IT and Data Security

Policy Type:	Information Management	**Policy Number:**	806
Original Issue:	04/19/2011	**Effective Date:**	08/29/2023
Document Owner's Approval:	 Howard Thibodaux, Information Technology Director		
Executive Director's Approval:	 Kristin Bonner, MHA, BSN, RN, Executive Director		

Policy Statement:

South Central Louisiana Human Services Authority (SCLHSA) requires that use of computer equipment and systems comply with safety and security standards necessary to protect electronic Protected Health Information (ePHI) stored on all forms of hardware and software, from unauthorized access, viruses, any form of damage or unauthorized alteration. All sensitive data, networks, and equipment will be protected by administrative, physical and technical safeguards restricting access using unique user identification with strong passwords, virus protection software, routine data backups, and maintained in safe environments. Employees are granted access to those areas of the network and applications necessary and pertinent to their jobs for work-related purposes. The use of the term "employee" includes contract workers, interns, and other individuals working under agreements with the Authority. SCLHSA employees and contract staff are expected to abide by all policies governing the use of network resources. Failure to do so may result in corrective and/or disciplinary action including termination from employment.

Rationale:

To ensure the security and integrity of Protected Health Information (PHI) stored in the SCLHSA computer network by implementing administrative, physical and technical safeguards to prevent unauthorized access to and use of all data systems.

Procedure:

A. Data Classification

1. Information must be protected according to its sensibility, criticality, and value, regardless of the media on which it is stored, the systems that process it, or the methods by which it is distributed.
2. Information is classified by the following three levels:
   a. **Public** – Information normally available in the public domain and readily available for access and use through authorized department channels. Considered to be non-sensitive and requires limited protection.
   b. **Internal** – Information intended and authorized for use by SCLHSA employees when conducting business. Intended for internal use only.
   c. **Confidential** – Information, that, if disclosed, could violate the privacy of individuals, negatively impact the credibility and public trust. Unauthorized disclosure can cause severe impact to reputation, credibility, or be the cause for major liability or penalty.

3. Employees are responsible for protecting sensitive information from unauthorized access, modification, destruction, or disclosure whether accidental or intentional at any of their work locations.

B. Workstation and Equipment Usage

1. Staff are routinely assigned the use of SCLHSA personal computing assets, including desktop, laptop or hand-held computing devices, as well as associated ancillary storage, backup, and communications devices, herein referred to as personal computing devices.
2. Personal privacy protection is NOT provided to employees and must not be expected when using SCLHSA personal computing devices and may be accessed (both physically and logically), audited, reviewed, monitored and modified as deemed appropriate. SCLHSA reserves the right to regulate, control, direct, specify, limit, and/or terminate the usage of its personal computing devices, at any time, for any reason.
3. Use of SCLHSA personal computing devices is encouraged where such use supports the goals and objectives of SCLHSA. Use of these devices for inappropriate purposes is prohibited.
4. SCLHSA recognizes that personal computing devices may be used on an occasional basis for personal needs as long as such use is in compliance with all of the SCLHSA policies and standards, and:
    a. Does not affect job performance or disrupt others.
    b. Is truly occasional in nature, based on supervisor's recommendation.
    c. Is not in the furtherance of the business activity of any entity other than SCLHSA.
    d. Does not result in any additional billing or direct cost to SCLHSA.
    e. Does not access or transmit material containing derogatory racial, gender, religious or hate-oriented comments, sexual content, offensive language, material which would negatively reflect upon SCLHSA or be likely to offend co-workers, or contents prohibited by law or regulation.
    f. Is not used to solicit funds, collect signatures, conduct membership drives, distribute literature or gifts, sell merchandise or services or carry on any other form of business without approval.
    g. Does not represent a personal position as that of SCLHSA.
5. Except in the furtherance of SCLHSA business, the personal computing devices may not be used for the dissemination or storage of:
    a. Commercial or personal advertisements,
    b. Solicitations,
    c. Promotions,
    d. Destructive programs (that is, viruses or self-replicating code),
    e. Political material, or
    f. Any other unauthorized use.
6. SCLHSA personal computing devices must not be used to create, transmit, receive or store:
    a. Threats,
    b. Pornographic or sexually explicit material,
    c. Material containing derogatory racial, gender, religious or hate-oriented comments,
    d. Offensive language, or material which is otherwise inappropriate or unlawful, or
    e. Discriminatory language or remarks that would constitute harassment of any type.
    f. Users must exercise good judgment when using a SCLHSA personal computing device. At all times, users have the responsibility to use the SCLHSA personal computing devices in a professional, ethical and lawful manner.
7. Concerns about appropriate use of SCLHSA personal computing devices should be addressed with a Supervisor.
8. Use of software installed on a SCLHSA personal computing devices must be in accordance with the license agreement and copyright for that software. **WARNING! – Software provided to employees for work use is governed by licensing agreements that dictate how and**

where that software may be legally used. SCLHSA expects employees to abide by these licensing agreements, strictly prohibits violation of the licensing agreement and will subject employees to appropriate disciplinary action. Proof of purchase for business use is required for all licensed software installed on a SCLHSA personal computing device. The IT Director must approve any non-SCLHSA software before it is installed on any SCLHSA device. The IT Director will validate software ownership and terms of use in a business environment.

