BEACON
Specialized Living

Training Acknowledgment

Employee Name: Tammy Gillis Policy/Procedure/Topic: HIPAA/internet/compute

Trained By: Lee-ellen Bailey Date Trained: 10/28/2021

I acknowledge that I have received training on the above topic, along with supporting policies, forms and procedures.

I understand that it is my responsibility to adhere to the requirements of the training fully, and if I do not understand my responsibility or need clarification, I will seek immediate assistance from a Home Manager in order to act in accordance with state policy, procedures and company expectations.

I understand that this Training Acknowledgment will become part of my permanent employment record, and that failure to apply the principles I was taught in my training will result disciplinary action, up to and including my termination of employment for failure to follow company policy.

Tammy Gillis — 10/28/2021
Employee Signature — *Date*

Lee-ellen Bailey — 10/28/2021
Home Manager Signature — *Date*

✓ Copy to Employee
✓ Copy to Employee Personnel File/HR

BEACON Specialized Living

HIPAA & HITECH Policy

Policy: To ensure that the Organization complies with the Health Insurance Portability and Accountability Act and the HITECH Act in protecting both the Residents' and Employees' Protected Health Information (PHI) and in accordance with The Joint Commission and Department of Health and Human Services requirements.

The privacy of health information is a critical information management concern. PHI can be transmitted through electronic, paper and verbal communication. This policy addresses:

1. Uses of PHI and security
2. Training
3. Notification of Clients' and Employees' HIPAA rights
4. Retention and destruction of medical records
5. Reporting procedures for HIPAA violations.
6. Maintaining environmental HIPAA standards

Procedure:

1. **Uses of PHI and Security:**
    - Security measures are taken with initial employee background checks, including but not limited to source verification and criminal background checks, etc. Management will determine what screening is appropriate for its personnel with access to confidential medical and personal information by considering the risk factors and the cost of the security measure.
    - Business Associate Agreements are given to all vendors/contractors who may have access to our Residents' and/or Employees' PHI.
2. **PHI is shared with only those who NEED TO KNOW**, (caregivers, health plan administrators, health care claims handling, etc.). PHI is shared with the minimum number of people necessary to perform needed functions. PHI will generally be used or disclosed only for purposes of treatment, payment and health care operations. The Organization is permitted by law to use and disclose PHI for additional purposes, including: health care and legal compliance activities; to a public health authority in certain situations as required by law; for health oversight activities, including audits or government investigations, inspections, disciplinary proceedings, or other administrative or judicial actions undertaken by a governmental agency by law to oversee the health care system; for certain judicial and administrative proceedings; for law enforcement activities in limited situations; to avert a serious threat to the health and safety of a person or the public at large; and for workers' compensation purposes.
    - The Compliance Department performs regular security audits to ensure that all vulnerabilities to our system can be identified and corrected.

BEACON Specialized Living

HIPAA & HITECH Policy

- All medical records are secured in a safe and locked area. Electronic information is shared through EHR and EMAR systems, company e-mails and e-faxes that all require passwords to access.

3. **Training**
   - Pre-employment training is given to all new applicants. Once an employee is hired, they are evaluated on HIPAA/HITECH through performance evaluations and competency assessments. They receive annual in-service training.
4. **Notification of Rights**
   - Residents are given the Rights Policy at the time of intake and on an annual basis. Employees are given a Notice of Privacy Policy and Practices for the Organization's Health and Welfare Plan.
5. **Retention and Destruction of Medical Records**
   - Refer to this policy for details.
6. **Reporting Violations and Consequences of Violations**
   - All employees are responsible for promptly reporting any security breaches that may occur. Employees should feel free to report breaches without fear of reprisal, and they should also understand they have a duty to do so.
   - Breach of confidentiality is defined as the acquisition, access use or improper disclosure of PHI to a person or entity not authorized to receive the information. The person discovering the breach must:
     - Initiate any necessary correction action (e.g., report a lost or stolen computer with client or employee PHI contained therein);
     - Notify Facilities Manager, IT Manager or other emergency services if equipment or storage housing PHI is in danger;
     - Report the matter to management, e.g., immediate supervisor and HIPAA Compliance Officer;
     - As soon as possible, make a written report including: person submitting report, date and time of incident and report, location of incident, equipment involved, suspects, facts witnessed, nature of breach, what harm was caused, who was notified, remedial action and recommendations for corrective action.
   - A HIPAA Log should be used by all Managers and the Compliance Officer when an employee requests PHI or discusses PHI with them. The log should include date and time and employee's name, the issue or request, any witnesses or other individuals involved, and how it was resolved.
   - An employee who makes an improper use or disclosure of PHI will be subject to disciplinary action, up to and including termination.

BEACON
Specialized Living

HIPAA & HITECH Policy

- No cameras will be used in the public areas of the home. The residents may not be filmed while residing in their residence as those spaces are private. There may be cameras located in the medications rooms as that is not a public space and there may be cameras located in the parking lots for resident safety.

