WELCOME PACKET

The welcome packet consists of 4 documents:

1) **Patient Privacy Act Policy** (pages 2-8) – Read
2) **Protected Health Information Pledge** (page 9) – Read, sign and date
3) **SLHS Information Security Training** (pages 10-24) — Read and take test using answer sheet
4) **Answer key** (pages 25-28) – Grade your test and understand correct answers

Upload your completed pledge and training test to the website when completed

Saint Luke's Health System

SLHS POLICY & PROCEDURE
ECPS-202

TITLE: Patient Privacy and Information Security – General Guidelines
SECTION: Ethics, Compliance, Privacy and Security (ECPS)

PURPOSE

To establish a policy which governs the use, storage, and release of PHI (protected health information) (computerized and non-computerized) vital to the Saint Luke's Health System (SLHS). This policy is based on the principle that all information is confidential, proprietary, and vital to the continued operation of the Health System.

POLICY

All information in a patient's health record belongs to the patient and is confidential. The patient's medical record belongs to the facility where the record is stored. All such information shall be maintained to serve the patient, health care providers, and the SLHS in accordance with legal, accrediting, and regulatory agency requirements.

PROCEDURE

I. General Guidelines

A. The types and amount of PHI gathered and recorded about a patient shall be limited to that information needed for treatment, payment, and healthcare operations. Supplementary data that is not required for patient care but desirable for research, education, etc., may be recorded after obtaining written authorization from the patient following explanation of the purpose for which the information is needed. (See PRIV-23 Authorization Policy)

B. All individuals engaged in the collection, handling or dissemination of PHI shall be specifically informed of their responsibility to protect said data. Inappropriate use of PHI may result in the termination of access privileges to data and termination of any employer-employee, employer/contractor and/or contractual relationship with prejudice for rehire or discontinuation of contractual relationship. (See PRIV-67 Sanctions Policy)

C. The collection, manipulation and summation of PHI for internal studies, presentation or reports, will be performed by associates, or authorized researchers/contractors. The release of such PHI to other than an authorized system associates may result in immediate termination of continued employment or contractual agreement.

D. This policy shall be made known to all associates at the time of employment, or at such time as there is need for associates, researchers and/or contractors to have access to PHI collected manually or electronically. Acknowledgement of this policy shall be indicated through a signed statement at either the time of original employment or when access to manual or computerized information is granted. (See "Forms" folder of SLHS Policy on I:/Drive). Signed associate statements will be kept with associate's personnel records, and acknowledged annually according to Human Resources policy.

ISSUED BY:	Privacy & Security Steering Committee
EFFECTIVE DATE:	08/2013
SUPERCEDES EFFECTIVE DATE:	04/2003, 05/2006, 06/2006, 08/2006, 01/2007, 03/2007, 05/2007, 01/2009, 01/2010, 08/2010, 10/2010, 06/2011, 01/2012, 06/2012
APPROVED BY:	Privacy & Security Steering Committee
PAGE:	1 of 7

E. Any non-employees (students, vendors, volunteers, etc.) must sign a "Pledge of Confidentiality Statement" before accessing any PHI. The signed statement must be kept in the department responsible for the non-employee. All confidentiality statements must be kept for 6 years from the date of signature. (See Confidentiality Policy)

Pledge of Confidentiality Statement Form

F. For purposes other than treatment, payment or healthcare operations, the names, addresses, dates of admission or discharge of patients shall not be released to the news media, commercial organizations, or any other outside agency or organization without the express written authorization of the patient or their authorized agent and then such information must be released through Public Relations. (See PRIV-72 Media Policy)

G. Any employee when using or disclosing patient information (PHI) or when requesting patient information from another covered entity, will make reasonable efforts to limit patient information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. (See PRIV-05 and PRIV-05 Minimum Necessary Policies)

II. Patient Information

Saint Luke's Health System recognizes privacy as a patient's right and is committed to protecting the confidentiality of health information.

