



INFORMATION SECURITY MANAGEMENT PROCESS POLICY

1.0 PURPOSE

Information Technology is intended to improve access to information, enhance efficiency, and facilitate communication. The purpose of this policy is to define the security management process for information technology resources utilized in support of SJHS/CHS.

2.0 SCOPE

This policy applies to all Users, and the information covered in this policy includes Protected Health Information (or PHI).

3.0 POLICY

It is SJHS/CHS policy to establish a security management process to involve the creation, administration, and oversight of policies to address the full range of security issues and to ensure the prevention, detection, containment, and correction of security violations.

Performance of these activities should be consistent with pertinent policies and procedures.

4.0 PROCEDURE

- 4.1.** SJHS/CHS shall define and document the assignment of a singular centralized SJHS/CHS IT Security Officer who is responsible for:
 - 4.1.1.** the development and deployment of reasonable and appropriate policies, standards, procedures, forms, technical implementations, assessments, and training methods for the prevention, detection, containment, and correction of security violations;
 - 4.1.2.** the accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI held by SJHS/CHS;
 - 4.1.3.** the implementation at SJHS/CHS of security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level;



INFORMATION SECURITY MANAGEMENT PROCESS POLICY

- 4.1.4. the periodic technical and non-technical evaluation that establishes the extent to which SJHS/CHS's security implementation meets the requirements of the HIPAA Security Rule, and
- 4.1.5. the guidance, integration, and direction of security measures as they relate to other information technology objectives, projects, and activities.
- 4.2. An IT Security Task Force shall act as the governing body for promulgating decisions made and, where required, achieving consensus on items 4.1.1 through 4.1.4 above.
 - 4.2.1. The IT Security Task Force shall include standing members from Legal/Compliance, SJHS/CHS IT Leadership, subject matter expertise in information security, and SJHS/CHS IT, as well as SJHS/CHS Ministry Peers representing site interests in Legal/Compliance and IT.
 - 4.2.2. The IT Security Task Force shall schedule meetings and convene at least 4 times per year.
 - 4.2.3. Activities of the IT Security Task Force shall be reportable to SJHS/CHS Leadership.

5.0 REFERENCES

- 45 CFR 164.308(a)(1)(i), "HIPAA" - Health Insurance Reform: Security Standards (Security Management Process)
- 45 CFR 164.308(a)(1)(ii)(A) and (B), "HIPAA" - Health Insurance Reform: Security Standards (Security Management Process – Risk Analysis and Risk Management)
- 45 CFR 164.308(a)(2), "HIPAA" - Health Insurance Reform: Security Standards (Assigned Security Responsibility)
- 45 CFR 164.308(a)(8), "HIPAA" - Health Insurance Reform: Security Standards (Evaluation)



INFORMATION SECURITY MANAGEMENT PROCESS POLICY

6.0 DEFINITIONS

Confidential Information	financial data, proprietary reports, human resources information, marketing and sales information, and other similar privileged “need to know” information
Information Technology	any computer, telephone, messaging system (i.e. voicemail or e-mail), electronic media, application, protocol, or other equipment utilized on a public or private internetwork)
Protected Health Information (PHI)	individually identifiable information relating to the past, present, or future physical or mental health or condition of an individual or can be used to identify an individual
SJHS/CHS IT	Members of the SJHS/CHS Information Technology staff, other SJHS/CHS employees performing IT-specific tasks, Perot Systems associates performing IT services on behalf of SJHS/CHS, and other contractors of SJHS/CHS performing IT-specific tasks
Users	members of the SJHS/CHS workforce including its employees, volunteers, and trainees. Independent Contractors and vendors are considered Business Associates of an SJHS/CHS entity, and thus not members of its workforce.



INFORMATION TECHNOLOGY ACCESS AND USAGE POLICY

1.0 PURPOSE

Information Technology is intended to improve access to information, enhance efficiency and facilitate communication. The purpose of this policy is to define the appropriate use and physical security requirements of Information Technology utilized in support of SJHS/CHS.

2.0 SCOPE

This policy applies to all Users, and the information covered in this policy includes Protected Health Information (or PHI), Confidential Information, and general company information.

3.0 POLICY

It is SJHS/CHS policy to specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes and safeguards for those workstations that access electronic protected health information.

Users of Information Technology are responsible to exercise good judgment and ensure all usage is professional, ethical, and lawful. Use should be consistent with pertinent policies and procedures regarding individual conduct and the expressions of the values of SJHS/CHS.

Performance of these activities should be consistent with pertinent policies and procedures.

4.0 PROCEDURES

- 4.1.** Users are advised to exercise great care when accessing Confidential or PHI-related information. For Confidential Information, accesses should be limited and specifically related to a SJHS/CHS business purpose. For PHI, Users should make reasonable efforts to limit the PHI accessed to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request in compliance with relevant policies and procedures. Users should consider the implementation of physical safeguards for all Information Technology that accesses electronic PHI or confidential information in order to restrict access to authorized users.



INFORMATION TECHNOLOGY ACCESS AND USAGE POLICY

- 4.2.** Users are advised to exercise great care when transmitting Confidential or PHI-related information. For Confidential Information, disclosures should be limited and specifically related to a SJHS/CHS business purpose. For PHI, Users should make reasonable efforts to limit the PHI disclosed to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request in compliance with relevant policies and procedures. All disclosed information should identify the User and their organization by name. Information may not be sent that hides the identity of the User or represents the User as someone else or someone from another organization.
- 4.3.** All information created, transmitted, accessed, received, stored, or otherwise utilized via Information Technology is SJHS/CHS property and should not be considered private property. Users are responsible for the content of such information. Users understand and agree that SJHS/CHS should monitor activities at any time, and as such, should not have any expectation of privacy when using Information Technology.
- 4.4.** Users should ensure that any method of authentication for Information Technology (such as a password or a token) is kept confidential, used only by the authorized individual, and not shared with anyone at any time.
- 4.5.** Users are responsible for placing content in pre-determined locations for sharing, backup, and the like. Users also understand that SJHS/CHS information is stored in various forms; deletion of information does not insure its permanent removal.
- 4.6.** Users should not download or install software that is not registered to SJHS/CHS, does not conform to SJHS/CHS technology standards, and that does not meet the other copyright and trademark requirements of this policy. Users of Information Technology are responsible for complying with all relevant laws and regulations related to the transmission of copyrighted and trademarked materials, information privacy, and PHI.
- 4.7.** Users are responsible for maintaining the confidentiality and security of any Information Technology access to PHI. Unless directed by an appropriate authority, Users should not install, circumvent, remove, delete, modify, or otherwise tamper with methods of connectivity, monitoring, integrity assurance, or protection of Information Technology.
- 4.8.** Information Technology is provided for conducting job-related duties, research, and Reasonable Personal Use. Users may not intentionally utilize Information



INFORMATION TECHNOLOGY ACCESS AND USAGE POLICY

Technology to create, transmit, access, receive, or otherwise utilize content that contains:

- 4.8.1. information contrary to stated policies regarding User conduct, business conduct, objectionable content, or values of SJHS/CHS,
- 4.8.2. information about Users, SJHS/CHS's position on any issue, or about an SJHS/CHS competitor or any other organization without the express approval of a SJHS/CHS manager responsible for approving such communications;
- 4.8.3. information intended for the personal or commercial gain of the User
- 4.8.4. information prohibited by this or any other policy, procedure, guideline, standard, or values statement of SJHS/CHS.
- 4.9. Where reasonable and appropriate, users are advised to log off workstations, disable workstations, or implement screensavers when not in use.
- 4.10. Users are advised that the ability to connect to (or receive) content does not in itself imply that access is permitted, whether private (i.e. Meditech modules, Human Resource information) or public (i.e. a Web site containing objectionable content).
- 4.11. Users are encouraged to notify their manager or Information Technology support personnel for the resolution or escalation of questions, comments, or clarifications regarding the use of Information Technology. Users should bring violations of this policy to the attention of their manager, the V.P. of Human Resources, or any other management employee with whom the individual feels comfortable.
- 4.12. Violation of this policy may result in loss of access and additional disciplinary action, including the possibility of immediate termination.

