ID:	C, SH, PC	Monitor:	Risk Management Officer
Updated By:	Nancy Headley	Reviewed By:	Nancy Headley
Last Update Date:	03/02/2022	Review Date:	03/02/2022

Risk Management

Policy:

Risk management is defined as the identification, assessment, and prioritization of risk followed by the application of resources to minimize, monitor, and control the probability or impact of unfortunate events.

Serenity Hospice and Home (SH&H) is dedicated to the identification, assessment, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities.

SH&H Administration, in consultation with the Information Technology (IT) vendor and supported by other key departments, is responsible for the drafting and overall management of the program. The Risk Management Officer, with support from the IT vendor, is responsible for the maintenance of the Risk Management program as well as conducting, evaluating, and documenting all drills and actual events.

The Risk Management Plan (RMP) will be reviewed with each new employee upon hire and with the entire staff once a year at the annual meeting. The entire plan is reviewed by the Risk Management Officer and IT vendor on an annual basis to assess the goals and objectives, scope, performance, and effectiveness of the plan. Recommendations for future action are also included in the annual review. This Risk Management Plan can be found electronically on the o-drive (policies/risk management plan/RMP), and in the Employee Section of the Members Area on www.serenityhospiceandhome.org. The hard copy RMP manuals are located at the nurses' station and in the administration building outside of the HR office.

Table of Contents

Risk Management Communication

The “Order of Authority” is utilized to maintain continuous leadership and authority in key positions as defined in the Emergency Preparedness Plan (EPP).

In the event of a major breach or other incident which could potentially result in negative publicity for the organization, no staff member, other than the Authority, shall speak on behalf of the organization. If the Authority is assumed by anyone other than the CEO, the Authority will immediately notify the CEO as soon as possible. The CEO will notify the Board President of the extent of the breach or incident as soon as possible.

Under no circumstances should any employee who has not been authorized by the CEO or the Board President speak on behalf of the organization to any media regarding any security breach or incident.

In the event of a major incident that would likely be harmful to the public image of the organization, a Public Relations Liaison will be contracted to handle all media activities.

Antivirus

SH&H promotes a secure computing environment for all employees, patients, and affiliates. Computing platforms (including but not limited to: desktop workstations, laptops, tablets, servers and network devices) are integral elements in the operations of SH&H and as such are vital to the organization’s mission. This policy will help ensure all vulnerable computing platforms on campus are guarded against vulnerabilities and protected by antivirus software at all times.

This policy describes the measures taken by SH&H to counter computer viruses and identifies the responsibilities of individuals, departments and the Information Technology (IT) vendor in protecting SH&H against viruses and other vulnerabilities.

The principal concern of this computer virus protection policy is effective and efficient prevention of all network virus outbreaks and network security attacks involving all computers associated with SH&H. The primary focus is to ensure SH&H-affiliated users (staff) are aware of and take responsibility for the proper use of the SH&H-provided and IT supported virus protection software.

This policy is intended to ensure:

- the integrity, reliability, and good performance of SH&H computing resources;
- the resource-user community operates according to a minimum of safe computing practices;
- the SH&H licensed virus software is used for its intended purposes; and
- appropriate measures are in place to reasonably assure this policy is honored.

1. Any computer, server or network device (except cell phones) that are connected to the SH&H staff network (HP Aruba Ethernet and Netgear Wi-Fi Router (“netgear-ap” WiFi SSID) infrastructure appliances) shall be protected by antivirus software for protection against malicious electronic intrusion.

   Devices connected to the “charity” (the guest Wi-Fi) are isolated from the "netgear-ap” (the staff Wi-Fi network).

2. All computers or networked devices shall have applicable operating system and application security patches and updates installed prior to initial connection to the network. Software patching is managed by the Information Technology vendor.

3. The IT vendor is solely responsible for the purchase of antivirus software for all SH&H computers, servers, or any Windows based OS network device connected to the SH&H staff network. Employees are prohibited from purchasing any antivirus software for any SH&H computer systems, unless given permission by the IT vendor.

4. No software shall be loaded on to a computing device owned and supported by Serenity Hospice and Home without permission of the CEO.

5. Tablets and smart phones security configurations are not to be altered without permission from the IT vendor.

Information Technology (IT) Vendor Responsibilities:

1. The IT vendor purchases antivirus software and licenses for all Windows based computer systems.

2. Installation of the antivirus software is required on ALL SH&H owned computers and laptops in the facility. This product is provided to all SH&H computers, servers, and network devices. Product is configured to automatically receive virus definition and program updates from a centralized-managed server.

3. The Information Technology vendor keeps the antivirus products it provides up to date utilizing centralized policy management. This allows the Information Technology vendor to automatically deploy new virus definitions to workstations.

Containment of Virus incident:

1. If an employee suspects their computer or device may have been infected with a virus the Authority or IT vendor should be notified immediately (see EPP – Authority).

2. The IT vendor will take appropriate action to contain virus infections and assist in their removal. In order to prevent the spread of a virus, or to contain damage being caused by a virus, the IT vendor may remove a suspect computer from the network or disconnect a segment of the network.

3. The IT vendor will provide advice to individuals on the function and installation of the antivirus products and on virus protection. This includes advice on virus hoaxes, including occasional circulars on specific hoaxes.

4. The IT vendor will assist individuals with recovery from viruses. This includes advice on containment to stop the spread, help with removing viruses, taking note of information about the incident, and advising on how to prevent a recurrence.

Individual Responsibilities:

1. All administrators and staff are responsible for taking suitable measures to protect against virus infection and failure to do so may constitute an infringement of this policy. A user who allows their computer to become infected puts their own work and other people's computers and data within SH&H and beyond at risk.

2. Administrators and staff must have antivirus software installed and ensure it is working. Anyone not sure if his or her computer system has the latest or updated antivirus software should contact his or her immediate supervisor.
3. Staff should notify the Authority immediately if they suspect they may have a computer virus.

Antivirus at Home

It is recommended that in addition to the above, it is best practice to:

1. Have antivirus software installed on all computer systems.

2. Update virus protection software frequently (recommend automatic setup).

3. Install any recommended security patches for the operating system and applications that are in use.

Breach Notification

A breach is defined as the acquisition, access, use, or disclosure of protected health information (PHI) in a manner not permitted, which compromises the security or privacy of the PHI. Final breach notification regulations, effective for breaches discovered on or after September 23, 2009, implement section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act and finalized by the Omnibus Bill, effective March 23, 2013, by requiring HIPAA covered components and their business associates to provide notification following a breach of ***unsecured*** PHI.

Some examples of breaches include the following:

- Lost or stolen laptop, desktop, iPad, mobile phone, flash drives, etc.
- Misdirected fax of email
- Nursing bag containing PHI
- Viewing displayed PHI by an unauthorized individual.

The regulations, developed by the Office for Civil Rights, require HIPAA covered components to promptly notify affected individuals of a breach of their PHI, as well as the Health and Human Services (HHS) Secretary and the media in cases where a breach affects more than 500 individuals. Breaches affecting fewer than 500 individuals will be reported to the HHS Secretary on an annual basis. The regulations also require business associates of covered components to notify the covered component of breaches at or by the business associate or its workforce, agents or subcontractors. SH&H has designated the Risk Management Officer as the HIPAA Privacy Officer. All HIPAA Privacy Officer References below are, in actuality, performed by the Education Manager/Compliance Officer. It is the policy of SH&H to comply with these regulations and, therefore, the following procedures have been implemented to assure compliance.

1. **Steps for Notifying HIPAA Administration**

    a. The following procedures are in place for reporting uses and disclosures in violation of the HIPAA Privacy Rule to the HIPAA Privacy Officer, by SH&H's covered components or business associates.

        i. The inadvertent disclosure of PHI will be recorded on the HIPAA PHI Disclosure Logs (located at the office of the HIPAA Officer) and copies will be provided to the HIPAA Privacy Officer.

        ii. The business associates of SH&H's covered components are required by the Business Associate Agreement, to notify SH&H of any unauthorized use or disclosure by the business associate or its workforce, agents or subcontractors that violates the HIPAA Privacy or Security Rules and the remedial action taken or proposed to be taken with respect to the use or disclosure.

