SOUTHERN ILLINOIS HEALTHCARE

System **Policy and Procedure**

Title:	Internet Access and Usage	**Number:**	SY-IT-007
Applies to:	All users of the Southern Illinois Healthcare Internet services	**First Created:**	3/97
Issuing Dept:	Information Technology Services	**Last Revised:**	7/9/07
Approved by:	Frank Sears, Vice President / Chief Information Officer		

I. POLICY

Southern Illinois Healthcare (SIH) provides Internet access to provide patient care, aid employees in performing their job duties, and offers Internet access to interested physicians as a chargeable service. The Internet provides a source of information from which almost every professional discipline represented in SIH can benefit. SIH believes use of the Internet can enhance the quality of care delivered, improve productivity, and increase customer satisfaction. Upon request Internet access will be provided to members of the workforce and medical staff.

II. DEFINITIONS

Corporate Information – is information that is available to the staff of Southern Illinois Healthcare, but is not available to the general public. Information in this area may include strategic planning for Southern Illinois Healthcare, employee telephone extensions, corporate policies and procedures, and information available on the Southern Illinois Healthcare intranet.

Encryption – Information that has been encrypted has been rendered unintelligible. The recipient must decrypt the information before the information would have meaning.

Highly Confidential Information - shall mean 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;
- Sexually transmitted disease(s);
- Genetic testing;
- Child abuse and neglect;
- Domestic abuse of an adult with a disability; or
- Sexual assault.

Individually Identifiable Health Information - shall mean 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.

Internet or World Wide Web - The term Internet or World Wide Web (WWW or Web) is a collection of web pages that are developed in accordance with the hypertext markup language (HTML) format standard, and may be accessed via Internet connections using a Web browser.

Malware – Malware includes software that was developed for the specific purpose of causing harm to information systems or networks. This includes computer viruses, worms or trojans. Malware can cause information systems to shutdown, provide inaccurate information, or send information to an external unauthorized source.

MSO- (Management Service Organization) Southern Illinois Healthcare's Information Technology Services department provides services to healthcare providers who have agreed to purchase the services for their healthcare enterprise.

Proxy Server- A proxy server is a server that acts as an intermediary between a workstation user and the Internet so that the enterprise can provide security, administrative control, and caching service. A proxy server is associated with or part of a gateway server that separates the enterprise network from the outside network and a firewall server that protects the enterprise network from outside intrusion.

Protected Health Information - shall mean 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.)

Remote Access Software – Remote access software is software that would allow access to information on the computer, or information that could be available to the user signed on to that computer from a place other than the computer. Although this software can be helpful for hosting meetings or demonstrations, this software is not implemented to assist in problem resolution or maintenance of information system which have sensitive information or are in production. Information systems that are not in production may use this software for initial setup and installation under the supervision of the Information Technology Services staff. Web-Ex, PCANYWHERE, GOTOMYPC are all examples of remote access software.

Sensitive Information – Information which if improperly disclosed could cause damage to the reputation, privacy, image and/or financial viability of the patient, medical staff, employees, 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.

Sexual Harassment – Sexual Harassment in the workplace is unlawful. Sexual Harassment is defined as unwelcome advances, requests for sexual favors and/or other verbal, written, visual or physical conduct of a sexual or sexually suggestive nature by employees, supervisors, management, medical staff, customers, visitors, volunteers, contractors, vendors, agents, or any other person where such conduct is either made in explicit or implicit terms as a condition of employment; used as the basis for employment decisions affecting

employees; has the purpose or effect of substantially interfering with an employee's work performance; or creates an intimidating, hostile, or offensive work environment. This may involve the behavior of a person of either sex toward a person of the opposite or same sex.

Spyware – Spyware is software that was developed for the specific purpose of capturing information from the host computer. This may include keystrokes used, websites visited, or information accessed by the user.

Streaming Media – Streaming media is sound (audio) and/or pictures (video) that are transmitted on the Internet in a streaming or continuous fashion. This can include but is not limited to live or pre-recorded sound and / or pictures available from various types of internet sites such as television broadcasts, radio station programming, weather radar monitoring, web cameras, etc.

Workforce - shall mean 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 Accounting Department – The accounting department is responsible for the billing and collection of fees associated with access the physicians and members of their staff might have as part of a billable service contract.

2.0 Authorized users of Southern Illinois Healthcare's Internet service – Users of the Southern Illinois Healthcare are responsible to use their access for the completion of job duties and in conjunction with the Mission and Values of Southern Illinois Healthcare. Particular attention is to be paid to the values of stewardship and integrity. Users are to use the Internet in a manner that would not violate federal, state or local laws, including copyright, anti-spam, etc. Users are to take care and not expose the Southern Illinois Healthcare information systems network to malicious software, such as malware, spyware, etc.