A. USES AND DISCLOSURES

1. **Associates -** PHI shall be available for use within the facility for treatment, payment and healthcare operations by all authorized personnel. Records will not be removed from the Health Information Management Department for non-patient care activities without permission from the department management. Direct access to patient health information records for routine administrative functions, including billing, will not be permitted.

   For facilities that have HPF (Horizon Patient Folder), please refer to PRIV-05 Minimum Necessary Policy for the proper steps in gaining access to patient records in the system.

2. **Patient -** Subject only to specific contraindications by the attending physician or any legal constraints, a patient, after discharge and completion of the health record may have access to view such record after submitting a written authorization with reasonable notice. Photocopies of the health record will be provided following receipt of a written authorization and payment of a reasonable fee from the patient. (See PRIV-23 Authorization Policy)

   It is very important that we respect the privacy of our patients here at Saint Luke's Health System. This includes when our employees are patients at our hospitals. When employees are patients at a SLHS facility, unless you are providing care or a service to them as a patient, you are to keep their information private as you would any other patient at SLHS; this includes speaking to the employees themselves regarding their care.

If a patient or an authorized representative asks to see the patient's record during a current healthcare visit, they should be encouraged to wait until the record is completed after discharge. If they are not agreeable to that option, the patient or their authorized representative may see the record after obtaining verbal authorization. **Documentation must be made in the medical record (i.e.: Nursing Progress Notes) of actions taken. The primary physician (and risk management when appropriate) should be notified of the request to review the record.**

Determination as to who should be notified of the request to review the medical record during treatment will be based on whether the reason is to resolve an issue or discuss treatment. **The healthcare provider must stay with the patient and/or their authorized representative as they review the record to ensure integrity of the documentation and respond to any questions if appropriate.** Once the record is reviewed, the nurse should note what documents where viewed by the patient or authorized person in the medical record. (See also PRIV-23 – Authorizations and PRIV-28 – Individuals Right to Access Records)

3. **Students** - PHI shall be available to authorized students enrolled in educational programs affiliated with the institution for use within the sponsoring department. Students must present proper identification and written permission from the instructor with their request. Data compiled in educational studies must be de-identified as referenced in the HIPAA regulations.

   All students must go through the SLHS Privacy Training and sign a confidentiality statement prior to beginning their affiliation with SLHS. The department must keep proof of training and the confidentiality statement responsible for the student. This document must be kept for 6 years from the date of signature.

4. **Research -** PHI shall be made available for research to individuals who have obtained approval for their research projects from the appropriate Medical Staff Committee and Administrator or other designated authority (IRB). Data compiled, as part of research studies must be de-identified as referenced in the HIPAA regulations, unless prior authorization from the patient is obtained. Any research project which would involve contact of patient by the researcher must have written permission of the patient's attending physician, or in his absence a physician designated by the current Chief Executive Officer of the facility, and consent of the Chief Executive Officer to conduct this study prior to contact.

B. RELEASE OF HEALTH INFORMATION

Release of information from the health record shall be carried out in accordance with all applicable legal, accrediting, regulatory agency requirements, and in accordance with written institutional health information management policies.

All outside requests for information from our health information records shall be directed to the Health Information Management Department for processing. Original health information records, other than x-rays and other materials that will be returned, may only be removed from the premises pursuant to a valid subpoena or court order.

1. Minimum Necessary – a reasonable effort will be made to limit disclosure of personal health information to "the minimum necessary to accomplish the intended purpose of the use, disclosure, or request." (See policy PRIV-05 and PRIV-06 regarding Minimum Necessary for additional information.)