2. **Timeliness of Discovery:**

    a. A breach shall be treated as discovered by a covered entity, business associate or its subcontractor, as of the first day on which such breach is known or should reasonably have been known to the covered entity, business associate or its subcontractor, not when the investigation of the incident is complete, even if it is initially unclear whether the incident constitutes a breach, as defined in the rule.

3. **Breaches Reported by a Business Associate:**

    a. If a breach of unsecured PHI information occurs at or by a business associate or its subcontractor, the business associate must notify SH&H's HIPAA Privacy Officer following the discovery of the breach. A business associate must provide notice to SH&H without unreasonable delay and no later than 24 hours from the discovery of the breach. To the extent possible, the business associate should provide the HIPAA Privacy Officer with the identification of each individual affected by the breach as well as any information required to be provided by SH&H in its notification to affected individuals. Also, provided by the business associate is a description of the cause and action plan for preventing reoccurrence. If the breach was discovered by the business associate's subcontractor, the subcontractor will notify and provide the pertinent information to the business associate and the business associate will then provide notification to SH&H.

    b. With respect to timing, if a business associate is acting as an agent of SH&H then, the business associate's discovery of the breach will be communicated to SH&H at the time of discovery. In such circumstances, SH&H must provide notifications based on the time the business associate discovers the breach, not from the time the business associate notifies SH&H. In contrast, if the business associate is not an agent of SH&H, then SH&H is required to provide notification based on the time the business associate notifies SH&H of the breach.

4. **Identification of a Breach**.

    a. Breaches can include PHI in any form or medium, including electronic, paper, or oral. When the HIPAA Privacy Officer receives a report of an inappropriate use or disclosure, the Privacy Officer will conduct a risk assessment to determine whether a reportable breach has occurred and then work together with counsel to determine the appropriate reporting requirements.

    b. In the case of a security incident, the HIPAA Privacy Officer will be notified, a risk assessment will be completed by the HIPAA Privacy Officer to determine whether a HIPAA breach has occurred and then the HIPAA Privacy Officer and the CEO will work with Counsel to determine the HIPAA and other legal implications of the incident. If the incident has been determined to be a

HIPAA breach, the HIPAA Privacy Officer will coordinate with the department who owns the data to accumulate the information necessary for reporting.

5. Once a potential breach has been reported to the HIPAA Privacy Officer, the following ***assessment*** will be conducted to determine whether the incident is reportable. An impermissible use or disclosure of PHI is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates there is a low probability the PHI information has been compromised or one of the other exceptions to the definition of breach applies.

    a. Did the potential breach occur on or after September 23, 2009?

    b. Was the PHI secured (encrypted or rendered unusable, unreadable or indecipherable to unauthorized individuals)?

    c. Did the use or disclosure of PHI violate the HIPAA Privacy Rule (including disclosures of more than the minimum information necessary for the intended purpose)?

    d. Does the use or disclosure fall under one of the following exceptions to the notification requirement? The potential breach was an:

        i. Unintentional acquisition, access, or use of PHI by an employee or individual acting under the authority of a covered entity, business associate or their subcontractor (if the act was by an individual acting under the authority of a covered entity or a business associate, in good faith, within the course and scope of employment or professional relationship) and did not result in further use or disclosure.

        ii. Inadvertent disclosure of PHI from one person to another person, both authorized to access PHI at a covered entity, business associate or their subcontractor, at the same facility if the information was not further used or disclosed without authorization. For example, to person's :

            - Working onsite who are not workforce members, such as medical providers with staff privileges.

            - Unauthorized disclosure in which the covered entity had a good faith belief that an unauthorized person to whom PHI was disclosed would not have been able to retain the information (e.g. mailings sent to the wrong individual that are returned as undeliverable, a nurse hands discharge papers for one patient to another patient but retrieves the papers prior to the patient having a chance to read or retain what they saw).

    e. Is there a low probability the PHI has been compromised, based on a risk assessment that considers at least the following factors?

i. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification; For example, was the information involved sensitive in nature? If there were few identifiers, what is the probability that the information could be re-identified?

ii. The unauthorized person who used the PHI or to whom the disclosure was made. For example, is the recipient obligated to protect the privacy and security of the information?

iii. Whether the PHI was actually acquired or viewed (or only the opportunity existed to acquire or view the information).

iv. The extent to which the risk to the PHI has been mitigated. For example, were satisfactory assurances obtained from the recipient that the information will not be further used or disclosed (e.g. confidentiality agreement) or will be destroyed (e.g. with a destruction certificate).

6. **Notification of Individuals:**

The HIPAA Privacy Officer will work with SH&H counsel to determine whether a breach has occurred and what notification requirements may be required for a particular breach.

The covered component who owns the data will be responsible to ensure the required reporting to individuals occurs, with assistance from the HIPAA Privacy Officer. Reports to Health and Human Services will be made and documented by the HIPAA Privacy Officer.

7. **Methods of Notice:**

a. SH&H will provide breach notice to the individual in written form by first-class mail at the last known address of the individual.

b. Where the individual affected by a breach is a ***minor*** (a person under the age of 18) or otherwise lacks legal capacity due to a physical or mental condition, notice will be provided to the parent or other person who is the personal representative (e.g. power of attorney or guardian) of the individual.

c. If the individual is known to be ***deceased***, notice will be sent to the last known address of the next of kin or personal representative, if this contact information is known and up-to-date.

8. **Substitute Notice:**

a. If SH&H does not have sufficient contact information for some or all of the affected individuals, or if some notices are returned as undeliverable, SH&H will provide substitute notice for the unreachable individuals. The substitute form of notice will be reasonably calculated to reach the individuals for whom it is being provided. If there are ***fewer than 10 individuals*** for whom SH&H

has insufficient or out-of-date contact information to provide the written notice, SH&H will provide substitute notice to such individuals through an alternative form of written notice, by telephone, or other means, such as posting a notice on SH&H's web site.

b. If SH&H has insufficient or out-of-date contact information for ***10 or more individuals***, then SH&H will provide substitute notice through either a conspicuous posting for a period of 90 days on SH&H's home page or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside. SH&H will provide a toll-free phone number in the notice, active for 90 days, where an individual can learn whether their unsecured PHI may be included in the breach

c. If SH&H uses a hyperlink on the home page to convey the substitute notice, the hyperlink will be prominent so it is noticeable given its size, color, and graphic treatment in relation to other parts of the page, and it will be worded to convey the nature and importance of the information to which it leads.

9. **Content of the Notice:**

a. In addition to HIPAA breach notification, if other notifications or actions are required, such as those associated with social security numbers or where Gramm-Leach-Bliley Act of 1999 (GLBA) red flag procedures apply, the HIPAA Privacy Officer and SH&H counsel will coordinate actions to be taken. The HIPAA breach notification will include, to the extent possible, the following elements:

i. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

ii. A description of the types of unsecured PHI that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved). Covered entities should not include a listing of the actual PHI that was breached and should avoid including any sensitive information in the notification itself (e.g. SSN or credit card numbers);

iii. Any steps individuals should take to protect themselves from potential harm resulting from the breach;

iv. A brief description of what the covered entity involved is doing to investigate the breach, mitigate the harm to individuals, and to protect against any further breaches; and

v. Contact procedures for individuals to ask questions or learn additional information, which must include a toll-free telephone number, an e-mail address, Web site, or postal address.

b. SH&H is permitted to send one breach notice addressed to both a plan participant and the participant's spouse or other dependents under the plan who are affected by a breach, so long as they all reside at a single address and the covered entity clearly identifies on the notice the individuals to which the notice applies. Further, where a plan participant (and/or spouse) is not the personal representative of a dependent under the plan, a covered entity must address a breach notice to the dependent himself or herself.

