MED STAFF MEETING

POLICY DEVELOPMENT COMMITTEE

November 10, 2021

SoHum Health

733 Cedar Street
Garberville, CA 95542
(707) 923-3921
shchd.org

NEW POLICIES

SoHum
Health
Southern Humboldt
Community Healthcare District
733 CEDAR STREET
GARBERVILLE, CA 95542
(707) 923-3921

DEPARTMENT: Human Resources	NO:	Page 1 of 1
SUBJECT: **Education Reimbursement/ Student loan debt repayment Policy**	EFFECTIVE DATE: 12/02/2021	SUPERSEDES: NEW

POLICY:

Southern Humboldt Community Health District (SHCHD) will reimburse an employee up to a maximum of $5,250 per year for continuing education through an accredited program that either offers growth in an area related to his or her current position or that may lead to promotional opportunities. This education may include college credit courses, continuing education unit courses, seminars and certification tests that are job-related. An employee must secure a passing grade or obtain a certification to receive any reimbursement. Expenses must be validated by receipts and a copy of the final grade or certification received.

Under Section 127 of the Internal Revenue Code (IRC), SHCHD is allowed to provide tax-free payments of up to $5,250 per year to eligible employees for qualified educational expenses. To be considered qualified, payments must be made in accordance with an employer's written educational assistance plan. The Coronavirus Aid, Relief and Economic Security (CARES) Act amended Section 127 to include student loan repayment assistance as a qualified educational expense. The expansion of Section 127 allows employers to make payments for student loans without the employee incurring taxable income and the payment is a deductible expense for the employer, resulting in tax advantages to both parties.

PROCEDURE:

- Prior to enrolling in an educational course, the employee must provide his or her manager with information about the course for which he or she would like to receive reimbursement and discuss the job-relatedness of the continuing education.
- Once the course is successfully completed, the employee should resubmit the original tuition reimbursement request form with the reimbursement section filled out, including appropriate signatures, as well as receipts and evidence of a passing grade or certification attached.
- For student debt reimbursements request forms should be completed by the employee, and the appropriate signatures obtained.
- Student debt repayment and educational reimbursement combined together cannot exceed $5,250 in a calendar year.
- The HR department will coordinate the reimbursement with the finance department.

REQUIREMENTS:

- Education reimbursement eligible employees are full-time, regular employees who have completed their 90 day introductory period. On a case by case basis education reimbursement may be approved before the introductory period ends.
- Student debt repayment eligible employees are full-time, regular employees who have completed 6 months of employment with SHCHD.
- Have a written education agreement, tuition reimbursement or debt repayment agreement completed and have the appropriate signatures obtained and copies filed with Human Resources.
- For Education reimbursements over $1000.00 the direct supervisor must take the request to Human Resources for Administrative Team Approval.
- No Cash in Lieu of Benefits - SHCHD does not offer employees benefits under the program in lieu of a cash payment, employees cannot "opt-in" or "opt-out" of benefits.
- Payments of principal or interest can be made directly to employees as reimbursement for amounts already paid (support for student loan payments should be provided by the employee) or payments can be made directly to the lender. Other educational expenses that qualify under Section 127 include: Tuition for graduate or undergraduate level programs, which do not have to be job-related Books, supplies, and necessary equipment, not including meals, lodging, transportation, or supplies that employees may keep after the course is completed

REFERENCE:

Internal Revenue Code (Code) Section 127, IRS Publication 970

REVIEWED BY:

Human Resources
Chief Executive officer

REVISED POLICY

INFORMATION SERVICES

SoHum Health
Southern Humboldt
Community Healthcare District
733 CEDAR STREET
GARBERVILLE, CA 95542
(707) 923-3921

DEPARTMENT: Information Services	NO:	Page 1 of 17
SUBJECT: **Information Technology Manual**	EFFECTIVE DATE: 12/02/2021	SUPERCEDES: 07/28/2021

SCOPE:
This policy applies to all SHCHD workforces:

- Employees
- Volunteers
- Patients and residents
- Temporary staff
- Agency and contracted staff
- Members of the Board of Directors

Section 01 - HIPAA SECURITY: DATA AUTHENTICATION, PHYSICAL SAFEGUARDS

Southern Humboldt Community Healthcare District (SHCHD) maintains formal policies and procedures designed to protect electronic protected health information (ePHI) from improper access, alteration or destruction. This includes mechanisms to ensure that ePHI has not been accessed, altered or destroyed in an unauthorized manner.

1. This section applies to all forms of electronic protected health information (ePHI) maintained or transmitted by SHCHD, regardless of the manner of access (on-site, VPN, etc.).
2. SHCHD workforce members are required to report to the SHCHD Information Technology Manager (ITM) any suspected or known unauthorized data access, modification or destruction.

Data Authentication

1. ePHI shall be protected by authentication controls on all IT resources.
2. Authentication controls shall minimally include a unique user login and password combination.
3. Files containing ePHI intended for transmission outside the SHCHD Intranet shall be encrypted and transmitted using the approved secure file transfer product(s) determined by the SHCHD ITM.
4. Mail messages containing ePHI intended for transmission outside the SHCHD Intranet shall be encrypted and transmitted using the approved secure messaging product(s) determined by the SHCHD ITM.
5. All other ePHI transmissions, e.g. client/server connections, shall be encrypted using approved mechanisms, e.g. virtual private networks, whenever feasible, or whenever deemed necessary by the risk analysis or evaluation in accordance with SHCHD Policy.
6. ePHI integrity will be sustained using approved mechanisms, e.g. hashing algorithms, electronic signatures, and digital signatures, whenever available and feasible or whenever deemed necessary by risk analysis or evaluation under this policy.

Physical Safeguards

1. IT resources shall be secured using physical safeguards for protection from unauthorized access.
2. Screen locks (currently set at 15 minutes) and session timeouts, and auto log off with password controls shall be activated on all IT resources.
3. Portable IT resources, e.g. laptops, shall be physically secured when not in use.
4. Virus protection shall be installed and activated on all IT resources containing ePHI where available. Additional mechanisms shall be implemented to further protect IT resources from malicious software whenever deemed necessary by the Information Security Officer (ISO).
5. All computers running Windows 10 or greater shall have Bitlocker hard drive encryption enabled.
6. Communication between the EMR server and computers shall be encrypted using SSL.

Section 02 - HIPAA SECURITY: ADMINISTRATION

The purpose of this section is to comply with the HIPAA Security Rule's requirements pertaining to policies and procedures and documentation, and the appointment of an Information Security Officer (ISO). All duties of the ISO are incorporated into the responsibilities of the Information Technology Manager (ITM).

1. Department heads, along with the ISO, are responsible for establishing, implementing, and enforcing IT Related HIPAA Security policies and procedures. This responsibility may not be delegated to other staff members. District HIPAA Security policies and procedures do not preempt any existing or similar laws or policies.
2. HIPAA policies and procedures apply to all ePHI and IT resources that store, process, have access to, and/or transmit ePHI held by the district.
3. Procedures shall be reasonable and appropriate to comply with the standards, implementation specifications, or other requirements of the HIPAA Security Rule, taking into account the size, complexity, and capabilities of the department; the departmental technical infrastructure, hardware, and software capabilities; the costs of security measures; and the probability and criticality of potential risks to ePHI.
4. The ISO, for those procedures that are to be used by all departments, shall develop centralized procedures. Departments shall develop and maintain decentralized procedures that are specific to their department in order to define specific operational steps for policy compliance.
5. Guidelines that set forth "best practices" shall be developed by the ISO for the purpose of assisting departments to comply with policies and procedures.
6. Policies, procedures, and guidelines shall be documented and stored electronically, and be available to all departments and the ISO.
7. HIPAA Security Rule policies and procedures and actions, activities or assessments required by the HIPAA Security Rule, including but not limited to, risk analysis, evaluations, and documentation related to security incidents and their outcomes, shall be maintained for six years from the creation date or the date when it last was in effect, whichever is later.
8. Documentation shall be made available to anyone responsible for implementing, managing, and auditing the procedures.
9. Documentation shall be reviewed, updated and modified, as needed if environmental or operational changes affect the security of ePHI.
10. ISO responsibilities:
    - Overall final responsibility for the security of district information assets
    - Working with district administration to develop and maintain policies and procedures, standards and guidelines that contribute to the realization of district goals and objectives for information security management
    - Coordinating and directing specific actions to provide a secure and stable information systems environment consistent with district goals and objectives
    - Development and implementation of ongoing training and awareness programs for end users of the information network assets and ePHI
    - Investigation of and reporting on information security incidents

Section 03 – HIPAA SECURITY: FACILITY ACCESS CONTROL

The purpose of this section is to comply with the HIPAA Security Rule's requirements pertaining to the limiting of physical access to all forms of electronic protected health information (ePHI) and the facility or facilities in which they are housed while ensuring that only properly authorized access is allowed. SHCHD will safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

1. This policy applies to all forms of ePHI maintained or transmitted by SHCHD pertaining to an individual.
2. This policy applies to all areas of the facility.
3. SHCHD Security policy serves as the standard for safeguarding the facility and from unauthorized physical access, tampering or theft, including the equipment contained therein.
4. Options used to restrict access include but are not limited to:
    a. Restricted room keys
    b. Electronic keypad type locks
5. Any location with department server(s) not located in the IT Office shall assure that the ISO has an updated list of departmental emergency contacts and person(s) who are authorized to utilize those resources.
6. IT shall be locked and secure at all times. Access to the area is restricted to IT staff.
7. IT Department has clearance to all departments throughout the district.