5.0 REFERENCES

- 45 CFR 164.310(b), "HIPAA" - Health Insurance Reform: Security Standards (Workstation Use)
- 45 CFR 164.310(c), "HIPAA" - Health Insurance Reform: Security Standards (Workstation Security)



INFORMATION TECHNOLOGY ACCESS AND USAGE POLICY

6.0 DEFINITIONS

Confidential Information	Financial data, proprietary reports, human resources information, marketing and sales information, and other similar privileged "need to know" information
Information Technology	Any computer, telephone, messaging system (i.e. voicemail or e-mail), electronic media, application, protocol, or other equipment utilized on a public or private internet work)
Protected Health Information (PHI)	Individually identifiable information relating to the past, present, or future physical or mental health or condition of an individual or can be used to identify an individual
Reasonable Personal Use	Any use of Information Technology that is not job-related (in function or research) and: A) does not interfere with the User's work performance, B) does not interfere with any other User's work performance, C) impacts the operation of SJHS/CHS, or D) violates provisions of this or any other policy, procedure, guideline, standard, or corresponding values statement of SJHS/CHS.
SJHS/CHS IT	Members of the SJHS/CHS Information Technology staff, other SJHS/CHS employees performing IT-specific tasks, Perot Systems associates performing IT services on behalf of SJHS/CHS, and other contractors of SJHS/CHS performing IT-specific tasks



ST. JOSEPH HEALTH SYSTEM

DIVISION: (HR, Finance, etc.) IS
LAST DATE REVISED: 02/23/2005
LAST DATE REVIEWED: 02/23/2005
ORIGINAL DATE ADOPTED: 06/04/2003
PAGE NUMBER: 8 of 71
POLICY/PROCEDURE: IS401
APPROVED BY: Security Task Force
CHS REVIEW DATE: 01/18/2006;
4/12/2007
REVIEWED BY: CHS Compliance
Committee

INFORMATION TECHNOLOGY ACCESS AND USAGE POLICY

Users	Members of the SJHS/CHS workforce including its employees, volunteers, and trainees. Independent Contractors and vendors are considered Business Associates of an SJHS/CHS entity, and thus not members of its workforce.
-------	---

MEDIA RE-USE AND DISPOSAL POLICY

1.0 PURPOSE

Information Technology is intended to improve access to information, enhance efficiency and facilitate communication. The purpose of this policy is to define the re-use and final disposition of information technology utilized in support of SJHS/CHS.

2.0 SCOPE

This policy applies to all Users, and the information covered in this policy includes Protected Health Information (or PHI) and confidential information.

3.0 POLICY

It is SJHS/CHS policy to govern and control the re-use and final disposition of information technology on which electronic PHI or confidential information is stored.

SJHS/CHS employees whose responsibilities include the re-use or final disposition of information technology shall ensure the irrecoverable destruction of electronic PHI or confidential information prior to re-use or disposal.

Performance of these activities should be consistent with pertinent policies and procedures.

4.0 PROCEDURES

4.1. Authorized methods for the most commonly used information technology appear below:

Magnetic Tape	Degauss or destroy
Floppy Disks and Compact Disks	Destroy
Other Magnetic Disks (e.g. hard drives)	Three-pass overwrite, degauss, or destroy
Optical Disks	Destroy
Random-access memory (RAM)	Three-pass overwrite, remove from power, or destroy
Cathode-ray tubes (CRT)	Inspect for burned-in information - if present, destroy.
Impact printers	Inspect for burned-in information - if

MEDIA RE-USE AND DISPOSAL POLICY

	present, destroy. Otherwise, destroy ribbons and clean platens
Laser Printers	Run five font test pages

- 4.2.** Information technology that is not destroyed should have all power removed, including battery and standby power, and shall be clearly marked to indicate that the activity has taken place.
- 4.3.** Independent contractors, vendors, and other entities that perform any of the above methods should be evaluated to determine whether or not the independent contractor, vendor, or other entity is defined as a business associate.
 - 4.3.1.** All independent contractors, vendors, and other entities identified as business associates as defined in existing SJHS/CHS policies should have in place contractual provisions intended to protect the privacy and provide for the security of PHI disclosed to such independent contractors, vendors, and other entities. Existing SJHS/CHS policies should dictate the content of the contractual provisions.
- 4.4.** At a minimum, Asset Control (e.g., Inventory, Material Management) and Financial Control (e.g., Accounting, Finance) departments should be notified of any information technology above that is destroyed or is no longer intended for re-use (e.g., marked for donation, release to employee).
 - 4.4.1.** As appropriate, information technology disposed or re-used according to the above should include a documented record of the date, the type of asset processed (including asset tracking/tagging information), the method used, the entity performing the action, and the final disposition (e.g., destroyed, marked for donation, release to employee). Business Associates should provide documentation of these activities.
- 4.5.** Each SJHS/CHS Information Services Planning Council (ISPC) should be advised of and/or approve as necessary the intended actions of final disposition.

5.0 REFERENCES

45 CFR 164.310(d)(2)(i) and (ii), "HIPAA" - Health Insurance Reform: Security Standards (Device and Media Controls – Disposal and Media Re-Use)

Cleaning and Sanitization Matrix, U.S. D.O.D. NISPOM 5220.22-M, 1995



MEDIA RE-USE AND DISPOSAL POLICY

6.0 DEFINITIONS

Business Associate	a person, independent contractor, vendor, consultant, etc. who on behalf of SJHS/CHS performs, or assists in the performance of a function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administrative, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and re-pricing; or provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for SJHS/CHS where the provisions of such service involves the disclosure of protected health information from SJHS/CHS or from another Business Associate of SJHS/CHS
Confidential Information	financial data, proprietary reports, human resources information, marketing and sales information, and other similar privileged "need to know" information
Degauss	To generate a magnetic force that orients magnetic media particles at random, erasing the data from media
Destroy	To disintegrate, incinerate, pulverize, or otherwise manipulate to ensure the irrecoverable destruction of data
Information Technology	any computer, telephone, messaging system (i.e. voicemail or e-mail), electronic media, application, protocol, or other equipment utilized on a public or private



ST. JOSEPH HEALTH SYSTEM

DIVISION: (HR, Finance, etc.) IS
LAST DATE REVISED: 01/12/2005
LAST DATE REVIEWED: 01/12/2005
ORIGINAL DATE ADOPTED: 09/08/2003
PAGE NUMBER: 12 of 71
POLICY/PROCEDURE: IS402
APPROVED BY: Security Task Force
CHS REVIEW DATE: 01/18/2006;
4/12/2007
REVIEWED BY: CHS Compliance
Committee

MEDIA RE-USE AND DISPOSAL POLICY

	internetwork)
Protected Health Information (PHI)	individually identifiable information relating to the past, present, or future physical or mental health or condition of an individual or can be used to identify an individual
SJHS/CHS IT	Members of the SJHS/CHS Information Technology staff, other SJHS/CHS employees performing IT-specific tasks, Perot Systems associates performing IT services on behalf of SJHS/CHS, and other contractors of SJHS/CHS performing IT-specific tasks
Three-pass overwrite	To replace existing data with a character, its complement, and a random character
Users	members of the SJHS/CHS workforce including its employees, volunteers, and trainees. Independent Contractors and vendors are considered Business Associates of an SJHS/CHS entity, and thus not members of its workforce.



FACILITY MAINTENANCE RECORDS POLICY

1.0 PURPOSE

Information Technology is intended to improve access to information, enhance efficiency, and facilitate communication. The purpose of this policy is to define the records of maintenance performed on the physical locations of information technology resources utilized in support of SJHS/CHS.

2.0 SCOPE

This policy applies to all Users, and the information covered in this policy includes Protected Health Information (or PHI) and confidential information.

3.0 POLICY

It is SJHS/CHS policy to maintain records for the physical components of a facility where electronic PHI or confidential information is stored.

