Saint Luke's HEALTH SYSTEM

# SLHS Information Security Training

## Paper Version

*All SLHS Employees should complete the online version via HealthStream.*

Please read the summary of each policy then answer the questions. For additional information, the policies can be found on PolicyStat.

***Record your answers on the Answer Sheet (separate page)***

## IMPORTANT DEFINITIONS

Please refer to these definitions when completing the training tool.

**Electronic Protected Health Information (EPHI)** – individual electronic health information. (See PHI below)

**Protected Health Information (PHI)** means individually identifiable health information:

1. Except as provided in paragraph (2) of this definition, that is:
   i. Transmitted by electronic media;
   ii. Maintained in any medium described in the definition of electronic media at § 162.103 of this subchapter; or
   iii. Transmitted or maintained in any other form or medium.
2. *Protected health information* excludes individually identifiable health information in:
   i. Education records covered by the Family Educational Right and Privacy Act, as amended, 20 U.S.C. 1232g;
   ii. Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and
   iii. Employment records held by a covered entity in its role as an employer.

**Workforce –** persons whose performance of work conduct is under the direct control of a SLHS entity, whether or not they are paid by that entity. This includes full and part-time employees, affiliates, associates, medical staff, students, volunteers, and staff from third party affiliates who provide services (contractors, agency, consultants, etc.)

## ECPS-401: Acceptable Use of Information Technology, System, and Services

The purpose of this policy is to outline the acceptable use of information technology, systems, and services at Saint Luke's Health System (SLHS). These "acceptable use" rules are needed to protect the employee, SLHS and the patients/customers of SLHS. Inappropriate use of information technology exposes SLHS to unnecessary risks (i.e. virus attacks, compromise of network systems and services, legal issues).

Users should be aware that the data they create on the SLHS systems remains the property of SLHS. Employees are responsible for exercising good judgment regarding the reasonableness of personal use, if there is any uncertainty, employees should consult their supervisor or manager.

For confidential electronic information, including but not limited to Protected Health Information, corporate strategies, competitor-sensitive information, and research data, employees should take necessary steps to prevent unauthorized access to this information.

Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. User level passwords should be changed annually.

All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off when the host will be unattended.

Under no circumstances is an employee/workforce member of SLHS authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing SLHS-owned resources, to include but not limited to:

- The installation or distribution of "pirated" or other software products that are not appropriately licensed for use by SLHS
- Unauthorized copying of copyrighted material
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws

1. Inappropriate use of information technology can expose SLHS to unnecessary risks such as virus attacks, compromise of systems/services, or legal issues.

   True (T)
   False (F)

2. Due to safeguards installed, employees/workforce do not have to take steps to prevent unauthorized access to confidential electronic information and protected health information (PHI).

   True (T)
   False (F)

3. All SLHS network users have unique IDs and passwords. Users select a password which...

   A. May be shared with other users within the same department.
   B. Can be written on a note and taped to the computer monitor.
   C. Should be kept secure and never shared.
   D. Can only be shared with IS personnel.

4. All PCs, laptops and workstations should be secured with a password-protected screensaver with automatic activation feature set at 30 min.

   True (T)
   False (F)

## ECPS-402: Encryption of Confidential Information
## EPCS-413 Transmitting Confidential Information

Saint Luke's Health System (SLHS) recognizes that at times, the protection of confidential electronic information, especially protected health information (PHI), requires extra steps to ensure that such information cannot be read by others. Such extra steps typically involve scrambling information in a unique, secret way—called encryption--so others cannot read it unless they have been provided secret keys to de-encrypt the information.

Only Federal Information Processing Standards (FIPS) 140-2 approved encryption will be used to protect electronic protected health information (ePHI). The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by the Director, Information Security.

Approved encryption solutions must be implemented in the following situations:

- Confidential data is being transmitted outside of the SLHS production network
- Confidential data is being stored on removable media
- All SLHS corporate owned laptops
- Computer systems that store confidential data in areas where management deems physical access controls are not appropriate and the system may be at risk of being lost or stolen

5. Electronic confidential information (such as PHI) that is transmitted over the internet must be protected through the use of FIPS 140-2 approved encryption technology.