3.0 Information Technology Services department – The Information Technology Services department is responsible to allow access to the internet for members of the workforce or MSO subscribers who have completed the internet access agreement.

4.0 Management – Department managers, directors, and above are responsible for requesting access to the Internet for their employees. Requests must be made only when not having access to the Internet will prevent the employees from completing their job duties. Requests for Internet access are to identify the business need for the requested access.

5.0 Physician Services – The Physician Services group is responsible for the requesting of access and termination of access for members of the medical staff who purchase Internet services access as part of their service agreement. The Physician Services group will notify the Accounting department of the services for billing purposes.

IV. EQUIPMENT/MATERIALS

1.0 Personal Computer connected to the Southern Illinois Healthcare network

2.0 Microsoft Internet Explorer version 5.1 service pack 2 or higher with the ability to cipher strength of 128-bits

V. PROCEDURE

1.0 Gaining access to the internet through an SIH PC

1.1 For members of the Southern Illinois Healthcare workforce, including contract staff:

A. All requests for Internet access must be made by SIH employees who are the supervisor, or their designee, of the person for whom the Internet access is needed. The requestor

must submit the request using the Information Technology Services Project/Capital Request form which is available on the Southern Illinois Healthcare Intranet site under the Information Technology department.

1.2 For affiliated physicians or clinics:

A. All requests for Internet for persons or entities who are not part of the Southern Illinois Healthcare workforce, such as an affiliated physician or clinic, must be made through the Physician Services group.

1) The Physician Services group is to submit an issue or a request using the Information Technology Services Project/Capital Request form which is available on the Southern Illinois Healthcare Intranet site under the Information Technology department.

2) The Physicians Services group is to also forward billing information to the Accounting Department.

1.3 A copy of this policy will be provided to anyone Internet access has been requested for. The Internet Access Agreement form must be completed and returned as the written acknowledgement, stating that the user has read the policy, before access will be granted.

2.0 The following general guidelines identify acceptable use of the Internet when accessed through the Southern Illinois Healthcare Internet connection:

2.1 Employees are accessing information to meet the requirements of their jobs. If the information will include patient identifiable information, review the Use of Sensitive Information on the Internet section (V.5.0) below.

2.2 Workforce members are not to save account names and/or passwords for Internet applications. This does violate Southern Illinois Healthcare policy SY-IT-005 User Account and Password.

2.3 Participation in on-line group activities, such as discussion groups, that have a direct relationship to the user's job.

2.4 Authorized Internet users may access the Internet for non-job-related information provided

A. The access is done on the employee's personal time (before and after work, lunch breaks, or on days off),

B. Use of the equipment and/or Internet access does not interfere with normal Southern Illinois Healthcare operations, and

C. These policy guidelines are followed.

2.5 Physicians will determine when their employees may use the Internet for personal use, as long as the personal use does not interfere with normal Southern Illinois Healthcare operations, and these policy guidelines are followed.

2.6 Authorized Internet users are not permitted to engage in the following activities at any time using Southern Illinois Healthcare equipment or facilities, or when using a SIH Internet Address:

A. Access, download, print or anyway retrieve information that would be in violation of policy SY-HR-403 Sexual Harassment.

B. The use is contrary to the Southern Illinois Healthcare mission and values,

C. Engage in activities which would violate federal, state, or local laws.

D. Engage in personal commercial activities on the Internet, including offering services or merchandise for sale.

E. Allowing others to use your Internet account.

F. Send or receive information considered sensitive under the policy SY-IT-001 Confidentiality of Sensitive Information, except as identified in the Use of Sensitive Information on the Internet section (V.5.0) below.

G. Allow access to a computer though the internet on the Southern Illinois Healthcare network through a remote access software which has not been approved by the Vice President of Information Technology Services / designee.

H. Modifing settings on the internet browser which allows a user to bypass Southern Illinois Healthcare proxy server.

I. Using additional software or internet sites to mask internet activity from Southern Illinois Healthcare monitoring.

J. Access streaming media, either video or audio, unless it is specificly job related.

3.0 Individuals using SIH equipment to access Internet are subject to having activities monitored by the Information Technology Services department. Use of this system constitutes consent to monitoring.

4.0 Limited Information Technology Services personnel shall have unrestricted access to Internet and related information stored on corporate owned equipment. This access is required for reasons that include retrieving business-related information, trouble-shooting hardware and software problems, preventing unauthorized access and system misuse, determining compliance with software copyright and distribution policies, and complying with legal and regulatory requests for information.

5.0 Use of sensitive information on the Internet

5.1 Employees of SIH must use extreme caution when using the Internet in conjunction with sensitive information as identified in policy SY-IT-001 Confidentiality of Sensitive Information.

5.2 Employees may only transmit or retrieve information which has been approved by the director of the department, the Privacy Officer or his designee, and the Security Officer or his designee.