C. STORAGE OF PATIENT INFORMATION

1. All primary health information records shall be housed in physically secure areas under the immediate control of the Health Information Management department or their designee and the Information Services department, or designated business partner. Home Health records will be stored in a secure manner until returned to the facility.
2. Secondary records such as departmental records, indices, or other individually identifiable patient health information maintained by the institution are subject to the stated policies for maintenance of confidentiality of patient health information. A listing of these secondary health information records with a brief description of content and location shall be maintained in a central location, preferably in the Health Information Management Department.
3. Primary and secondary health information records, including financial records, shall be retained according to legal, accrediting or regulatory agency requirements, and then destroyed according to an approved institutional retention schedule unless there is specific need for preservation of these records. The method of destruction shall be specified and the actual destruction witnessed or attested to in writing by the individual(s) responsible for destruction.
4. All records kept for privacy purposes (i.e. Proof of training, forms, logs, compliance, etc.) must be kept for 6 years. (See PRIV-57 Retention/Destruction)

D. NOTICE OF PRIVACY PRACTICES

Every patient will be provided with the Saint Luke's Health System Notice of Privacy Practices at their first visit after April 14, 2003. The notice will be displayed in the registration areas. The notice will include information on how we use patient information (PHI) and the patient's rights with regards to their information. (See PRIV-45 Notice of Privacy Practices Implementation)

E. COMPLAINTS

Patients are informed in the Notice of Privacy Practices of their right to file a complaint when their privacy rights have been violated. The notice includes information on how to file the notice. This process also includes employees who view violations of privacy policies and procedures. They also have the right and obligation to file a complaint. (See PRIV-01 Complaint Policy)

F. SECURITY OF HEALTH INFORMATION AND RECORDS

1. Access to areas housing health information records shall be limited to Health Information Management personnel. The sole exception to this policy shall be the individual designated by the Manager/Supervisor of Health Information Management at each facility for access at times when the department is not staffed. Health information records must be available and accessible at all times for patient care.
2. When in use within the institution, health information should be kept in secure areas at all times. Health information records and computer terminals should not be left unattended in areas accessible to unauthorized individuals. Users should log off the computer when leaving the area. Health information records or charts in patient care areas are considered to be secure when closed and in the chart holder.
3. Patient confidential clinical information should not be displayed in public areas. For example, information outside patient rooms, on unit white erase boards, etc. is appropriate only if it does not indicate diagnostic specific information AND if only the patient's initials are used if possible. When patient safety is a concern, the first 3 letters of the last name and first initial of first name will be used. No full first or last name of the patient will be displayed where public (non-employees) can access the information.

G. TRAINING

SLHS will train every employee and member of its workforce (physicians, agency staff, volunteers, etc.) on their Privacy and Information Security policies and procedures as is appropriate for their individual role and function within the organization.

New employees hired after effective regulation enforcement dates will be trained within 30 days of hire as informed during orientation within each facility. Disciplinary action may occur if an employee is not compliant with this policy. All employees will be re-educated on any significant update to a current policy or procedure within a reasonable time period following the change.

Employees **rehired** one year or longer after termination of employment will be required to retake HIPAA training, both Privacy and Information Security within 30 days of rehire.

Any non-employees, such as students, volunteers, medical staff, etc, must be trained on SLHS Privacy and Information Security Policies and Procedures. Any HIPAA training from any other facility OTHER than SLHS will not be acceptable. HIPAA regulations require that Privacy and Information Security training be specific to the entity. The Privacy Office must approve any exemption to the training.

Documentation of training for employees is to be kept in each employee's file. The department shall keep documentation of training on non-employees. ALL Privacy documentation must be kept for 6 years from the date of termination (employees) or date of affiliation termination (non-employees).

H. POLICIES AND PROCEDURES

SLHS has developed policies and procedures to document its compliance with the privacy regulations. The policies and procedures are available on the I:drive under the folder marked Privacy. Each policy also contains scenarios describing real life situations that would be answered by documentation within the policy.

SLHS will modify in a prompt manner our policies and procedures to comply with changes in relevant law. These changes will be documented in the revised policies and implementation of these changes will be made within a reasonable time.