SJHS/CHS employees whose responsibilities include the maintenance of records for the physical components of a facility where electronic PHI or confidential information is stored shall ensure that repairs and modifications related to security (for example, hardware, walls, locks and doors) are documented.

Performance of these activities should be consistent with pertinent policies and procedures.

4.0 PROCEDURES

- 4.1.** All equipment should be correctly maintained to provide availability and protect the integrity and confidentiality of information.
 - 4.1.1.** All physical components relating to security (e.g., walls, doors, locks) should be correctly maintained to provide adequate protection against physical threats.
- 4.2.** Equipment should be monitored and inspected in accordance with manufacturer's specifications.
- 4.3.** Only authorized maintenance personnel are allowed to perform repairs and all repairs or service work should be recorded.
- 4.4.** If equipment should be sent offsite for repairs, the confidentiality and integrity of any information should be ensured.



DIVISION: (HR, Finance, etc.) IS
LAST DATE REVISED: 01/12/2005
LAST DATE REVIEWED: 01/12/2005
ORIGINAL DATE ADOPTED: 09/08/2003
PAGE NUMBER: 14 of 71
POLICY/PROCEDURE: IS403
APPROVED BY: Security Task Force
CHS REVIEW DATE 01/18/2006,
 4/12/2007
REVIEWED BY: CHS Compliance
 Committee

FACILITY MAINTENANCE RECORDS POLICY

5.0 REFERENCES

45 CFR 164.310(a)(2)(iv), "HIPAA" - Health Insurance Reform: Security Standards (Maintenance Records)

6.0 DEFINITIONS

Confidential Information	financial data, proprietary reports, human resources information, marketing and sales information, and other similar privileged "need to know" information
Information Technology	any computer, telephone, messaging system (i.e. voicemail or e-mail), electronic media, application, protocol, or other equipment utilized on a public or private internetwork)
Protected Health Information (PHI)	individually identifiable information relating to the past, present, or future physical or mental health or condition of an individual or can be used to identify an individual
Users	members of the SJHS/CHS workforce including its employees, volunteers, and trainees. Independent Contractors and vendors are considered Business Associates of an SJHS/CHS entity, and thus not members of its workforce.



INFORMATION SECURITY INCIDENT RESPONSE AND REPORTING POLICY

1.0 PURPOSE

Information Technology is intended to improve access to information, enhance efficiency, and facilitate communication. The purpose of this policy is to define the methods of security incident response and reporting for information technology resources utilized in support of SJHS/CHS.

2.0 SCOPE

This policy applies to all Users, and the information covered in this policy includes Protected Health Information (or PHI) and confidential information.

3.0 POLICY

It is SJHS/CHS policy, for information technology where electronic PHI or confidential information is stored, to a) identify and respond to suspected or known security incidents, b) mitigate (to the extent practicable) harmful effects of known security incidents, and c) document security incidents and their outcomes.

Performance of these activities should be consistent with pertinent policies and procedures.

4.0 PROCEDURES

4.3. An information security incident is an unauthorized attempted or successful:

4.3.1. access, use, disclosure, modification, or destruction where electronic information is potentially at risk (examples include, but are not limited to: unauthorized access, theft of a physical asset that contains information such as a database or mailing list, or the unauthorized transmission or disclosure of electronic information)

OR

4.3.2. interference with systems where patient care or SJHS/CHS business operations are negatively impacted, but electronic information is not



INFORMATION SECURITY INCIDENT RESPONSE AND REPORTING POLICY

potentially at risk (examples, include, but are not limited to: computer virus outbreaks).

- 4.4. While the following outlines the sequence of escalating a security incident, timely reporting is of the essence. If one or more of the parties in the described sequence is not available, all parties involved in the process should escalate security incidents as required.
- 4.5. Users should report security incidents to the SJHS/CHS IT Help Desk and receive a ticket number for tracking. Users should then report the security incident and the tracking number to their supervisor.
- 4.6. The supervisor should then determine if the security incident leaves information at risk.
- 4.5 If the security incident does not leave electronic information at risk, the supervisor should report the security incident and the tracking number to their Local IT Manager.
 - 4.5.1 The Local IT Manager should then contact individuals appropriate to respond to the security incident with details of the security incident and the tracking number.
- 4.6 If the security incident leaves electronic information at risk, the supervisor should report the security incident and the tracking number to their Local HIPAA Coordinator.
 - 4.6.1 The Local HIPAA Coordinator should then report the security incident and the tracking number to their Local IT Manager, and follow up with local HR, Legal, Compliance, and other departments as appropriate.
 - 4.6.2 The Local IT Manager should then contact individuals appropriate to respond to the security incident with details of the security incident and the tracking number



INFORMATION SECURITY INCIDENT RESPONSE AND REPORTING POLICY

- 4.6.3 As appropriate, the Local HIPAA Coordinator should report the security incident to SJHS/CHS System-Wide Privacy and Security officers

- 4.7 SJHS/CHS IT individuals appropriate for responding to the security incident should then coordinate and govern the appropriate actions to respond to, mitigate, and document security incidents via existing problem resolution methods.
 - 4.7.1 Communication regarding security incident response should continue between the local HIPAA Coordinator and SJHS/CHS IT individuals appropriate for responding to the security incident.

- 4.8 Following mitigation, SJHS/CHS IT individuals appropriate for responding to the security incident should then close the tracking ticket with the SJHS/CHS IT Help Desk and provide information regarding resolution to the SJHS/CHS IT Security Task Force

- 4.9 SJHS/CHS IT individuals appropriate for responding to the security incident should then coordinate and govern the root cause analysis activities and the composition and execution of after-action activities. The Local HIPAA Coordinator should then document and act/apply sanctions as appropriate; HR, Legal, Compliance, and other departments should also document and act/apply sanctions as appropriate. Information regarding any after-action activities should be provided to the SJHS/CHS IT Security Task Force.

5.0 REFERENCES

HIPAA Regulations; 45 CFR 164.308(a)(6)(i) and (ii), "HIPAA" - Health Insurance Reform: Security Standards (Security Incident Procedures – Response and Reporting)

SJHS/CHS HI324 Mitigation of Improper Uses and Disclosures Policy

SJHS/CHS HI413 Minimum Necessary to the Use and Disclosure of PHI Policy



INFORMATION SECURITY INCIDENT RESPONSE AND REPORTING POLICY

6.0 DEFINITIONS

Confidential Information	financial data, proprietary reports, human resources information, marketing and sales information, and other similar privileged “need to know” information
Help Desk	a central point through which problems or issues are reported and subsequently managed and co-ordinated
Information Technology	any computer, telephone, messaging system (i.e. voicemail or e-mail), electronic media, application, protocol, or other equipment utilized on a public or private internetwork)
Protected Health Information (PHI)	individually identifiable information relating to the past, present, or future physical or mental health or condition of an individual or can be used to identify an individual
Root-Cause Analysis	gathering and ordering data in a centralized location, identifying causes that have generated or permitted the reporting of an issue, and analyzing reasonable and appropriate prevention options with the intent to implement
SJHS/CHS IT	Members of the SJHS/CHS Information Technology staff, other SJHS/CHS employees performing IT-specific tasks, Perot Systems associates performing IT services on behalf of SJHS/CHS, and



ST. JOSEPH HEALTH SYSTEM

DIVISION: (HR, Finance, etc.) IS
LAST DATE REVISION: 02/23/2005
LAST DATE REVIEWED: 02/23/2005
ORIGINAL DATE ADOPTED: 09/08/2003
PAGE NUMBER: 19 of 71
POLICY/PROCEDURE: IS404
APPROVED BY: Security Task Force
CHS REVIEW DATE: 01/18/2006.
4/12/2007
REVIEWED BY: CHS Compliance
Committee

INFORMATION SECURITY INCIDENT RESPONSE AND REPORTING POLICY

	other contractors of SJHS/CHS performing IT-specific tasks
Users	members of the SJHS/CHS workforce including its employees, volunteers, and trainees. Independent Contractors and vendors are considered Business Associates of an SJHS/CHS entity, and thus not members of its workforce.