   True (T)
   False (F)

## ECPS-403: Acceptable Access/Usage of E-mail, Voicemail, and Internet

E-mail, voice mail and the Internet are to be used for business purposes and each individual with access is expected to use them in a productive manner for the benefit of Saint Luke's Health System. Messages will not:

- be electronically sent outside of SLHS (i.e., via the Internet) if they contain confidential or protected health information, unless it is sent through approved secure e-mail methods;
- contain harassing language or messages that could reasonably be considered offensive by others, to include remarks about an individual or group's race, religion, national origin, physical attributes or sexual preference;
- involve junk mail, chain letters or hoaxes;
- be solicitations for personal gain or profit, or advancement of individual views;
- involve any kind of illegal activity, such as gambling, hacking and pornography; and
- utilize customized backgrounds or stationeries and / or personal phrases / popular quotes at the end of emails.

Incidental personal use of e-mail, voice mail and the Internet are acceptable provided the use is reasonable and professional with minimum impact to SLHS resources, and does not interfere with job responsibilities. Non-business related e-mails (i.e., shopping ads, joke lists, personal pictures, club or personal newsletters) should not be received at SLHS. Employees/workforce are expected to have such e-mails delivered to their personal/home e-mail address.

Once an employee/workforce member leaves SLHS or an individual is no longer associated with SLHS, their e-mail box will be suspended immediately by Information Services upon notification of the employee's status.

Because the e-mail and voicemail systems are owned and solely provided by SLHS as tools to complete SLHS business, SLHS retains ownership rights to all data and information saved or captured within these systems.
To prevent computer viruses from being transmitted through the system, workforce members are expected to scan files downloaded from the Internet before opening or executing them.
E-mail and the Internet will not be used to send (upload) or receive (download) copyrighted materials, trade secrets, proprietary financial information, or similar materials without prior authorization.

6. The use of personal phrases and popular quotes at the end of an email or in your signature block without marketing approval is acceptable.

   True (T)
   False (F)

7. Can e-mail, voice mail and internet use on the SLHS network be used for personal purposes?
   A. Yes, incidental use is authorized as long as the use is reasonable and does not interfere with job responsibilities.
   B. No, personal use of email, voicemail and internet on the SLHS network is never authorized.

8. SLHS retains ownership rights to all data and information saved or captured within their e-mail and voicemail systems because……..
   A. SLHS purchased the equipment.
   B. E-mail and voicemail systems are owned and solely provided by SLHS as tools to complete SLHS business.
   C. SLHS created the systems.
   D. SLHS is widespread.

## ECPS-404: Device and Media Control

This policy reflects Saint Luke's Health System (SLHS)'s commitment to appropriately control information systems and electronic media containing Protected Health Information (PHI) moving into, out of and within the

SLHS facilities. Only workforce members who have received explicit permission to use removable media and storage devices to transfer electronic PHI to / from the organization's network may do so.

All movement of SLHS information systems and electronic media containing PHI into and out of SLHS facilities will be tracked and logged by those responsible for such movement. Unless appropriately protected with FIPS 140-2 approved encryption and authorized, PHI must not be stored on SLHS workforce member home computers or removable media.

Backup copies of all PHI on electronic media and information systems must be made regularly. This includes both PHI received by and created within SLHS.

9. Who is allowed to transfer electronic confidential information or PHI to/from the organization's network on removable media and storage devices?
    A. Only employees/workforce members who have received explicit permission to use removable media and storage devices.
    B. Only Information Services personnel.
    C. Those who show proof of ownership.
    D. Only SLHS Administrative and Executive staff.

## ECPS-406: Facility Access Control

SLHS information systems that process and store confidential information, especially EPHI (Electronic Protected Health Information), must be physically located in areas where unauthorized access is minimized. All visitors must show proper identification and sign in prior to gaining physical access to SLHS areas where information systems containing EPHI are located.

SLHS will have procedures to control and validate individuals' access to SLHS's facilities based on their roles or functions. Access to SLHS information systems containing EPHI should be limited to SLHS employee/workforce members and software programs that have a need to access specific information in order to accomplish a legitimate task.

10. All visitors must show proper identification and sign in prior to gaining physical access to areas where information systems containing _________ are located.
    A. Database files
    B. EPHI & confidential information
    C. Multiple circuit boards
    D. Physical access inventories

11. Access to information systems containing EPHI should be limited to SLHS employees/workforce members that have a need to access specific information in order to accomplish a legitimate task.
    True (T)
    False (F)

## ECPS-416: Workforce Security

Only properly authorized and trained SLHS workforce members may access SLHS information. Access to electronic information, especially PHI contained within SLHS information systems will be strictly controlled. Until properly authorized, no workforce member or other individual will be allowed to have access to SLHS information systems.