Section 04 – HIPAA SECURITY: INFORMATION SYSTEMS ACCESS CONTROL

The purpose of this section is to comply with the HIPAA Security Rule's requirements pertaining to ensuring that all workforce members have appropriate levels of access to all forms of electronic protected health information (ePHI) and to prevent that personnel who should not have access to such information from obtaining access to ePHI. SHCHD

shall verify that an individual or entity seeking access to ePHI is the one claimed. SHCHD shall also implement technical policies and procedures for electronic information systems that maintain electronic ePHI to allow access only to those persons or software programs that have been granted access rights.

Access to ePHI

1. The use and access of SHCHD's information systems are restricted to appropriately identified, validated and authorized individuals. Unauthorized access is a violation of SHCHD's policies.
2. Valid business and patient care reasons are the only reasons for accessing ePHI.
3. Department managers are responsible for ensuring that workforce clearance and authorization to access to ePHI shall be performed for all workforce members prior to granting access requests to IT resources.
4. Access rights shall be properly authorized and documented by the department manager.
5. Access rights shall be periodically audited as required by the SHCHD Information Security Officer (ISO).
6. The department manager shall re-evaluate access rights when a workforce member's access requirements to ePHI change (e.g., job assignment change). Modifications to workforce member's access to IT resources shall be properly authorized documented, and processed in accordance with the appropriate system access control procedures.
7. Access rights shall not exceed the minimum necessary for a workforce member's assigned duties.
8. SHCHD organization-wide procedures authorizing workforce members use shall be developed and implemented by the IT Department and approved by the ISO in conjunction with department heads and administration.
9. Security configurations shall be maintained on IT resources to restrict access to ePHI to only those workforce members or software programs that have been granted access.
10. Only Information Technology Department staff or system administrators are permitted to create or change access control settings.

User ID and Password Administration

1. The Information Technology Department shall receive a minimum of 2-business days notice about new user accounts needing to be created. Notifications for new user accounts must be sent using the Ticket System located on ThePulse, or an email to Group ITHelp, which will generate a ticket. No other means of communication will be accepted.
2. SHCHD will utilize user authentication mechanisms to control access to information systems. Each individual user will have a unique user name or number sign-on. This unique name or number sign-on shall be coupled with strong passwords as a second level authentication mechanism.
3. Workforce Members shall not modify assigned unique system identifiers (or login names) unless it is necessary for authorized support purposes.
4. Anonymous access, including the use of guest, group shared, and public accounts, to any IT resource, is specifically prohibited.
5. Passwords must meet SHCHD Secure/Strong Password Procedure.
6. Passwords shall be encrypted for storage and transmission whenever available, or whenever deemed necessary by the risk analysis or evaluation in accordance with the SHCHD HIPAA Security Risk Management, Evaluation, and Audit Policy
7. The system administrator or system supervisor passwords will be changed every ninety days.
8. Password controls shall force periodic password changes every ninety days whenever available.
9. Password controls shall lockout login accounts after three unsuccessful login attempts, whenever available. Electronic sessions will be automatically terminated after a period of time deemed appropriate for the work environment.
10. Password protected screen savers shall be used on all systems where available.

Termination of System Access

1. SHCHD organization-wide procedures shall be developed and implemented for terminating Workforce Member access.
2. The Workforce Member's direct supervisor shall be responsible for making appropriate and timely requests for IT resource account deactivation.
3. Upon separation from employment or affiliation or change of job responsibilities within SHCHD, Human Resources in coordination with Information Technology shall make necessary changes to security levels within a reasonable time; except in the case of adverse separation which will be done immediately.

SECTION 05 - HIPAA SECURITY: ACCEPTABLE USE

The purpose of this section is to comply with the HIPAA Security Rule's requirements pertaining to the acceptable use of district IT resources and electronic Protected Health Information (ePHI).

1. Workforce members are responsible for the appropriate use and security of ePHI when using any IT resource authorized by the appropriate department of SHCHD.
2. Appropriate use includes using authorized IT resources, as assigned, in accordance with duties and responsibilities. Using IT resources in violation of policy, or any negligent or unlawful activity is considered inappropriate use.
3. Written SHCHD HIPAA Security policies and procedures are available to workforce members.
4. Individual procedures specific to a single department shall be developed and implemented for workforce acknowledgment by the department manager in collaboration with the ISO.
5. IT resources shall be protected from misuse, including, but not limited to: theft, unauthorized access, fraudulent manipulation and alteration of data, attempts to circumvent security controls, and any activity that could compromise the confidentiality, integrity, or availability of data.
6. Workforce members shall not tamper with or disable any security devices, including but not limited to, virus protection software and login account controls.
7. Workforce members are prohibited from introducing any unauthorized IT resources into the SHCHD environment. Furthermore, the introduction of any IT resources that could disrupt any operations or compromise security is prohibited.
8. Any IT resources assigned to or in the possession of a workforce member shall be returned to a designated individual within his department when it is determined by department management that the use of those resources is no longer necessary.
9. All workforce members are to immediately report lost or stolen IT resources to their department management who shall report to the ISO.
10. Workforce members learning of or reasonably suspecting any violation of any HIPAA Security policy shall immediately report to their supervisor and/or the ISO. Once the department manager has received notification of a known or suspected HIPAA Security policy violation, he or she shall report to the ISO.

SECTION 06 - HIPAA SECURITY: INFORMATION SYSTEM ACTIVITY REVIEW

We review system activity in order to detect and minimize security violations to Electronic Patient Health Information (ePHI). SHCHD shall continually assess potential risks and vulnerabilities to protected health information in its possession, and develop, implement, and maintain appropriate administrative, physical, and technical security measures.

1. This policy applies to all forms of ePHI.
2. IT resources that store, access, or transmit ePHI shall electronically log activity into created log files.
3. Logging shall include system, application, database, and file activity whenever available or deemed necessary by risk analysis or evaluation.
    a. Logging shall include creation, access, modification and deletion activity.
    b. Log files shall be retained electronically for a period no less than 12 months.
4. Department managers are responsible for developing and implementing procedures for logging activity specific to their areas.
5. IT resources and log files shall be periodically examined for access control discrepancies, breaches, and policy violations.
6. System activity review cycles shall include a review of audit logs, access reports, and security incident tracking reports, shall not exceed 30 days, and shall include daily exception reporting.

SECTION 07 - HIPAA SECURITY: RISK MANAGEMENT, EVALUATION, AND AUDIT

The district will take effective steps to minimize or eliminate potential risks and vulnerabilities to ePHI, and shall continually assess potential risks and vulnerabilities to ePHI in our possession, and develop, implement, and maintain appropriate security.

Risk Management

1. This policy applies to all forms of ePHI.
2. Department managers shall conduct, on a routine schedule, a risk analysis process of security and access control measures using the ISO approved risk analysis methodology. The process shall include both technical and non-technical evaluations performed to establish the extent to which its computer systems and networks meet a pre-specified set of security requirements.
3. The ISO will develop and ensure the implementation of an organization-wide procedure for performing risk analysis. The risk analysis shall demonstrate, at a minimum, the following information:
    a. The level of risk associated with each potential vulnerability exploitation
    b. Steps to be taken to reduce the risk of vulnerability exploitation

   c. Processes for maintaining no more than the acceptable level of risk
   d. Technical evaluations including security functional testing, penetration testing analysis and verification as appropriate.
4. The ISO, along with department managers, will ensure that the risk analysis and risk management procedures are conducted.
5. Non-compliant and unacceptable risks shall be mitigated to a reasonable and appropriate level as defined by the ISO.
6. Results of all risk analysis shall be securely stored using authorized mechanisms determined by the ISO.
7. The ISO, Administrator and the Management Team will review the outcome of the risk analysis findings.