ST. JOSEPH HEALTH SYSTEM

DIVISION: (HR, Finance, etc.) IS
LAST DATE REVISED: 01/12/2005
LAST DATE REVIEWED: 01/12/2005
ORIGINAL DATE ADOPTED: 09/08/2003
PAGE NUMBER: 20 of 71
POLICY/PROCEDURE: IS405
APPROVED BY: Security Task Force
CHS REVIEW DATE: 01/18/2006;
4/12/2007
REVIEWED BY: CHS Compliance
Committee

FACILITY SECURITY AND ACCESS CONTROL POLICY

1.0 PURPOSE

Information Technology is intended to improve access to information, enhance efficiency, and facilitate communication. The purpose of this policy is to define the physical security and access controls for information technology resources utilized in support of SJHS/CHS.

2.0 SCOPE

This policy applies to all Users, and the information covered in this policy includes Protected Health Information (or PHI) and confidential information.

3.0 POLICY

It is SJHS/CHS policy to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

SJHS/CHS employees whose responsibilities include facility security and access control shall ensure a) that the facility and the information technology therein is safeguarded from unauthorized physical access, tampering, and theft, b) that authorized physical access to the facility and the information technology therein is based on a user's role or function, c) that the physical movements of information technology are documented, d) that the physical access to software programs for testing and revision is controlled, and e) that proper visitor validation and control practices for physical access are implemented.

Performance of these activities should be consistent with pertinent policies and procedures.

4.0 PROCEDURE

- 4.7.** Each SJHS/CHS entity shall create and maintain a Facility Security Plan that outlines and documents the procedures and implementations used to safeguard the facilities, systems, and equipment from unauthorized physical access, tampering, or theft.



FACILITY SECURITY AND ACCESS CONTROL POLICY

- 4.8.** Each SJHS/CHS entity shall implement a method of authenticating a workforce member's physical access to facilities and facility areas. An example of this would be through the wearing of a photo identification badge.
- 4.9.** Each SJHS/CHS entity should implement a method of authorizing a workforce member's physical access to facilities and facility areas based on role or function. An example of this would be through color-coded photo identification badges, badges that grant electronic access, or keys and keycodes that control access.
- 4.10.** Each SJHS/CHS entity should implement a method of authorizing and authenticating a non-workforce member's physical access to facilities and facility areas. An example of this would be through the wearing of temporary identification badges after the non-workforce member's identity and purpose have been verified by a workforce member with appropriate authority, or by escorting the non-workforce member during their visit.
- 4.10.1.** Non-workforce members are vendors, repair personnel, or other individuals who require access to electronic PHI on behalf of SJHS/CHS IT.
- 4.11.** Each SJHS/CHS entity should identify a method of authorizing and authenticating visitor physical access to facilities and facility areas. An example of this would be through the wearing of temporary identification badges after the visitor's identity and purpose have been verified, or by escorting the visitor during their visit.
- 4.11.1.** Visitors are individuals who do not require access to information technology that accesses electronic PHI.
- 4.12.** Each SJHS/CHS entity should implement a method of recordkeeping that keeps track of the receipt, movement, and removal of hardware and electronic media, along with the individuals that perform related activities.

5.0 REFERENCES

45 CFR 164.310(a)(1), "HIPAA" - Health Insurance Reform: Security Standards (Facility Access Controls)



DIVISION: (HR, Finance, etc.) IS
LAST DATE REVISED: 01/12/2005
LAST DATE REVIEWED: 01/12/2005
ORIGINAL DATE ADOPTED: 09/08/2003
PAGE NUMBER: 22 of 71
POLICY/PROCEDURE: IS405
APPROVED BY: Security Task Force
CHS REVIEW DATE: 01/18/2006;
 4/12/2007
REVIEWED BY: CHS Compliance Committee

FACILITY SECURITY AND ACCESS CONTROL POLICY

45 CFR 164.310(a)(2)(ii), "HIPAA" - Health Insurance Reform: Security Standards (Facility Security Plan)

45 CFR 164.310(a)(2)(iii), "HIPAA" - Health Insurance Reform: Security Standards (Access Control and Validation Procedures)

45 CFR 164.310(d)(1), "HIPAA" - Health Insurance Reform: Security Standards (Device and Media Controls)

45 CFR 164.310(d)(2)(iii), "HIPAA" - Health Insurance Reform: Security Standards (Device and Media Controls - Accountability)

SJHS/CHS Policy IS402 Media Re-Use and Disposal

6.0 DEFINITIONS

Confidential Information	financial data, proprietary reports, human resources information, marketing and sales information, and other similar privileged "need to know" information
Information Technology	any computer, telephone, messaging system (i.e. voicemail or e-mail), electronic media, application, protocol, or other equipment utilized on a public or private internetwork)
Protected Health Information (PHI)	individually identifiable information relating to the past, present, or future physical or mental health or condition of an individual or can be used to identify an individual
SJHS/CHS IT	Members of the SJHS/CHS Information Technology staff, other SJHS/CHS employees performing IT-specific tasks, Perot Systems associates performing IT services on behalf of SJHS/CHS, and



ST. JOSEPH HEALTH SYSTEM

DIVISION: (HR, Finance, etc.) IS
LAST DATE REVISED: 01/12/2005
LAST DATE REVIEWED: 01/12/2005
ORIGINAL DATE ADOPTED: 09/08/2003
PAGE NUMBER: 23 of 71
POLICY/PROCEDURE: IS405
APPROVED BY: Security Task Force
CHS REVIEW DATE: 01/18/2006;
4/12/2007
REVIEWED BY: CHS Compliance
Committee

FACILITY SECURITY AND ACCESS CONTROL POLICY

	other contractors of SJHS/CHS performing IT-specific tasks
Users	members of the SJHS/CHS workforce including its employees, volunteers, and trainees. Independent Contractors and vendors are considered Business Associates of an SJHS/CHS entity, and thus not members of its workforce.



DATA BACKUP POLICY

1.0 PURPOSE

Information Technology is intended to improve access to information, enhance efficiency, and facilitate communication. The purpose of this policy is to define the backup of information technology resources utilized in support of SJHS/CHS.

2.0 SCOPE

This policy applies to all Users, and the information covered in this policy includes Protected Health Information (or PHI) and confidential information.

3.0 POLICY

It is SJHS/CHS policy to create and maintain retrievable exact copies of electronic PHI, confidential information, and other enterprise system data.

SJHS/CHS employees whose responsibilities include the copying of electronic PHI, confidential information, and other enterprise system data shall ensure a) that copies are exact, b) that copies are retrievable, c) that copies are periodically tested, and d) that copies are made, when needed, before the physical movement of equipment.

Performance of these activities should be consistent with pertinent policies and procedures.

4.0 PROCEDURES

4.1. Each site should ensure that all information related to their business on SJHS/CHS' servers is backed up in a manner consistent with corporate guidelines. Each site should work with SJHS/CHS IT Operations team onsite to ensure that all information is backed up and available to be restored in the case of an emergency.

4.1.1. Site-specific applications should follow processes in accordance with disaster recovery and business continuity planning.

4.2. Each site should have documented backup and recovery procedures.

4.3. Information systems data or functions are considered non-essential if the unavailability of that information poses no disruption or minimal disruption of



DATA BACKUP POLICY

service to users. Information classified as non-essential should be backed-up periodically, as determined jointly by the Information Owner and the SJHS/CHS IT Operations team, and periodically moved to a secure location.

- 4.4. Information systems data or functions are classified as essential if the unavailability of the information would completely interrupt the business from functioning (i.e., the process cannot be performed manually) and impact would be highly adverse. Information classified as essential must be backed-up daily and stored in a suitable location. Decisions should be made between the Information Owner and the SJHS/CHS IT Operations Team as to whether incremental backups must occur between daily backups.
- 4.5. Users should backup critical files by transferring or duplicating files onto the local area network, which is backed up on a scheduled basis. User data on SJHS/CHS' PCs consists of information systems data that is owned by the User (e.g., files created in Microsoft Office). This type of information, when unavailable, should not pose a disruption of service to users. Non-business files or applications should not be backed up to network servers.
- 4.6. The SJHS/CHS IT Operations Team should ensure that quarterly restorations of tape backups are performed. The purpose of the quarterly restoration will be to test the capability of restoring tape backups. Only members of the SJHS/CHS IT Operations Team are authorized to recall backups and restores based on requests from authorized Information Owners. Restoration testing should be performed with live production backup data on the test systems in the test environment only.
- 4.7. If backups are performed at the server or host level, the backup schedule of the most critical application determines the backup frequency of the server.
- 4.8. Electronic messages, like all other network information, should be periodically backed-up and retained by automated devices.