10. **Health Information Organizations**

When multiple covered entities participate in electronic health information exchange and there is a breach of unsecured PHI at a Health Information Organization (HIO), the obligation to notify individuals of the breach falls to the covered entities. In such circumstances, it may be necessary for the HIO to notify all potentially affected covered entities and for those covered entities to delegate to the HIO the responsibility of sending the required notifications to the affected individuals. This would avoid the confusion of individuals receiving more than one notification about the same breach.

11. **Timeliness of Notice:**

SH&H will make the individual notifications as soon as reasonably possible after the covered entity takes a reasonable time to investigate the circumstances surrounding the breach in order to collect and develop the information required to be included in the notice to the individual. Notifications to individuals must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach, except when law enforcement requests a delay. SH&H may provide the required information to individuals within the required time period in multiple mailings as the information becomes available.

12. **Law Enforcement Delay**

A temporary delay of notification is required in situations in which a law enforcement official provides a statement in writing that the delay is necessary because notification would impede a criminal investigation or cause damage to national security, and specifies the time for which a delay is required. In such instances, SH&H is required to delay the notification, notice, or posting for the time period specified by the official. Also SH&H is required to temporarily delay a notification, notice, or posting if a law enforcement official states orally that a notification would impede a criminal investigation or cause damage to national security. However, in this case, SH&H must document the statement and the identity of the official and delay notification for no longer than 30 days, unless a written statement meeting the above requirements is provided during that time.

13. **Media Notice:**

If SH&H experiences a breach affecting more than 500 residents of a State or jurisdiction, in addition to notifying the affected individuals, will provide notice to prominent media outlets serving the State or jurisdiction. SH&H will likely provide this notification in the form of a press release to appropriate media outlets serving the affected area. Like individual notice, this media notification will be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and will include the same information required for the individual notice.

14. **Notice to the HHS Secretary:**

a. In addition to notifying affected individuals and the media (where appropriate), SH&H will notify the HHS Secretary of breaches of unsecured PHI. The HHS Secretary will be notified by SH&H of breaches using the HHS web site, filling out and electronically submitting a breach report form (www.HHS.Gov).

b. If a breach affects 500 or more individuals, SH&H will notify the HHS Secretary without unreasonable delay and in no case later than 60 days following a breach.

c. For breaches of unsecured PHI involving less than 500 individuals, the HIPAA Privacy Officer will maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification required for breaches discovered during the preceding calendar year, not occurred in the previous calendar year, in the manner specified on the HHS web site.

15. **Follow-up with a Business Associate**

When a breach has been reported by a business associate, the HIPAA Privacy Officer, as appropriate, will obtain from the business associate a written description of the cause of the breach and action plan for preventing reoccurrence. The HIPAA Privacy Officer will follow up with the business associate to receive assurances the action plan has been completed by either the business associate or its contractor, depending on where the breach occurred. The follow up will be documented and included with the incident documentation.

Business Associate Agreements

Under the U.S. Health Insurance Portability and Accountability Act of 1996, a HIPAA business associate agreement (BAA) is a contract between a HIPAA covered entity and a HIPAA business associate (BA). The contract protects personal health information (PHI) in accordance with HIPAA guidelines.

1. As a HIPAA covered entity, SH&H enters into a BAA with all HIPAA business associates.
2. Entities requiring a BAA are specifically marked in the Vendor Contracts and Services Contracts Spreadsheets, as reflected in the Contract Management Policy (SH&H Policies & Procedure Manual).

Computer Software

Only SH&H approved software is allowed to run/access the SH&H staff network. Software brought in by staff must be qualified by the CEO or the IT vendor.

Computer Users

1. All staff computer users comply with our Mobile Devices and Computer Use Policy (SH&H Policies & Procedure Manual).
2. Password saving on any application that accesses patient records or employee information is prohibited.
3. Employees are prohibited from sharing their passwords or posting them near their workstations.
4. Strong network passwords are enforced and are changed every 90 days. See Logical Security section for password complexity components.

Disclosure of PHI to Patient/POA

Per the HIPAA Notice of Patient Privacy, section Right to Inspect and Copy, located in the Patient Handbook and Caregiver Training Guide, the patient/POA is notified of their right to request PHI in writing. The information will be either hand delivered, mailed, or sent via secured fax.

Disposal of Protected Health Information

The HIPAA Privacy Rule requires covered entities apply appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information (PHI), in any form (45 CFR 164.530 (c)). Covered entities must implement reasonable safeguards to limited incidental, and avoid prohibited, uses and disclosures of PHI, including in connection with the disposal of such information. SH&H disposes of PHI using the following procedures:

1. PHI paper records, including data sheets from recent decedents, are shredded so PHI is rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed.

2. Families are instructed on the methods recommended by the Drug Enforcement Administration (DEA), October 9, 2014, and the Office of National Drug Control Policy (ONDCP), October 2009, on available options for disposing of unused medications. This information is documented in the Patient Handbook and Caregiver Training Guide which is given to a patient/family member upon admission to hospice.

3. Medications for patients who received care in the Serenity Home are disposed of according to the Office of National Drug Control Policy (ONDCP), as defined in the Disposal of Medications in Serenity Home Policy (SH&H Policies & Procedure Manual).

4. Laptops no longer in use are turned over to the IT vendor to be "cleared/wiped" as follows:

    a. All programs associated with the Hospice are removed.

    b. If a retail copy of Office installed, it is uninstalled.

    c. If the laptop is part of our Domain, it is reverted back to a workgroup.

    d. All user profiles are removed.

    e. All data is removed.

    f. Laptop is recycled

5. Tablets no longer in use are destroyed by submersion in water.

6. Employees are instructed to reset their personal phones to factory settings prior to trading it in for an upgrade. If they are unsure of how to do this, the Director of Administration and/or the CFO is available to assist.

Electronic Medical Records (EMR)

1. SH&H uses a vendor supported EMR. The security, back-up procedures, and disaster recovery information on the EMR can be found in Section 3: Security Risk Assessment.

2. Passwords for the EMR are changed every 90 days.

    a. The EMR System Administrator will force password changes by going into Agency, Security, and setting the parameter to 90 days for each user.

    b. Every 90 days a user will be prompted to change his/her password.

3. The system automatically times out after 30 minutes of inactivity.
4. Employees are instructed not to leave a patient record open when they walk away from their workstation.
5. Community nurses and CNAs access the EMR from tablets and must use a security code to gain access to applications on the device.

Employee Termination

1. Upon termination from employment at Serenity Hospice and Home the Employee Termination Checklist form will be completed within 48 business hours (sent out to management team via email by the HR Director) and a notification will be put on a group message to all employees by either the CEO or HR Director that the individual is no longer with Serenity.

Facility Security

1. To help insure the safety of staff, patients, and visitors, cameras are present at all entrances/exits of Serenity Home. When doors are locked during off-hours, the cameras allow for staff to view a visitor before allowing entrance to the facility.
2. A camera also exists over the controlled substance medication storage area to help identify an individual should drugs be removed from the storage area inappropriately.
3. A monitor displays camera activity at the nurse's station 24-hours a day. Once a month a random review of activity that happened on a prior date and time is performed to insure the system is functioning properly (O:\Policies\Risk Management Plan\Camera Review Spreadsheet.xls)
4. Front door access to the Serenity Home will be locked each evening at dusk. Visitors must press a button to alert staff of their desire to access the facility. A voice box exists for communication between the visitor and staff.
5. Patient room patio doors are equipped with alarms that signal the nurse's station whenever a patio door is opened.
6. Two silent alarm buttons are located at the nurse's station that signals Per Mar Security to contact local police.
7. Back door access to the Serenity Home, the mechanical room, the IT server room, and the front and side door of the administration office building are monitored by a card reader. All employees have a swipe card to allow entrance into the buildings. Access to the IT server room is restricted to those with a need for access. Swipe cards are distributed / managed by the Human Resources Director.

8. Patients / visitors are not allowed in secured areas where patient information is stored (patient charts, fax machines, etc.) These areas are locked when employees are not present.

