



System

Policy and Procedure

Title:	Confidentiality of Sensitive Information	Number:	SY-IT-001
Applies to:	All employees, interns, physicians, clergy, volunteers, temporary staff, contract employees, contractors, and persons providing services to any Southern Illinois Healthcare entity or affiliate.	First Created:	5/97
Issuing Dept:	Information Technology Services	Last Revised:	3/3/09
Approved by:	Dave Holland, Vice President / Chief Information Officer		

I. POLICY

Privacy and confidentiality are essential components of fostering trust between health care consumers and providers. All members of the Southern Illinois Healthcare (SIH) workforce are obligated to maintain the confidentiality of sensitive information acquired as a result of employment or privileges. Southern Illinois Healthcare strives to maintain the confidentiality of sensitive information related to our patients, medical staff, business activities, employees or peer review functions.

II. DEFINITIONS

Guarded Operational Information – operational information about any or all entities of SIH that is available to the staff on a need to know basis, but is not available to the general public. Information in this area may include financial information, strategic planning, employee directory information, corporate policies and procedures, information available on the Southern Illinois Healthcare intranet, or other operational information or work products as specified by supervisory staff.

Highly Confidential Information - psychotherapy notes and the subset of protected health information that is related to:

- Treatment of mental health and developmental disabilities;
- Alcohol and drug abuse prevention and treatment;
- HIV/AIDS testing;
- Venereal disease(s);
- Genetic testing;
- Child abuse and neglect;
- Domestic abuse of an adult with a disability; or
- Sexual assault.

Individually Identifiable Health Information - information that is a subset of health information, including demographic information collected from an individual, and

- Is created or received by a health care provider, health plan, or health care clearinghouse; and
- Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and
 - Identifies the individual, or

- With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Non-employees - all persons who are considered part of the workforce, but are not paid employee of Southern Illinois Healthcare. This group includes volunteers, members of the clergy, physicians, contract employees, student trainees, interns, contractors, temporary employees, etc

Public Information – information that is available to the general public. This information includes facility addresses, services offered and other information available on the Southern Illinois Healthcare website (www.SIH.NET)

Protected Health Information (PHI) - the subset of individually identifiable health information that is (i) transmitted by electronic media; (ii) maintained in any medium constituting electronic media; or (iii) transmitted or maintained in any other form or medium. "Protected health information" shall not include (i) education records covered by the Family Educational Right and Privacy Act, as amended, 20 U.S.C. §1232g, (ii) records described in 20 U.S.C. §1232g(a)(4)(B)(iv), and (iii) employment records held by a covered entity in its role as employer. (Note that highly confidential information is a subset of protected health information.)

Sensitive Information – Information in any form, including but not limited to paper, electronic, or oral, which if improperly disclosed could cause damage to the reputation, privacy, image and/or financial viability of the patient, medical staff, employees, board of trustees and/or Southern Illinois HealthCare. Sensitive information includes, but is not limited to

- All individually identifiable health information;
- Anything marked or stated as confidential
- Employee information;
- Financial information;
- Guarded Operational Information;
- Marketing and general business strategies
- Patient billing information;
- Physician information; and
- Proprietary products and product development.

Workforce - employees, volunteers, trainees and other persons whose conduct in the performance of work for a covered entity is under the direct control of such entity, whether or not they are paid by the covered entity. (A covered entity may treat an independent contractor that performs a substantial portion of his/her activities on the premises of the covered entity as a member of its workforce.)

III. RESPONSIBILITIES

- 1.0 Members of the Southern Illinois Healthcare workforce review and/or disseminate sensitive information on an as needed basis based on what is required to perform the workforce members role in the healthcare delivery system.
- 2.0 Workforce members report suspected breaches of confidentiality to their supervisor, director, administrator, Corporate Compliance department or the Privacy Office.
- 3.0 Department supervisors, managers, directors and administrative staff develop a work environment that allows workforce members access to the minimum information needed to perform their duties. In addition, when a member of the workforce terminates or is terminated, his/her supervisor retrieves any items owned by SIH that would allow the user physical access to sensitive information (e.g. keys, ID badge, change combination locks, etc.) and initiates termination of electronic access to sensitive information (notify Human Resources and/or Information Technology Services).