5.0 REFERENCES

45 CFR 164.308(a)(7)(ii)(A), "HIPAA" - Health Insurance Reform: Security Standards (Data Backup Plan)



DATA BACKUP POLICY

45 CFR 164.310(d)(2)(iv), "HIPAA" - Health Insurance Reform: Security Standards (Data Backup and Storage)

6.0 DEFINITIONS

Confidential Information	financial data, proprietary reports, human resources information, marketing and sales information, and other similar privileged "need to know" information
Information Technology	any computer, telephone, messaging system (i.e. voicemail or e-mail), electronic media, application, protocol, or other equipment utilized on a public or private internetwork)
Protected Health Information (PHI)	individually identifiable information relating to the past, present, or future physical or mental health or condition of an individual or can be used to identify an individual
SJHS/CHS IT	Members of the SJHS/CHS Information Technology staff, other SJHS/CHS employees performing IT-specific tasks, Perot Systems associates performing IT services on behalf of SJHS/CHS, and other contractors of SJHS/CHS performing IT-specific tasks
Users	members of the SJHS/CHS workforce including its employees, volunteers, and trainees. Independent Contractors and vendors are considered Business Associates of an SJHS/CHS entity, and thus not members of its workforce.



INFORMATION SYSTEM ACTIVITY REVIEW POLICY

1.0 PURPOSE

Information Technology is intended to improve access to information, enhance efficiency, and facilitate communication. The purpose of this policy is to define the activity review for information technology resources utilized in support of SJHS/CHS.

2.0 SCOPE

This policy applies to all Users, and the information covered in this policy includes Protected Health Information (or PHI) and confidential information.

3.0 POLICY

It is SJHS/CHS policy to periodically review the activity of its information technology systems activity.

SJHS/CHS employees whose responsibilities include information technology activity review shall ensure that a) records of information system activity such as audit logs, access reports, and security incident tracking reports are regularly reviewed and b) corrective activities are executed.

Performance of these activities should be consistent with pertinent policies and procedures.

4.0 PROCEDURE

4.1. An individual or group should be responsible to monitor applicable records of information system activity to ensure that inappropriate behavior or potential intrusions are recognized and addressed. This monitoring includes the regular review of automated functions (such as log files or reports) as well as manual procedural functions (such as the granting of access through signoff of a form or through e-mail acknowledgement).

4.1.1. Due to the large volume of information generated to log files, manual review of these types of files is not recommended. Instead, exception reports should be generated and automatically sent to the appropriate administrative personnel.

4.1.2. Centralized monitoring is preferred over individual system monitoring.



INFORMATION SYSTEM ACTIVITY REVIEW POLICY

- 4.2.** Individuals monitoring SJHS/CHS records of information system activity should watch for the following types of activities, including but not limited to:
- 4.2.1.** Deviations from normal usage, multiple failed password change attempts, and multiple failed login attempts with a valid User ID (also known as “account user security events”).
 - 4.2.2.** Unauthorized additions and changes to the privileges of users, and the unauthorized creation, modification, and deletion of User Id’s (also known as “account administrator security events”).
 - 4.2.3.** Changes to file security levels and changes to critical application system files (also known as “file access events”).
 - 4.2.4.** Wireless access point activity, firewall activity, and remote access activity (also known as “boundary traversal events”).
 - 4.2.5.** Anti-virus system logs and intrusion detection/prevention device activity (also known as “network integrity events”).
- 4.3.** All records of applicable information system activity should be configured to record activity specific to the network, server, application, or database being monitored. Records should be created in such a manner that individual events are attributed to individuals whenever possible. Records of computer security events should provide data to:
- 4.3.1.** Meet regulatory and contractual requirements.
 - 4.3.2.** Indicate when an improper act or event has occurred, allowing the discovery of such acts or events in the review process.
 - 4.3.3.** Provide data to support the investigation of Computer Security Incidents.
 - 4.3.4.** Provide data to support comprehensive audits of the effectiveness of (and compliance with) SJHS/CHS Policies and Procedures.
- 4.4.** Security tools and software should be periodically reviewed and recommendations made by SJHS/CHS IT and the Security Officer for upgrades.

INFORMATION SYSTEM ACTIVITY REVIEW POLICY

4.5. Events that reveal a known, suspected, or reasonably anticipated security incident shall be reported in accordance with pertinent policies. Examples of these events include, but are not limited to: computer virus outbreaks, unauthorized access, theft of a physical asset that contains information such as a database or mailing list, or the unauthorized transmission or disclosure of electronic information.

4.5.1 Detail regarding the definition and reporting requirements of a possible security incident are located in SJHS/CHS Policy IS404, Security Incident Response and Reporting Policy.

4.6. Access to security logs should be allowed only for authorized persons. Logs should be retained on read-only media if possible.

4.7. Physical Inspection

4.7.1. This right to audit may involve inspection of physical documentation (such as an individual’s file folder) as well as electronic documentation (such as e-mail) in the investigation of an incident or anomaly in log reports.

5.0 REFERENCES

45 CFR 164.308(a)(1)(ii)(d), “HIPAA” - Health Insurance Reform: Security Standards (Information System Activity Review)

SJHS/CHS Policy IS410 Audit Controls Policy

SJHS/CHS Policy IS404 Security Incident Response and Reporting Policy

6.0 DEFINITIONS

Confidential Information	financial data, proprietary reports, human resources information, marketing and sales information, and other similar privileged “need to know” information
Information Technology	any computer, telephone, messaging



ST. JOSEPH HEALTH SYSTEM

DIVISION: (HR, Finance, etc.) IS
LAST DATE REVISION: 01/21/2005
LAST DATE REVIEWED: 01/21/2005
ORIGINAL DATE ADOPTED: 01/21/2005
PAGE NUMBER: 30 of 71
POLICY/PROCEDURE: IS407
APPROVED BY: Security Task Force
CHS REVIEW DATE: 01/18/2006;
4/12/2007
REVIEWED BY: CHS Compliance
Committee

INFORMATION SYSTEM ACTIVITY REVIEW POLICY

	system (i.e. voicemail or e-mail), electronic media, application, protocol, or other equipment utilized on a public or private internetwork)
Protected Health Information (PHI)	individually identifiable information relating to the past, present, or future physical or mental health or condition of an individual or can be used to identify an individual
SJHS/CHS IT	Members of the SJHS/CHS Information Technology staff, other SJHS/CHS employees performing IT-specific tasks, Perot Systems associates performing IT services on behalf of SJHS/CHS, and other contractors of SJHS/CHS performing IT-specific tasks
Users	members of the SJHS/CHS workforce including its employees, volunteers, and trainees. Independent Contractors and vendors are considered Business Associates of an SJHS/CHS entity, and thus not members of its workforce.



IDENTITY MANAGEMENT AND WORKFORCE SECURITY POLICY

1.0 PURPOSE

Information Technology is intended to improve access to information, enhance efficiency, and facilitate communication. The purpose of this policy is to define the methods for ensuring workforce security and access management to information technology resources utilized in support of SJHS/CHS.

2.0 SCOPE

This policy applies to all Users, and the information covered in this policy includes Protected Health Information (or PHI) and confidential information.

3.0 POLICY

It is SJHS/CHS policy to ensure that all members of its workforce have appropriate access to electronic protected health information, and to prevent those workforce members who do not have access from obtaining access to electronic PHI.

Performance of these activities should be consistent with pertinent policies and procedures.