I. SAFEGUARDS

SLHS has implemented appropriate administrative, technical, and physical safeguards to protect the privacy of patient information (PHI). These safeguards are intended to protect health information from any intentional or unintentional use or disclosure that is in violation of our policies and procedures.

III. Personnel Designations

A. **Chief Privacy Officer** – as required by the privacy regulations, SLHS has designated a privacy official to be responsible for:

- receiving complaints concerning the substance of policies and procedures created to document compliance with the privacy regulations;
- receiving complaints concerning compliance with the privacy policies and procedures or with requirements of the privacy regulation in general; and
- Providing further information about matters covered in the notice of privacy practices.
- The contact information for the SLHS privacy official is:

Barb Beckett, RHIT
SLHS Chief Privacy Officer
10920 Elm Ave.
Kansas City, MO, 64134
(816) 932-6880 or (816) 932-6282 (hot line)
privacy@saint-lukes.org

B. **Site Coordinators** – SLHS has designated a Privacy & Information Security Site Coordinator for each entity within the SLHS. These individuals are responsible for serving as a resource and assisting the Chief Privacy Officer with any privacy or information security matters pertaining to their facility.

The site coordinators are:

Saint Luke's Hospital and	Angie Fergen	816-932-2299	
SL East-Lee's Summit and	Trina Wright	816-347-4807	
SL Northland	Amy Johnston	913-684-1353	
SL South	Austin Ray	913-317-7582	
Anderson County Hosp.	Susan Ramsey	785-204-4029	
Cabot Westside Health Center	Anaxis Maceira	816-471-0900	(x290)
Crittenton Children's Center	Meredith Roland	816-767-4341	
Cushing Memorial Hosp.	Amy Johnston	913-684-1353	
Hedrick Medical Center	Lucy Sweiger	660-707-4278	
Med Plaza Imaging	Jackie Turner	816-561-5858	(x503)
SL Cardiovascular Consultants	Marilyn Meshover	816-751-8352	
SL Homecare/Hospice	Troy Sorbo	816-360-8073	
SL Medical Group	Cherry Pence	913-384-8518	
SL Neurological Consultants	Whitney Brosh	816-932-3978	
SL Physician Specialists	Whitney Brosh	816-932-3978	
Wright Memorial Hosp.	Lucy Sweiger	660-358-5734	
Saint Luke's Health System			
Chief Privacy Officer	Barb Beckett	816-932-6880	
Dir. IT Security	Dave Wiseman	816-251-9912	

IMPACTED INDIVIDUALS

- Clinical
- Non-Clinical
- PA/ADM
- Physicians
- Executive/HIM/Risk

ISSUED BY:	Privacy & Security Steering Committee
EFFECTIVE DATE:	08/2013
SUPERCEDES EFFECTIVE DATE:	04/2003, 05/2006, 06/2006, 08/2006, 01/2007, 03/2007, 05/2007, 01/2009, 01/2010, 08/2010, 10/2010, 06/2011, 01/2012, 06/2012
APPROVED BY:	Privacy & Security Steering Committee
PAGE:	7 of 7

Saint Luke’s Health System

Protected Health Information
Pledge of Confidentiality

I, the undersigned, have read and understand the Saint Luke’s Health System’s policy on confidentiality of protected health information as described in this Confidentiality Pledge.

In consideration of my association with Saint Luke’s Health System, and as an integral part of the terms and conditions of my association, I hereby agree, pledge and undertake that I will not at any time, during my association with Saint Luke’s Health System, or after my association ends, access or use protected health information, or reveal or disclose to any persons within or outside the Saint Luke’s Health System, any protected health information, except as permitted or required by law.

I understand that my obligations outlined above will continue after my association with Saint Luke’s Health System ends.

I further understand that my obligations concerning the protection of the confidentiality of protected health information relate to all protected health information acquired through my association with Saint Luke’s Health System.

I also understand that unauthorized use or disclosure of such information could result in the imposition of fines pursuant to applicable state, or federal regulations and a report to my professional regulatory body.

