LOUISIANA STATE UNIVERSITY HEALTH SCIENCES CENTER – SHREVEPORT

SECURITY, CONFIDENTIALITY AND INTEGRITY OF INFORMATION

Purpose:
To outline minimal guidelines for insuring reliable, accurate, confidential and secure information resources.

Definitions:
A. AIC: Availability, Integrity and Confidentiality

B. Security: The protection of information to insure availability, integrity and confidentiality (AIC).

C. Information Resources: Includes, but is not limited to, computers, faxes, telecommunication hardware, software, storage media, computer sign on codes, medical records documentation, and information stored, printed and/or processed by a computer system.

D. Storage Media: Includes, but is not limited to, paper, magnetic media, optical disk, film and other methods of retaining information.

E. Integrity: Protecting information from accidental or unauthorized intentional change.

F. Information Browsing: Viewing of information by unauthorized or legitimate user.

G. LSUHSC-S Confidentiality Statement: A signed statement that verifies the individuals understanding of the information security standards and implications for inappropriate access or disclosure of information.

H. Access: Permissions, rights and privileges to perform a set of functions.

I. User ID/Password: Personal identification key that authorizes a specific user to access information resources and establishes accountability for transactions.

J. Accountability: Responsibility is assumed for actions performed when interpreting, handling, and transmitting, transcribing or reporting information.

K. Audit or Activity Logs: Detailed documentation of events (read, write, etc.)

L. Protected Health Information (PHI): Individually identifiable health information that relates to the past, present, or future healthcare services provided to an individual.


N. Protected Health Information (PHI): Individually identifiable health information that relates to the past, present, or future healthcare services provided to an individual as described by HIPAA rules.
O. ePHI: Electronic PHI (Protected Health Information) or information transmitted or viewed electronically such as faxing or displaying on computer screens.

P. ITSP: Information Technology Security Plan outlines plans for implementing information technology security “best practices” to address procedures and plans of healthcare and educationally related information security needs. It insures AIC of all information assets associated with LSUHSC-S.

Policy:
A. Administrative Responsibilities

1. LSUHSC-S Human Resource Management
   a. Newly appointed faculty, staff and volunteers or other personnel authorized to access LSUHSC-S information assets shall receive information regarding the facilities’ standards regarding the AIC of information and use of information resources.
   b. Newly appointed faculty, staff and volunteers or other personnel authorized to access LSUHSC-S information assets shall be presented with the LSUHSC-S Confidentiality Statement for signature. (See Appendix A – LSUHSC-S Confidentiality Statement.)
   c. A copy of the Confidentiality Statement shall be filed in the permanent record in Human Resource Management and a copy shall be given to the individual.

2. LSUHSC-S Department Manager/Supervisor/Head
   a. Faculty, staff and volunteers or other personnel authorized to access LSUHSC-S information assets shall receive “hospital-wide” and “department specific” orientation and periodic review of access to LSUHSC-S information assets, security and appropriate processing of information relative to their job function and role that should include, but not be limited to:
      1). log in and sign off procedures
      2). lawful or legitimate information browsing
      3). release of information
      4). access rights
      5). processing and handling of information resources and storage media
      6). accountability and audit logs
      7). Viewing the online videos – Computer Access Training for New Employees and Protecting Electronic Health Information (ePHI)
   b. All non-compensated observers, students, vendors, or other persons conducting business with LSUHSC-S shall receive specific instructions on the principles of appropriately processing information received or observed within the facility.
   c. Affiliations agreements shall require that all persons associated with the agreement be informed, understand, and comply with the standards of AIC prior to entry into the facility.
   d. Departments who acquire and are responsible for maintenance of information systems shall establish policies and procedures consistent with facility standards and recommended guidelines.
B. Access

1. System administrators (database, hardware, security, etc.) shall:
   a. Define system and network access policies, procedures and controls to ensure the AIC of LSUHSC-S information assets.
   b. Provide guidance and expertise to application administrators for operation of their application.

2. Application administrators (generally departmental resources assigned management tasks associated with an application) shall:
   a. Define application access policies and procedures, including assignment of user ID and password, for any system containing restricted, confidential or personal information.
   b. Define policies and procedures to ensure the AIC of the information within their applications and in accordance with facility standards.
   c. Provide mechanisms for audit purposes in accordance with facility standards.
   d. Define password expiration policies and procedures in accordance with facility standards.
   e. Shall comply with all applicable facility polices, administrative directives or memorandums that address server based systems, networks, security and integrity of data, and maintenance of systems.