5.3 Transmission of sensitive information over the internet is only acceptable if the following encryption protections are used:

A. Acceptable encryption algorithms include:

1) Symmetric: Triple DES with 112 bit key

2) Asymmetric: 1024 bit key (e. g. RSA)

3) Elliptical Curve: 160 bit key

B. Encryption may be

1) Hardware-based: Symmetric password “private” key devices such as link-encryptors

2) Software-based:

a) Secure Sockets Layer (SSL) implementations at a minimum SSL level of version 3.0, standard commercial implementations of PKI, or some variation thereof, implemented in the Secure Sockets layer

b) S-MIME for encryption in the e-mail layer

c) Offline encryption/decryption of files at the user sites which are then attached to or enveloped (tunneled) within an unencrypted header and/or transmission

C. The recipient of the information has signed a nondisclosure statement, business associate language was included in the contract with the recipient, or the release is an allowable release as defined by the Health Insurance Portability and Accountability Act of 1996.

6.0 Tracking Abuse

6.1 Information Technology Services may perform random audits of visited Internet web sites. Suspected abuse will be investigated and brought to the attention of the Senior Management

member responsible for the area where the incident occurred, along with copies of trace reports showing the web sites accessed. Abuse by physicians from hospital workstations will be brought to the attention of the Hospital Administrator.

6.2 Suspected abuse.

A. If an Internet user suspects that the security of their user account was breached, refer to the policy SY-IT-005 User Account and Password to request a new password.

B. If a internet user is suspected of breaching this policy, the following steps must be completed:

1) In the event that there is a suspected breach of this policy, the breach is to be reported to the Information Technology Services Compliance and Quality Assurance department. The report must be specific as to what type of abuse is suspected, the time frame the abuse occurred, and other specific details that will target the investigation.

2) The incident will be reviewed, and based on the situation, the Vice President of Information Technology Services or the Information Technology Services Compliance and Quality Assurance Coordinator will give approval for specific review of the Internet access account, which is suspected of abuse.

3) The staff who is reviewing the internet access log will review only those sites accessed in the suspected time frame, suspected subject, and suspected internet user(s). Any Internet sites that are found to support the abuse will be forwarded to either the Vice President of Information Technology Services or the Information Technology Services Compliance and Quality Assurance Coordinator.

7.0 Penalties for violations of this policy.

7.1 Employees.

A. Violation of this policy will lead to the Improvement Counseling process and possible suspension of Internet access privileges.

B. Per policy SY-HR-401: Improvement Counseling, SIH management reserves the right to modify the improvement counseling schedule to reflect extreme circumstances.

C. See policy SY-HR-401: Improvement Counseling for further information.

7.2 Non-employees.

A. The Non-employees include all persons who are considered part of the workforce, but are not an employee of Southern Illinois Healthcare or are accessing the internet through the MSO arrangement with a doctor's office or clinic. This group includes volunteers, members of the clergy, physicians, contract employees, student trainees, interns, contractors, temporary employees, etc.

B. SIH management reserves the right to modify the improvement counseling schedule to reflect extreme circumstances

C. Violation of this policy may also be a violation of federal or state law. Incidents may be reported to the appropriate law enforcement agencies.

VI. DOCUMENTATION

1.0 Information Technology Services Project/Capital Request form available on the Southern Illinois Healthcare intranet site. (https://intranet.Sih.net/ProjecTrack.nsf/WebRequest?OpenForm)

2.0 Internet access agreement signed by the user who will receive Internet access. The signed forms are retained in the Information Technology Services department.

VII. CHARGES

1.0 Charges are applicable if the Internet access is provided as part of a MSO agreement, and will be set based on that agreement.

Additional Approvals and Review/Revision Dates			
Review Dates:	7/9/07		
Revision Dates:	9/17/04		
Replaces:	N/A		
Additional Approvals:	**Name (print)**	**Title**	**Signature**

Internet Access Agreement

I hereby acknowledge that I have received a written copy of the Southern Illinois Healthcare (SIH) Internet Access and Usage Policy. I understand and agree to abide by the policy. Access will not be granted to Internet through SIH until this form is completed and returned to Information Technology Services.

Any violation of the Internet Access and Usage policy and procedure will result in disciplinary action per the Internet Access and Usage Policy. The Internet Access and Usage policy may at some time be modified. Users understand that by signing this agreement, they are required to review and comply with any of those changes.

Workforce member (print name) _____

Employee Number: _____

Facility ○**MHC** ○**HH** ○**SJ** ○**System** ○**MMHC** ○**Physician Services** ○ **SIMS**

Department _____

Employee Signature _____ **Date**_____

Witnessed by (print name) _____

Facility ○**MHC** ○**HH** ○**SJ** ○**System** ○**MMHC** ○**Physician Services** ○ **SIMS**

Department _____

Witness Signature _____ **Date**_____

Return this form to:

Southern Illinois Healthcare

Information Technology Service

Compliance/QA Section