Acceptable Use Policy

BACKGROUND: Health Care for the Homeless ("Agency") invests in and maintains computing resources in order to record, track, manage and protect our clients' health records and to support the productivity of our employees. These computing resources include, but are not limited to, software - such as electronic mail (email) and an Electronic Health Records (EHR) system, and hardware - such as desktops, laptops, smart phones, servers and networks. It is the policy of Health Care for the Homeless that all employees and subcontractors will protect health records on behalf of the Agency's clients, and will comply fully with the Health Information Portability and Accountability Act (HIPAA).

PURPOSE: This policy establishes conditions of use, stipulates constraints and lays out best practices for all use of the Agency's computing resources. This policy applies to all Agency authorized personnel and computing devices. Personnel must be aware that access to all computing resources is subject to monitoring by Health Care for the Homeless.

DEFINITIONS:

1. **Authorized personnel** – includes all employees, board members, subcontractors, volunteers and interns who are granted access to the Agency's computing resources.
2. **Guest devices** – are computing devices that are managed and maintained by their owners. These devices may not meet the Agency's security standards.
3. **Information Technology (IT) Department –** The department within the agency responsible for administering, managing and maintaining Agency computing resources.
4. **Managed devices** – are computing resources such as desktop computers, laptops, encrypted thumb drives, smart phones, servers, network equipment, etc., that are purchased by the Agency and are maintained by the IT Department for use by authorized personnel.
5. **Protected Health Information (PHI)** – individually identifiable health information held or transmitted by the Agency in any form or media, whether electronic, paper or oral. This individually identifiable health information includes demographic data that relate to:
    - **a.** An individual's past, present or future physical or mental health or condition;
    - **b.** The provision of health care to an individual; or
    - **c.** The past, present, or future payment for the provision of health care to an individual; and
    - **d.** 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.).[i]
6. **Remote Storage Device (RSD)** – portable storage devices that are able to download or upload data. Examples includes USB thumb drives, CD Drives, DVD Drives, external hard drives, smart phones, iPods, etc.

POLICY:

I. <u>General</u>

1. It is the policy of the Agency to provide managed devices that will cost effectively provide authorized personnel with access to the computing resources they need to be productive in their roles.
2. Because the Agency is committed to protecting the PHI of its clients, all managed devices provided by the Agency are intended only for transacting agency business, and are not for use by anyone other than the authorized user.
3. All information on an Agency device may be monitored or reviewed at any time by the Agency. 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 Agency's computer equipment. The computing network and all related resources are the property of the Agency, and the Agency retains the right to limit personal use.
4. If criminal activity is suspected, the Agency reserves the right to turn over all information to law enforcement.
5. If a managed device breaks, becomes lost, stolen or otherwise no longer functional, the employee responsible for the device must immediately report it to their supervisor or the IT Department.
6. All devices assigned to employees remain the sole property of the Agency. All devices must be returned if the employee takes medical leave, extended leave or when their employment and/or association with the Agency 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 agency desktops and laptops must be encrypted.
8. Password protected screen savers must be enabled to protect computer displays within 15 minutes of user inactivity. No authorized personnel shall leave their computer unattended with the user logged on. When an authorized personnel leaves their computer unattended, they must engage the screen lock 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 Agency's Information Technology resources reflect negatively upon the Agency'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 Agency accurately and honestly through electronic information or service content whenever they are using an Agency device and/or Agency credentials.

II. User ID and Password

1. 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 Agency's computing resources.
2. In some cases, authorized personnel may need more than one user ID and password to access resources such as ADP timecards or the Agency's staff portal, which are hosted outside the Agency's computing environment. These systems also require a unique user ID and password.
3. Authorized personnel must not share their password 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 member's user ID and password are the responsibility of that authorized personnel member.
4. Passwords must be a minimum of 8 characters and include 3 of the following:
    a. Upper case letters;
    b. Lower case letters;
    c. Digits; and
    d. Special characters.
5. Passwords must be changed every 60 days.
6. 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.
7. If authorized personnel need permission to access computing resources, they must contact their supervisor or enter a tech support ticket.
8. An employee who becomes 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.
9. The user ID and password of an authorized user will be revoked within 24 hours of a normal employee termination and within 1 hour of an accelerated termination.

III. Protection of Personal Health Information (PHI)

Health Care for the Homeless has implemented the Centricity Practice System (CPS) to centrally manage all health care records for its clients. The Agency is committed to protecting the personal health information of all its clients.

1. **Extracts and Custom Reports** - Requests for extracts of PHI must be submitted to the Health Informatics team to ensure that the extracts are stored and maintained in a secure manner.
2. **Storage of extracts and soft copy reports that contain PHI** - Extracts that contain PHI are to be stored in an Agency folder that has been set up with restricted access. Only team members authorized by the extract owner shall have access to the shared folder.
3. **Email** – *see section **VI. Email.***
4. **Remote Storage Devices** – *see section **V. Remote Storage Devices***.
5. **Transmitting PHI to External Entities** - If authorized personnel are required to electronically transmit PHI to an external entity, they must contact the IT Department or the Health Informatics Department so that a secure encrypted connection can be established.

6. **Printing PHI** – The Agency requires employees use their badge fob before retrieving any printouts in order to prevent unauthorized individuals from accessing PHI. Employees must not lend their fob or share their printer security code with other employees.
7. **Paper faxing PHI** – Received documents shall be removed promptly from the fax machine to prevent the document from being viewed by unauthorized individuals to view the PHI.