4.0 PROCEDURE

- 4.13.** Categories of electronic PHI shall be used based on the principles of role-based access and minimum necessary.
- 4.14.** Methods of workforce clearance should be used to determine that the potential access of a workforce member to electronic PHI is appropriate. An example of this is the Human Resources department verifying that the individual should have access.
- 4.15.** Methods of access authorization and/or supervision should be used to associate a workforce member to a category or categories of electronic PHI. An example of this is a manager authorizing and/or supervising an individual to participate in a role (nurse, billing clerk, etc.)
- 4.16.** Methods of access establishment should be used to request the granting or changing of access to electronic PHI. An example of this is a manager submitting a request to the Help Desk to create a computer account.



IDENTITY MANAGEMENT AND WORKFORCE SECURITY POLICY

- 4.17. Methods should be used to establish or change access to electronic PHI. An example of this is the help desk verifying that a manager's request for a computer account is genuine prior to execution.
- 4.18. Methods of establishing unique names and/or numbers for identifying and tracking user identity should be used. An example of this is the assignment of unique user ID's.
- 4.19. Methods of communicating login information back to the user should be used. An example of this is an e-mail with initial user ID and password information sent back to the manager or trainer for the purposes of training and orienting the user.
 - 6.1.1. In order to properly track user activity, any initial logon information should be changed by the user once the initial logon information is verified by the user.
- 4.20. Methods to verify that a person or entity seeking access to electronic PHI is the one claimed should be used. An example of this is the requirement for a user to enter their user logon ID and password to gain access.
- 4.21. Methods of workforce management should be used to maintain the appropriate access to electronic PHI. An example of this is the periodic review by managers of their department's computer access lists and computing needs.
- 4.22. Methods for terminating access to electronic PHI should be used when the employment of a workforce member ends or as appropriate. An example of this is a manager submitting a request to the Help Desk to delete an account.
- 4.23. Methods should be used to revoke access to electronic PHI. An example of this is the help desk verifying that a manager's request for disabling a computer account is genuine prior to execution.

5.0 REFERENCES



DIVISION: (HR, Finance, etc.) IS
LAST DATE REVISION: 01/21/2005
LAST DATE REVIEWED: 01/21/2005
ORIGINAL DATE ADOPTED: 01/21/2005
PAGE NUMBER: 33 of 71
POLICY/PROCEDURE: IS409
APPROVED BY: Security Task Force
CHS REVIEW DATE: 01/18/2006;
4/12/2007
REVIEWED BY: CHS Compliance
Committee

IDENTITY MANAGEMENT AND WORKFORCE SECURITY POLICY

45 CFR 164.308(a)(3)(i), "HIPAA" - Health Insurance Reform: Security Standards (Workforce Security)

45 CFR 164.308(a)(3)(ii)(A), "HIPAA" - Health Insurance Reform: Security Standards (Workforce Security – Authorization and/or Supervision)

45 CFR 164.308(a)(3)(ii)(B), "HIPAA" - Health Insurance Reform: Security Standards (Workforce Security – Workforce Clearance)

45 CFR 164.308(a)(3)(ii)(C), "HIPAA" - Health Insurance Reform: Security Standards (Workforce Security – Termination Procedures)

45 CFR 164.308(a)(4)(i), "HIPAA" - Health Insurance Reform: Security Standards (Information Access Management)

45 CFR 164.308(a)(4)(ii)(B), "HIPAA" - Health Insurance Reform: Security Standards (Information Access Management – Access Authorization)

45 CFR 164.308(a)(4)(ii)(C), "HIPAA" - Health Insurance Reform: Security Standards (Information Access Management – Access Establishment and Modification)

45 CFR 164.312(a)(1), "HIPAA" - Health Insurance Reform: Security Standards (Access Control)

45 CFR 164.312(a)(2)(i), "HIPAA" - Health Insurance Reform: Security Standards (Access Control - Unique User Identification)

45 CFR 164.312(d), "HIPAA" - Health Insurance Reform: Security Standards (Person or Entity Authentication)

SJHS/CHS Policy HI413 Minimum Necessary Standard Regarding the Use and Disclosure of Protected Health Information

SJHS/CHS Policy HI454 Role-Based Access Review

SJHS/CHS Policy HI516 Sanction/Disciplinary Process



IDENTITY MANAGEMENT AND WORKFORCE SECURITY POLICY

6.0 DEFINITIONS

Confidential Information	financial data, proprietary reports, human resources information, marketing and sales information, and other similar privileged “need to know” information
Information Technology	any computer, telephone, messaging system (i.e. voicemail or e-mail), electronic media, application, protocol, or other equipment utilized on a public or private internetwork)
Protected Health Information (PHI)	individually identifiable information relating to the past, present, or future physical or mental health or condition of an individual or can be used to identify an individual
Role-Based Access	A type of access which fulfills the principle of least privilege, where a User is given no more privileges that reasonably necessary to fulfill a role. Ensuring least privilege requires defining a category or categories of information required to fulfill the role, determining the reasonable and appropriate minimum set of privileges required to access the electronic PHI commensurate to the defined role, and implementing reasonable and appropriate methods to restrict the user to the defined category or categories of information.
SJHS/CHS IT	Members of the SJHS/CHS Information Technology staff, other SJHS/CHS employees performing IT-specific tasks, Perot Systems associates performing IT services on behalf of SJHS/CHS, and other contractors of SJHS/CHS performing IT-specific tasks



ST. JOSEPH HEALTH SYSTEM

DIVISION: (HR, Finance, etc.) IS
LAST DATE REVISION: 01/21/2005
LAST DATE REVIEWED: 01/21/2005
ORIGINAL DATE ADOPTED: 01/21/2005
PAGE NUMBER: 35 of 71
POLICY/PROCEDURE: IS409
APPROVED BY: Security Task Force
CHS REVIEW DATE: 01/18/2006;
4/12/2007
REVIEWED BY: CHS Compliance
Committee

IDENTITY MANAGEMENT AND WORKFORCE SECURITY POLICY

Users	members of the SJHS/CHS workforce including its employees, volunteers, and trainees. Independent Contractors and vendors are considered Business Associates of an SJHS/CHS entity, and thus not members of its workforce.
-------	---



AUDIT CONTROLS POLICY

1.0 PURPOSE

Information Technology is intended to improve access to information, enhance efficiency, and facilitate communication. The purpose of this policy is to define the audit controls to be employed for information technology resources utilized in support of SJHS/CHS.

2.0 SCOPE

This policy applies to all Users, and the information covered in this policy includes Protected Health Information (or PHI) and confidential information.

3.0 POLICY

It is SJHS/CHS policy to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic PHI.

Performance of these activities should be consistent with pertinent policies and procedures.

4.0 PROCEDURE

4.24. Hardware, software, and/or procedures should be implemented for the purposes of recording activity in information systems that contain or use electronic PHI. The types of activity that should be recorded and examined should include, but not be limited to:

4.24.1. Deviations from normal usage, multiple failed password change attempts, and multiple failed login attempts with a valid User ID (also known as “account user security events”)

4.24.2. Unauthorized additions and changes to the privileges of users, unauthorized creation, deletion, and modification of User IDs (also known as “account administrator security events”)

4.24.3. Changes to file security levels and changes to critical application system files (also known as “file access events”)

AUDIT CONTROLS POLICY

4.24.4. Wireless access point activity, firewall activity, and remote access activity (also known as “boundary traversal events”)

4.24.5. Anti-virus system logs and intrusion detection/prevention device activity (also known as “network integrity events”)

4.25. The information collected should be examined in accordance with the Information System Activity Review Policy and should support evaluation requirements defined in the Security Management process.