- 4.0 Suspected breaches of privacy are investigated by the Privacy Officer/Security Officer/designee. If it is determined that a violation did occur, the Privacy Officer/Security Officer/designee works with the supervisor and/or Human Resources department to discipline the violator. Improvement counseling occurs within 10 SIH business days. The supervisor and/or Human Resources report the outcome back to the Privacy or Security Officer.
- 5.0 This “Confidentiality of Sensitive Information Policy” is reviewed by Human Resources department with all newly employed workforce members. Human Resources has the workforce members sign the acknowledgement indicating they reviewed, understand and will comply with the policy. The signed acknowledgement is retained by Human Resources.
- 6.0 Supervisors, managers, directors, etc. who utilize unpaid workforce members (volunteers, contract workers, temp staffing, etc.) review this “Confidentiality of Sensitive Information Policy” with their unpaid workforce members. Incoming unpaid workforce members sign an acknowledgement that they have reviewed, understand and will comply with the policy. The supervisors, managers, directors, etc. maintain the signed acknowledgement in the department.

IV. EQUIPMENT/MATERIALS

N/A

V. PROCEDURE

- 1.0 Access to Sensitive Information
 - 1.1 The workforce members’ supervisor and the “owner” of the information system application approve access to sensitive information that is maintained on any computer system.
 - A. The information “owner”, in conjunction with the supervisor, assigns a level of access that allows the workforce member the right to use the access to the extent needed for the workforce member to perform his/her duties, review access levels of workforce members transferring between departments, and, if applicable, the supervisor requests changes to access as soon as possible.
 - B. Passwords to computer systems are confidential and not shared. This includes giving a password to someone else or allowing someone else to access information under an incorrect user account as found in SY-IT-005, Information Technology Services Password policy.
 - C. Sensitive information is not copied to or stored on personal storage media. Sensitive information is not copied to or stored on personal computers, personal digital assistants, or other digital equipment not owned by Southern Illinois Healthcare.
 - 1.2 Where and to the extent possible maintain paper or electronic access logs documenting an audit trail of who has accessed sensitive information.
 - 1.3 Sensitive information remains on the premises of Southern Illinois Healthcare facilities at which it was created and or is maintained unless:
 - A. Removal has been approved by the department manager or administrator,
 - B. Created at the request of another healthcare provider, or
 - C. Required by a SY-CO-003, Protocol for Search Warrants; SY-CO004, Protocol for Subpoenas; or SY-HI-966, Uses and Disclosures Based on Public Policy Which Do Not Require the Patient’s Authorization.
 - 1.4 Work areas where sensitive information is accessible are designed to allow access to only those who need to know that information. This includes:
 - A. Placement of equipment such as computer monitors, printers and fax machines;

