CONFIDENTIALITY / COMPLIANCE

STATEMENT AND ACKNOWLEDGMENT

Confidentiality:
As a user of information at Salina Regional Health Center (SRHC) you may develop, use, or maintain (1) patient information (for healthcare, quality improvement, peer review, education, billing, reimbursement, administration, research or for other approved purposes), (2) personnel information (for employment, payroll, or other business purposes), or (3) confidential business information of SRHC and/or third parties, including third-party software and other licensed products or processes. This information from any source and in any form, including, but not limited to, paper record, oral communication, audio recording, and electronic display, is strictly confidential. Access to confidential information is permitted only on a need-to-know basis and limited to the minimum amount of confidential information necessary to accomplish the intended purpose of the use, disclosure or request.

It is the policy of SRHC that users (i.e. employees, medical staff, students, volunteers, vendors and other outside affiliates) shall respect and preserve the privacy, confidentiality and security of confidential information and SRHC owned equipment/property.

Violations of this statement include, but are not limited to:

- Accessing information that is not within the scope of your duties;
- Misusing, disclosing without proper authorization, or altering confidential information;
- Disclosing to another person your sign-on code and/or password for accessing electronic or confidential information or for physical access to restricted areas;
- Using another person's sign-on code and/or password for accessing electronic confidential information or for physical access to restricted areas;
- Intentional negligent mishandling or destruction of confidential information;
- Leaving a secured application unattended while signed on; or
- Attempting to access a secured application or restricted area without proper authorization or for purposes other than official SRHC business.
- Failure to safeguard or the misuse of SRHC owned equipment/property; or
- Failure to safeguard SRHC confidential information on personally owned equipment/property.

Violation of this statement may constitute ground for corrective action up to and including termination of employment, volunteer, student privileges or contractual or affiliation rights in accordance with applicable SRHC procedures. Unauthorized use or release of confidential information may also subject the violator to personal, civil, and/or criminal liability and legal penalties.

By signing this statement, I am stating and acknowledging that I have read and understand the HIPAA Privacy and Security policies and procedures, the SRHC Compliance Program and Code of Ethical Conduct and agree to abide by their terms. By signing this statement, I am also stating that I understand that the Compliance Program (including privacy/security policies) and Code of Ethical Conduct require that I report in advance to my supervisor, or Compliance Officer any known or suspected violation of the kind set forth therein.

I have read this statement and understand that it will remain on file in my employee personnel file for the duration of my employment.

Name_____
(please print)

Employee ID_____

Signature_____

Date _____

Entity:
[ ] SRHC [ ] Lindsborg
[ ] Physician Clinic _____

Affiliation:
[ ] Employee [ ] Contract Employee
[ ] Medical Staff [ ] Resident
[ ] Student [ ] Volunteer
[ ] Other Providers
[ ] Vendor (specify)_____
[ ] Other_____

Effective Date: 10/01/2013

EXAMPLES OF BREACHES OF CONFIDENTIALITY

Accessing confidential information that is not within the scope of your duties: Unauthorized reading of patient account information; Unauthorized reading of a patients chart; Unauthorized access of personnel file information; Accessing information that you do not "need-to-know" for the proper execution of your duties.	**Misusing, disclosing without proper authorization, or altering confidential information:** Making unauthorized marks on a patients chart; Making unauthorized changes to a personnel file; Sharing or reproducing information in a patient chart or a personnel file with unauthorized personnel; Discussing confidential information in a public area such as a waiting room or elevator.
Disclosing to another person your sign-on code and password for accessing electronic confidential information or for physical access to restricted areas: Telling a co-worker your password so that he or she can log in to your work or access your work area; Telling an unauthorized person the access codes for personnel file, patient accounts, or restricted areas.	**Using another person's sign-on code and/or password for accessing electronic confidential information or for physical access to restricted areas:** Using a co-worker's password to log into the computer system or access their work area; Unauthorized use of a login code for access to personnel files, patient accounts, or restricted areas.
Intentional or negligent mishandling or destruction of confidential information: Leaving confidential information in areas outside of your work area, such as the cafeteria or your home. Disposing of confidential information in a non-approved container, such as a trash can. Failure to promptly report the loss or theft of SRHC owned equipment/property assigned to you or the misuse of this equipment/property. Failure to report the loss or theft of personally owned equipment containing SRHC confidential information.	**Leaving a secured application unattended while signed on:** Being away from your desk while you are logged into an application. Allowing a co-worker to use your secured application for which he or she does not have access after you have logged in.
Attempting to access a secured application or restricted area without proper authorization or for purposes other than official SRHC business: Trying passwords and login codes to gain access to an unauthorized area of the computer system or restricted area; Using a co-worker's application for which you do not have access after her or she is logged in.	**The examples above are only a few types of mishandling of confidential information. If you have any questions about the handling, use or disclosures of confidential information please contact your director, compliance officer, or privacy or security officer.**