Access to SLHS Information will be controlled through a process of granting and authorizing appropriate access based on "user defined roles". Any request for access outside the currently approved roles will require an approval exception from the application owner, Chief Privacy Officer or Director, Information Security.

Each SLHS position ID will be reviewed by Information Security / Privacy Resources and Application Owners to define the level of information access necessary to perform the position's Job Function. This will be a continuous process of establishing, documenting, and approving "user defined roles" based on Position, facility and employee type. Each defined role will have assigned the associated applications and access levels. All defined roles will be developed based on a "need to know" level of access to accomplish the work responsibilities of the specific user role.

To create access for a user, a service request will need to be submitted to the SLHS Information Services Client Support center by the manager.

12. Information access will be based on a **need-to-know** level of access to complete the work duties of the specific job/position.
    True (T)
    False (F)

13. For an employee or workforce member to gain access beyond that defined for their job function, a _______ form or e-mail message must be submitted to IS Client Support by the manager.
    A. Increased Access Level
    B. IS Service Request
    C. Security Approval

14. An intentional attempt by you to access electronic confidential information without proper authorization may result in disciplinary action, including termination.
    True (T)
    False (F)

## ECPS-408: Information Classification/Handling

The policy governs all electronic information used within SLHS to conduct business and deliver health care including, but not limited to, patient, administrative, associate, and financial information.

*ACCESS LIMITATIONS:*

- Need to Know: One of the fundamental principles of information security is the "need to know." Information should be disclosed only to those people who have a legitimate business need for the information and such disclosure will be limited to the minimum necessary to conduct the required duties.
- System Access Controls: All confidential computer-resident information must be protected via access controls to ensure that it is not improperly disclosed, modified, deleted, or rendered unavailable. Access control systems will employ fixed passwords, but these will be supplemented where deemed appropriate by more secure technologies including dynamic passwords and biometrics. The access control packages will also log which users accessed what confidential data.
- Access Granting Decisions: Access to SLHS confidential information must be provided only after express authorization of the information owner has been obtained. Custodians of the involved information must refer all requests for access to owners or their delegates.

Unless it has specifically been designated as public, third parties may be given access to SLHS internal information only when a need-to-know exists, and when such a disclosure has been expressly authorized by the relevant SLHS information owner. These disclosures must be accompanied by a signed non-disclosure agreement.

If confidential information is lost or disclosed (or suspected of being lost or disclosed) to unauthorized parties, the information owner, Risk Management, SLHS Privacy Office and Information Security must be notified immediately. Confidential SLHS information may not be removed from SLHS premises unless there has been prior approval from the information's owner.

Making additional copies of confidential electronic information must not take place without the advance permission of the information owner.

Workers in the possession of portable, laptop, PDA, notebook, palmtop, and other transportable computers containing confidential SLHS information must not leave these computers unattended at any time unless the confidential information has been encrypted. If SLHS confidential data is to be transmitted over any public network (such as the Internet) it must be sent only in encrypted form.

15. Information should only be disclosed to people who have a legitimate business need ("need to know") for the information. Such disclosure will be limited to maximum level necessary to conduct required duties.

    True (T)
    False (F)

## ECPS-409: Communication and Mobile Smart Device Security Standards and User Responsibilities PDA Hardware/Software Policy and User Responsibilities

Communication and Mobile Smart Devices used to conduct SLHS business, especially where confidential data is concerned, will comply with the all published SLHS security requirements and the specific security requirements outlined in this policy. Use of personally-owned Communication and Mobile Smart Devices to connect to SLHS email is restricted to exempt employees and must be authorized by Human Resources. Any exceptions to this rule must be approved by HR. Users must agree to configure and manage their Communication and Mobile Smart Devices within the requirements of this policy when connecting to SLHS email or other SLHS authorized services.