5.0 REFERENCES

45 CFR 164.312(b), “HIPAA” - Health Insurance Reform: Security Standards (Audit Controls)

SJHS/CHS Policy IS407 Information System Activity Review

6.0 DEFINITIONS

Confidential Information	financial data, proprietary reports, human resources information, marketing and sales information, and other similar privileged “need to know” information
Information Technology	any computer, telephone, messaging system (i.e. voicemail or e-mail), electronic media, application, protocol, or other equipment utilized on a public or private internetwork)
Protected Health Information (PHI)	individually identifiable information relating to the past, present, or future physical or mental health or condition of an individual or can be used to identify an individual
SJHS/CHS IT	Members of the SJHS/CHS Information



ST. JOSEPH HEALTH SYSTEM

DIVISION: (HR, Finance, etc.) IS
LAST DATE REVISED: 01/12/2005
LAST DATE REVIEWED: 01/12/2005
ORIGINAL DATE ADOPTED: 01/12/2005
PAGE NUMBER: 38 of 71
POLICY/PROCEDURE: IS410
APPROVED BY: Security Task Force
CHS REVIEW DATE: 01/18/2006,
4/12/2007
REVIEWED BY: CHS Compliance
Committee

AUDIT CONTROLS POLICY

	Technology staff, other SJHS/CHS employees performing IT-specific tasks, Perot Systems associates performing IT services on behalf of SJHS/CHS, and other contractors of SJHS/CHS performing IT-specific tasks
Users	members of the SJHS/CHS workforce including its employees, volunteers, and trainees. Independent Contractors and vendors are considered Business Associates of an SJHS/CHS entity, and thus not members of its workforce.

PASSWORD MANAGEMENT

7.0 PURPOSE

Information Technology is intended to improve access to information, enhance efficiency, and facilitate communication. The purpose of this policy is to define the procedures creating, changing, and safeguarding passwords.

8.0 SCOPE

This policy applies to all Users, and the information covered in this policy includes Protected Health Information (or PHI) and confidential information.

9.0 POLICY

It is SJHS/CHS policy to use and manage passwords, as well as educate users on password usage, as part of the methodology that verifies that a person or entity seeking access to electronic protected health information is the one claimed.

SJHS/CHS users are to be provided with a separate “account” or “accounts” based on their responsibilities so that access is limited to only those programs and data necessary in performing the user’s job tasks. Users should be responsible for safeguarding the user ID and password that secures their access.

Performance of these activities should be consistent with pertinent policies and procedures

10.0PROCEDURE

Password Construction

10.1. The following standards for passwords should be supported and enforced on all SJHS/CHS systems wherever technologically possible:

- Passwords should not be the same as the userID or user's name.
- Passwords should be at least 6 characters, with no maximum.
- Passwords can contain any alphanumeric character, with the exception of special characters, and should contain at least one numeric.
- Passwords should not allow letters repeated in succession.
- Passwords should be case sensitive.
- Ten (10) generations of passwords should be retained to limit reuse.
- Passwords should expire every 90 days.
- Logon ids should be suspended with 3 incorrect attempts of the password.



PASSWORD MANAGEMENT

- Passwords should have a minimum life of 1 day (24 hours) before the system allows the user to initiate a password change.
- User IDs not used for 90 days should be suspended, requiring the user contact a system / security administrator to re-activate the ID.
- User IDs not used for 180 days should be deleted from the system.
- On those systems that support a list of restricted passwords that may not be used, establish a list of restricted passwords.

Human Factors

10.2. When choosing a new password, a good standard rule is that the password should have three characteristics: it should be easy to remember, difficult to guess, and not need to be written. The length as well as the composition of a password are equally important in protecting a password from compromise, and therefore should conform to the following guidelines:

- Passwords should not be based on any information easily obtained about you. This includes your name, family names, license plate numbers, telephone numbers, social security numbers, vehicle brand, street address, favorite sports teams, etc.
- Passwords should not consist of a recognizable work or name, a userID or a user's real name.
- Passwords should not consist of a typical word from a dictionary. Most basic password cracking programs contain over 80,000 words and several variations.
- Users should try to have a password with a number of mixed case letters. Simple substitutions like a '1' for an 'l' and '0' for an 'O' are easily guessed. Add a '%' or a '\$' to the middle of a password.

Password Administration

- 10.3.** Users should not share his/her account with family, friends or make their password available to any other person.
- 10.4.** If your computer system does not automatically require password changes, it is recommended you manually change your password at least every 90 days.
- 10.5.** Users should not attempt to find or use the password of any other person.
- 10.6.** Passwords should be memorized – never written down and/or posted near the user's workstation.

PASSWORD MANAGEMENT

- 10.7.** In the event that an account requires a new password, Help Desk personnel should first verify the identity of the user requesting the password, verify the request with the manager of the user, then notify the user directly.
- 10.8.** In the event that the account requires resetting without changing the password, the reset should only be executed after verification of the user's identity and verifying the request with the manager of the user.
- 10.9.** Events that reveal a known, suspected, or reasonably anticipated security incident should be reported in accordance with pertinent policies. Examples of these events include, but are not limited to: computer virus outbreaks, unauthorized access, theft of a physical asset that contains information such as a database or mailing list, or the unauthorized transmission or disclosure of electronic information.
 - 4.5.1** Detail regarding the definition and reporting requirements of a possible security incident are located in SJHS/CHS Policy IS404, Security Incident Response and Reporting Policy.

11.0 REFERENCES

45 CFR 164.308(a)(5)(ii)(D): "HIPAA" – Health Insurance Reform: Security Standards (Password Management)

SJHS/CHS Policy IS404 Security Incident Response and Reporting Policy

12.0 DEFINITIONS

Confidential Information	financial data, proprietary reports, human resources information, marketing and sales information, and other similar privileged "need to know" information
Information Technology	any computer, telephone, messaging system (i.e. voicemail or e-mail), electronic media, application, protocol, or other equipment utilized on a public or private internetwork)
Password	confidential authentication information composed of a string of characters



ST. JOSEPH HEALTH SYSTEM

DIVISION: (HR, Finance, etc.) IS
LAST DATE REVISED: 04/14/2005
LAST DATE REVIEWED: 02/23/2005
ORIGINAL DATE ADOPTED: 02/23/2005
PAGE NUMBER: 42 of 71
POLICY/PROCEDURE: IS411
APPROVED BY: Security Task Force
CHS REVIEW DATE: 01/18/2006,
4/12/2007
REVIEWED BY: CHS Compliance
Committee

PASSWORD MANAGEMENT

Protected Health Information (PHI)	individually identifiable information relating to the past, present, or future physical or mental health or condition of an individual or can be used to identify an individual
SJHS/CHS IT	Members of the SJHS/CHS Information Technology staff, other SJHS/CHS employees performing IT-specific tasks, Perot Systems associates performing IT services on behalf of SJHS/CHS, and other contractors of SJHS/CHS performing IT-specific tasks
Users	members of the SJHS/CHS workforce including its employees, volunteers, and trainees. Independent Contractors and vendors are considered Business Associates of an SJHS/CHS entity, and thus not members of its workforce.
Workstation	an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment



PROTECTION FROM MALICIOUS SOFTWARE

13.0PURPOSE

Information Technology is intended to improve access to information, enhance efficiency, and facilitate communication. The purpose of this policy is to define the procedures for guarding against, detecting, and reporting malicious software.

14.0SCOPE

This policy applies to all Users, and the information covered in this policy includes Protected Health Information (or PHI) and confidential information.

15.0POLICY

It is SJHS/CHS policy to guard against, detect, and report malicious software use, as well as educate users on this process as part of the methodology.

SJHS/CHS users are responsible for exercising good judgment and SJHS/CHS IT personnel are responsible for implementing reasonable precautions to ensure that malicious software are not introduced into the SJHS/CHS network.

Performance of these activities should be consistent with pertinent policies and procedures.

16.0PROCEDURE

Note: For the purposes of this procedure, terms such as “virus” and “anti-virus” should be used to explain the processes for safeguarding against malicious software.

16.1. SJHS/CHS supplied anti-virus software should be enabled on all computers and updated with the latest validated anti-virus data files. It is the responsibility of the end user to ensure this process is running on their assigned laptop(s) or desktop(s).

4.1.1 If the user has any reason to believe the process is not running properly, he/she should contact the Help Desk immediately.

16.2. If a user believes that they have a virus, he/she should contact the Help Desk immediately.



PROTECTION FROM MALICIOUS SOFTWARE

4.2.1 Virus outbreaks or attacks should be reported to the Help Desk in accordance with the SJHS/CHS Incident Response Policy.