System

- B. Placement of distribution areas such as orders for pickup, patient medical records, medication dispensing equipment, and patient schedules;
 - C. Access to storage areas such as medical records, reports and billing information; and
 - D. Ability to dispose of sensitive information in a manner that maintains its confidentiality per SY-IT-550, Disposition of Sensitive Information.
- 1.5 Do not discuss or display sensitive information in a public area or in an area where persons who do not need to know the information would have access to the information such as waiting rooms, cafeterias, hallways, elevators, etc.
- A. Discuss sensitive information in private areas such as an office or exam room.
 - B. Do not leave sensitive information on desktops or electronic devices where it might be viewed or removed by unauthorized individuals.
 - C. Take reasonable precautions when there is no alternative to discussing or displaying sensitive information in areas where it may be overheard or seen by unauthorized individuals.
- 1.6 Do not disclose sensitive information, either accidentally or intentionally, to unauthorized individuals.
- A. Do not communicate sensitive information via unsecured e-mail, or voice mail where there is a reasonable chance that an unauthorized party might have access to the information.
 - B. If sensitive information is couriered to someone within SIH and the information cannot be hand delivered by the sender, the information is marked confidential, sealed and sent via Southern Illinois Healthcare courier. Sensitive information is sent in a manner that would make accidental disclosure difficult.
 - C. Fax sensitive information as needed in emergency situations as stated in SY-HI-008, Facsimile.
 - D. Patient authorization is needed to send individually identifiable health information to those who are not involved in the healthcare management of the patient or where the release of information is not required by law. (See SY-HI-964, Obtaining Patient Authorization for Uses and Disclosures Other Than Payment, Treatment, and Healthcare Operations, and SY-HI-966, Uses and Disclosures Based on Public Policy Which Do Not Require Patient Authorization).
 - E. Sensitive information is disposed of in accordance with the SY-IT-550, Disposition of Sensitive Information.
- 1.7 Do not use sensitive information in any form for personal use.
- A. Do not make copies of sensitive information, in whole or in part, for personal or any other use that may violate federal or state laws.
 - B. Do not make personal documentation of specific sensitive information.
- 1.8 Workforce members follow the formal request process found in SY-HI-964, Obtaining Patient Authorization for Uses Other Than Treatment, Payment, Healthcare Operations, to obtain their own Protected Health Information stored in any of Southern Illinois Healthcare information systems (e.g. Meditech, ChartMaxx, Med Series 4, etc). Self access to personal PHI or the PHI of family members is prohibited.
- 2.0 Termination of a Workforce Member's Access to Sensitive Information.
- 2.1 Termination or modification of access to sensitive information occurs once notified by either the SIH payroll system or the workforce member's supervisors.
- 3.0 Confidentiality policy acknowledgement.

- 3.1 All persons covered under this policy sign a confidentiality policy acknowledgement upon engagement.
- 3.2 Other persons who may have access to sensitive information as a result of some form of working relationship (contractual, volunteer, student, etc.) with Southern Illinois Healthcare must also sign a confidentiality agreement and / or must have included the Business Associate Agreement as part of the contract with Southern Illinois Healthcare. The agreements and / or business associate agreements are kept by the supervisor for that department.
- 4.0 Reporting Violations
 - 4.1 All suspected violations of this Confidentiality of Sensitive Information Policy are reported immediately to the workforce member's supervisor, director, administrator, Corporate Compliance, or the Privacy Officer.
 - 4.2 The facility complaint/incident reporting policies are followed for a suspected breach of protected health information.
 - 4.3 Workforce members are encouraged to also report areas where a violation is possible.
 - 4.4 The reported violations are investigated as soon as possible.
 - 4.5 If it has been determined that a breach of confidentiality did occur due to a workforce member's negligence, the person or persons are disciplined in accordance with SY-HR-401, Improvement Counseling.
 - 4.6 If it has been determined that a breach of confidentiality did occur due to a non-workforce issue (e.g., information system programming error, access / control issue, auto fax to incorrect phone number, etc), the supervisor(s) takes immediate action to restore confidentiality controls.
 - 4.7 Those who have a reasonable belief that a breach has occurred, but do not report the incident may be subject to the penalties listed in the Violations of the Confidentiality of Sensitive Information Policy section below.
- 5.0 Tracking abuse
 - 5.1 Audit logs maintained to track exposure to sensitive information are reviewed randomly and when a violation of this policy is suspected.
- 6.0 Penalties for violations of this policy.
 - 6.1 Employees
 - A. Confirmed violations of the Confidentiality of Sensitive Information policy are reported to the employee's supervisor and the Human Resources department for the employee's facility.
 - B. The violation is reflected on the employee's evaluation and leads to the Improvement Counseling process following the Breach of Confidentiality Criteria documented in this policy.
 - C. Per the Improvement Counseling policy, SIH management reserves the right to modify the improvement counseling schedule to reflect extreme circumstances. In the case of a breach of confidentiality, immediate termination may be warranted without progressing through the normal four (4) step process.
 - D. See SY-HR-401, Improvement Counseling policy for further information.
 - 6.2 Non-employees
 - A. In the case of a breach of confidentiality, immediate termination of privileges or services may be warranted.
 - 6.3 Violation of this policy may also be a violation of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or other federal, state, or local laws or regulations. Incidents may be reported to the appropriate law enforcement agencies.

