DISCIPLINARY CRITERIA FOR CONFIDENTIALITY VIOLATIONS

This Disciplinary Criteria for Confidentiality Violations is intended to provide criteria for applying SY-HR-401: Improvement Counseling policy in a uniform fashion for all areas of Southern Illinois Healthcare. The levels described are in conjunction with the levels described in SY-HR-401 and can be modified based on mitigating circumstances. Please refer to the definition of sensitive information as this applies to patient, financial, employee, physician, and other types of information deemed sensitive.

Level 1 – Failing to demonstrate appropriate care in handling sensitive information that results in accidental access, incidental access, or inappropriate access due to lack of awareness and/or education.

Examples include, but are not limited to:

- Leaving sensitive information unattended in areas outside of your work area
- Disposing of sensitive information in a non-approved manner such as putting paper, electronic media, or digital media in a trash can
- Inadvertently routing sensitive information to a wrong recipient
- Inadvertently releasing sensitive information without consent
- Being away from electronic device while logged into an application that could contain sensitive information, (exception: in case of patient emergency where delay could cause complications for the patient)
- Employee self access to their own sensitive information

Level 2 – Disregard of organization or departmental policy related to the appropriate use and disclosure of sensitive information

Examples include, but are not limited to:

- Access of immediate family member's (spouse, parents or child under the 12 years of age) sensitive information that is not for treatment, payment or healthcare operations and accessing the information is not part of the employee's assigned job duties
- Discussing sensitive information in public areas, such as cafeterias, hallways, or elevators within the hearing of persons not entitled to hear the information
- Inadvertent or unintentional public disclosure of sensitive information
- Discussing sensitive information with coworkers or other individuals who are not privy to the information – without intent to harm a patient, other workforce members or SIH
- Failure to report any violation of sensitive information, intentional or unintentional and/or suspected
- Knowingly sharing password with co-worker who has same level of access

Level 3 – Unauthorized access and/or disclosure of sensitive information

Examples include, but are not limited to:

- Access of a family member's (excluding spouse, parent and child under the age of 12) sensitive information that you do not need to know for the proper execution of your duties
- Sharing passwords or access to secured applications with a co-worker who is unauthorized to have access to sensitive information
- Intentionally exhibiting or divulging (verbal or written) sensitive information with coworkers or other individuals who are not privy to the information
- Copying or storing sensitive information on personal storage mediums, such as, but not limited to personal computer, personal digital assistant, cell or smart phone, USB drive, other optical or magnetic media or devices not owned by SIH, any unapproved Internet site
- Posting sensitive information on Internet sites, such as FaceBook, Instagram, Twitter, Yelp, etc. without intent to harm a patient, workforce member or SIH
- Removing any sensitive information in any form from the premises of SIH without prior permission from supervisor

Level 4 – Purposeful disregard of organization or departmental policies

- Seeking personal benefit or permitting others to benefit personally from sensitive information
- Accessing and/or disclosing sensitive information with malicious intent
- Repeated disregard and violation of any of the above levels