9. Patient charts are locked in secured cabinets/drawers when not in use. When possible, office doors are locked in secure areas when employees are not present.

Firewalls & Network Security

1. SH&H enterprise IT infrastructure sits behind a Sonicwall TZ300 Internet appliance whose firewall separates the Local Area Network (LAN) and WiFi from the Internet.

2. The Sonicwall logs inbound and outbound traffic. Intrusion prevention (detection) is set for high and medium level (detect and prevent) on the Sonicwall device. Gateway antivirus and Gateway malware have also been enabled. The Information Technology vendor proactively searches out intrusions. The Firewall has a one-year rolling log and Sonicwall Analytics is installed to capture the log and create reports. The reports are reviewed on a regular basis for intrusion alerts. Trends are reported to the information technology vendor and blocks may be put into place for repeat attempters.

3. The Firewall operates with stateful reassembly-free deep packet inspection that examines traffic simultaneously across all ports. The Sonicwall also provides VPN access, and other functionality.

4. Maintenance of the Sonicwall device, firmware updates, images of settings, etc., is performed by the Information Technology vendor.

5. All SH&H computing devices (Windows, Android, Apple, etc.) will have their firewalls and indigenous security systems turned ON unless otherwise instructed by the Information Technology vendor.

Hazard Communication

The following written hazard communication program has been established to protect employees of SH&H against exposure to hazardous chemicals in the workplace. The Risk Management Officer is responsible for managing all aspects of this program, and should be contacted with any questions or concerns.

1. **List of Hazardous Chemicals**
   SH&H will maintain a list that identifies current hazardous chemicals present in the workplace, and this list will be periodically reviewed and updated. The product identifier for each chemical on the list can be easily cross-referenced with the product identifier on its label and on the safety data sheet. This list can be found at: O:\Policies\Risk Management Plan\Hazardous Chemical List.

2. **Identification of Containers**
   All hazardous chemical containers used will either have the original manufacturer's label for the product or workplace labeling that includes the combination of signal words, hazard statements, and pictograms that provide general information regarding the hazards of the chemical. Any employee who transfers hazardous chemicals into portable containers (such as bottles, cans, spray bottles, etc.) will ensure the containers are appropriately labeled and the contents identified.

3. **Safety Data Sheets**
   The distributor or supplier of a chemical product is required to provide a Safety Data Sheet (SDS) to the purchaser. The SDS contains specific, detailed information about the physical, health, and other hazards of the chemical(s) within the product. These are readily available to all employees and can be located in 3-ring binders at the nurses' station in the Serenity Home.

   Whenever an employee is ordering a new chemical-based product, they are required to notify the Risk Management Officer so that the corresponding safety data sheet can be obtained prior to use.

   The safety data sheets will be periodically reviewed and updated. If an employee is unable to locate an SDS sheet they should contact the Risk Management Officer for assistance.

4. **Training**
   SH&H will provide employees with information on the OSHA hazard communication standard and also the location of this written hazard communication program, the list of hazardous chemicals, and the safety data sheets.

   Training may be provided either on-the-job, in a classroom setting or through on-line training, prior to exposure to any hazardous materials, and will include the following topics:

   - An overview of the OSHA hazard communication standard.
   - The location and a review of the SH&H written hazard communication plan.
   - The list of hazardous chemicals in the workplace.
   - The location and explanation of the Safety Data Sheets.
   - How to be protected from exposure to these hazardous chemicals through safe work practices and personal protective equipment.

   Prior to introducing a new chemical hazard into the work area, each employee in that work area will be given information and training as outlined above for the new chemical hazard.

5. **Non-Routine Hazardous Tasks**
   Tasks not done on a routine basis, that may expose employees to hazardous chemicals, will be handled with specific pre-task training. SH&H will evaluate the hazards of these non-routine tasks and provide additional training to employees. They will be informed about the specific hazards of the chemical and how to control exposure through the use of personal protective equipment. Employees in the affected work area will be notified of when these non-routine tasks are scheduled to be performed.

6. **Contractors**
   Any contractors working in the SH&H facilities will be informed where to locate the safety data sheets for hazardous chemicals used within the facility. If the contractor is performing work on behalf of SH&H that utilizes a hazardous chemical, they need to provide a safety data sheet for that product.

Infection Control

Effective measures have been developed to identify, control, and prevent infections. The Quality Assessment and Performance Improvement Council (QAPIC) oversees the Infection Control program per the Infection Control Policy (SH&H Policies & Procedures Manual).

Logical Security

1. SH&H staff network has two means of access, cabled Ethernet component and two wireless WiFi SSID systems.
2. Users access to the SH&H server data is restricted on a need to know basis. Server resources are split into the following functional groups; Nursing, Admin, Admin2, Social Services, Human Resources, etc. Users are assigned to groups as needed.
3. Users log into the network with a Username and Password. The password policy is such that User Passwords will be required to change at a minimum interval of every 180 days. If a password is entered incorrectly three times in a row, access is disabled. The complexity requirements for passwords are:
   - Be at least 10 characters in length
   - Contain characters from three of the following four categories:
     - English uppercase characters (A through Z)
     - English lowercase characters (a through z)
     - Base 10 digits (0 through 9)
     - Non-alphabetic characters (for example, !, $, #, %)
   - May not contain all or part of a user’s username or ID
   - May not be based on personal information such as name, birthday, address, phone number, etc.

- May not be based on company name, season, or geographic location
- May not be used for any other account on any other information system
- May meet or exceed Client's regulatory requirements
- May not be found in the dictionary
- Complexity requirements are enforced when passwords are changed or created.

4. SH&H WiFi has two separate SSID (WiFi systems). One is for public use having its own separate, isolated, IP subnet, the other WiFi SSID is for staff, it having the same IP subnet as the cabled network system but differing from the public WiFi.

5. The WiFi system is based upon a Netgear WC7520 controller. The software running on this system is from Juniper Systems, considered "the best in the industry." The Netgear controller is also a firewall, between our "in house" WiFi and our "guest" WiFi.

6. The IT vendor maintains the Netgear WiFi Controller (firmware updates, etc.)

Medical Gases

The safe handling and storage of medical gases is done in a manner consistent with the Food and Drug Administration, the Department of Transportation, and the Occupational Safety and Health Administration laws and regulations, as reflected in the Oxygen Administration and Storage Policy (SH&H Policy & Procedure Manual).

Mobile Devices (Cell Phones, Tablets, Bring Your Own Device (BYOD))

SH&H provides every clinician, social worker, and other key personnel with a mobile device, which is intended primarily for business use. Employees using mobile devices are accountable for behaving professionally, ethically, and responsibly. Whether at SH&H, at home, or elsewhere, employees must comply with the organization's Mobile Device Policy. Employees are expected to adhere to the Mobile Device Policy 24-hours a day, 365-days a year (SH&H Policies & Procedures Manual). Violations of the organization's Mobile Device Policy, whether they occur on SH&H time or the employee's own personal time, will result in disciplinary action, up to and including termination. All employees are required to adhere to the following rules, policies, and procedures.

Mobile devices include, but are not limited to, mobile phones, cell phones, laptops, and tablets.

HIPAA Compliance

1. When using mobile phones/devices (personal or employer provided), employees must comply fully with HIPAA guidelines, as well as SH&H rules governing the security, privacy, and retention of patient's protected health information (PHI) and electronic protected health information (ePHI).

2. HIPAA guidelines and the rules and procedures set forth in this Mobile Device Policy apply to email, text messaging, instant messaging, and other short message service (SMS) tools including WhatsApp and iMessage among others.

3. When using their own smartphones for work purposes, employees must agree to have third-party software installed, such as a telehealth or a secure messaging application.

4. Employees are forbidden to use unencrypted email/text messaging to communicate with other healthcare providers, medical professionals, business associates, and other HIPAA-covered entities. Adhere to our Protected Health Information Policy and the HIPAA Security Rule when emailing/texting HIPAA-covered entities.

