delete;
    2. Employees with company issued laptops and blackberries/cell phones or other electronic devices that may receive and/or store sensitive data should store the equipment in a secure place. When out of the office using the laptop, staff should never leave the laptop visible in a car, unattended at a SNF, a patient's residence or other facility.
- Breach Response Plan: Any suspected breach will be investigated immediately and steps will be taken to assure that information and records are not vulnerable. Notification will be given in accordance with established state and/or federal regulation to the appropriate authorities and possible affected individuals.

Employee Training: all employees will be encouraged to review this policy upon hire and annually during mandatory education days and encouraged to report any suspected breach in security as required by regulation.

Failure to abide by this policy will result in disciplinary action that may include termination of employment and legal remedies depending on the severity of the policy violation or breach of security.

Old Colony Hospice has designated as the Data Security Coordinator the Human Resources Manager in conjunction with the IT Coordinator to implement, supervise and maintain the WISP. The Data Security Coordinator will be responsible for:

- Initial implementation of the WISP
- Training employees
- Overseeing regular testing of the WISP's safeguards
- Evaluating the ability of each of our third party service providers to implement and maintain appropriate security measures for the personal information to which we have permitted them access consistent with 201 CMR 17.00; and requiring such third party service providers by contract to implement and maintain appropriate security measures
- Reviewing the scope of the security measures in the WISP at least annually, or whenever there is a material change in our business practices that may implicate the security or integrity of records containing personal information
- Conducting an annual training session for all owners, managers, employees and independent contractors, including temporary and contract employees who have access to personal information on the elements of the WISP. All attendees at such training sessions are required to certify their attendance at the training, and their familiarity with the agency's requirements for ensuring the protection of personal information.