Policy #: IM-005
Date Originated: 8/8/03
Date Revised: 12/6/18

BEACON
Specialized Living

Computer and Internet Access Policy

Purpose: The use of the Organization's automation systems, including computers, fax machines and all forms of Internet/Intranet access, is for company business and is to be used for authorized purposes only. Brief and occasional personal use of the electronic mail system or the Internet is acceptable as long as it is not excessive or inappropriate, occurs during personal time (lunch or other breaks), and does not result in expense to the Organization.

Use is defined as "excessive" if it interferes with normal job functions, responsiveness, or the ability to perform daily job activities. The Organization's automation systems are the Organization's resources and are provided as business communication tools. Electronic communication "should not be used to solicit or sell products, distract coworkers, or disrupt the workplace."

Tablets are to be used for MS Teams meetings with residents scheduled by a Beacon Clinician including but not limited to: Case Management, Therapy, and Behavior Treatment Monitoring. During these meetings, the resident may take this tablet to an area away from staff's sight or hearing. This tablet may be used when an employee is contacted by Beacon's internal Compliance department to participate in home audits of any kind. Additional Beacon departments may initiate TEAMs meetings with employees in which this tablet may be used.

Policy: Use of the Organization's computers, networks, and Internet access is a necessary part of office staff's job, therefore inappropriate conduct including, but not limited to the following, could result in sanctions from management. All staff will be given passwords to access the appropriate electronic system to be used to perform their duties.

1. Sending chain letters;
2. Engaging in private or personal business activities;
3. Accessing social media;
4. Misrepresenting oneself or the Organization;
5. Engaging in unlawful or malicious activities;
6. Using abusive, profane, threatening, racist, sexist or otherwise objectionable language in either public or private messages;
7. Sending, receiving, or accessing pornographic materials;
8. Becoming involved in partisan politics;
9. Causing congestion, disruption, disablement, alteration, or impairment of the Organization's networks or systems;
10. Add additional programs to computers or tablets;
11. Infringing in any way on the copyrights or trademark rights of others;
12. Using recreational games; and/or
13. Defeating or attempting to defeat security restrictions on the Organization's systems and applications;

BEACON Specialized Living

Computer and Internet Access Policy

14. Downloading and/or storing copyrighted materials on the Organization's systems, including but not limited to music and movies;
15. Giving out the Organization's email address to anyone or any organization not directly involved with the Organization. If you wish to receive personal email at work, you will need to sign up for a hotmail or other account. If you need help doing this, please contact the IT Manager.

Using the Organization's automation systems to create, view, transmit, or receive racist, sexist, threatening, or otherwise objectionable or illegal material is strictly prohibited. "Material" is defined as any visual, textual, or auditory entity. Such material violates the Organization's anti-harassment policies and is subject to disciplinary action. The Organization's electronic mail system must not be used to violate the laws and regulations of the United States or any other nation or any state, city, province, or other local jurisdiction in any way. Use of the Organization's resources for illegal activity can lead to disciplinary action, up to and including dismissal and criminal prosecution. Unless specifically granted in this policy, any nonbusiness use of the Organization's automation systems is expressly forbidden.

If you violate these policies, you could be subject to disciplinary action up to and including dismissal.

Procedure:

1. Ownership and Access of Electronic Mail and Computer Files
    - The Organization owns the rights to all data and files in any computer, network, or other information system used in the Organization. The Organization reserves the right to monitor computer and e-mail usage, both as it occurs and in the form of account histories and their content. The Organization has the right to inspect any and all files stored in any areas of the network or on any types of computer storage media in order to assure compliance with this policy and state and federal laws. The Organization will comply with reasonable requests from law enforcement and regulatory agencies for logs, diaries, archives, or files on individual computer and email activities. The Organization also reserves the right to monitor electronic mail messages and their content. Employees must be aware that the electronic mail messages sent and received using the Organization's equipment are not private and are subject to viewing, downloading, inspection, release, and archiving by the Organization's officials at all times. No employee may access another employee's computer, computer files, or electronic mail messages without prior authorization from either the employee or an appropriate Organization official.
    - The Organization has licensed the use of certain commercial software application programs for business purposes. Third parties retain the ownership and distribution rights to such software. No employee may create, use, or distribute copies of such

BEACON Specialized Living

Computer and Internet Access Policy

software that are not in compliance with the license agreements for the software. Violation of this policy can lead to disciplinary action, up to and including dismissal. All software is to be approved and installed by authorized system personnel only. When 3rd party software or hardware is returned or no longer used, it is the IT Manager's responsibility to delete all data that may contain resident and/or staff health/confidential information.