VI. DOCUMENTATION

- 1.0 Confidentiality of Sensitive Information Agreement is maintained by Human Resources for all employees and by the department manager/supervisor for all non-employee workforce members.
- 2.0 Business Associate agreement is maintained by General Counsel for all contracts.

VII. CHARGES

N/A

Additional Approvals and Review/Revision Dates			
Review Dates:	05/27/89, 09/30/06,		
Revision Dates:	04/14/04, 01/29/07, 03/26/07, 3/26/07		
Replaces:	N/A		
Additional Approvals:	<u>Name (print)</u> William S Sherwood	<u>Title</u> Vice President/General Counsel	<u>Signature</u>

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 desk while logged into an application that could contain PHI, (exception: in case of patient emergency where delay could cause serious complications for the patient)

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:

- Employee self access of own or family member's sensitive information that is not for treatment, payment or healthcare operations
- 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:

- Intentional unauthorized access to 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, USB drive, other optical or magnetic media or devices not owned by Southern Illinois Healthcare, any unapproved Internet site.
- Posting sensitive information on Internet sites, such as MySpace, FaceBook, Blogs, etc. without intent to harm a patient, workforce member or SIH.
- Removing any sensitive information in any form from the premises of Southern Illinois Healthcare 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.



CONFIDENTIALITY AGREEMENT

Security and confidentiality is a matter of concern for all persons who may come in contact with sensitive information. Each person who may come in contact with sensitive information (verbal, written or electronic) holds a position of trust relative to this information and must recognize the responsibilities entrusted in preserving the security and confidentiality of this information. The following specific principles are applicable to all Southern Illinois Healthcare (SIH) workforce, including but not limited to students, volunteers, and employees regardless of their classification.

I understand:

- **Sensitive Information** is information which if improperly disclosed could cause damage to the reputation, privacy, image and/or financial viability of the patient, medical staff, employees, board of trustees and/or SIH. Sensitive information includes, but is not limited to: all individually identifiable health information; anything marked or stated as confidential, employee information, financial information, guarded operational information, marketing and general business strategies, patient billing information, physician information and proprietary products and product development.
- that sensitive information should only be disclosed to those authorized to receive it.
- that any misuse or disclosure of sensitive information or permitting improper computer access to any unauthorized party may result in irreparable harm to SIH, its affiliates or patients, and may result in revocation of my access privileges and/or termination of my employment/relationship in accordance to the policies of SIH. I further understand that these activities may also be reportable to local, state and federal authorities for investigation and possible prosecution.
- that my obligations under this Agreement will continue after termination of my employment/relationship.

I will:

- respect the rules governing the use of any sensitive information and only utilize information necessary to fulfill my responsibilities (e.g., work assignment) to SIH. I understand that access, use, or disclosure of sensitive information for any other purpose is prohibited.
- prevent unauthorized use of and/or access to sensitive information including myself as a workforce member of SIH accessing/obtaining my own PHI and/or the PHI of a family member .
- not seek personal benefit or permit others to benefit personally from sensitive information or use of equipment available through my employment/relationship with SIH.
- not exhibit or divulge the contents of any sensitive information except to fulfill a work assignment.
- not discuss sensitive information in public areas, such as the cafeteria, hallways, or elevators, within the hearing of persons not entitled to hear the information.
- not remove any sensitive information, in any form, from the premises of SIH facilities where it is kept except in the performance of my job duties. If I am authorized to remove sensitive information from the premises of SIH for the performance of my job duties, I will agree to safeguard the information and/or the storage media to prevent unauthorized access.
- report any violations, intentional, unintentional and/or suspected to the appropriate SIH authority.
- not copy or store sensitive information on personal storage media, such as but not limited to my personal computer, personal digital assistant, or other optical or magnetic media or devices not owned by SIH.
- handle, store and dispose of sensitive information appropriately (e.g. shredding, degaussing).

By signing this, I agree that I have read and agree to comply with Southern Illinois Healthcare Confidentiality of Sensitive Information policy (SY-IT-001) and this Agreement.

Name (print)

Date

Facility and department SIH

Employee Number or last 4 digits SS # (non SIH employees)

Signature