I have been informed of Saint Luke’s Health System’s Personal Health Information Confidentiality Pledge requirements and the consequences of a breach.

Signature of Individual Making Pledge	Date Signed
Name of Individual Making Pledge (Print)	Department / Organization

Emergency Contact (Name/Phone number)
(for students/observers – if not already on file with the department)

(For IS Purposes):
Device Requested (if given SLHS Device)

I have discussed the Protected Health Information Confidential Pledge and the consequences of a breach with the above name.

Signature of Individual Administering Pledge	Date Signed

(Form must be retained for 6 years)

SLHS Information Security Training

Answer Sheet

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

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.* ***Thank you.***

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. _____
36. _____
37. _____
38. _____

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 Completed*

__________________________________ __________________

Print Name of Trainee *Date of Hire/Appointment*

Managers

(For non-medical staff affiliates only)

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

____________________________ ______________

Signature of Manager *Date*

__________________________ __________________________________

Print Name of Manager *Entity – Dept. – Ext. #*

Rev: Jun 2013

SLHS Information Security Training

(Paper Version – All SLHS Employees should complete the on-line version.)

Please read the summary of each policy then answer the questions. For additional information, the policies can be found on the I:drive\Security – Information(IT)\Final P&Ps folder.

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.)

SEC-01: 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)

SEC-02: Encryption of 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)

SEC-03: 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 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.

SEC-04: Device and Media Control

This policy reflect 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.

SEC-06: 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)

SEC-07: Information Access, Authorization, Establishment, Modification, and Management

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. Service Request (SR01)
    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)

<u>SEC-08: Information Classification/Handling</u>

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)

<u>SEC-09: Sanctions for Not Complying with Information Security Policy</u>
~~~~~~

While SLHS will provide regular training and awareness for workforce members on SLHS security policies and procedures, it is also the responsibility of each workforce member to understand and be aware of applicable information security and policies.

SLHS will use a formal, documented process for applying appropriate sanctions against workforce members who do not comply with its security policies and procedures.

Anytime an individual suspects non-compliance with information security policies, it is their obligation to immediately report the incident---what occurred, when, and by whom. This should be completed by contacting the Client Support Center at 816-251-9999 (x19999). Other means of reporting suspected non-compliance include:

- Reporting via the compliance or privacy hotlines;
- Notifying one's immediate supervisor, Privacy Site Coordinator, or
- Human Resource representative.

The Director, Information Security and/or Chief Information Security Officer will review the incident and provide a report on the circumstances surrounding the incident, policy involved, and impact or potential impact to SLHS. The Director, Information Security will review the details of the case with Human Resources and the immediate supervisor of the individual in non-compliance and together will issue recommendations for sanctions that are commensurate with the severity of the non-compliance and issues surrounding the incident. The SLHS Ethics and Compliance Officer and Chief Privacy Officer will be apprised of the findings and sanction recommendations.

Sanctions can include but are not limited to:

- Suspension
- Required retraining
- Letter of reprimand / warning
- Termination

~~~~~~

16. Anytime you suspect non-compliance with the information security policies, it is your obligation to immediately report the incident to: (what occurred, when, and by whom)
    A. Client Support Center 816-251-9999 (x19999)
    B. Compliance or Privacy hotlines/e-mails
    C. Immediate supervisor or entity Privacy Site Coordinator
    D. Human Resources representative
    E. Any of the above

17. The Director, Information Security will investigate an IS security breach or policy violation and review the details of the incident with HR and the immediate supervisor of the individual. Recommendations for possible sanctions will be provided.
    True (T)
    False (F)

18. An intentional violation of a Security Regulation could result in a monetary fine, up to 10 years in prison, loss of professional licensure, and these possible SLHS sanctions.
    A. Mandatory transfer to another department
    B. A dock in pay
    C. Suspension, retraining, letter of reprimand, termination
    D. None of the above

<u>SEC-10: Communication and Mobile Smart Device Security Standards and User Responsibilities</u>