- All approved users must sign and execute the form - "Responsibility and Liability Agreement for the use of Communication and Mobile Smart Devices with the SLHS Email System."
- Device and/or email application access passwords must be used on all Communication and Mobile Smart Devices if they are configured to sync with the SLHS email system. Passwords must comply with SLHS security policy – a minimum of six characters.
- All Communication and Mobile Smart Devices must be physically secured when left unattended.
- Communication and Mobile Smart Devices must be configured to automatically screen lock or power off following a maximum of 30 minutes of inactivity. Inactivity timeouts may be less depending on device and/or the type of SLHS authorized service being accessed.
- The use of Smart Phones to store individual network and/or application passwords in plain text is strictly prohibited.
- Users must agree to implement approved encryption software on any personally-owned Communication and Smart Mobile Device when storing patient health information within email, the device, or device applications.
- All Communication and Mobile Smart Devices synching with the SLHS network for email and other authorized services must be capable of remotely wiping the data upon notification of theft or loss. If a Communication or Mobile Smart Device that connects to SLHS network is lost or stolen, users are required to notify the Client Support Center to deactivate any user accounts where applicable and initiate a remote wipe of the device.
- SLHS is not responsible for loss of personal data and/or applications on Communication or Smart Mobile Devices that may occur while connected to the SLHS email system or when a remote wipe of the device is required to ensure protection of SLHS data.
- Users are responsible for backup and recovery of all data and applications on a personally-owned Communication or Smart Mobile Device.
- Users with camera capabilities on a Communication or Smart Mobile Device must abide by all SLHS policies governing the use of cameras within SLHS facilities.

Communication and Smart Phone Devices that connect to the SLHS network for access to email and other authorized services are subject to audits just like any other electronic device, even if the device is not owned by SLHS.

Employee/Workforce members using Communication and/or Smart Mobile Devices within SLHS who are found to be in violation of any part of this policy are subject to disciplinary action up to and including termination.

16. All Mobile Smart Devices configured to be used within SLHS must be _______ when left unattended.
    A. Physically secured
    B. Turned off
    C. Sitting by your computer
    D. All of the above

17. Users must agree to utilize encryption and allow remote wiping of personal Mobile Smart Devices if lost or stolen
    A. True
    B. False

18. It is ok to store my network and application UserIDs and passwords on my Mobile Smart Device as long as I have a password on the device.
    True (T)
    False (F)

## ECPS-411: Information Security Awareness

SLHS will provide initial training that covers its information security policies and key areas of potential threats, incidents, and procedures. This training will provide directions on where staff can find policies and report suspicious activities or incidents.
Annually, SLHS employees will reaffirm that they have reviewed and understand the SLHS information security policies as part of their performance reviews. SLHS will provide ongoing information security awareness of its information security policies, standards, and procedures.

SLHS will provide an orientation program for first-time employees/workforce members which includes an overview of the SLHS information security policies and procedures.

All SLHS employees/workforce members are responsible for familiarizing themselves with SLHS Information Security policies and the related responsibilities that arise for their job functions as well as specific information security measures they are expected to undertake as part of their jobs.

19. How often do SLHS employees need to reaffirm that they have reviewed and understand the SLHS Information Security Policies?
    A. Monthly
    B. Quarterly
    C. Semi-annually
    D. Annually

20. SLHS employees and workforce (temporary agency staff, medical staff, some students, etc.) are responsible for familiarizing themselves with SLHS Information Security Policies and how they relate to their job functions as well as what security measures they are expected to take.
    True (T)
    False (F)

## ECPS-412: Information Security Incident Procedures, Response, and Reporting

Saint Luke’s Health System (SLHS) will quickly and effectively detect, respond to, and report information security incidents that could impact the confidentiality, integrity, or availability of SLHS information systems.

The SLHS Chief Technology Officer and/or Director, Information Security is authorized to and will investigate any and all alleged violations of information security policies, and to take appropriate action to mitigate the infraction. The SLHS Chief Technology Officer and/or Director, Information Security will report all alleged violations of information security policies to the employee's supervisor and Human Resources who will be responsible for managing the discipline process as necessary. The SLHS Director of Technology and Security and/or Director, Information Security will assist the employee's supervisor and Human Resources as requested. Any incident involving electronic protected health information will also be shared with the SLSH Chief Privacy Officer.

21. Alleged violations of Information Security Policies will be investigated by:
    A. Chief Privacy Officer
    B. Human Resources
    C. Chief Technology Officer (also Chief Security Officer) and/or Director, Information Security
    D. None of the above.