3. Provisional access
   a. Computer Services shall:
      1) Coordinate department requests for application access approval with designated application data owners and ensure approved access results in appropriate permissions for access.
      2) Coordinate department requests for updating application access upon user transfer according to current business need.
      3) Remove user access upon termination or dismissal.
   b. Department administrative personnel responsible for the supervision of individual users must submit:
      1) A detailed request in writing (memo, approved access form, email) specifying specific access requirements, suitable to the employees job role (read, write, amend, etc.), to the appropriate owner.
      2) The Louisiana Revised Statute 14.73.1 et seq. and Administrative Directive 2.8.9 dictates access to information or systems without the consent of appropriate authorities constitutes illegal activity and the person(s) involved are subject to enforceable penalties that may include fine and imprisonment.
      3) Review access rights periodically to ensure that the rights granted are relevant to the assigned responsibilities for that individual.
      4) Notify Computer Services and data owners as soon as possible:
         • of termination or resignation of personnel.
         • of transfer of personnel to another area, unit or department.
   c. Data owners are responsible for approving or denying application access based on valid business need for access. Only the minimum necessary access may be approved.

4. The electronic health record provides the following options to comply with legal mandates, hospital policy and the patient’s wishes:
• Break the Glass (BTG) – designed to allow user’s access to a restricted patient’s information. An audit trail stores details of the events when a user chooses to break the glass.
• Confidential names (alias names)
• Confidential patient types
  ➢ Anonymous
  ➢ Confidential (VIP)
  ➢ Employee
  ➢ Prisoner
  ➢ Employee’s Family
• Confidential Departments
  ➢ Psychiatry Unit
  ➢ Psychiatry Clinic
  ➢ CARA Center
  ➢ Viral Disease Clinic
  ➢ PSY Faculty Clinic

5. All authorized users shall be accountable for:
   a. Properly safeguarding data under their control and/or direction according to its level of sensitivity.
   b. Maintaining the integrity of data.
   c. Accessing only the data and automated functions for which s/he is authorized, in the course of normal business activity
   d. Password control (in accordance with ITSP):
      1). password not easily guessed
      2). inadvertent disclosure
      3). immediate change if suspected disclosure
      4). report of any suspected misuse by another individual
   e. Appropriate log-off from the application(s).
   f. Safeguarding information, including ePHI, and resources available in the course of their job duties.

Refer to:

C. User termination or transfer

1. Department administrative personnel must insure that:
   a. Personnel who separate from the facility complete the Employee Clearance process.
   b. Appropriate system administrators receive notification of separation or termination of individuals who do not complete the Employee Clearance process or who involuntarily separate from the department. This notification shall be made as soon as possible.
   c. Appropriate system administrators receive notification when employees transfer to another unit, area or department.
   d. Timely review of staff’s access to systems is performed when job duties or assigned role is modified within the department.
2. Application administrators shall:
a. Disable access as soon as possible after receiving notification of separation or termination or notice of transfer.
b. Shall comply with all applicable facility policies, administrative directives or memorandums that address server based systems, networks, security and integrity of data, and maintenance of systems.

D. Securing Information

1. Storage Media
   a. Used to access, retrieve, and communicate confidential or sensitive information shall be maintained in accordance with facility standards. (See appropriate Chancellor Memorandums and or Administrative Directives).
   b. Are safeguarded against theft, tampering, and unauthorized access.
   c. Identified as confidential or sensitive information shall be labeled as “CONFIDENTIAL” and stored in areas that are restricted only to authorized personnel. Prior to discarding any CONFIDENTIAL storage media, the information shall be rendered unusable.
   d. Maintained to comply with all applicable facility polices administrative directives or memorandums.

2. Request for Information/Records
   a. Requests for health record information shall be made available only to those employees, medical staff members, support staff, students, and etc., with a need to know, after displaying their identification badges.
   b. All requisitions for the retrieval of medical records shall contain the patient’s name, medical record number, current date/time and requesting party’s name. The requesting party’s telephone number and room number are also required for records requested for administrative purposes.
   c. Telephone request for patient-identifiable information are discouraged and limited to emergency situations (emergency requests are usually generated by physicians or other ‘key’ hospital/physician office staff). Telephone request shall be handled using a ‘call-back’ procedure to verify the identity of the requesting party.
   d. Release or disclosure of protected health information from external parties should be referred to the HIM department for disposition. Guidelines for disclosure are outlined in Hospital Policy #6.3 and LSUHSC-S HIPAA Policies.
   e. Facsimile transmission of patient information is addressed in Hospital Policy 6.3.1.
   f. Voice messages containing confidential information should not be left on answering machines.
   g. Shall comply with all applicable facility polices, administrative directives or memorandums.