<u>PDA Hardware/Software Policy and User Responsibilities</u>

Corporate or personally owned 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.
- 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 Mobile Smart Device when storing patient health information or confidential data on the device, or device applications.
- All Communication and Mobile Smart Devices requiring access to SLHS email must utilize the SLHS approved mobile smart device email client. Any mobile smart device that requires direct connection to the SLHS production network must be capable of implementing security settings required by information services. If a Communication or Mobile Smart Device that connects to SLHS network directly or via a client 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 / client.
- SLHS is not responsible for loss of personal data and/or applications on Communication or Mobile Smart 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 Mobile Smart 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 Mobile Smart 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.

~~~~~~

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

20. Users must agree to utilize encryption and allow remote wiping of personal Mobile Smart Devices if lost or stolen
    True (T)
    False (F)

21. 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)
~~~~~~

SEC-12: 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 that 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.

~~~~~~

22. 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

23. 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)

SEC-13: 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.

~~~~~~

24. 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.

SEC-14: 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.

~~~~~~

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

    True (T)
    False (F)

SEC-15: Information Integrity and Authentication Controls

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.

~~~~~~

26. 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

SEC-16: 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 Technology Officer (also Chief Security Officer)** shall be responsible for facilitating a process for individuals to file an Information Security complaint.

~~~~~~

(No questions on this section)

SEC-17: 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.

~~~~~~

27. Employee logins are disabled after what length of inactivity?
    A. 30 days
    B. 90 days
    C. 180 days
    D. 270 days

SEC-18: Employee/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.

~~~~~~

28. 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

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

SEC-19: 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 10 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.

~~~~~~

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

31. 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

32. 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.

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

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

SEC-20: 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 Technology Officer or the SLHS Director, Information Security. 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 Technology Officer or the Director, Information Security 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.

SLHS employees and contractors with remote access privileges to SLHS's corporate network must not use non-SLHS email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct SLHS business, thereby ensuring that official business is never confused with personal business.

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.

~~~~~~

35. 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)

36. 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

SEC-22: 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.

~~~~~~

37. 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.

38. 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 (Level 2)

Answer Key

Please compare your answer sheet with the answer key. Under each answer is the explanation of why that answer is correct.

1. **T - True**
   "Inappropriate use of information technology exposes SLHS to unnecessary risks (i.e. virus attacks, compromise of network systems and services, legal issues"

2. **F - False**
   "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."*

3. **C. Should be kept secure and never shared.**
   "Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts".

4. **F - False**
   "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 when the host will be unattended."*

5. **T - True**
   "SLHS will protect electronic information that must remain confidential (i.e., such as PHI) through the use of encryption technology when such information leaves the SLHS premises in an electronic format."

6. **F – False**
   "Messages will not utilize customized backgrounds or stationeries and / or personal phrases / popular quotes at the end of emails"

7. **A - Yes, incidental use is authorized as long as the use is reasonable and does not interfere with job responsibilities**
   "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."

8. **B. E-mail and voicemail systems are owned and solely provided by SLHS as tools to complete SLHS business.**
   "Because the email 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."

9. **A. Only employees/workforce members who have received explicit permission to use removable media and storage devices.**
   "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."

10. **B. EPHI & confidential information**
    "All visitors must show proper identification and sign in prior to gaining physical access to SLHS areas where information systems containing EPHI are located."

11. **T - True**

"SLHS employee/workforce members cannot be granted access to information systems or software programs containing EPHI until properly authorized. 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."

12. T - True
"Access to SLHS Information will be controlled through a process of granting and authorizing appropriate only access; this will include the process for establishing, documenting, reviewing and modifying access. Only properly authorized and trained SLHS workforce members may access SLHS information, based upon an analysis conducted by Information System owners to determine which Job Position should have access the PHI Information. All Information access will be based on a need to know level of access to accomplish the work responsibilities of the specific job for the requestor."