Evaluation

1. The ISO will develop and ensure the implementation of an organization-wide procedure for performing evaluations.
2. The ISO and System Owners shall conduct an evaluation of district compliance with technical and non-technical HIPAA security standards on a scheduled basis.
3. Technical and non-technical evaluations shall be conducted when there is an environmental or operational change that possibly affects the security (confidentiality, integrity, or availability) of ePHI.
4. Results of non-compliance shall be remediated as soon as practicable, depending on specific circumstances and the acceptability of the risk determined by the ISO and department managers.
5. Results of all technical and non-technical evaluations shall be securely stored using authorized mechanisms determined by the ISO.

Audit

1. The ISO shall approve and execute an audit program for the purposes of measuring departmental compliance with SHCHD HIPAA Security Policies

SECTION 08 - HIPAA SECURITY: BREACHES OF PRIVACY & SECURITY OF ePHI: REPORTING REQUIREMENTS, SANCTIONS, AND MITIGATION

SHCHD policies regarding privacy and security of ePHI reflect its commitment to protecting the confidentiality of patient's medical records, patient accounts, clinical information from management information systems, confidential conversations, and any other sensitive material as a result of doing business. To ensure compliance with these policies and to ensure that the disciplinary actions taken as a result of a breach of patient confidentiality are applied consistently, SHCHD has adopted the disciplinary process in this policy.

POLICY STATEMENT

1. The process outlined in this policy includes initial reporting responsibilities, the investigation process followed sanctions and appeals, SHCHD's duty to mitigate damages created by breaches and the documentation requirements of these processes.
2. ePHI is confidential and must be treated with respect and care by any individual with access to this information.
3. A breach of confidentiality is defined as violating provisions of SHCHD's Confidentiality Policy or the HIPAA Privacy or HIPAA Security Policies. As a medical care provider, SHCHD is entrusted with demographic, financial and clinical information regarding our patients. Any breach of confidentiality by workforce members is subject to formal discipline up to and including termination as set forth in this policy. Policy guidelines shall be observed by the entire organization, and sanctions applied fairly and consistently to all individuals in violation of the policies. Examples of breaches of confidentiality and security; *this is not an all-inclusive list*:
   - Individual leaves a computer unattended in an accessible area with medical record information unsecured.
   - Failure to log off computer terminal.
   - Sharing or exposing passwords.
   - An individual improperly accesses, reviews and/or releases birth dates, addresses of friends or relatives, or requests another individual to do so.
   - An individual improperly accesses, reviews and/or releases the record of a patient out of concern or curiosity, or requests another individual to do so.
   - An individual improperly accesses, reviews and/or releases a patient record to use information in a personal relationship.
   - An individual accesses, reviews and/or releases the patient record of a public personality for the intent of giving or selling information to the media.
   - An individual improperly accesses, reviews and/or releases confidential information of another member of the SHCHD workforce that is also a patient.

- An individual improperly accesses, reviews and/or releases confidential information that may bring harm to the organization or individuals associated with it.

Initial Reporting Responsibilities

1. Breaches by persons or behaviors resulting in breaches of confidentiality or security: The individual who observes or is aware of some type of improper disclosure of information or security incident is required to report it in one of the following ways:
    a. Immediate Supervisor
    b. Department Head or Manager of the area in which the individual works
    c. Privacy Officer
    d. Corporate Compliance Officer
    e. Information Security Officer (ISO)
    f. Human Resources Manager
    g. Phone report (CEO extension 260)
    h. The original contact person notified under Section A must notify the ISO for breaches that are technological in nature.
2. Security Incident: Once a security incident or suspected incident has been reported, the ISO shall immediately execute its incident response procedures. The ISO, upper management, and any other designated agents, as appropriate, shall mitigate harmful effects of security incidents known to the ISO. Mitigation will include notifying individuals whose ePHI is divulged in error or through unauthorized means, to the extent practicable.
3. Confidentiality: Confidentiality of all participants in the situation shall be maintained to the extent reasonably possible throughout the investigation. Some circumstances may dictate notification to staff and third parties, but this is at the discretion of the administrator who may direct other persons to conduct the inquiry, as they deem appropriate.
4. Bad Faith Reports: Reporting a breach in bad faith or for malicious reasons may be interpreted as a misuse of the reporting mechanism(s) and may result in disciplinary action up to and including termination.

Investigations of Reported Breaches

1. Information pertaining to investigations of breaches will only be shared with those who have a need to know. The investigator(s) will conduct the necessary and appropriate review commensurate with the level of breach and the specific facts. This investigation may include, but is not limited to, interviewing the individual accused of the breach, interviewing other individuals, and reviewing pertinent documentation and system logs.
2. Existing procedures for disciplinary action shall be utilized. Sanctions may include, but are not limited to:
    a. Counseling
    b. Oral Warning
    c. Written Warning
    d. Suspension
    e. Termination

Duty to Mitigate Valid Breaches

1. SHCHD maintains this policy for mitigating to a practical extent, any harmful or injurious effect of unauthorized uses or disclosures of all forms of ePHI. To this end, oversight, detection, and reporting mechanisms have been established to know when violations occur. Additionally, processes are in place to limit the damage incurred.
2. SHCHD also has a duty to take reasonable corrective steps when notified of breaches of contract terms by business associates. While SHCHD is not required to monitor the activity of our business associates, we will address problems as we become aware of them and request that our associates remedy their behavior. SHCHD reserves the right to terminate contracts if it becomes clear that the business partner cannot be relied upon to maintain the privacy of information we provide to them.
3. District officials shall be prepared to contact law enforcement, regulatory, accreditation, and licensure bodies as necessary in order to properly mitigate policy violations.

Documentation and Tracking of Breaches

1. An analysis of reported privacy and/or security breaches is prepared by the ISO at least twice per year and reported to the Board of Directors.
2. All information documenting the process noted in this policy regarding the incident or violation will be retained for a period of six years.

SECTION 09 - HIPAA SECURITY: TRACKING AND DISPOSAL OF EQUIPMENT AND ELECTRONIC MEDIA CONTAINING ePHI

The purpose of this section is to comply with the HIPAA Security Rule's requirements pertaining to the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility and applies to all hardware and electronic media that contain ePHI at SHCHD.

Hardware Containing ePHI

1. Hardware shall be controlled and accounted for at all times by the department to which it is assigned in conjunction with the IT Department.
2. The IT Department will record the movement of all hardware containing ePHI in or out of the facility including the individual(s) responsible for the movement.
3. The movement of hardware shall be authorized and logged by the IT department manager prior to the hardware and electronic media entering or leaving a facility.
4. Hardware shall be properly logged and disposed of when no longer used.
5. ePHI shall be removed from hardware before it is made available for reuse.
6. A retrievable, exact copy of ePHI, (when appropriate) shall be created before any movement of hardware.
7. Hardware with little or no value shall be physically destroyed when no longer used or no longer needed.

Electronic Media

Electronic media containing PHI shall be physically destroyed when no longer used or no longer needed.

SECTION 10 - HIPAA SECURITY: INFORMATION SYSTEMS BUSINESS CONTINUITY AND DISASTER RECOVERY

The purpose of this section is to comply with the HIPAA Security Rule's requirements pertaining to responding to an emergency or other occurrence that damages systems that contain electronic protected health information (ePHI).

1. A contingency plan shall be developed, and maintained as needed, for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages IT resources that contain ePHI.
    a. An application and data criticality analysis shall be developed and maintained to assess the relative criticality of specific applications and data in support of the contingency plan components.
    b. Facility access procedures shall be developed and maintained for access to support recovery efforts.
    c. Contingency plan testing and revision procedures shall be developed and executed for verifying recovery capabilities.
2. A data backup plan shall be established and maintained to create and maintain retrievable exact copies of ePHI.
3. Emergency access procedures shall be established and maintained for the retrieval of ePHI during an emergency.
4. A disaster recovery plan shall be established and maintained to restore any loss of data in the event of a disaster. Disaster recovery plan testing and revision procedures shall be developed and executed for verifying recovery capabilities.
5. Departmental downtime procedures shall be developed and maintained to protect ePHI during emergency operations of business processes.

SECTION 11 - HIPAA SECURITY: VIRUS PROTECTION POLICY

SHCHD is committed to implementing formal procedures for guarding against, detecting, and reporting malicious software. Malicious software means software, for example, a virus, designed to damage or disrupt a system.

1. This section applies to all computer equipment connected to the SHCHD network.
2. The SHCHD Information Technology Department shall ensure anti-virus checking software is in place and up-to-date for all SHCHD systems to identify viruses, worms, Trojans, spyware, and other forms of malicious software. (Note: Due to industry terminology and widespread use of calling all malicious software a virus, "virus" refers to all malicious software in the context of countermeasure products.)
3. All computer equipment connected to the SHCHD network shall have SHCHD-approved virus protection software installed with current virus definitions. Virus protection shall be installed and activated on all SHCHD IT resources. Additional mechanisms shall be implemented to further protect SHCHD IT resources from malicious software whenever deemed necessary by the risk analysis or evaluation.
4. All computer equipment connected to the SHCHD network shall be up to date with the manufacturer's operating systems security software patches.
5. SHCHD workforce suspecting a malicious software infection will immediately report the issue following this policy's reporting requirements.