3. Patient Medical Records
   a. The “Lite Chart” (paper record) displays two warnings reminding of the obligation to maintain confidentiality and security of information: “Confidential Health Information” and “This folder may not be removed from the hospital premises”.
   b. The “Lite Charts” are transported to patient care areas and administrative offices via the pneumatic tubes, dumbwaiter, carts and/or courier staff. All staff transporting paper medical records must ensure the privacy of patient-identifiable information during the
transport process. Medical records and/or carts loaded with medical records shall not be left unattended during the transport process. “Lite Charts” shall not be left unattended during the transport process.

c. The “Lite Charts” are to be maintained in the patient care areas in locations that are not accessible by unauthorized individuals.

d. Protected health information, paper or electronic, shall not be removed from the hospital premises except upon receipt of subpoena duces tecum, court order or state statute.

e. Shall comply with all applicable facility policies, administrative directives or memorandums.

4. Disposing/Discarding Patient Identifiable Information
   a. PHI must be shredded or placed in a secured shredding container to ensure confidentiality.
   b. Labels containing patient identifiable information must be rendered illegible when discarded.
   c. Shall comply with all applicable facility policies, administrative directives or memorandums.

5. Hardware and System Access
   a. Personnel who are the primary user of a personal computer must maintain an approved anti-virus software package. Failure to do so will result in loss of ability to connect to the campus network.

   b. Remote access to systems shall be governed in accordance with facility standards.

   c. Screen savers, auto logoff, screen shields, or other means must be utilized to prevent unauthorized view of computer systems that contain sensitive or confidential data.

   d. Information Technology production areas shall be accessible only through a secured entrance by authorized personnel; unauthorized personnel must be accompanied by authorized personnel.

   e. Shall comply with all applicable facility policies, administrative directives or memorandums.

E. Security and Privacy Violations

1. Security and Privacy violations are described in Chancellor’s Memorandums, LSUHSC-S Confidentiality Statement, LSUHSC-S HIPAA policies and other applicable hospital policy resources.

2. Reported variances/ incidents:
   a. Will be investigated by administrative staff to determine if the events were intentional due to an individual’s negligence, accidental mistake, improper training, or misunderstanding the information resource and or policy.

   b. May result in suspension of an individual’s access.

   c. May result in disciplinary action up to and including termination. Violations, also, may constitute a criminal offense, Louisiana Revised Statutes 14.73.1 et seq.

   d. Shall comply with all applicable facility policies, administrative directives or memorandums.

3. Unauthorized or improper disclosure, modification, or intentional destruction of health information violates state and federal laws, and may result in disciplinary action and/or civil and criminal penalties.

Approved by Clinical Board: 3/20/01, 7/20/04, 7/17/07, 8/18/09, 10/16/12
Written: 3/98
Reviewed: 3/04, 12/06, 6/07, 7/09, 10/12
Revised: 4/98, 2/01, 7/04, 12/06, 6/07, 7/09, 10/12
LSUHSC-S CONFIDENTIALITY AGREEMENT

Louisiana State University Health Sciences Center has a legal and ethical responsibility to safeguard the privacy of all patients and protect information that is defined as confidential. Confidential information includes oral communication, information contained in manual documentation as well as information stored in the facilities computer systems. Patient, personnel, financial and other business records contain confidential information.

I understand that information regarded as confidential must be maintained in the strictest of confidence. As a condition of my affiliation with LSUHSC-S, I hereby agree that I will not at any time during or after my affiliation with LSUHSC-S, disclose any confidential information to any person, other than as necessary in the course of my affiliation with LSUHSC-S, and when accompanied by the appropriate, authorized personnel. I understand that I am directly responsible for the accuracy and completeness of data entries which are entered into the facilities storage media.

Information in the facilities storage media may be accessed only by authorization from the Assistant Dean for Information Technology; computer system access is granted only to persons who have submitted a written application, and have been issued user identification codes. I understand that all user identification codes and passwords are confidential, and may not be shared or disclosed to any other person.

It is a crime punishable by fine and or imprisonment to reveal user identification codes or passwords (La. R.S. 14.73.1 et seq.). Using another employee’s user identification code/password or giving your user identification code/password to another person may result in disciplinary action, which may include suspension and/or termination.

I understand that it constitutes a Security violation to fail to sign off when leaving the computer unattended; accessing any medical or employment record without appropriate need or approval; requesting another employee to access my employment or medical record; allowing another employee to utilize my password; accessing medical or employment records without having a legitimate reason; using another employee’s access code, revealing confidential information of patients, employees or business/financial details, etc. All security violations will be reported to and investigated by the appropriate authorities.

My signature below indicates I have read the Security, Confidentiality and Integrity of Information Policy and have been given the opportunity to have any questions regarding this statement explained to me, and the failure to abide by this agreement may result in disciplinary action, including dismissal from employment, according to the Civil Service Rules and Regulations, LSU System Guidelines, applicable Medical Staff By Laws and Louisiana State Law.