Background:

Palmer's Home care, LLC ("Company") invests in and maintains computing resources to record, track, manage, and protect our clients' health records; and to support the productivity of our employees. It is the policy of the Company that all employees will protect health records on behalf of the Company's clients. All employees will comply fully with the Health Information Portability and Accountability Act (HIPAA). This policy outlines the guidelines for acceptable use of the Company's technology systems.

Scope:

This policy must be followed in conjunction with other Company policies governing appropriate workplace conduct and behavior. Any employee who abuses the company-provided access to email, the internet, or other electronic communications or networks, including social media, may be denied future access and, if appropriate, be subject to disciplinary action up to and including termination. The Company complies with all applicable federal, state, and local laws as they concern the employer/employee relationship. Nothing in this policy is intended to, nor should be construed to limit or interfere with employee rights as set forth under all applicable provisions of the National Labor Relations Act, including Section 7 and 8(a)(1) rights to organize and engage in protected, concerted activities regarding the terms and conditions of employment.

Definitions:

Authorized personnel – includes all employees, owners, subcontractors, volunteers, and interns who are granted access to the company's computing resources.

Guest devices – are computing devices that are managed and maintained by their owners. These devices may not meet the company's security standards.

Information Technology (IT) Department – The department within the company responsible for administering, managing, and maintaining Company computing resources.

Managed devices – are computing resources such as desktop computers, laptops, encrypted thumb drives, smart phones, servers, network equipment, etc., that are purchased by the Company and are maintained by the IT Department for use by authorized personnel.

Protected Health Information (PHI) – individually identifiable health information held or transmitted by the Company in any form or media, whether electronic, paper or oral. This individually identifiable health information includes demographic data that relate to:

- An individual's past, present or future physical or mental health or condition;
- The provision of health care to an individual; or
- The past, present, or future payment for the provision of health care to an individual; and Identifies the individual or there is a reasonable basis to believe it can be used to identify the individual. This includes many common identifiers (e.g., name, address, birth date, Social Security number, picture, etc.).

Policy

I. **General**

1. It is the policy of the Company to provide managed devices that will provide authorized personnel with access to cost-effective computing resources they need to be productive in their roles.

2. Because the Company is committed to protecting the PHI of its clients, all managed devices provided by the Company are intended solely for transacting company business and are not for use by anyone other than the authorized user.

3. All information on a Company device may be monitored or reviewed at any time by the IT Department. This includes monitoring and reviewing the health of the device to ensure the operating system and applications are up to date and operating effectively, as well as any content on the device. Authorized users shall have no expectation of privacy in anything they create, store, send or receive using the Company's computer equipment. The computing network and all related resources are the property of the Company, and the Company retains the right to limit personal use.

4. If criminal activity is suspected, the Company reserves the right to turn over all information to law enforcement.

5. If a managed device breaks, becomes lost, stolen, or no longer functional, the authorized personnel responsible for the device must immediately report it to their supervisor or the IT Department.

6. All devices assigned to authorized personnel remain the sole property of the Company. All devices must be returned if authorized personnel take medical leave, extended leave, or when their employment and/or association with the Company is terminated. All devices must be returned in good condition, along with any accessories that were provided, such as power adapters, protective covers, privacy screens, etc.

7. All data stored locally on Company desktops and laptops must be encrypted.

8. No authorized personnel shall leave their computer unattended with the user logged on. When authorized personnel leave their computer unattended, they must lock their computer or log off.

9. Authorized personnel have an obligation to use their access in a responsible and informed way, conforming to proper etiquette, customs, courtesies and all applicable laws or regulations.

10. Authorized personnel must be aware that any misuse or abuse of the Company's Information Technology resources reflects negatively upon the Company's image to their clients and stakeholders and is to be avoided. Professionalism in all communications both internally and externally is of the utmost importance.

11. All authorized personnel must represent themselves and the Company accurately and honestly through electronic information or service content whenever they are using a Company device and/or Company credentials.

II. User ID and Password

- Authorized personnel will be provided with a unique user ID and will be required to create a password. The user ID shall be unique to each authorized personnel. The user ID and password shall be used to authenticate or gain access to the Company's technology systems.
- Authorized personnel must not share their passwords with anyone. Passwords must not be written down and left in any unprotected or unlocked area. Actions performed on a managed device using an authorized personnel's user ID and password are the responsibility of that authorized personnel.
- Passwords must be a minimum of 12 characters and include 3 of the following:
    - Upper case letters;
    - Lower case letters;
    - Digits; and
    - Special characters.
- Passwords must be changed every 180 days, or when requested by the IT Department.
- Authorized personnel must not bypass the privileges or access rights granted to them by logging on as a different user or by circumventing security controls.
- If an authorized personnel needs permission to access computing resources, they must contact their supervisor or the IT Department.
- Any authorized personnel who become aware that a user ID and password has been shared, or aware that anyone has accessed computing resources without permission, must immediately report it to their supervisor or Human Resources.
- The user ID and password of an authorized personnel will be revoked within 24 hours of a normal termination and within 1 hour of an accelerated termination.

III. Protection of Personal Health Information (PHI)

Palmer's Home Care, LLC utilizes the Health Risk Screening Tool (HRIS), provided by the Missouri Department of Mental Health, and Therap to centrally manage all health care records for its clients. The Company is committed to protecting the personal health information of all its clients.

1. Email – *see section IV. Email.*
2. Transmitting PHI to External Entities - If authorized personnel are required to electronically transmit PHI to an external entity, they must do so in a secure and encrypted manner.
3. Printing PHI – Printed documents shall be removed promptly from printers to prevent the PHI from being viewed by unauthorized individuals.
4. Paper faxing PHI – Received documents shall be removed promptly from fax machines to prevent PHI from being viewed by unauthorized individuals.