SECTION 12 - HIPAA SECURITY: TRAINING OF WORKFORCE

The purpose of this section is to identify the mechanism by which appropriate staff receives education and training, both initial and ongoing, on Federal HIPAA regulations and SHCHD organizational policies related to security and privacy of electronic protected health information (ePHI).

1. The SHCHD workforce is trained on the HIPAA privacy and security regulations, including SHCHD policies and procedure. District directives for information security include communicating expectations concerning information security to all users of information and information assets of SHCHD, promoting information security awareness, and providing guidelines and techniques for the protection of ePHI and district information assets.
2. Training content is established by the SHCHD Information Security Officer (ISO). Human Resources is responsible for maintaining a record of staff participation and department managers shall assure their staff completes the training.
3. New employees who are required to complete the training will do so during the standard orientation period.
4. When significant changes in policy and/or procedure occur, all affected workforce will receive training as soon as possible after the changes.
5. Training is documented in written or electronic form and retained for at least six years.
6. All staff will be provided periodic security updates.

SECTION 13 – SECURE/STRONG PASSWORD PROCEDURE

SHCHD maintains formal procedures designed to limit access to all forms of ePHI, including the use of Secure/Strong Passwords.

Passwords must contain at least six characters, cannot be a common word, and must contain at least one each of the following:

- **Special Characters** (!@#$%^&*()-=+_~`\][|}{';":/.,?><)
- **Numbers** (1234567890)
- **Letters** (ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqurstuvwxyz)

The good way to pick a password is to think of a phrase that is easy to remember. Choose the first letter of each word.

The **r**ain **i**n **S**pain **f**alls **m**ainly **o**n **t**he **p**lain

This would give you **TriSfmotp.** You should also add either a number or special character or change one of the existing letters to a number or special character. If you do this, you might end up with something like this… **Tr1$fmotp!**

This is a very secure password and is fairly easy to remember and very difficult to guess (though this example is widely used, so you should not…). You will notice that you should not use the initials of family members, pet's names, favorite sports teams, etc. because these passwords are easily guessed.

Password Do's and Don'ts

- ***Do*** use a password with mixed-case characters.
- *Do* use a password containing non-alphabetic characters (digits and/or punctuation)
- *Do* use a password that is easy to remember, so that you don't need to write it down.
- ***Don't*** use your login or user name in any form (as-is, reversed, capitalized, doubled, etc.)
- *Don't* use your first, middle, or last name in any form.
- *Don't* use your spouse's, significant other's, children's, friend's, or pet's name in any form.
- *Don't* use other information easily obtained about you, including your date of birth, license plate number, telephone number, social security number, make of your automobile, house address, etc.
- *Don't* use a password of all digits or all the same letter.
- *Don't* use a word contained in English or foreign language dictionaries, spelling lists, acronym or abbreviation lists, or other lists of words.
- *Don't* use a password containing fewer than six characters.
- *Don't* give your password to another person for any reason.
- *Don't* write your password down or post it at or near your workstation.

Periodically, IT staff will review your passwords with you.

SECTION 14 - INFORMATION SYSTEM AND COMPUTER USE

SHCHD wishes to provide staff with a clear understanding of appropriate use of the Information System. The following list outlines acceptable use of the district Information System.

1. Use of the SHCHD Information Systems is restricted to employees and individuals who have contractual agreements with the district. All users of SHCHD Computing facilities are required to adhere to these guidelines.
2. All users of SHCHD computing facilities shall comply with applicable laws, policies, and procedures. *Computing facilities* means computing resources and network systems, including, but not limited to, computer time, data processing or storage functions, computers, computer systems, servers, networks and their input and output and connecting devices, including wireless access points, and any related programs, software, work product and/or documentation.
3. Users shall not examine, change, or use another person's or district files, output, or usernames for which they do not have explicit authorization. Users shall not represent themselves as another individual in electronic communication. In general, all computer and electronic files should be free from access by any but the authorized users of those files. Users who discover access to information not related to the performance of their job duties should immediately notify their supervisor and Information Services
4. User accounts are assigned to a specific individual and may not be shared. Passwords associated with a user account are to be kept confidential. Employees who suspect that another individual has access to their password should report their suspicion to the Information Services and their supervisor immediately.
5. Access or attempts to gain access to district system computing facilities for any unauthorized purpose, including attempts to obtain, modify, or destroy information or degrade performance, is forbidden.
6. Users shall not use computing facilities for any illegal purpose or to enter or send any material that is obscene or defamatory or to enter or send material that is intended to annoy, harass or alarm another person which serves no legitimate purpose.
7. All users shall use software only in accordance with applicable license agreements.
    a. Users shall not make unauthorized copies of any software under any circumstances.
    b. Duplication of licensed software for any purpose except for backup and archival purposes or when otherwise specifically authorized is prohibited.
    c. All software must be lawfully purchased or acquired prior to use on district computing facilities. Users shall not install or use software on district computing facilities in a manner contrary to law or this policy.
8. Use of computing facilities and databases shall be limited to the purpose(s) for which access is granted. **Use of computing facilities or databases for political purposes, for personal or private use or for profit, or for other purposes not related to the employee's or other users duties or purposes for which access is granted, is strictly prohibited**.
9. Supervisors of users with access to district computer facilities are responsible for notifying Information Services when their employee/user either changes jobs within the District or terminates employment. When affiliation ends, the district will terminate the user's account access and transfer the account data according to the direction of the individual's department director. Any new incoming e-mail will be returned to the original sender or be redirected for review. Information Services personnel will delete or modify the user's login as appropriate.
10. Requests for service from Information Services must be made in writing via email to ithelp@shchd.org unless unavailable. Requests should include information on the program being used, a clear description of the problem, and the phone extension and name of the person making the request.
11. Users who violate any part of this policy may be denied access to district computing facilities and shall be subject to discipline up to and including termination and/or criminal prosecution.

SECTION 15 – USE OF ELECTRONIC EQUIPMENT

SHCHD maintains telephones, voicemail, computers, email, and Internet services to facilitate District business. Therefore, all messages and files sent, received, composed and/or stored on these systems are the property of the District.

Personal Use is Extremely Limited
These systems are to be used by employees in conducting District business and are not for employees' personal use. The District understands that on occasion immediate family members may need to leave messages on the voicemail or email system for an employee, and is willing to accommodate such personal use of the system to a limited degree. Personal use of the telephone, voicemail, computer or email system which interferes with an employee's work performance is not tolerated and may result in disciplinary action.

Employees may not install personal software, download software via the Internet or run any software on any computer provided by the District without specific written approval from District management. The unauthorized software will be removed. No employee or third party is permitted to work on District-owned electronic systems to provide troubleshooting or maintenance services without written authorization from the ISO.

Privacy is Not Guaranteed
The District reserves the right to access employees' computer systems, voicemail (outgoing and incoming) and email messages at any time, randomly or as necessary to ensure that there is no misuse or violation of any District policy or any law. In most cases, the employee's outgoing voice-mail message must not indicate to the caller that incoming messages are confidential or private. The existence of a password on any District system is not intended to indicate that the file or communication will remain private from access by District management.

Erasure is Not Reliable
Employees should be aware that even when a message or file has been deleted, it still may be possible to retrieve it from a backup system. Therefore, employees should not rely on the deletion of messages or files to assume they have remained private from access by District management.

File and Message Access
Files on computers and messages on voice-mail and e-mail systems are to be accessed only by the intended user or recipient and by others at the direct request of the intended user or recipient. However, the District reserves the right to access its computers and electronic media systems at any time. Any attempt by persons other than those above to access files or messages on any District system constitutes a serious violation of District policy and may result in disciplinary action up to and including immediate termination.

Harassment and Discrimination
Messages or other electronic communications on District equipment or systems are subject to the same policies regarding harassment and discrimination as are any other workplace communications. Offensive, harassing or discriminatory content in such communications are not tolerated and may result in disciplinary action up to and including immediate termination.

SECTION 16 – Maintenance of Equipment

- Computers/Servers will receive monthly security updates from Microsoft using a WSUS server.
- Computers need to be left on daily to allow for software updates and Anti-Virus scanning to occur.
- Computers will have a full Anti-Virus scan every Wednesday.
- Computers shall be rebooted a minimum of every 7 days. Computers will automatically reboot every Sunday at 4 am to finish installing updates and provide a better user experience. The IT Department is not responsible for lost or damaged files or any data that was not saved before the reboot, including usage in the EMR.
- Servers shall be rebooted at a minimum of every 30 days.