9. All equipment and methods of communication including but not limited to fax machines, copiers, phone systems, email, scanners, portable devices and storage devices must be used in a safe and secure manner that protects the equipment and the data from any form of unauthorized access, modification, destruction, or disclosure. All equipment and communication methods must be used for approved business purposes, and any use that is not clearly authorized in this policy, must be pre-approved through the IT Director and SCLHSA Administration.
10. Any violations or suspected violations must be reported to the IT Director and/or Compliance Officer.

C. Physical Safeguards

1. Physical safeguards will be maintained to ensure the appropriate range of temperatures, ventilation, electrical requirements, the prevention of unauthorized access or minimize incidental disclosure, and to prevent or minimize risks / damage from water, theft, vandalism, electromagnetic interference, or forces of nature. Staff will take steps to minimize incidental access by positioning computer monitors away from doorways, and employing device and media controls such as privacy screens, enabling password protected screen savers and logging off workstations.
2. Site specific facility access controls such as signage, barrier doors, visitor policies and restricted areas are established to safeguard and prevent unauthorized access, tampering, and theft of ePHI and any other PHI generated or received.
3. IT Staff will routinely inspect and assess the effectiveness of physical safeguards at each location.
4. IT staff will adhere to SCLHSA policy on property control and privacy when undertaking repair of any personal computing device.

D. Technical Safeguards

1. Employees requiring access to any SCLHSA computer networks or data systems must request specific rights/access via the Personnel Authorization and Access form. The form is generated upon hire and authorized by the employee's Supervisor and then approved by the Executive Director. IT Department staff will assign rights to data systems as approved by this form. Any changes in access must be requested by this same process.
2. An employee's level of access to the network and individual applications is authorized based on the need to perform his/her job, while maintaining network security and integrity, including safeguards for Protected Health Information (PHI).
3. The Information Technology Department issues each user's unique identification and password. This information must be protected in a secure manner.
4. SCLHSA Network Passwords:
    a. Must be a minimum of six characters; including one capital letter and one number
    b. Must be kept confidential at all times; shared with no one
    c. Must be changed whenever it is determined network security may have been compromised
    d. Must be changed upon first use after the Information Technology department resets a password. When changing a password, the user must first enter the old password and then the new password before the new password becomes valid. This is to ensure the password is secure and that it is the employee who is changing the password, not

someone else. Password change prompts occur every 90 days.

5. Other Data System Passwords:
   a. Must be kept confidential at all times; shared with no one;
   b. Must have specific requirements for length, alphanumeric combinations, complexity, and expiration settings;
   c. Must be changed whenever it is determined PHI may have been compromised or as prompted by the system.
   d. Passwords should not be written where it can be seen by another person.
6. The employee's supervisor or designated trainer is responsible for requesting logon and security level for other data or software. The electronic record administrator coordinates access to needed permissions in that system or software.
7. If access to the network or other data systems is denied for reason, the employee must contact the Information Technology department via its "Help Desk" to request restoration of access or to the designated administrator of the system being denied.
8. Employees are responsible for securing their passwords. Corrective and/or disciplinary action may be taken with an employee whose passwords must be reset three times within a 14 day time period.
9. Supervisors, Human Resources, or other Administrative staff should notify the IT Department and other system administrators of any changes in personnel (new hires, promotions, terminations, changes in location, other changes in job duties) that may result in the need for changes to IT authorization and access. Adding or changing IT access should be requested using the Personnel Authorization Form. Employee separations should result in immediate disabling of all related system access codes and passwords for the terminated employee.
10. The SCLHSA network has automatic log off and sleep modes settings, which requires the authorized user to re-enter unique log on information in order to prevent unauthorized user access data on unattended workstations.
11. Encryption can be enabled by an email administrator through the Office of Technology Services. The below information is provided to help all staff understand and utilize the Secure Email Feature that SCLHSA has implemented. IT has added this feature for all of our email accounts as a way to send highly confidential and private information via our la.gov emails. Using the secure email feature is easy, but you must be careful to do it correctly. How to send a [secure] email:
    a. To send a secure email you have to bracket the word **secure** in the subject line, anywhere.
    b. Nothing can touch the outer parts of the brackets.
    c. If any letter or character should touch any part of the brackets, the email is no longer secure.
    d. You must utilize the Brackets [ ] and not the parenthesis { }.
12. The Human Resources Department is responsible for providing timely e-mail notification to the Information Technology Department of all employee separations processed through that department. The Clinic Manager or Supervisor is responsible for providing timely e-mail notification to the Information Technology Department of separations of contract worker, interns, and other individuals working under agreements with the Authority. Information Technology is responsible for removing all access to SCLHSA network and applications according to notification received. 3rd party applications, such as eCW, are managed by a local system administrator.
13. By e-mail notification from the Clinic Manager or Supervisor, the Information Technology Department may provide access to the terminated employee's personal drive and email to that Clinic Manager or Supervisor for a period of time not to exceed 90 working days. During this time, he/she is responsible for reviewing stored documents and for copying those considered to be public records for retention per SCLHSA's Record Retention Schedule. At the close of the 90 working days, the terminated employee's personal drive is deleted or archived.
14. Remote access to ePHI is allowed when the following conditions are met:

a. Secure remote access must be strictly controlled through password authentication.
b. Wireless connections on personal networks must be encrypted using WEP, LEAP, or other acceptable encryption methods. If connecting through a router that has a wireless transmitter, the transmitter must be configured in an encrypted mode or it must be turned off.
c. All computer or devices connecting to a SCLHSA or other internal network must use active anti-virus software with the most recent virus definitions, and must be updated with the latest security patches for that operating system.
d. Remote access connections directly to SCLHSA workstations are acceptable provided that:
    i. The software is approved by IT Director or the Executive Director.
    ii. The software uses encryption from end to end.
    iii. Both of the connecting computers meet the minimum-security requirements for virus software and password requirements.
    iv. The user knows and approves access to that computer.
e. All administrative, technical and physical safeguards must be followed while operating in a remote access mode.

15. Virus scanning software must be active on all equipment at all times with current versions of the virus definitions.
    a. All flash drives, external hard drives, or any other types of portable storage must be verified as free from viruses prior to connecting to SCLHSA equipment or networks.
    b. If a workstation or other equipment is determined to be infected by a virus, IT staff will take methods to isolate that equipment from the network until the equipment is verified as clean.
    c. Virus scanning is scheduled on a weekly basis and all users receive notification on instructions for workstation preparation.
    d. IT staff routinely monitor the use of all external storage devices to assure the integrity and security of the network.

E. Administrative Safeguards

1. SCLHSA requires that all PHI generated or received be protected by policy, procedure and practice and that personnel conduct is defined in regard to the utilization, dissemination and documentation of PHI.
2. Rooms that house paper-based PHI are locked and personnel are authorized limited access as determined by on-site Managers based on job function and role.
3. Site-specific procedures define the return of PHI to locked storage areas after use and at the end of the business day and the disposal of discarded PHI by shredding.
4. ePHI is secured through password protection in all systems where it is generated.
5. Business associate contracts and other outside contract entities that are entrusted with PHI generated by SCLHSA are expected to be HIPAA compliant and have products that are HIPAA compliant.
6. Office machines such as multi-function copiers/printers shall have auto-clearing features so that PHI duplicated, faxed, scanned, or printed documents will not be stored. Applicable policies of the Louisiana Property Assistance Agency (LPAA) should be followed.
7. Data that is stored on any device or electronic media shall be kept according to record retention policies and thereafter sanitized by destruction, purging or clearing. The Data Sanitization Standards of the State of Louisiana Office of Technology Services shall be followed. Specific requirements are found in those standards and requirements and are attached to this policy for information. The IT Department is responsible for maintaining a Sanitization Log with the recommended fields of information. Applicable policies and practices from the (LPAA) should be followed.
8. Contingency plans to manage PHI sources such as patient accounting and financial records,

medical and health records and any other ePHI or PHI created have been developed. A formal back up process is in place and includes:

a. Performing regular backups of all critical data (as determined by the IT Director or Executive Director) on the system.
b. Ensuring the availability of installation media/files for all application software, as well as patches and updates required to rebuild the system to the previous state.
c. SCLHSA's data network was created as mesh topology, which means the data is distributed to each of the servers daily, ensuring that backup copies of all critical programs and data are stored in a protected area.
d. Performing a periodic verification of the backup restore process.
e. Employees are required to save their work-related documents on the designated network drives, which are backed up daily. Employees who save their work on their local drive or external media risk losing the data. Any files or documents initially stored on their local drive must be copied to the approved network drives and folders. Protected Health Information (PHI) should never be stored on the local hard drives of workstations.
f. Shared folders are created by the Information Technology Department by a Help Desk ticket from a Clinic Manager or Supervisor. A single form may be completed to list employees who need access to the folder and the degree of that access, i.e. read only or read/write capabilities. Any change in access is submitted via this same form. The Clinic Manager or Supervisor is responsible for managing the folder. The Information Technology Department is responsible for maintaining documentation and security.
g. The Information Technology Department routinely monitors data stored in the Shared folders and deletes personal data (documents, photographs, etc.) at the discretion of the IT Staff after e-mail notification is sent to the employee and his/her Clinic Manager or Supervisor.

9. eClinicalWorks, the electronic health record utilized by SCLHSA features a secure, cloud-based system that routinely performs scheduled backups (both incremental and full backups). The cloud-based system can be accessed through any device with a Google Chrome browser.
10. A formal Security Risk Assessment is completed annually in a collaborative manner with associated departments and is based on ongoing regular inspection and monitoring by the IT Department of security and administrative, physical and technical safeguards developed for the integrity of all PHI generated by SCLHSA and that provided by outside agencies for the service provision to our clients and stakeholders.

Compliance Requirement:

- Louisiana Property Assistance Agency (LPAA)
- The Data Sanitization Standards of the State of Louisiana Office of Technology Services
- HIPAA Compliance

Attachments:

There are no attachments for this policy.

Linkages:

There are no linkages for this policy.