5. Do not access, view, transmit, post, download, print, duplicate, or share ePHI/PHI without authorization.

6. Do not disclose ePHI/PHI to unauthorized individuals. This includes data related to patients' health status, medical care, treatment plans, and payment issues. Unauthorized exposure of ePHI/PHI is a violation of the HIPAA and could trigger legal claims or regulatory penalties.

7. Do not use mobile devices to photograph, videotape, or otherwise copy ePHI/PHI.

8. Do not alter, destroy, or otherwise diminish the integrity of ePHI/PHI.

9. Do adhere to HIPAA's Security Rule and Privacy Rule, as set forth in our Protected Health Information policy.

10. Do adhere to SH&H's Retention of Clinical Records, governing the retention and disposition of ePHI/PHI.

11. Texting patient information, including orders, is only permitted via Serenity's secure messaging application. Sending this information via normal cell phone texting apps is strictly prohibited. If use of the secure messaging application is not possible, sending the message of "Please call me" via regular cell phone texting is allowable. All staff will inform the CEO and/or the Education Manager/Compliance Officer if a text with PHI is received by them.

12. When not in use, mobile devices must be stored in a secure location for protection from loss or theft.

13. When travelling, mobile devices should not be placed in checked baggage and should remain with the traveler, or stored in a secure location, at all times.

Content Rules

Always adhere to SH&H's content rules. Whether you are engaged in a phone conversation, sending a text/email, or leaving a voicemail message, you must always use a professional tone and business-appropriate language. Whether you are talking, texting, emailing, or otherwise communicating via mobile device, never use language that is obscene, vulgar, abusive, harassing, profane, discriminatory, sexually suggestive, intimidating misleading, defamatory, bullying, or otherwise offensive, objectionable, inappropriate, or illegal. Jokes, disparaging remarks, and inappropriate comments related to ethnicity, race, color, religion, sex, age, disabilities, physique, sexual orientation, and sexual preference are prohibited by law and SH&H policy.

Distracted Driving

It is against SH&H policy (and illegal) for employees to text while driving. Pull off the road and stop driving if you need to send a text message, compose email, check messages, or post content. Additionally, making or receiving phone calls while driving must be done using "hands free" Bluetooth technology. If someone lacks that capability they must pull off the road for a call.

Personal Use

Employees may not use SH&H systems, SH&H accounts, SH&H provided mobile phones, or other SH&H-owned mobile devices to solicit for any purpose, campaign for political candidates, espouse political views, promote religious causes, or advertise the sale of merchandise.

Passwords

Employees are issued passwords by the Office Manager for the electronic devices issued to them by the organization (i.e.- tablets, IPad, cell phones). Only authorized personnel are permitted to use passwords to access employees' electronic content without consent. Misuse of passwords, the sharing of passwords with non-employees, the unauthorized use of another employee's password, or failure to provide the Office Manager with current passwords will result in disciplinary action, up to and including termination.

Privacy

Privacy does not exist when using SH&H's computer system, telecommunications system, mobile phones, or other devices including desktop computers, laptops, and mobile devices among others. Employees are required to allow SH&H to examine company devices if necessary. Confidential SH&H, patient, staff, or personal information never should be sent via email or text without the understanding that it could be intercepted. This includes the transmission of electronic protected health

information (ePHI), intellectual property, financial information, Social Security numbers, personnel records, proprietary data, trade secrets, and other confidential material.

Do not use a mobile phone or other mobile device to discuss SH&H business or patient matters in any public setting in which your conversation could be overheard or your messages read by prying eyes. Not every location is right for a business-related mobile phone conversation. Always locate a secluded spot in which to conduct SH&H or patient business via your mobile device.

Do not mention passwords, user names, account numbers, financial data, patients, PHI, or other confidential or proprietary SH&H, patient, or personal information if there is any chance that your phone conversation could be overheard. An overheard one-sided conversation may be all a malicious party needs in order to gain access to valuable business, patient, or personal data. Don't assume your public mobile phone conversation is "safe" just because you don't mention SH&H by name. If you wear or carry an item that features the SH&H logo, your name or our business address, a third party may put two and two together and identify the organization, simply by overhearing your conversation.

Photos & Videos

Employees are prohibited from using personal or SH&H-provided mobile phones or other mobile devices to take, transmit, acquire, download, upload, print, or copy photos or videos that are related to SH&H business. Prohibited photos and videos include, but are not limited to, photos/videos of patients and their families/friend; "funny" or embarrassing images of any internal or external party; photos or videos of SH&H buildings (internal and external), offices, facilities operations, products, services, confidential data, and internal documents. Do not used an SH&H-provided or personal mobile device to take, transmit, acquire, download, upload, print, or copy photos or videos of coworkers, executives, patients, family members, business associates, suppliers, or any other third party without getting the express permission of your subject and SH&H management.

Netiquette Rules

Adhere to the rules of netiquette, or electronic etiquette. Do not distract others by engaging in unnecessary, loud, or otherwise excessive mobile phone chatter. Turn off all SH&H-provided and personal mobile devices during business-related meetings, seminars, conferences, luncheons, dinners, receptions, brainstorming sessions, and any other situation in which a ringing phone is likely to disrupt proceedings or interrupt a speaker's or participant's train of thought. Don't assume that texting is any less annoying or distracting than talking. If a pressing business matter requires you to check email or transmit text messages during a meeting or other business gathering, leave the room, briefly, to-do so.

Policy Violations

Any violation of this Mobile Device Policy (or any other employment policy) may result in disciplinary action, up to and including termination.

Patient Charts

1. Active patient paper charts are kept in a locked file cabinet when not in use.
2. Paper charts of decedents are stored in a locked room for two months. After two months the paper chart is scanned into eFileCabinet (Secure Cloud Storage) and the paper charts are shredded.

Phishing

Phishing is the fraudulent attempt to obtain data such as usernames, passwords, account details, or other sensitive information through an electronic communication such as text or email that is disguised to look as though it comes from a trusted source. The message itself will often tell a story to trick the individual who received it into either opening an attachment or clicking on a link.

Phishing is also a threat to the confidentiality, integrity, and availability of electronic protected health information (ePHI) and is covered under the administrative requirements of the HIPAA Security Rule, specifically 45 C.F.R. 164.308.(a).(5).(i), that requires security awareness training to be provided.

1. **Indicators of a potential phishing communication**:
    a. Generic greeting. Rather than being addressed specifically to the recipient, the message starts with a generic greeting such as “Dear Sir or Madam” or “Dear Account Holder.”
    b. Request for account or personal information. A financial institution, credit agency, or public agency will never ask someone to provide their account number, social security number, or pin code by email. Never provide this information in response to an email.
    c. Call for immediate action. Phishers want people to act quickly without thinking. They will make the situation appear urgent such as:
        i. Say they’ve noticed suspicious activity or log-in attempts.
        ii. Request information to avoid having your account suspended.
        iii. Claim there is a problem with your account or with payment information.
        iv. Entice you with a discount offer, coupon, or promised refund.

d. Invitation to view a video or read an article. Phishers will often use current event topics of interest such as celebrities or tragedies to encourage someone to click on their false link.

e. Spelling and grammatical mistakes. Less experienced phishers often send emails containing spelling and grammar mistakes, while more experienced phishers have gotten much better at avoiding these errors.

2. **Steps to protect yourself from phishing**:

    a. Utilize security software on all devices and set preferences for the software to update automatically so it can deal with new threats.

    b. Protect your accounts by using multi-factor authentication. Some accounts offer extra security by requiring two or more credentials to log into the account.

    c. Hovering the mouse over the sender of an email, shortcut link, or file attachment will show you the specific address, path, or file type. This can often reveal an issue that would otherwise be overlooked.

    d. Make direct contact with the sender rather than using any links included on the email. Even if there are no obvious indicators that the communication is a phishing scam, it is prudent to go directly to their website or contact them by a known customer service number.

    e. Never send personal or financial information via email unless a form of email encryption is being used.

    f. Never send a reply to a suspicious email, as that will validate to them that your email address is active.