SECTION 17 – Bring Your Own Device (BYOD)

POLICY:
It is the policy of the Southern Humboldt Community Healthcare District ("SHCHD" or "District") to provide extra compensation to those employees whose job duties include the frequent need for a cell phone, in the form of a cell phone allowance, to cover business-related costs on their personal cell phone. No further reimbursement for cell phone costs is available to employees who receive such an allowance.

As a general rule, cell phones should not be selected as an alternative to other means of communication -- e.g., landlines -- when such alternatives would provide adequate but less costly service to the SHCHD.

PURPOSE:
The purpose of this policy and procedure is to establish SHCHD guidelines for employee use of personally owned electronic devices for work-related purposes.

PROCEDURE:
Employees of SHCHD may have the opportunity to use their personal electronic devices for work purposes when authorized in writing, in advance, by the employee and management. Personal electronic devices include personally owned cellphones, smartphones, and tablets.

The use of personal devices is limited to certain employees and may be limited based on compatibility of technology. Contact the human resource (HR) department for more details.

Device Protocols
To ensure the security of SHCHD information, authorized employees are required to have anti-virus and mobile device management (MDM) software installed on their personal mobile devices. This MDM software will store all company-related information, including calendars, e-mails and other applications in one area that is password=protected and secure. SHCHD's IT department must install this software prior to using the personal device for work purposes.

Employees may store company-related information only in this area. Employees may not use cloud-based apps or backups that allow company-related data to be transferred to unsecure parties. Due to security issues, personal devices may not be synchronized with other devices in employees' homes. Making any modifications to the device hardware or software beyond authorized and routine installation updates is prohibited unless approved by IT. Employees may not use unsecure internet sites.

Devices shall not be rooted (Android), or jailbroken (Apple), tampering of the MDM Software is strictly prohibited. Uninstalling or tampering with the MDM Software without approval from SHCHD Information Technology or management will result in dispensary action.

Personal devices should be turned off or set to silent or vibrate mode during meetings and conferences and in other locations where incoming calls may disrupt normal workflow.

When a personal device is replaced with a new personal device, SHCHD Information Technology Department shall be notified immediately. The MDM Software will be removed on the old device, and then installed on the new device.

Restrictions on Authorized Use
Employees who personal devices have camera, video or recording capability are restricted from using those functions anywhere in the building or on company property at any time unless authorized in advance by management.

While at work, employees are expected to exercise the same discretion in using their personal devices as is expected for the use of company devices. SHCHD policies pertaining to harassment, discrimination, retaliation, trade secrets, confidential information and ethics apply to employee use of personal devices for work-related activities.

Nonexempt employees may not use their personal devices for work purposes outside of their normal work schedule without authorization in advance from management. This includes reviewing, sending and responding to e-mails or text messages, responding to phone calls, or making phone calls.

Employees may not use their personal devices for work purposes during periods of unpaid leave without authorization from management. SHCHD reserves the right to deactivate the company's application and access on the employee's personal device during periods of unpaid leave.

An employee may not store information from or related to former employment on the company's application.

Family and friends should not use personal devices that are used for company purposes.

Privacy/Company Access
No employee using his or her personal device should expect any privacy except that which is governed by law. SHCHD has the right, at any time, to monitor and preserve any communications that use the SHCHD's networks in any way, including data, voice mail, telephone logs, internet use and network traffic, to determine proper use.

Management reserves the right to review or retain personal and company-related data on personal devices or to release the data to government agencies or third parties during an investigation or litigation. Management may review the activity and analyze use patterns and may choose to publicize these data to ensure that SHCHD's resources in these areas are being use according to this policy. Furthermore, no employee may knowingly disable any network software or system identified as a monitoring tool.

SHCHD Information Technology Department or Management can at any time request to inspect the device to insure it is in compliance with company policy.

Company Stipend
Employees authorized to use personal devices under this policy will receive an agreed-on monthly stipend based on the position and estimated use of the device. If an employee obtains or currently has a plan that exceeds the monthly stipend, SHCHD will not be liable for the cost difference. Only one personal device will be provided a stipend to the employee. The stipend is treated as taxable income to the employee, but not considered part of their base salary or

used in calculation of retirement benefits. Southern Humboldt Community Healthcare District ("SHCHD" or "District") reserves the right to request employees' cell phone bills.

If a stipend is provided to an employee for a personal device, the device must be maintained in good working order. This includes regular firmware updates, app updates, etc. The personal device should be able to power on and be able to make and receive calls. If the phone is no longer functioning this should be reported to SHCHD Information Technology Department immediately. If the device is no longer in good working order the stipend can be forfeited.

Safety
Employees are expected to follow applicable local, state and federal laws and regulations regarding the use of electronic devices at all times.

Employees whose job responsibilities include regular or occasional driving are expected to refrain from using their personal devices while driving. Exception to this will be handsfree mode, which all applicable state/local laws shall be followed for handsfree usage.

Employees who are charged with traffic violations resulting from the use of their personal devices while driving will be solely responsible for all liabilities that result from such actions.

Employees who work in hazardous areas must refrain from using personal devices while at work in those areas, as such use can potentially be a major safety hazard.

Lost or Stolen Equipment
Employees are expected to protect personal devices used for work-related purposes from loss, damage or theft. In an effort to secure sensitive company data, employees are required to immediately notify SHCHD Information Technology Department and management in the event the device is lost, or stolen. The MDM Software will be immediately uninstalled from the personal device. This allows the company-related data to be erased remotely.

SHCHD will not be responsible for loss or damage of personal applications or data resulting from the use of company applications or the removal of company information.

Separation of Employment
Upon separation of employment, the MDM Software will be immediately uninstalled by SHCHD Information Technology Department. The employee may be asked to produce the personal device for verification of removal of company data.

Violations of policy
Employees who have not received authorization in writing from SHCHD management and who have not provided written consent will not be permitted to use personal devices for work purposes. Failure to follow SHCHD policies and procedures may result in disciplinary action, up to and including termination of employment.

Bring Your Own Device (BYOD) User Agreement

Security of information, and the tools that create, store and distribute that information are vital to the long-term health of our organization. It is for this reason we have established our Electronic Devices: Bring Your Own Device (BYOD) Policy.

All employees are expected to understand and actively participate in this program. Southern Humboldt Community Healthcare District encourages its employees to take a proactive approach in identifying potential problems or violations by promptly reporting them to their supervisor.

Prior to using personal devices for company purposes, each employee is expected to have read the entire Electronic Devices: Bring Your Own Device (BYOD) Policy.

If you have any uncertainty regarding the content of these policies, you are required to consult your supervisor. This should be done prior to signing and agreeing to the Electronic Devices: Bring Your Own Device (BYOD) Policy.

SoHum Health IT Department or Human Resources will provide the approved employee the Bring Your Own Device (BYOD) User Agreement form that needs to be signed and stored in S:\Human Resources\BYOD Signed Agreement

SECTION 18 – REMOTE ACCESS

Access to SoHum Health Remote Gateway/DirectAccess is on an as-needed basis. If an internal employee needs remote access, a request should be made through the employees' manager who will send an email/ticket to SoHum Health IT Department. Exclusions to this are our outside billing company, quarterly reports will be sent to the outside billing companies manager verifying their employees still need access. Once remote access is no longer needed for an employee, the manager shall send an email/ticket to SoHum Health IT Department advising to remove access.

SoHum IT Department is not responsible for any outside factors that would prevent a user from connecting to Remote Access/DirectAccess. Examples of these would include unstable internet connection, slow internet connection, issues with any personal networking equipment (routers, modems, home wireless, home wiring, etc), firewalls blocking access to Remote Access, or using a personal computer to connect to our Remote Access. Anything outside the confines of the SoHum Health Facility is the responsibility of the user. SoHum Health IT Department can provide very limited assistance (though not guaranteed) for Laptops owned by the district while working remotely Any attempt for SoHum Health to remotely connect to a district-owned laptop will need to be connected to the internet, with a stable connection. Once again SoHum Health IT Department will not assist with internet connection issues even on District Owned Laptops.

Verifying you can work remotely:

Minimum internet connection speed needed to connect are:

A stable internet connection that has a minimum download speed of 5 Mbps and a minimum upload speed of 5 Mbps. Latency cannot be greater than 70 milliseconds for ping time. To be eligible to work remotely, all users will need to check their connection to verify that they meet the minimum requirements to access our Remote Access. As mentioned, these speed requirements are the minimum necessary required to support using the SoHum Health Remote Access. You can verify your connection speed at https://speedtest.net. If your internet connection does not meet these minimum requirements you will need to speak to your manager.

SoHum Health IT Department does not provide any support or advice for personal equipment owned by the employee/contractors/vendors.