IV. Mobile Devices

1. Because the Agency has access to PHI that is stored and shared electronically, authorized personnel who are assigned a mobile device must use a minimum 6 digit personal identification number to access features on their phone.
2. All data sent and received over an agency mobile device may be monitored or reviewed including all personal communications, texts, photos, web browsing history, social media usage, etc.
3. The Agency has a limited data allowance. Employees are prohibited from using agency provided mobile devices to stream video, audio or music, or engage in any other activity that would cause excessive data usage. The cellular telephone bill will be reviewed monthly, and authorized personnel found to be using excessive data may lose cell phone privileges or receive disciplinary action.
4. Authorized personnel who are assigned a mobile device are expected to return a phone call or text promptly after being contacted by anyone at the Agency unless they are on PTO and have arranged for alternative coverage.
5. Authorized personnel are prohibited from transacting agency business on any mobile device while operating a vehicle. This includes holding the device or using it in hands free mode.
6. Authorized personnel must sign a statement acknowledging their responsibility to protect the device and the data it stores.

V. Remote Storage Devices

1. Remote storage devices (RSD) can be lost, misplaced or stolen. Any unencrypted data on a lost, misplaced or stolen RSD is at risk of compromise and is a potential breach of HIPAA regulations. Therefore, access to RSDs shall be turned off by default on all managed devices for all authorized personnel.
2. Exceptions will be made for authorized personnel who have a legitimate Agency requirement to use RSDs in order to fulfill their role. Any exception request must be made by VP level or above.
3. Authorized personnel who receive an exception will be provided with an encrypted RSD that will protect Agency sensitive data and PHI. The encrypted RSD shall be used for Agency purposes only. Lending out the encrypted RSD to anyone is strictly prohibited.
4. Authorized personnel must sign a statement acknowledging their responsibility to protect the RSD and the data it stores.
5. Authorized personnel who are issued an encrypted RSD will maintain an 8-character password with at least three of the following: upper case letters, lower case letters, digits and special characters.

6. Authorized personnel must not transfer PHI from their remote storage device to any other device or organization, unless the following conditions are met:
    a. The authorized personnel is providing required PHI to another covered entity, or
    b. The authorized personnel is providing required PHI to an organization that has a signed Business Associate Agreement (BAA) with the Agency, or
    c. The authorized personnel is providing required PHI to authorized governmental agencies.

B. Authorized personnel shall not transfer Agency-related sensitive or confidential data to any other device or organization unless it has been authorized from a Director level or above.

7. A list of authorized personnel granted an exception for an RSD will be reviewed annually by the executive team members to whom they report.
8. If an RSD is lost or stolen, it must be reported immediately to the IT Department.

VI. <u>Email</u>

1. Health Care for the Homeless maintains an electronic mail (email) system to support the mission of the Agency. All data and information sent and received through the agency email system including, but not limited to, messages, attachments, photos, calendar appointments, reminders, etc. are the property of the Agency and may be monitored at any time without the permission of authorized personnel. Health Care for the Homeless retains the right to review or audit all information sent or received via the Agency email system.
2. Personal Health Information (PHI) must not be sent to any external email address outside of the Agency unless it is encrypted. This includes attachments or screen shots containing PHI and PHI in the text body of an email. Users must use caution when sending email outside of the Agency. Email features like auto-fill make it easy to send or forward an email to the wrong address, which can result in sharing of PHI outside the Agency, which is considered a breach under HIPAA. Authorized personnel are expected to verify that all recipients have an Agency email address, and have prior knowledge the PHI is being sent.
3. If PHI must be transmitted electronically to an external entity, authorized personnel must contact the IT Department or Health Informatics Department prior to sending the information.
4. The email system is for Agency use only. Any personal messages sent or received are subject to monitoring and are property of the Agency. Authorized personnel have no reasonable expectation of privacy with respect to any communications conducted over Agency email. Even deleted messages and attachments are accessible by administrators.
5. All employees must act as stewards of Agency resources. It is prohibited to send, forward or reply to chain letters, junk mail, jokes, multimedia files (such as videos or songs) and executable files.
6. Authorized personnel shall not use the Agency email to send, upload, receive, download any copyrighted materials, trade secrets or proprietary information without the appropriate authorization of the owner of this material.
7. The Agency email system shall not be used to create or foster a hostile environment. This includes sending, forwarding or replying to emails that contain offensive language, including messages 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.

8. The Agency email system shall not be used to solicit donations for personal charities, advertise or run a business, or solicit for commercial purpose, 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 agency's mission.

VII. <u>Internet</u>

1. Health Care for the Homeless provides access to the internet for use by authorized personnel. Providing this access represents a considerable investment on the part of the Agency. Access to the internet is for the benefit of the Agency and shall be used primarily to transact Agency business.
2. The Agency 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 Agency maintains the right to identify and associate the content downloaded or accessed with the user ID of all authorized personnel.
3. The Agency 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. Authorized personnel must contact their supervisor or the IT Department if they are required to transmit or receive PHI.
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. Use of the internet or any Agency 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 purpose 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 Agency's mission.

VIII. <u>Software and Applications</u>

1. The Agency 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 Centricity, Raiser's Edge or ADP. These applications may be hosted on a server in our data center or on a server in the cloud.

2. The principal of least privilege will be used to provide authorized personnel with access to hosted applications. This means that employees will be provided access to only the applications and features they need to perform their roles. E.g., only employees that need access to our clients' PHI will be provided with access to the Centricity Practice System.
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 Agency-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 Agency will maintain an inventory of all COTS software and will comply with license quantities and distribution requirements.
7. Any software or scripts created by authorized personnel to support the Agency mission becomes the property of the Agency.
8. Authorized personnel are prohibited from downloading software onto Agency-managed desktops and laptops. If authorized personnel needs software to perform their role, they must open a tech support ticket.

Signed by:
Position:
Date:
Reviewed annually

[i] https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/