## ECPS-414: Information Security Evaluation

Saint Luke's Health System (SLHS) is committed to ensuring that its Information Security policies and procedures are effective in reducing and mitigating risks to the confidentiality, integrity, and availability of its electronic information, particularly Protected Health Information (PHI). Moreover, SLHS is committed to ensuring that these policies and procedures are followed. To do so, it is recognized that periodic technical and non-technical evaluation of its security controls and processes is necessary to document compliance.

22. Information Security evaluations can be conducted on any system where SLHS electronic information is created, transported, or stored.

    True (T)
    False (F)

## ECPS-4153: Transmitting Confidential Information

SLHS is committed to ensuring the confidentiality, integrity, and availability of its electronic information, particularly Electronic Protected Health Information (EPHI) and will implement controls to appropriately and reasonably protect confidential information when it is being transmitted over electronic communication networks or via any form of removable media.

The network connecting SLHS entities together relies on dedicated links and therefore, all transmissions of EPHI between the SLHS networks are permitted with no additional security mechanisms. The transmission of EPHI from SLHS to a **patient** via an email or messaging system is permitted if the sender has ensured that the following conditions are met:

- The patient has been made fully aware of the risks associated with transmitting EPHI via email or messaging systems.
- The patient has formally authorized SLHS to utilize an email or messaging system to transmit EPHI to them.
- The patient's identity has been authenticated.
- An approved encryption mechanism is used.

Email accounts that are used to send or receive EPHI can only be forwarded to non-SLHS accounts if the email transmission path is configured to force the use of Transport Layer Security (TLS).
The transmission of EPHI from SLHS to an **outside entity** via an email or messaging system is permitted if the sender has ensured that the following conditions are met:

- The receiving entity has been authenticated.
- The receiving entity is aware of the transmission and is ready to receive said transmission.
- The sender and receiver are able to implement an approved, compatible encryption mechanism.

- All attachments containing EPHI are encrypted with an approved encryption solution.

23. E-mail transmission of electronic PHI is permitted if:
    - A. Contains non-critical information only
    - B. E-mail is encrypted
    - C. Only Hotmail is used
    - D. All of the above are in place

## ECPS-414: Information Security Responsibility

This policy applies primarily to employees across SLHS entities. However, when non-SLHS employees access electronic information, especially electronic PHI, this policy applies to those employees and their companies as well. The SLHS Management Committee sets the overall direction for managing information security risks across the enterprise.

All SLHS personnel or agents acting for SLHS have a duty to:

- Be aware of and comply with SLHS information security policies
- Safeguard hardware, software and information in their care
- Report any suspected or actual breaches in security

The **Chief Information Security Officer** shall be responsible for facilitating a process for individuals to file an Information Security complaint.

*(No questions for this section)*

## ECPS-415: Data Network Access Management

After data network access accounts have been created, they will be managed by Information Security to ensure that the accounts are used appropriately and are still necessary.

Monitoring for inactive accounts will be accomplished by automatically auditing a rolling 90-day period for inactivity for employees. Each account will be audited for use and determined to be either active or inactive. Inactive accounts will be deactivated with access revoked.

Accounts may be disabled at any time at the request of a supervising manager, or at the discretion of Information Services according to existing access and usage policies and procedures.

24. Employee logins are disabled after what length of inactivity?
    - A. 30 days
    - B. 60 days
    - C. 180 days
    - D. 270 days

## ECPS-416: Workforce Security

This policy is applicable to all SLHS departments that use or disclose PHI for any purposes. The policy provides guidelines for appropriate use of computer facilities and services at SLHS.

Only properly authorized workforce members are to be provided access to SLHS information systems containing electronic business-critical information, especially PHI. All SLHS workforce members who access SLHS information systems containing PHI will sign a confidentiality agreement in which they agree not to provide PHI or to discuss confidential information to which they have access to unauthorized persons.

SLHS will protect the confidentiality, integrity, and availability of its information systems containing business-critical information, such as electronic PHI, by preventing unauthorized access while ensuring that properly authorized workforce members are allowed needed access. All third parties who access SLHS information systems containing PHI will have their company first complete a "Business Associate Agreement" or sign a confidentiality agreement, as appropriate.

SLHS will follow a formal, documented process for terminating access to PHI when the employment of a workforce member ends.