SECTION 19 – EMAIL USE

1. Email is to be used for company business only. Confidential company information must not be shared outside of the company, without authorization, at any time.
2. Southern Humboldt Community Healthcare District Information Technology Department will not setup forwarding of emails from SHCHD to personal email accounts such as Gmail, Hotmail, Yahoo, etc.
3. Email usage must conform to Southern Humboldt Community Healthcare District harassment and discrimination policies. Messages containing defamatory, obscene, menacing, threatening, offensive, harassing, or otherwise objectionable and/or inappropriate statements and/or messages that disclose personal information without authorization will not be tolerated. If you receive this type of prohibited, unsolicited message, do not forward it. Notify your supervisor, the HR department, and the Director of Information Technology about the message.
4. All communications and information transmitted, received, or archived in the Southern Humboldt Community Healthcare District computer system belong to the District. Information Technology and Southern Humboldt Community Healthcare District Administrate Team have the right to access and disclose all employee email messages transmitted or received via the organization's computer system. Southern Humboldt Community Healthcare District may exercise its legal right to monitor employees' email activity. Regarding email, employees should have no expectation of privacy. Be aware Information Technology and Southern Humboldt Community Healthcare District Administrate Team may access and monitor email at any time, for any reason, with or without prior notice.
5. E-mail messages should be treated as formal business documents. E-mail creates permanent and documented communication and must not be treated casually. Employees are prohibited from sending jokes, rumors, gossip, or unsubstantiated opinions via email. These communications, which often contain objectionable material, are easily misconstrued when communicated electronically. Employees should not waste Southern Humboldt Community Healthcare District computer resources or colleagues' time by engaging in these types of prohibited actions. Send email messages and copies only to those with a legitimate need to read your message. Chain messages, jokes and large graphics should be deleted, not forwarded, as they can overload the system.
6. Emails sent outside of the Southern Humboldt Community Healthcare District network that contains PHI shall be encrypted using a Secure Email Service. It is expected of every end user to use Outlook when using a Southern Humboldt Community Healthcare District provided computer. Emails sent within the Southern Humboldt Community Healthcare District network are Encrypted through Exchange. When an end-user is offsite and authorized, Outlook Web Access shall be used to send communication inside or outside the

network. Personal email accounts are prohibited from being used while working at a Southern Humboldt Community Healthcare District computer to send an email into the network. Example of prohibited activity include sending an email from a non-SHCHD affiliated Gmail account to a Southern Humboldt Community Healthcare District employee. At no time shall patient data be transmitted or sent through personal email accounts.

7. Emails sent from outside recipients that contain zip files (.zip, .7z), executable files (.exe), batch files (.bat) com files (.com), and Microsoft Office macros will be removed before delivery to internal employees for security purposes. These attachments cannot be retrieved or restored.
8. Misuse and/or abuse of the email system of Southern Humboldt Community Healthcare District will result in disciplinary action, up to and including termination.

SECTION 20– EMAIL RETENTION

1. Email shall be backed up using an email archive server, and retained for at least 7 years. Outlook folders that shall not be backed up are; deleted items, and junk emails.
2. Deleted Items, and Junk Email folders will be purged on a regular basis. Deleted Items will be purged every 90 days, Junk Email will be purged every 14 days in order to preserve space on the Exchange Servers. Items in these folders will not and cannot be restored after purging.

SECTION 21 – Security Cameras

PURPOSE:
This policy provides guidelines regarding the use of security cameras at SHCHD, including both Closed Circuit Television (CCTV) and internet-enabled cameras (Webcams). The policy outlines when and how security cameras are to be installed, how images are to be stored and recorded, and the conditions under which stored images or videos are to be used.

PROCEDURE:
Video monitoring for security purposes is conducted in a professional, ethical, and legal manner. Monitoring individuals based on characteristics of race, gender, sexual orientation, disability or other protected classification is prohibited.

Surveillance cameras assist in protecting the safety and property of SHCHD, the public, and district staff. The primary use is to record images for future identification of individuals in the event of legal, criminal, or policy violations. There will be no audio associated with any camera. The district will not install cameras in staff offices or in non-public areas of the facility, excluding patient monitoring when deemed appropriate and necessary.

All requests for the installation of security cameras on SHCHD property must be routed to the Information Technology Department with a written justification of the perceived need. The IT staff will consult with the Chief Operations Officer to determine if additional equipment is needed.

While real-time monitoring is possible at some locations within the facility, recorded images will not be routinely checked and will only be reviewed in the event SHCHD feels it is necessary. Recorded information is stored in a secure location with access by authorized staff only. Recorded footage is retained for two weeks. After two weeks the oldest data is overwritten.

All requests for retrieval of Security Camera footage must go through a member of the SHCHD Administrative team, who will then create an online work order for the Information Technology Department. Members of the public are not able to view recorded images. Law enforcement is allowed to view and/or be provided with a copy of recorded video when needed for investigative purposes. Staff requests must be routed through the employee's direct manager to the administrative team.

Information obtained through video monitoring will be used exclusively for safety, security, compliance with SHCHD policy, and for possible law enforcement purposes. Should monitoring reveal activity that violates policy or law, the proper channels will be contacted.

Violations of policy
Any person who tampers with or destroys video security equipment will be subject to termination at Southern Humboldt Community Healthcare District and/or criminal prosecution.

SECTION 22 – OFFICE MOVES

Office moves require a 3-day notice in advance to both the Engineering Department and SoHum Health IT Department. Even with a 3-day notice, office moves can be complex and could take several weeks or months to complete. An email shall be sent that includes Group Work Orders for SoHum Health Engineering Department | WorkOrders@shchd.org (this will generate a ticket for Engineering) and Group ITHelp | ITHelp@shchd.org for SoHum Health IT Department (this will generate a ticket for the IT Department). Engineering is responsible for moving/setting up desks, and furniture. Once Engineering has completed the setup of desks/furniture, SoHum Health IT Department will be responsible for moving/setting up computers, printers, monitors, and telephone(s).

SECTION 23 - INFORMATION TECHNOLOGY ON CALL -CALLBACK COVERAGE

SHCHD understands the need for on-call Information Technology (IT) staff. The following method is used to contact IT staff after hours:

1. Confirm that the tech you are calling is the tech on-call. The tech name and contact number will be entered on the Acute Nursing and Emergency Room contact white boards.
2. Phone the Tech's number as posted. If there is no answer repeat call in 5 minutes. If there is still no response, call the Chief Operations Officer phone listed at the nursing station. For most issues, the tech will have the ability to resolve your problem via a remote connection. Generally, the on-call tech should be able to be onsite within 90 minutes if needed.
3. Issues that are able to be resolved during regular business hours should be referred to the IT service contact email address ithelp@shchd.org, by utilizing the in-house email service.

With the implementation of Electronic Health Records, the need for IT support increased greatly. Recognizing this, the District will include IT on-call and callback coverage as a part of daily operations.

SECTION 24 - STANDARD OPERATING PROCEDURES (SOP)

DELETION OF USER ACCOUNTS

The following describes the method used when an end user has separated from SHCHD, and their Active Directory account needs to be deleted.

1. Immediately disable users Active Directory account
2. Move account to SBSUsers | Disabled Accounts
3. In the description field of the disabled user place the date account was disabled next to the user's job title
4. After 90 days delete the user account from Disabled Accounts, thus removing them from Active Directory.

USERNAME CHANGE FOR NETWORK ACCESS

The following process is used for times when an end user has had a legal name change that needs to be reflected in Active Directory:

1. Change username in Active Directory
2. Through Exchange Administration. forward old the user’s old email address to their new email address
3. After 90 days remove the forward from their old email and remove that address from Exchange.

INACTIVITY ON NETWORK

The following SOP is used when a login has had no activity on the network during a sequential 30 day period:

1. Disable the account, removing all access to district systems, until they return to work or terminate their association with the district.
2. Re-enable the account upon written (ithelp@shchd.org) Department Manager request.
3. If a period of 90 days of inactivity has passed, the login will be removed from Active Directory.
4. Exception: persons with a valid leave of absence (FMLA) require notification from Human Resources to the ISO for reinstatement.

Personal Devices

1. SHCHD IT Department will not work on personal devices including desktops, laptops, tablets, cell phones, home networks, and any other personal electronic devices/equipment.

Equipment Provided

- Users will have a choice of either a desktop or a laptop but not both (in rare instances there will be exceptions made to this policy).
  Southern Humboldt Community Healthcare District Information Technology Department has a minimum 3-day turnaround for equipment being imaged and setup (dependent on the equipment being in stock and available). Notifications for new equipment must be sent using the Ticket System located on ThePulse, or an

email to Group ITHelp which will generate a ticket. No other means of communication will be excepted.

Equipment Replacement

- SHCHD IT Department will enact a schedule for replacement of equipment to provide a better experience for our Customers and Employees. Desktops will be replaced every 3 years, Servers will be replaced every 5 years (5).