3. **Steps taken by Serenity Hospice and Home to protect from phishing**:

    a. Security awareness training provided through several mediums.

        i. New hire orientation.

        ii. Annual training.

        iii. Simulated phishing emails with integrated training through the KnowBe4 platform.

    b. Use of firewall technology, anti-virus software, and email spam filters.

4. **What to do if you become the victim of phishing**:

    a. Notify the Risk Management Officer or CEO immediately. Steps will be taken so that the system can be scanned for malware/viruses.

    b. If you are concerned the phishers have your personal information (i.e.- credit card or bank account number, social security number, etc.), go to the IdentityTheft.gov website and take the specific steps listed based on the type of information you lost.

Physical Security of Hardware

1. SH&H Servers, routers, switches, etc. reside in a secure room with fireproof walls and a locked door with card reader access.
2. The server, phone switch, backup devices, WiFi Switch, and Ethernet switch are plugged into outlets that are connected to an uninterruptible power system (UPS) and powered by an emergency generator.

Printers & Fax Machines

1. Printers and fax machines are located in secure areas (i.e. areas where patients and visitors are prohibited).
2. PHI will only be printed on printers that have the ability to secure the print feature to a private mailbox or individual security code. Staff will retrieve printed PHI as soon as possible.
3. Information received or sent by fax will be retrieved from the fax machine as soon as possible.
4. If PHI is found by an employee on a printer or fax, the PHI will immediately be taken to the Clinical Manager or designee.
5. When copiers are returned to vendors or swapped out for new equipment, hard drives will be cleared / wiped.

Protected Health Information (PHI)

1. Employees and/or volunteers of SH&H will not send any emails that contain any patient information using unsecure email. PHI and other secure information may be sent using Serenity's secure, encrypted email system.
2. Charting will be done at the bedside using a laptop or tablet. Travel charts are acceptable (data sheets), but must be locked in the trunk when not directly in sight of a clinician.
3. Travel chart information (data sheets) will be kept to the minimum amount of information necessary.
4. Paper PHI, which is no longer needed, will be put into locked shredding containers and shredded periodically.
5. PHI will not be left unattended at a desk in any form (paper, electronic, flash drive, CD). If working in the EMR it must be shut down before leaving a desk unattended.

6. Faxed PHI will be retrieved as soon as possible and taken to the appropriate destination.
7. PHI sent to a copier to be printed will be sent to a private mailbox or printed with a security code.
8. Laptops, desktops, tablets, mobile devices, copiers, flash drives, CDs or any other medium in which PHI may be stored will be wiped prior to the devices being reused, destroyed, returned to a vendor, etc.
9. The storing of patient health information on a home computer, laptop, tablet, or any other device is strictly prohibited.
10. Staff will notify the Authority of any lost or stolen mobile device or lap top as soon as reasonably possible and follow the Breach Notification policy if applicable.

Ransomware

Ransomware is a type of malware (malicious software) distinct from other malware; its defining characteristic is that it attempts to deny access to a user's data, usually by encrypting the data with a key known only to the hacker who deployed the malware, until a ransom is paid. After the user's data is encrypted, the ransomware directs the user to pay the ransom to the hacker (usually in a cryptocurrency, such as Bitcoin) in order to receive a decryption key. However, hackers may deploy ransomware that also destroys or exfiltrates (the unauthorized transfer of information from an information system) data.

The presence of ransomware (or any malware) on a covered entity's or business associate's computer systems is a security incident under the HIPAA Security Rule. A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. (45 C.F.R. 164.304).

1. Serenity Hospice and Home has the following measures in place to protect against and recover from a ransomware attack:
    a. Server data is backed up nightly and stored in a fireproof safe and is also backed up via Microsoft Imaging Software. Critical workstations are backed up throughout the day. The Electronic Medical Record system is housed offsite and backed up daily (See EPP).
    b. A Security Risk Assessment (SRA) is completed annually.
    c. Access controls have been implemented to limit access to ePHI to only those persons or software programs requiring access.
    d. The Sonicwall Hosted Email Server (HES) email service disallows files with extensions of .pif, .reg, .bat, .scr, .com, .si, and .exe attachments.

e. Local Windows firewall and facility Sonicwall firewall have been turned on, and are managed by Windows Group Policy Object (GPO)

f. Local Windows autoplay has been deactivated, and are managed by Windows GPO.

g. Local Windows file sharing and remote services have been turned off, and are managed by Windows GPO.

h. Users have been trained, and receive ongoing education using KnowB4 software, on malicious software protection, so they can assist in detecting malicious software and how to report such detections, in the following ways:

    i. Being wary of an email from an unknown sender. Word and Excel docs can have malicious macros.

    ii. Watching for odd attachments (hovering the mouse focus over an attachment will display the type of file). “Phishing” allows an email to appear as if it is from a known person. When a phishing email is suspected, the IT vendor is contacted and the email is forwarded if requested.

    iii. Using strong passwords (change forced in the Electronic Medical Record system and the network every 90 days).

    iv. Immediately stopping the internet connection by shutting the system down.

    v. Inform the Authority and notify staff (see EPP - Communication Section).

    vi. Immediate reporting that a link that was clicked on, or a file attachment that was opened, or a website that was visited, once realized that it may have been malicious in nature;

    vii. Reporting an increase in activity in the central processing unit (CPU) of a computer and disk activity for no apparent reason (due to the ransomware searching for, encrypting and removing data files);

    viii. Detection of suspicious network communications between the ransomware and the attackers’ command and control server(s) (this would most likely be detected by IT personnel via an intrusion detection or similar solution).

2. With the assistance of the IT vendor, security incident procedures for responding to a ransomware attack include:

    a. Contacting the FBI Field Office Cyber Task Force (www.fbi.gov/contact-us/field/field-offices) or the US Secret Service Electronic Crimes Task Force (www.secretservice.gov/investigation/#field) immediately to report the ransomware event and to request assistance. These professionals work with state and local law enforcement and other federal international

partners to pursue cyber criminals globally and to assist victims of cyber-crime.

b. Reporting the cyber incident to the US-CERT (www.us-cert.gov/ncas) and the FBI's Internet Crime Complaint Center (www.ic3.gov).

c. If the cyberattack affects medical devices, contact the vendor.

d. Detecting and conducting an initial analysis of the ransomware. This includes:

    i. Determining the scope of the incident to identify what networks, systems, or applications are affected;

    ii. Determining the origination of the incident (who/what/where/when);

    iii. Determining whether the incident is finished, is ongoing or has propagated additional incidents throughout the environment; and

    iv. Determining how the incident occurred (e.g. tools and attack methods used, vulnerabilities exploited)

e. Containing the impact and propagation of the ransomware;

f. Eradicating the instances of ransomware and mitigating or remediating vulnerabilities that permitted the ransomware attack and propagation;

g. Recovering from the ransomware attack by restoring data lost during the attack and returning to "business as usual" operations; and

h. Conducting post-incident activities, which could include a deeper analysis of the evidence to determine if the entity has any regulatory, contractual or other obligations as a result of the incident (such as providing notification of a breach of protected health information), and incorporating any lessons learned into the overall security management process of the entity to improve incident response effectiveness for future security incidents.)

3. If assessment of the incident results in an impermissible disclosure of PHI in violation of the Privacy Rule and a breach, depending on the facts and circumstances of the attack (45 C.F.R. 160.103 and 45 C.F.R. 164.402. the Breach Notification process is followed.

4. For recovery, Serenity Hospice and Home maintains nightly backups and ensures the ability to recover data from backups (see EPP - Server Outage section).

5. Serenity Hospice and Home's critical systems are housed offsite by vendors, including our accounting software, payroll system, pharmacy and Electronic Medical Records System (EMR) and will therefore not be affected by local attacks.

6. If key laptop or desktop computers are affected, two tablets are available for use to access the EMR. Hard copy charts for active patients are also available.