13. B. Service Request (SR01)
"To request access beyond that defined for each Job Function, a Service Request form or electronic mail message must be submitted to the Information Service's Client Support Center from the employee's manager. Access request must have justification and appropriate approval for Access Modification".

14. T - True
"Effective management of information access is critical for protecting the confidentiality, integrity, and availability of electronic information. Any attempts to gain access to SLHS information systems containing PHI for without proper authorization may result in disciplinary action, including termination."

15. F - False
"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."*

16. E. Any of the above
"Anytime an individual suspects non-compliance with information security policies, it is their obligation to immediately report the incident---what occurred, when, and by whom. This should be completed by contacting the Client Support Center at 816-251-9999 (1-9999). Other means of reporting suspected non-compliance include:"

1) Reporting via the compliance or privacy hotlines;
2) Notifying one's immediate supervisor, or
3) Human Resource representative.

17. T - True
"The Information Security Manager and/or Chief Technology Officer will review an IS Security incident and provide a report on the, policy involved, and impact or potential impact to SLHS. This report will be provided to the Chief Privacy Officer, Chief Information Security Officer and the Vice President of Human Resources."

18. C. Suspension, retraining, letter of reprimand, termination.
"Sanctions can include but are not limited to suspension, required retraining, letter of reprimand, and/or termination. Each sanction will be documented and securely maintained by Human Resources."

19. A. Physically secured
"All Communication and Mobile Smart Devices must be physically secured when left unattended."

20. T - True

"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."

21. **F - False**
"The use of Smart Phones to store individual network and/or application passwords in plain text is strictly prohibited."

22. **D. Annually**
"Annually, SLHS employees will reaffirm that they have reviewed and understand the SLHS information security policies as part of their performance reviews."

23. **T - True**
"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. They must also understand the specific information security measures they are expected to undertake as part of their jobs."

24. **C. Chief Technology Officer (also Chief Security Officer) and/or Information Security Manager**
"The SLHS Chief Technology Officer and/or Information Security Manager is authorized to and will investigate any and all alleged violations of information security policies, and to take appropriate action."

25. **T - True**
"Evaluations can be conducted on any of SLHS information security policies, procedures, and controls, and anywhere that SLHS electronic information is created, transported, or stored."

26. **B. E-mail is encrypted**
"To appropriately guard against unauthorized access to or modification of EPHI that is being transmitted from SLHS to an outside entity, an encryption mechanism must be utilized between the sending and receiving entities or the file, document, or folder containing said EPHI must be encrypted before transmission.

27. **B. 90 days**
*"Inactive accounts will be deactivated with access revoked.
Monitoring for inactive accounts will be accomplished by automatically auditing a rolling 90-day period for inactivity."*

28. **C. After properly authorized**
"*Only properly authorized workforce members are to be provided access to SLHS information systems containing electronic business-critical information, especially PHI. Access will only be granted to properly trained workforce members who have a need for business-critical information to accomplish their job role within SLHS."*

29. **T - True**
"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. This confidentiality agreement will be reaffirmed yearly."

30. **C. Authorized purposes**
"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."

31. **A. 10 minutes**
"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 10 minutes should have locking software activated."

32. **D. In a place to minimize risk of unauthorized individuals gaining access**
"Workstations containing EPHI must be physically located in such a manner as to minimize the risk that unauthorized individuals can access them."

33. **T - True**
"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."

34. **F - False**
"Mobile workstations (lap tops, notebooks, etc,) must be carried as carry-on baggage when workforce members use public transportation. They must be concealed and/or locked when in private transport, taking measures to provide protection."

35. **T - True**
"All remote access connections are subject to random auditing and periodic review by Information Services, to determine on-going business need."

36. **B – No**
"At no time should any SLHS employee provide their login or email password to anyone, not even family members."

37. **C. At a minimum, annually.**
"Standard UserID: Passwords are to be changed at a minimum annually."

38. **C. 5**
"*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."*

Rev: Jun 2013