Personal Data Saved To Local Computers

- The IT Department shall not be responsible for data stored on end users local desktop. The IT Department has provided a U drive in order to save data that is personal to one's self. Department data should be saved into the appropriate folder on the S:\ drive. The IT Department will not/cannot restore data saved to the local computer, and will not move data stored on the local computer to the U drive during a computer replacement, fresh image of the OS, hardware failure, etc.

Handling of Equipment

- Staff shall handle equipment provided by the IT Department with due diligence. As equipment is often moved around between various staff members, homogeneity of equipment matters, and helps us keep a professional appearance. Do not write on equipment with pens, sharpies, crayons, etc. Stickers, tape or other foreign objects shall not be attached to laptops, desktops, monitors, printers, scanners nor any other IT equipment. Labels that the IT Department places on equipment for asset tracking purposes shall not be removed nor defaced.

References:

American Health Information Management Association. (2003). *Final Rule for HIPAA Security Standards, Analysis by Policy and Government Relations Team* www.ahima.org

American Medical Association. (2003). HIPAA Security Preparedness. www.ama-assn.org

Department of Health and Human Services. (2013). 45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule.

HIPAA Collaborative of Wisconsin. (2013). HIPAACOW Deliverables. www.hipaacow.org

Implementing Information Security in Healthcare: Building a Security Program presented at HIMSS (2013) by Lisa Gallagher, Terrell Herzig, and Tom Walsh.

(5) How Often Should I Replace My Servers? | https://www.revolutiongroup.com/blog/how-often-should-i-replace-my-servers/

Western Michigan University | https://wmich.edu/it/policies/securitycamera

REVIEWED BY:

Chief Operations Officer
Information Technology Manager

REVISED POLICY

HUMAN RESOURCES

SoHum
Health
Southern Humboldt
Community Healthcare District
733 CEDAR STREET
GARBERVILLE, CA 95542
(707) 923-3921

DEPARTMENT: Human Resources	NO:	Page 1 of 2
SUBJECT: **Remote Work Policy** (Previously Telecommuting Policy)	EFFECTIVE DATE: 12/02/2021	SUPERSEDES: 08/31/2017

Policy:
It is the policy of the Southern Humboldt Community Healthcare District ("SHCHD" or "District") to occasionally grant employees the privilege of working remotely when appropriate.

Objective:
SHCHD considers remote work to be a viable alternative work arrangement in cases where individual, job and supervisor characteristics are best suited to such an arrangement. Remote work allows employees to work at home, on the road or in a satellite location for all or part of their regular workweek. Remote work is a voluntary work alternative that may be appropriate for some employees and some jobs. It is not an entitlement, it is not a company-wide benefit, and it in no way changes the terms and conditions of employment with SHCHD. Working from a remote location adds challenges to effective communication, teamwork and collaboration. The telecommuting employee is responsible for ensuring effective communication and participation while working remotely and for ensuring that coworkers and his/her manager feel informed and confident about the work results being produced.

Procedure:
All telecommuting employees are responsible for the following:
- Maintain consistent work hours.
- Establish a routine of periodic work plans and reports to your manager/team to establish goals and document results.
- Be readily available for impromptu video, email and phone conversations.
- Maintain a dedicated home office environment free of distractions and background noise.
- Devote 100% of attention when working from home as if you were in the office.
- Comply with all requirements in the Information Technology Manual
- Store all work product on the company network and do not store it on any local storage of the home computer or laptop.
- Report to the Company's offices and/or other locations in person for meetings or other activities as required by the employee's manager.
- Managers may require additional methods of communication and reporting to ensure employees are accessible and reliable.

Approval Process:
- For full time remote work the request must be submitted to the Human Resources office for approval by the Administrative Team.
- For regularly scheduled remote work the request must be approved by that Departments Administrator.
- For circumstantial remote work the request must be approved by the direct Supervisor.

Home Office Requirements:
Ongoing remote work arrangements require the employee to establish a fully functioning home office environment. The Company will decide on a case-by-case basis whether or not to provide the remote working employee a computer or monitors for the home office. All other equipment and services are the responsibility of the employee to be paid at his/her expense including:

- Phone and voicemail with professional outgoing message
- DSL or other high speed Internet connection
- If wireless network is used, a secure, password-protected connection
- Fax capabilities (if required to perform job duties)
- Repairs or adjustments necessary to maintain a safe working environment

Remote work is for the personal convenience of the employee. The Company maintains work facilities and equipment in its offices. Therefore, if the employee uses his/her personal computer the Company will not:

- Provide support for personal systems
- Provide maintenance, repairs or adjustments of any kind
- Provide upgrades for hardware
- Provide upgrades for operating systems
- Reimburse for the purchase of any software programs

At the conclusion of employment, employees who use their own computer or other personal equipment will be required to certify that there is no company information on their computer or equipment, and to certify that all company data, information and property has been returned.

Reference:

Telecommuting Policy 8/31/2017.

Reviewed By:

Human Resources
Chief Executive Officer

SOUTHERN HUMBOLDT
SHCHD
COMMUNITY HEALTHCARE DISTRICT
733 CEDAR STREET
GARBERVILLE, CA 95542
(707) 923-3921

DEPARTMENT: Human Resources	NO:	Page 1 of 2
SUBJECT: **Telecommuting Policy**	EFFECTIVE DATE: 08/31/17	REVISED:

POLICY:
It is the policy of the Southern Humboldt Community Healthcare District ("SHCHD" or "District") to occasionally grant employees the privilege of working remotely when appropriate.

OBJECTIVE:
SHCHD considers telecommuting to be a viable alternative work arrangement in cases where individual, job and supervisor characteristics are best suited to such an arrangement. Telecommuting allows employees to work at home, on the road or in a satellite location for all or part of their regular workweek. Telecommuting is a voluntary work alternative that may be appropriate for some employees and some jobs. It is not an entitlement, it is not a company-wide benefit, and it in no way changes the terms and conditions of employment with SHCHD.

PROCEDURE:

1. Either an employee or a supervisor can suggest telecommuting as a possible work arrangement. Telecommuting is a privilege and employees are only permitted to work from home with prior permission from their immediate supervisor. Any attempt to work at home without prior permission, with or without reporting such time, will result in disciplinary action in accordance with the company's discipline policy.
2. Telecommuting is an occasional work alternative, such as working from home for a short-term project or on the road during business travel. Other informal, short-term arrangements may be made for employees on family or medical leave, to the extent practical for the employee and the organization and with the consent of the employee's health care provider, if appropriate. All informal telecommuting arrangements are made on a case-by-case basis, focusing first on the business needs of the organization. Such informal arrangements are not the focus of this policy.
3. Individuals requesting telecommuting arrangements must have been employed with SHCHD for a minimum of 12 months of continuous, regular employment and must have exhibited above-average performance, in accordance with the company's performance appraisal process.
4. Before granting permission for short-term, work-at-home arrangements, supervisors should know the specific work to be performed and the projected amount of time expected. If the work at home will cause a nonexempt employee to work enough hours per day or week to become eligible for overtime under federal and state law, then the supervisor should consult the overtime policy before granting permission.
5. Equipment supplied by the organization is to be used for business purposes only. The telecommuter should sign an inventory of all office property and agrees to take appropriate action to protect the items from damage or theft. Upon termination of employment all company property will be returned to the company, unless other arrangements have been made.
6. Consistent with the organization's expectations of information security for employees working at the office, telecommuting employees will be expected to ensure the protection of proprietary company and customer information accessible from their home office. Steps include use of locked file cabinets and desks, regular password maintenance, and any other steps appropriate for the job and the environment.
7. The employee will establish an appropriate work environment within his or her home for work purposes. SHCHD will not be responsible for costs associated with initial setup of the employee's home office such as remodeling, furniture or lighting, nor for repairs or modifications to the home office space.
8. The employee and manager will agree on the number of days or hours telecommuting is allowed each week, the work schedule the employee will customarily maintain, and the manner and frequency of communication. The employee agrees to be accessible by phone or modem within a reasonable time period during the agreed-on work schedule.
9. Telecommuting employees who are not exempt from the overtime requirements of the Fair Labor Standards Act will be required to record all hours worked in a manner designated by the organization. Telecommuting employees will be held to a higher standard of compliance than office-based employees due to the nature of the work arrangement. Hours worked in excess of those specified per day and per workweek, in accordance with state and federal requirements, will require the advance approval of the supervisor. Failure to comply with this requirement can result in the immediate cessation of the telecommuting agreement.