25. SLHS employees and workforce (physicians, clinicians, students, other working non-employees, etc.) will be given access to information systems only…..
    A. When a SLHS badge is displayed
    B. After a Security Agreement has been signed
    C. After properly authorized
    D. After passing the test given at new hire orientation

26. All SLHS workforce members and employees who access systems containing PHI must sign a Confidentiality agreement.
    True (T)
    False (F)

## ECPS-417: Workstation Use and Security

SLHS workstations must be used only for authorized purposes. Employee/workforce members must not use SLHS workstations to engage in any activity that is either illegal under local, state, federal, or international law or is in violation of SLHS policies. Access to a SLHS workstation containing EPHI will be restricted to only those workforce members who have been properly authorized.

SLHS workstations containing EPHI must be logged off by the user once they have completed their tasks on the computer, and if left for more than 15 minutes should have locking software activated. All employee /workforce members using workstations with EPHI must take all reasonable precautions to protect confidentiality, integrity, and availability of the EPHI and report any misuse or inappropriate access to Information Security or their Privacy Site Coordinator.

To appropriately manage its information system assets and enforce appropriate security measures, SLHS may log, review, or monitor any data stored or transmitted on its information assets, at any time. Workstations containing EPHI must be physically located in such a manner as to minimize the risk that unauthorized individuals can access them. Mobile workstations must be carried as carry-on baggage when workforce members use public transportation. They must be concealed and/or locked when in private transport.

27. SLHS workstations must be used for __________.
    A. Illegal activities
    B. Business and recreation
    C. Authorized purposes
    D. Searching for extra-terrestrials on the web

28. SLHS workstations containing electronic PHI must be logged off once tasks are completed or locked after ______ minutes of inactivity.
    A. 10
    B. 15
    C. 20
    D. 30

29. Where must workstations containing electronic PHI be located?
    A. Near patients for ease of use
    B. In physician directed areas
    C. At nurses/employees discretion
    D. In a place to minimize risk of unauthorized individuals gaining access.

30. SLHS may log, review, or monitor any data stored or transmitted on its equipment at any time.
    True (T)
    False (F)

31. Mobile workstations/lap tops can be stored with other luggage when using public transportation.
    True (T)
    False (F)

## ECPS-420: Network Access – Remote Connections

It is the responsibility of SLHS employees, contractors, vendors and agents with remote access privileges to SLHS's corporate network to ensure that their remote access connection is given the same consideration as a user's on-site connection to SLHS.

Client Based VPN access to SLHS will be permitted only on a limited basis to support IS administration functions or applications not supported in the SLHS Citrix environment. Access via client based VPN must be approved by the SLHS Chief Information Security Officer. All client based VPN connections will be configured to restrict split tunneling while connected to the SLHS network.

Site to Site VPN access will be provided to affiliated business partners on a case by case basis in the event that the SLHS Citrix Remote Access Portal or client based VPN cannot meet the business need. Each Site to Site connection will be restricted to only the required access to accomplish the business requirement and will be approved by the Chief Information Security Officer prior to implementation. A Memorandum of Understanding defining the security requirements of both parties to establish the remote connection must be on file with SLHS prior to implementation.
Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. At no time should any SLHS employee provide their login or email password to anyone, not even family members.

All hosts that are connected to SLHS internal networks via remote access technologies must use the most up-to-date anti-virus software.

Remote users will manage all SLHS files created or received in accordance with applicable laws and regulations regarding patient identifiable information; and provide timely notification to the Information Security in Information Services when their remote access is no longer required. All remote access connections are subject to random auditing and periodic review by Information Services, to determine on-going business need.

A telecommuter is a computer user who is directly affiliated with SLHS and requires remote access for medical reasons or business reasons. These users must sign the Telecommuting Users Agreement which is available from the Information Services Department or in the Policy Forms" folder of the network I:/ Drive, SLHS Policies.

This policy does not preclude a person from using his or her own personal computing equipment for telecommuting. However, if privately-owned equipment is used, then it is at the user's personal expense and liability and the remote access is restricted to the Citrix Remote Access Portal connection.

32. ALL remote access connections are subject to random auditing and periodic review by Information Services to determine on-going business need. True or False?
    True (T)
    False (F)

33. Is it OK for a SLHS employee to share their login or email password with their family if they are using a home personal computer?
    A. Yes
    B. No

## ECPS-420: User Identification and Password Policy

Computer users must be identified by an assigned unique UserID and authenticated in order to gain access to information systems and networks. The owner of a UserID is personally responsible for activities performed, whether intentional or unintentional with their assigned UserID. Therefore, UserID owners are not allowed to share their account and password, and should ensure that they log off information systems and networks when they are no longer using them.