IV. **Email**

1. Palmer's Home Care, LLC maintains an electronic mail (email) system to support the mission of the Company. All data and information sent and received through the Company's email system including, but not limited to, messages, attachments, photos, calendar appointments, reminders, etc. are the property of the Company and may be monitored at any time without the permission of authorized personnel. Palmer's Home Care, LLC retains the right to review or audit all information sent or received via the Company's email system.

2. Personal Health Information (PHI) must not be sent to any external email address outside of the Company unless it is encrypted. This includes attachments or screen shots containing PHI and PHI in the subject or body of an email. Sending or forwarding an email to the wrong address can result in sharing of PHI outside the Company, which is considered a breach under HIPAA. Authorized personnel are expected to verify that all recipients have a Company email address and have prior knowledge that PHI is being sent.

3. If PHI must be transmitted electronically to an external entity, authorized personnel must use the encryption process provided by the Company's email system.

4. The email system is for company use only; however, minimal personal use is acceptable. Any personal messages sent or received are subject to monitoring and are the property of the Company. Authorized personnel have no reasonable expectation of privacy with respect to communications conducted over Company email. Even deleted messages and attachments are accessible by administrators.

5. No email or other electronic communications may be sent that hide the identity of the sender or represent the sender as someone else. Palmer's Home Care, LLC's corporate identity is attached to all outgoing email communications, which should reflect corporate values and appropriate workplace language and conduct.

6. Authorized personnel shall not use the Company's email to send, upload, receive, or download any copyrighted materials, trade secrets, or proprietary information without the appropriate authorization of the owner of this material.

7. The Company's email system shall not be used to create or foster a hostile, intimidating, or discriminatory environment. This includes sending, forwarding, replying to, or storing emails that contain offensive, threatening, or harassing language or content. Examples include, but are not limited to, messages of a sexual nature, racially insensitive material, gender specific comments, comments on sexual orientation, comments related to a disability, religious or political beliefs, national origin, age, marital status, or anything else that targets an individual or group based on a protected class under federal, state, or local law.

8. The Company's email system shall not be used to solicit donations for personal charities, advertise or run a business, or solicit for commercial purposes, including advertising items for sale. It is not to be used for religious or political causes, or to support outside organizations, unless sanctioned by executive staff as part of our company's mission.

V. **Internet**

1. Palmer's Home Care, LLC provides access to the internet for use by authorized personnel. Access to the internet is for the benefit of the Company and shall be used primarily to transact Company business; however, minimal personal use is acceptable.
2. The Company maintains the right to monitor the volume of internet traffic and the content of all internet traffic. Access to the internet is not anonymous. The Company maintains the right to identify and associate the content downloaded or accessed with the user ID of all authorized personnel.
3. The Company maintains the right to block sites that may impact productivity, contribute to a hostile work environment or pose a cyber-security risk.
4. PHI shall not be sent or received over the internet unless it is encrypted.
5. The internet shall not be used to create or foster a hostile environment. This includes downloading, uploading or viewing content that contains offensive language, including messages or pictures of a sexual nature, racially insensitive material, gender specific comments, comments on sexual orientation, religious or political beliefs, national origin, or comments related to a disability.
6. Authorized personnel shall not use the internet to send, upload, receive, or download any copyrighted materials, trade secrets or proprietary information without the appropriate authorization of the owner of this material.
7. Authorized personnel are prohibited from using the internet to violate federal, state, or local laws. Abusive, excessively profane, or offensive language and any illegal activities—including piracy, cracking, extortion, blackmail, copyright infringement, and unauthorized access to any computers on the internet or email—are forbidden. Use of the internet or any Company resources for illegal activity is grounds for disciplinary action up to and including dismissal.
8. The internet shall not be used to solicit donations for personal charities, advertise or run a business, or solicit for commercial purposes, including advertising items for sale. It is not to be used for religious or political causes, or to support outside organizations unless sanctioned by executive staff as part of the Company's mission.
9. Authorized personnel are prohibited from downloading software or other program files or online services from the internet without prior approval from the IT Department. All files or software should be passed through virus-protection programs prior to use. Failure to detect viruses could result in corruption or damage to files or unauthorized entry into the Company's systems and networks.

VI. **Software and Applications**

1. The Company provides access to two main categories of software:
    a. Commercial Off the Shelf (COTS) software installed on all managed desktops and laptops such as Microsoft Office and Acrobat Reader.
    b. Hosted applications such as Therap, HRST, or Paycom. These applications may be hosted on a server in our data center or on a server in the cloud.
2. The principle of least privilege will be used to provide authorized personnel with access to hosted applications. This means that authorized personnel will be provided access to only the applications and features they need to perform their roles.
3. All hosted applications will require a user ID and password to authenticate or gain access. Authorized personnel shall not bypass the privileges or access rights granted to them by logging on as a different user or by circumventing security controls. All access to Company-hosted applications is logged.
4. All hosted applications will be assigned a functional owner. That owner shall maintain least privilege within the application.
5. The IT Department will work with all application owners to plan and execute annual upgrades.
6. The Company will maintain an inventory of all COTS software and will comply with license quantities and distribution requirements.
7. Any software or script created by authorized personnel to support the Company mission becomes the property of the Company.
8. Authorized personnel are prohibited from downloading software or other program files or online services onto Company-managed desktops and laptops from the internet without prior approval from the IT Department. If authorized personnel need software to perform their role, they must contact their supervisor and the IT Department.