10. Before entering into any telecommuting agreement, the employee and manager, with the assistance of the human resource department, will evaluate the suitability of such an arrangement paying particular attention to the following areas:

    a. Employee suitability. The employee and manager will assess the needs and work habits of the employee, compared to traits customarily recognized as appropriate for successful telecommuters.
    b. Job responsibilities. The employee and manager will discuss the job responsibilities and determine if the job is appropriate for a telecommuting arrangement.
    c. Equipment needs, workspace design considerations and scheduling issues.
    d. Tax and other legal implications for the business use of the employee's home based on Internal Revenue Service (IRS) and state and local government restrictions. Responsibility for fulfilling all obligations in this area rests solely with the employee.

REFERENCE:
Telecommuting Policy and Procedure #1, Society for Human Resources Management, 5/30/2014.

REVIEWED BY:
Human Resources
Chief Executive Officer

REVISED POLICIES

PHARMACY

SoHum Health
Southern Humboldt
Community Healthcare District
733 Cedar Street
Garberville, CA 95542
(707) 923-3921

DEPARTMENT: Pharmacy	NO:	Page 1 of 1
SUBJECT: **Emergency Medication Supply (Crash Carts)**	EFFECTIVE DATE: 12/02/2021	SUPERCEDES: 05/28/2020

POLICY:
It is the policy of the Southern Humboldt Community Healthcare District ("SHCHD" or "District") to properly maintain and store emergency medications in our crash carts.

PURPOSE:
The purpose of this policy and procedure is to ensure that our crash carts are always supplied with emergency medications and sealed properly.

Cardiac arrest medications, and medications used in medical emergencies, are immediately available in the crash cart in the emergency room, between bed 1 and 2; and the crash cart in room 109 on the Acute Floor. The Pediatric crash cart is located in the emergency room by bed 4. During a pediatric code blue, staff is to utilize the pediatric crash cart supplies in conjunction with the medications in either of the other two crash carts. The emergency drug supply is stored in a clearly marked portable container which is sealed by the pharmacist in such a manner that a seal must be broken to gain access to the medications. On the side of each cart is a list of all medications and their expiration dates. Contents of the medications drawers of the emergency crash cart shall be the responsibility of the pharmacy staff or the nursing staff when the pharmacist is unavailable.

PROCEDURE:
1. After the crash cart is stocked it will be sealed with a red plastic lock by the pharmacy staff. Each time a crash cart is sealed, the lock number will be recorded in the crash cart log along with the date and initial of the pharmacy staff.
2. When it is necessary to use a crash cart, it is imperative that it be restocked as soon as possible after use. Pharmacy is responsible to restock medications in the crash carts. In the absence of pharmacy staff, nursing staff will restock the cart.
3. Nursing staff is responsible ~~It is the responsibility of the nurse on duty~~ to notify the pharmacy department via email that the crash cart has been opened and seal it with a yellow lock. The yellow lock indicates the cart has been used, while preventing diversion.
5. Once restocked, the pharmacist will verify and seal the cart with a red lock per procedure # 1, above.
6. If emergency medications from both crash carts have been used, pharmacy staff will be notified immediately and will restock both crash carts according to procedure as soon as possible.
7. ~~The RN on duty~~ Nursing staff is responsible for making sure the Pediatric crash cart is restocked as soon as possible with the correct supplies and resealed with a red plastic lock.

REVIEWED BY:
ER/Acute Nurse Manager
Chief Nursing Officer/Director of Patient Care Services
Clinic Nurse Manager
Clinic Medical Director
ER/Hospital Medical Director

SoHum Health
Southern Humboldt
Community Healthcare District
733 Cedar Street
Garberville, CA 95542
(707) 923-3921

DEPARTMENT: Pharmacy	NO:	Page 1 of 1
SUBJECT: Patient's Own Medications	EFFECTIVE DATE: 12/02/2021	SUPERCEDES: 01/18/2021

POLICY:
It is the policy of the Southern Humboldt Community Healthcare District ("SHCHD" or "District") to prohibit the use of home medications while receiving treatment in the hospital with the exception of certain non-formulary items or which will result in delay of treatment.

PURPOSE:
The purpose of this policy and procedure is to describe the procedure to be followed for the use of medications brought into the hospital by a patient.

PROCEDURE:
All efforts will be made to use the hospitals medication supply. This will ensure accuracy, consistency, and proper storage and handling of medication use.

The procedure below outlines the steps taken when a physician's order warrants the use of a patient's home medication:

1. Only non-formulary or out of stock medications with an active order can be used as home medication.
2. The physician or pharmacist shall verify the identity and integrity of all home medications prior to their drop-off for home medication use.
3. If the directions stated on the home medication differs from current orders, a removable flag label shall be placed on the home medication to ensure accurate administration throughout their stay.
4. The medications will be marked in the electronic record as home medications to avoid improper charges.
5. If a home medication is discontinued, it shall be placed in a clear ziploc bag, stickered with a registration label and a second label stating, "MEDICATION FROM HOME TAKEN TO PHARMACY" then stored in the appropriate bin for patient's own discontinued medications.
6. A label stating "MEDICATION FROM HOME TAKEN TO PHARMACY" shall be placed on the Personal Belongings Listing form as a reminder to review any home medications taken from the patient on arrival and return them upon discharge.
7. Home medications for a controlled substance shall be recorded to include the name, quantity, and dates for accuracy. The clear bag will be stored inside safe at the nurses' station. A signature is required for controlled substances dropped-off and picked upon discharge.
8. If the stored medications have not been picked up within 30 days of discharge or in the unfortunate event the patient expires, pharmacy staff will destroy them appropriately in the pharmaceutical waste containers.
9. No medications will be administered ~~returned~~ which do not meet proper labeling or integrity requirements.
10. ~~Medications will also need physician approval to be returned.~~

REVIEWED BY:
Pharmacist
Chief Nursing Officer
Director of Patient Care Services
ER/Acute Nurse Manager
Skilled Nursing Manager

SoHum Health
Southern Humboldt
Community Healthcare District
733 Cedar Street
Garberville, CA 95542
(707) 923-3921

DEPARTMENT: Pharmacy	NO:	Page 1 of 2
SUBJECT: Prescription Pads	EFFECTIVE DATE: 12/02/2021	SUPERCEDES: 10/28/2020

Policy:
It is the policy of the Southern Humboldt Community Healthcare District ("SHCHD" or "District") to maintain control of provider prescription blanks to prevent fraudulent use.

Purpose:
The purpose of this policy and procedure is to describe the storage, issuance, use, and monitoring of the District's blank prescription pads.

Procedure:

Ordering and Storing

1. Prescription pads will be ordered by the Pharmacy ~~Operations~~ Manager.
2. Prescription pads belonging to Emergency room providers will be stored in the med room.
3. Prescription pads belonging to clinic providers will be stored in a locked cabinet in the clinic manager's office.
4. Pads will be individual and numbered for each provider, listing that provider's name and other pertinent information on the top. Providers will use only their pad.
5. Emergency Room physicians will use a standard ER pad listing the ER Medical Director's name on the top. A stamp clearly indicating each physician's name, license and DEA number should be placed on the top of the pad in the space provided. The District will supply the stamps.
6. Physicians who are no longer on duty will give their unused pad of prescriptions and their name stamp to either the ER RN or Pharmacy ~~Operations~~ Manager who will put them into the drug room for storage until he/she returns ~~again.~~ Newly arriving physicians should contact the ER RN or Pharmacy ~~Operations~~ Manager to retrieve their pad and stamp.

Pad Distribution

1. Each provider shall be given one control pad.
2. Each provider is responsible for his/her pad. Pads must NEVER be left in a drawer in an exam room or in the ER.
3. When the pad is filled, the provider shall contact the Pharmacy ~~Operations~~ Manager, turn in the completed pad, and be issued a new one.
4. Final storage of the filled pads is the responsibility of the Pharmacy ~~Operations~~ Manager.

Pad Use

1. All prescriptions must be written and signed in ink by a licensed independent practitioner authorized to prescribe medications.
2. Original prescriptions are given to the patient; the copy is kept in the pad and returned to the Pharmacy ~~Operations~~ Manager when the pad is filled.
3. A copy of the original shall should be put into the patient's medical record. DO NOT PUT the copy from the pad into the medical record. It is not permanent material and it fades with time.

Pad Stolen

1. First, the theft or loss must be reported to the local law enforcement and create an incident report.
2. The theft or loss of any tamper-resistant prescription forms must be reported by the physician to the Department of Justice (DOJ) Controlled Substance Utilization Review and Evaluation System (CURES) program no later than three days after the discovery of the theft or loss. Email SecurityPrinter@doj.ca.gov
3. Notify the California State Board of Pharmacy at BOPcomplaint@dca.ca.gov.
4. Notify the Medical Board by an email to complaint@mbc.ca.gov

REFERENCES:
California Pharmacy Law 2021
Medical Board of California

REVIEWED BY:
Pharmacist
Chief Nursing Officer
Director of Patient Care Services
ER/Acute Nurse Manager
Skilled Nursing Manager