A functional or group-shared UserID may be assigned to a group of computer users with proper business justification to Information Services. Approval for shared UserIDs will be granted only when individual accountability is not required.

Temporary UserIDs may be issued to non-employees such as temporary workers or contractors whose position or contract requires access to the SLHS network or systems. Access requests must be made by an SLHS sponsor and is set up for a period of time not to exceed the term of the contract. If the contract is for an indefinite period of time, accounts are created with a life span of one year and must be reviewed annually by their SLHS sponsor. SLHS sponsors are required to inform Information services to terminate the T account whenever the contract or term of use is completed.

UserIDs that have not been used within a 90 day period will be automatically suspended or deleted.

Access to the network and information systems is granted after a computer user authenticates themselves by entering their UserID and password. All user accounts are created with a generic password. During the orientation process, the user will be notified of his/her password and will be given instructions on how to change it. (Generic passwords should expire automatically the first time a user logs on, forcing the user to create a new password.)

User responsibilities include:

- Users are responsible for changing the generic password and creating their own “strong” password.
- Passwords for **Standard, Temporary and Group UserID** accounts must be changed at a minimum annually.
- **Administrator UserID** passwords are to be changed at a minimum every 90 days.
- Users must immediately contact the Client Support Center if they suspect that their password was compromised. The Client Support Center will follow security incident reporting procedures and verify that the user’s password was changed.
- UserID owners are not allowed to share their account and password. Any attempt by a user to share their assigned UserID and password or the unauthorized use of another user’s assigned UserID and password may result in disciplinary action.
- Passwords must not be accessible to others. For example, passwords must not be displayed on office walls or written on the back of their employee badge. Passwords are only authorized to be stored electronically in SLHS approved password management software. Hardware or software features must not be used to bypass normal network, system, and/or application logon process.

- After five consecutive unsuccessful logon attempts, the systems will revoke or lock out any further attempt to use the UserID. User accounts will remain locked for a period of 30 minutes.

When a user needs to have their access or password reset, the following steps must be followed:

- The user will use the published self service method for resetting their password or they will call the Client Support Center requesting that their access or password be reset.
- The Client Support Center personnel must verify the identity of the caller by a method that allows them to be reasonably sure the caller is the owner of the UserID. (For example, the Client Support Center may ask the caller for the last six digits of their social security number or day and month of their birth date).
- The access or password will be reset only after the user's identity has been verified.

34. How often should a Standard user's password be changed?
    A. Two times a year.
    B. Never, it is their password; they shouldn't have to change it.
    C. At a minimum, annually.
    D. Every quarter.

35. How many consecutive unsuccessful login attempts can you attempt before the system locks out any further attempts to use the UserID?
    A. 20
    B. 3
    C. 5
    D. 10

# SLHS Information Security Training

## Answer Sheet

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____
9. _____
10. _____
11. _____
12. _____
13. _____
14. _____
15. _____
16. _____
17. _____
18. _____
19. _____
20. _____
21. _____
22. _____
23. _____
24. _____
25. _____
26. _____
27. _____
28. _____
29. _____
30. _____
31. _____
32. _____
33. _____
34. _____
35. _____

Comments:___________________________________________________________________
______________________________________________________________________
______________________________________________________________________
______________________________________________________________________
______________________________________________________________________
______________________________________________________________________
______________________________________________________________________
________________________________________________________________

*By signing this, I acknowledge completion of my Information Security training and have an understanding of the policies and procedures that pertain to my job/affiliation.*

_________________________________ ____________________ ____________________
*Signature of Trainee* *Date of Hire/Appointment* *Date Completed*

_________________________________ ________________________
***Print Name of Trainee*** *(Medical Office - Phone #)*

## Managers

**(For non-medical staff affiliates only)**

*I have reviewed and discussed all questions with the above trainee*.

_________________________ ________________ __________________________
*Signature of Manager* *Date* *Entity – Dept. – Ext. #*

***Managers:*** *Please keep original copy of answer sheet in department files. Document completion in department reports. Send copy to both HR for inclusion in Personnel File.*

***Medical Staff Affiliates:*** *Keep copy for your office and send original answer sheet to Central Verification, at Saint Luke's Hospital or FAX to* ***816-932-5689****.*

*REV: Feb. 2021*