7. If phones are affected follow the EPP - Phone Outage section.

8. If internet access is affected attempt to connect to the “hot spot” on your phone.

Tag Out

In compliance with the Occupational Safety and Health Administration (OSHA) standard (29 CFR 1910.147), Serenity Hospice and Home has developed a tag out policy and procedure. The objective of this procedure is to establish a means of positive control to prevent the accidental starting or activating of machinery or systems while they are being repaired, cleaned and/or serviced. All employees will be trained on the procedure upon hire. Additionally, refresher training will be done periodically.

Exclusions:

This Tag Out policy and procedure does not apply to servicing and maintenance operations if employees are not exposed to the risk of injury from the unexpected energization, start up, or release of hazardous energy and these operations do not require the removal of a safeguard while performing service or maintenance tasks.

Cord and plug connected electric equipment, when unplugging the equipment from the energy source that completely controls the hazardous energy and when the plug is under the exclusive control of the employee performing the servicing and/or maintenance. This exclusion applies to portable electric tools, as well as to cord and plug connected equipment which is intended for use at stationary or fixed locations.

Definitions:

Affected Employee: An employee whose job requires him or her to:

- operate or use a machine or equipment on which servicing or maintenance is being performed under tag out; or
- work in an area in which such servicing or maintenance is being performed.
- All employees of the facility are responsible for insuring they do not attempt to restart or re-energize machines or equipment that have an **Out of Service Tag** placed.

Authorized Employee: A person who tags out machines or equipment in order to perform servicing or maintenance. An affected employee becomes an authorized employee when his or her duties include servicing or performing maintenance covered under this section.

Contractor: A non-company employee being paid to perform work in our facility.

Energy Sources: Mechanical, electrical, hydraulic, pneumatic, chemical, thermal, stored or other energy source.

Stored Energy Source: A hidden energy source that is capable of releasing energy suddenly. These energy sources can cause injury or death. Examples include: springs, capacitors, heavy objects held against gravity, and hydraulic or pneumatic cylinders.

Tag out: Placing an **Out of Service Tag** on an energy isolating device, in accordance with an established procedure, to indicate that the energy isolating device and the equipment being controlled may not be operated until the **Out of Service Tag** is removed.

Out of Service Tag: A prominent tag and a means of attachment, which can be securely fastened to an energy isolating device in accordance with an established procedure, to indicate the energy isolating device and the equipment being controlled may not be operated until the **Out of Service Tag** is removed.

Procedure

This procedure applies to all of our company employees, all contractors and vendors performing work on company property, and all other individuals who are visiting or have business with our company. This procedure establishes the minimum requirements for the tag out of energy isolating devices whenever maintenance or servicing is done on machines or equipment. It shall be used to ensure that the machine or equipment is stopped, isolated from all potentially hazardous energy sources and tagged out before personnel perform any servicing or maintenance where the unexpected energization or start-up of the machine or equipment or release of stored energy could cause injury.

Authorized Employee or Contractor

1. An authorized Employee or Contractor should take the following steps to “tag out” a device.

    a. Notify all affected employees that servicing or maintenance is required on a machine or equipment and that the machine or equipment must be shut down and tagged out to perform the servicing or maintenance.

    b. The authorized employee or contractor shall identify the type and magnitude of the energy that the machine or equipment utilizes, shall understand the hazards of the energy, and shall know the methods to control the energy.

    c. If the machine or equipment is operating, it should be shut down by the normal stopping procedure (depress the stop button, open switch, close valve, etc.).

    d. De-activate the energy isolating device(s) so that the machine or equipment is isolated from the energy source(s).

    e. Tag out the energy isolating device(s) with assigned individual **Out of Service Tag(s)**. This tag(s) shall indicate the equipment removed from service and the name of the Authorized person placing the **Out of Service Tag.**

    f. Stored or residual energy (such as that in capacitors, springs, elevated machine members, rotating flywheels, hydraulic systems, and air, gas, steam, or water

pressure, etc.) must be dissipated or restrained by methods such as grounding, repositioning, blocking, bleeding down, etc.

g. Authorized employees shall take whatever means are necessary to test the equipment to reliably verify that isolation and de-energization have been effectively accomplished, before starting servicing / maintenance work on equipment that has been tagged out. Ensure that the equipment is disconnected from the energy source(s) by first checking that no personnel are exposed, then verify the isolation of the equipment by operating the push button or other normal operating control(s) or by using test equipment (volt meter, etc.) to make certain the equipment will not operate. (Caution: Return operating control(s) to neutral or "off" position after verifying the isolation of the equipment.)

h. When servicing and/or maintenance is performed by more than one person, each authorized employee shall place his/her own **Out of Service Tag** on the energy isolating source.

i. The machine or equipment is now properly tagged out.

2. When the servicing or maintenance is completed and the machine or equipment is ready to return to normal operating condition, the following steps shall be taken.

   a. Only the Authorized Person who placed the Out of Service Tag is allowed to remove this tag.

   b. Check the machine or equipment and the immediate area around the machine to ensure that nonessential items have been removed and that the machine or equipment components are operationally intact.

   c. Check the work area to ensure that all employees have been safely positioned or removed from the area.

   d. Verify that the controls are in neutral.

   e. Remove the lockout devices and reenergize the machine or equipment. (Note: The removal of some forms of blocking may require reenergization of the machine before safe removal.)

   f. Ensure that all employees have been removed from machine/equipment areas and are positioned safely. Notify affected employees that the servicing or maintenance is completed and the machine or equipment is ready for use, if there are no other **Out of Service Tags** on the equipment.

   g. If the Authorized Person who placed the **Out of Service Tag** is not available and the equipment needs to be returned to service, the following additional steps must be taken:

      i. Verify that the authorized employee, who applied the **Out of Service Tag**, is not in the facility. Attempt to contact the Authorized Employee to

communicate the intent to restore the equipment to operation and to verify there is no reason this should not be done.

ii. Make reasonable efforts to advise the employee that his/her **Out of Service Tag** has been removed. (This can be done when he/she returns to the facility).

iii. Ensure that the authorized employee has this knowledge before he/she resumes work at the facility.

[54 FR 36687, Sept. 1, 1989 as amended at 54 FR 42498, Oct. 17, 1989; 55 FR 38685, Sept. 20, 1990; 61 FR 5507, Feb. 13, 1996]

Vetting New Software Vendors

SH&H uses due diligence in the selection of new software vendors. A vendor selection committee is formed with representatives from senior management, outside subject matter experts, and affected staff. When selecting a new software vendor, the following steps are used to assist in arriving at the best option:

1. Business requirements are defined (and agreed upon). When appropriate, a Request for Proposal (RFP) is created defining the exact business requirements, and is sent to potential candidates.
2. Software selections are vetted. Vendors are scrutinized to ensure they can provide the resources needed. This may include vetting the balance sheets of startups to ensure they will be around for the foreseeable future.
3. References are requested. Committee members will request client references and talk to clients similar to SH&H in size and industry.
4. Pilot programs are leveraged. If the software company offers a pilot program that allows potential clients to use a limited version of the product for a brief period of time, the software is tested to verify it has the required functionality. Pilot programs provide proof that the software works as stated, and gives senior management a chance to get acclimated to the software.
5. Security protocols are requested. Vendors are asked to submit their most recent security risk assessment to make sure the company has a proven track record in terms of security.

Volunteer Data Access

1. SH&H volunteers do not have access to a patient's clinical record in the Electronic Medical Record system.
2. Volunteers receive, via postal mail, the minimal amount of information necessary for them to visit the patient and meet the patient's requested volunteer needs.

3. Volunteers are to use only first name and last initial of the patient on their visit documentation.

4. Volunteer visit notes are scanned into the Electronic Medical Records system by the volunteer coordinator or designee.

Virtual Private Network (VPN)

1. SH&H employees and authorized third parties (customers, vendors, etc.), may utilize remote access to connect to SH&H computing resources for which they have been granted access.

2. Regular, full-time SH&H staff employees who have a valid SH&H Domain User Account may request remote access to the SH&H staff network by completing a **Remote Access Request Form**. A letter of justification must accompany the request. The letter should address, in sufficient detail, what resources will be accessed and why they cannot be accessed by conventional means. Requests omitting a letter of justification will be returned to the requestor as incomplete.