2. Confidentiality of Electronic Mail
    - As noted above, electronic mail is subject at all times to monitoring, and the release of specific information is subject to applicable state and federal laws and the Organization's rules, policies, and procedures on confidentiality. Existing rules, policies, and procedures governing the sharing of confidential information also apply to the sharing of information via commercial software. Since there is the possibility that any message could be shared with or without your permission or knowledge, the best rule to follow in the use of electronic mail or non-work-related information is to decide if you would post the information on the bulletin board with your signature. It is a violation of the Organization's policy for any employee, including system administrators and supervisors, to access electronic mail and computer system files to satisfy curiosity about the affairs of others. Employees found to have engaged in such activities will be subject to disciplinary action.
3. Message Tone for Electronic Mail
    - Users are expected to communicate with courtesy and restraint with both internal and external recipients. Electronic mail should reflect the professionalism of the Organization and should not include language that could be construed as profane, discriminatory, obscene, sexually harassing, threatening or retaliatory. It is recommended that using all capital letters, shorthand, idioms, unfamiliar acronyms, and slang be avoided when using electronic mail. These types of messages are difficult to read.
4. Electronic Mail Tampering
    - Electronic mail messages received should not be altered without the sender's permission; nor should electronic mail be altered and forwarded to another user and/or unauthorized attachments be placed on another's electronic mail message.
5. Policy Statement for Internet/Intranet Browser(s)
    - This policy applies to all uses of the Internet, but does not supersede any state or federal laws or Organization policies regarding confidentiality, information dissemination, or standards of conduct. The use of Organization automation systems is for business purposes only. Brief and occasional personal use is acceptable as long as it is not excessive or inappropriate, occurs during personal time (lunch and other breaks), and does not result in expense to the Organization. Use is defined as "excessive" if it interferes with normal job functions, responsiveness, or the ability to perform daily job

BEACON Specialized Living

Computer and Internet Access Policy

activities. Examples of inappropriate use are defined in "inappropriate Use of the Internet/Intranet." Managers determine the appropriateness of the use and whether such use is excessive.

- The Internet is to be used to further the Organization's mission, to provide effective service of the highest quality to the Organization's customers and staff, and to support other direct job-related purposes. Supervisors should work with employees to determine the appropriateness of using the Internet for professional activities and career development. The various modes of Internet/Intranet access are Organization resources and are provided as business tools to employees who may use them for research, professional development, and work-related communications. Limited personal use of Internet resources is a special exception to the general prohibition against the personal use of computer equipment and software.
- Employees are individually liable for any and all damages incurred as a result of violation the Organization's security policy, copyright and licensing agreements.
- All Organization policies and procedures apply to employees' conduct on the Internet, especially, but not exclusively, relating to: intellectual property, confidentiality, company information dissemination, standards of conduct, misuse of company resources, anti-harassment, and information and data security.
- Violation of these policies and/or state and federal laws can lead to disciplinary action, up to and including dismissal and possible criminal prosecution.

6. Inappropriate Use of the Internet/Intranet
   - Use of the Organization's computer, network, or Internet resources to access, view, transmit, archive, or distribute racist, sexist, threatening, or otherwise objectionable or illegal material is strictly prohibited. "Material" is defined as any visual, textual, or auditory item, file, page, graphic, or other entity. Such material violates the Organization's anti-harassment policies and is subject to Organization disciplinary action.
   - No employee may use the Organization's Internet/Intranet facilities to deliberately propagate any virus, worm, Trojan horse, trap-door program code, or other code or file designed to disrupt, disable, impair, or otherwise harm either the Organization's networks or systems or those of any other individual or entity.
   - The Organization's Internet/Intranet facilities and computing resources must not be used to violate the laws and regulations of the United States or any other nation or any state, city, province, or other local jurisdiction in any way. Use of the Organization's resources for illegal activity can lead to disciplinary action, up to and including dismissal and criminal prosecution.
7. Internet/Intranet Security
   - The Organization owns the rights to all data and files in any information system used in the Organization. Internet use is not confidential and no rights to privacy exist. The

BEACON Specialized Living

Computer and Internet Access Policy

Organization reserves the right to monitor Internet/Intranet usage, both as it occurs and in the form of account histories and their content. The Organization has the right to inspect any and all files stored in private areas of the network or on any types of computer storage media in order to assure compliance with this policy and state and federal laws. The Organization will comply with reasonable requests from law enforcement and regulatory agencies for logs, diaries, archives or files on individual Internet activities.

- Existing rules, policies and procedures governing the sharing of work-related or other confidential information also apply to the sharing of information via the Internet/Intranet. The Organization has taken the necessary actions to assure the safety and security of our network. Any employee who attempts to disable, defeat, or circumvent Organization security measures is subject to disciplinary action, up to and including dismissal.

8. Tablet Use:
    - Clinicians are responsible for purchasing a protective cover for the device suitable to the needs and abilities of the residents in the home.
    - Home managers will be in-serviced in the use of the tablets by a Beacon clinician.
    - Home managers are responsible for in-servicing this policy to all employees in the home.
    - The tablet is to be kept in a safe location accessible to staff when it is not in use by a resident.
    - The tablet is to be charged during night shift at the least.