3. With the exception of Remote Desktop Gateway (RDG) (see Operational Procedures below), remote access is valid for a set period of time. The Requestor should indicate the date remote access should take effect and the date access should expire. Remote access may be granted for a period of up to twelve months, after which remote access for the account will expire. Requestors will be notified via phone or email approximately thirty (30) days before remote access expires. Account holders may resubmit a Remote Access Request Form up to thirty (30) days before the remote access expiration date to continue remote access without disruption.

    a. Operational Procedures: SH&H's current VPN solution has one or two steps: VPN and network file access, and then optional 2nd step RDP

        - Sonicwall SSL VPN Client
            - Allows you to connect to the SH&H network from off-campus
            - Requires software installation
            - Expires, at minimum, every 12-months
        - Microsoft Remote Desktop (RDP)
            - Sonicwall SSL VPN Client required for RDP
            - Allows you to log in to your SH&H computer from on or off-campus
            - Requires no software installation

- RDP does not expire (subject to periodic review)

4. In order to use remote access, you need a connection to the Internet from your off-campus location. SH&H does not provide you with an Internet connection, so in order to use VPN you must have your own Internet Service Provider. While dialup Internet connections may utilize a remote access connection, performance is very slow and is not recommended or supported.

    a. Remote access users will be automatically disconnected from the SH&H staff network after 30 minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes to keep the connection open are prohibited.

    b. Support will only be provided for remote access clients approved by the IT vendor.

    c. VPN usage is logged by the Sonicwall, reports are generated

    d. If you have any questions related to the use of SH&H remote access, please contact the IT vendor (EPP – Suppliers & Contractors).

5. The Guidelines for Access are as follows:

    a. Departmental Accounts shall not be granted remote access due to lack of accountability. These accounts are typically shared among several users and there is no way to trace a specific user back to the account at any given time.

    b. Temporary Accounts shall not be granted remote access.

    c. Clerical or Support accounts shall not be granted remote access without prior telecommuting approval (Endorsement required).

    d. Executive and Administrative accounts may be granted remote access.

    e. Vendor Accounts may be granted remote access. Vendor accounts are setup specifically for vendors to access SH&H resources for support purposes. Vendor accounts must be sponsored by an SH&H Employee. The account sponsor bears responsibility for the account and its use by the vendor. If the vendor account does not already exist, a request to establish one must be made at the same time remote access is requested.

    f. All remote access account holders are subject to the Remote Access Terms of Use.

6. A Site to Site Virtual Private Networks (VPN) connects the Serenity Hospice and Home network to ‘The Shed’ and to the ‘Dixon office’ networks.

Remote Access Terms of Use

1. It is the responsibility of all SH&H employees and authorized third parties with remote access privileges to ensure unauthorized users are not allowed access to internal networks and associated content.
2. All individuals and machines, including SH&H -owned and personal equipment, are a de facto extension of SH&H's network, and as such are subject to all sections of the Risk Management Policy.
3. All computers connected to SH&H's internal network via remote access or any other technology must use a properly configured, up-to-date operating system and antivirus software; this includes all personally owned computers. Antivirus software may be available for SH&H faculty and staff.
4. Redistribution of the SH&H remote access installers or associated installation information is prohibited.
5. All network activity during a remote access session is subject to SH&H policies.
6. All users of the SH&H remote access services shall only utilize resources for which they have been granted permission and rights to use.

Any user found to have violated the terms of use may be subject to loss of privileges or services and other disciplinary action.

Request Access: Begin Date:_____ End Date: _____

_____

Name (Please Print) Title

_____

Signature Date

_____

CEO Authorization Date

Policy Maintenance

The CEO is charged with the responsibility to periodically review the policy and propose changes as needed.

Workstation Backup

SH&H has several mission critical workstations; finance, social services, human resources, and others. There is an ASUS device connected to local network workstations to place workstation backups onto the Network Attached Storage (NAS). The NAS has two mirrored (RAID 1) volumes and is the repository for the workstation images. These backups are performed once a week, first a Full, then incremental backups thereafter. After (5) incremental backups, the cycle starts over with a new Full image and incremental thereafter.
The Acronis TrueImage // NAS system protects workstations in case of:

a. HDD failure; replace the HDD and restore with the latest Image/increments from NAS storage.

b. Virus/Trojan that can't be removed or logical error on the workstation HDD; restore latest image

References:
45 C.F.R. 164.304
45 C.F.R. 160.103
45 C.F.R. 164.402

Change Log:

Change Date	Description	Board Approval Date
12/08/2016	New Policy	02/22/2016
04/29/2016	New item under Facility Security that states that a monitor displays camera activity 24 hours a day at the nurse's station and camera history is reviewed monthly to insure it is functioning properly.	
05/13/2016	New section for Disclosure of PHI	06/27/2016
07/18/2016	Added a Section on Ransomware	11/28/2016
10/24/2016	Added an item to the Computer Users section prohibiting employees from sharing passwords or posting them near their workstations. Also added that strong network passwords are enforced.	11/28/2016
11/7/2016	Added "Employee Termination" Section.	11/28/2016
01/09/2016	Added card reader security for the new office building under "Facility Security."	02/27/2017
01/26/2016	Added statement that "the storing of patient health information on a home computer, laptop, tablet, or any other device is strictly prohibited to the "Protected Health Information" section.	02/27/2017
1/20/2017	Per Security Risk Cyber Self-Assessment, enabled Intrusion Prevention, Gateway Antivirus and Gateway malware as reflected in Firewalls and Network Security section.	02/27/2017
04/27/2017	Added to the Risk Management Communication Section to cover any type of situation that could result in a negative public image (instead of just a breach).	09/06/2017
07/20/2017	Added review of intrusion reports to Firewalls & Network Security	09/06/2017
1/19/2018	Added contact information for reporting of cybersecurity attacks.	04/30/2018
1/22/2018	Added statement about locked shredding containers and alerting the Authority when a mobile device or lap top is stolen to the section about Protected Health Information.	04/30/2018
3/7/2018	Added to Computer Users section prohibiting the sharing of passwords or posting them near their workstations.	04/30/2018

3/8/2018	Added to Antivirus section stating that staff should notify the Authority if they suspect they have a computer virus. Added to Logical Security section the required complexity for network passwords.	04/30/2018
11/02/2018	Updated Patient Charts section to reflect that they are scanned into eFileCabinet (Secure Cloud Storage). Added to Ransomware section: • Two tablets are available to use for back up if lap tops or desk tops are affected with Ransomware. • Phone outage procedure • Internet outage procedure • Reordered some procedures.	11/25/2018
02/27/219	• Added statement indicating the IT/server room is secured by a card reader. • Added secure data may be sent via encrypted email. • Added statements indicating that mobile devices should be stored in a secure location and should not be stored in checked baggage. • Added a section on vetting new software.	04/29/2019
06/07/2019	Major updates to the Mobile Devices Section.	08/26/2019
4/20/2020	• Updated Facility Security section to reflect the silent alarms at nurse's station and badge access added to the mechanical room. • Updated Password section to denote that Serenity issues passwords for all work devices rather than employees setting their own. • Added requirement to the Antivirus containment section that if an employee suspects their computer or device may have been infected with a virus, they should immediately notify Authority or the Information Technology vendor.	

	• Replaced the Safety Committee role of support & review of the RMP to being the IT vendor instead.	
5/20/2020	• Added Hazard Communication section	11/23/2020
10/29/2020	• Added Phishing section	11/23/2020
04/30/2021	• Updated HIPAA Compliance section with the use of secure messaging application (i.e.- Backline). • Disposal of PHI section updated to reflect that tablets are now destroyed by submersion in water rather than by crushing. • Added into Facility Security that patient room patio doors are equipped with alarms that sound at the nurse's station whenever the patio door is opened. • Added to Antivirus section that software patching is maintained by the Manage Engine.	08/23/2021
12/06/2021	• Updated the password complexity requirements in the Logical Security section	n/a