16.3. Anti-virus software should be installed on all information systems as part of the start-up process and remain resident throughout the computing session.

16.3.1. For desktop and laptop computers, all files resident on the system should be scanned during operation.

16.3.2. For server computers, if required, certain files may be excluded based on the recommendations of the application manufacturer and confirmed via test results from SJHS/CHS IT.

16.4. E-mail content, e-mail attachments, Internet content, shared network files, content on external storage media (e.g. portable drives), and any other content that does not reside on the desktop, laptop, or server computer should be scanned before use.

16.5. Periodic full scans of desktops, laptops, and server computers should be conducted.

16.6. If it is determined that anti-virus software cannot be used, SJHS/CHS IT is responsible for documenting the reason and developing a strategy to implement an alternative and/or a strategy to migrate to configurations that can support anti-virus software.

16.7. Intentional possession or development of viruses without the consent and control of SJHS/CHS IT is prohibited. Non-compliance with this IS Policy can result in disciplinary action up to and including legal action and termination.

17.0 REFERENCES

45 CFR 164.308(a)(5)(ii)(B): "HIPAA" – Health Insurance Reform: Security Standards (Protection from Malicious Software)

SJHS/CHS IS404 Security Incident Response and Reporting Policy

18.0 DEFINITIONS

Confidential Information	financial data, proprietary reports, human resources information, marketing and sales information, and other similar privileged "need to know" information
--------------------------	--



ST. JOSEPH HEALTH SYSTEM

DIVISION: (HR, Finance, etc.) IS
LAST DATE REVISED: 02/23/2005
LAST DATE REVIEWED: 02/23/2005
ORIGINAL DATE ADOPTED: 02/23/2005
PAGE NUMBER: 45 of 71
POLICY/PROCEDURE: IS412
APPROVED BY: Security Task Force
CHS REVIEW DATE: 01/18/2006, 4/12/2007
REVIEWED BY: CHS Compliance Committee

PROTECTION FROM MALICIOUS SOFTWARE

Information Technology	any computer, telephone, messaging system (i.e. voicemail or e-mail), electronic media, application, protocol, or other equipment utilized on a public or private internetwork)
Malicious Software	software, for example, a virus, designed to damage or disrupt a system
Protected Health Information (PHI)	individually identifiable information relating to the past, present, or future physical or mental health or condition of an individual or can be used to identify an individual
SJHS/CHS IT	Members of the SJHS/CHS Information Technology staff, other SJHS/CHS employees performing IT-specific tasks, Perot Systems associates performing IT services on behalf of SJHS/CHS, and other contractors of SJHS/CHS performing IT-specific tasks
Users	members of the SJHS/CHS workforce including its employees, volunteers, and trainees. Independent Contractors and vendors are considered Business Associates of an SJHS/CHS entity, and thus not members of its workforce.

LOG-IN MONITORING

19.0PURPOSE

Information Technology is intended to improve access to information, enhance efficiency, and facilitate communication. The purpose of this policy is to define the procedures for monitoring log-in attempts and reporting discrepancies.

20.0SCOPE

This policy applies to all Users, and the information covered in this policy includes Protected Health Information (or PHI) and confidential information.

21.0POLICY

It is SJHS/CHS policy to monitor log-in attempts and report discrepancies, as well as educate users on this process as part of the methodology.

SJHS/CHS IT should ensure that monitoring tools are installed in order to log activity and security violations against critical data. Only authorized individuals with prior management approval will use network or screen monitoring software or hardware.

Performance of these activities should be consistent with pertinent policies and procedures

22.0PROCEDURE

- 22.1. Before being given the opportunity to log onto a computer, intended users should be presented with a login banner. This provides users a chance to terminate the login before accessing a system that they are not authorized to access.
- 22.2. Every login banner on SJHS/CHS' computers should include a special notice which includes:
 - 22.2.1. the system is to be used only by authorized users;
 - 22.2.2. by continuing to use the system, the user represents that he/she is an authorized user; and
 - 22.2.3. use of the system constitutes consent to monitoring
- 22.3. Identification of the SJHS/CHS network, location, or host should not appear prior to a successful login.



LOG-IN MONITORING

22.4. Systems should be configured to not give specific information on an unsuccessful login. For example, the identification of which portion of the login sequence (username or password) was incorrect.

22.5. User access activity or log-in records should be kept for those users that access information. Audit controls should be implemented, activities should be recorded, and records should be reviewed in accordance with pertinent policies, and these records should be maintained in accordance with documentation retention guidelines.

23.0 REFERENCES

45 CFR 164.308(a)(5)(ii)(C): "HIPAA" – Health Insurance Reform: Security Standards (Log-in Monitoring)

SJHS/CHS IS 407 Information Systems Activity Review Policy

SJHS/CHS IS410 Audit Controls Policy

24.0 DEFINITIONS

Confidential Information	financial data, proprietary reports, human resources information, marketing and sales information, and other similar privileged "need to know" information
Information Technology	any computer, telephone, messaging system (i.e. voicemail or e-mail), electronic media, application, protocol, or other equipment utilized on a public or private internetwork)
Protected Health Information (PHI)	individually identifiable information relating to the past, present, or future physical or mental health or condition of an individual or can be used to identify an individual
SJHS/CHS IT	Members of the SJHS/CHS Information



ST. JOSEPH HEALTH SYSTEM

DIVISION: (HR, Finance, etc.) IS
LAST DATE REVISION: 01/21/2005
LAST DATE REVIEWED: 01/21/2005
ORIGINAL DATE ADOPTED: 01/21/2005
PAGE NUMBER: 48 of 71
POLICY/PROCEDURE: IS413
APPROVED BY: Security Task Force
CHS REVIEW DATE: 01/18/2006.
4/12/2007
REVIEWED BY: CHS Compliance
Committee

LOG-IN MONITORING

	Technology staff, other SJHS/CHS employees performing IT-specific tasks, Perot Systems associates performing IT services on behalf of SJHS/CHS, and other contractors of SJHS/CHS performing IT-specific tasks
Users	members of the SJHS/CHS workforce including its employees, volunteers, and trainees. Independent Contractors and vendors are considered Business Associates of an SJHS/CHS entity, and thus not members of its workforce.



TRANSMISSION SECURITY POLICY

1.0 PURPOSE

Information Technology is intended to improve access to information, enhance efficiency, and facilitate communication. The purpose of this policy is to define the methods of ensuring transmission security and integrity for information technology resources utilized in support of SJHS/CHS.

2.0 SCOPE

This policy applies to all Users, and the information covered in this policy includes Protected Health Information (or PHI) and confidential information.

3.0 POLICY

It is SJHS/CHS policy to guard against unauthorized access to or modification of electronic PHI transmitted over an electronic communications network.

Performance of these activities should be consistent with pertinent policies and procedures.

4.0 PROCEDURE

- 4.26. Users should make reasonable efforts to verify the e-mail address, file transfer name (FTP address), or other appropriate identification of the receiving person or entity prior to the electronic transmission of PHI.
- 4.27. Users should make reasonable efforts to limit the electronic PHI transmitted to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.
- 4.28. All electronic transmissions of electronic PHI from the SJHS/CHS network that is intended to leave the SJHS/CHS network should utilize an encryption mechanism that encrypts the information before it leaves the SJHS/CHS network.
 - 4.28.1. Encryption mechanisms implemented to comply with this policy should support a minimum of, but not limited to, a 128-bit level of encryption.
- 4.29. Because SJHS/CHS employs administrative, physical, and technical safeguards within the SJHS/CHS network, electronic transmissions of

TRANSMISSION SECURITY POLICY

electronic PHI from the SJHS/CHS network that are intended to remain within the SJHS/CHS network should not require encryption as long as the requirements of entity validation, minimum necessary, and a reasonable expectation of delivery are met (as specified in 4.1 and 4.2 above).

- 4.29.1.** Wireless transmissions, by their nature of transmission, leave the SJHS/CHS network and are bound by the encryption requirements of 4.3 above.

5.0 REFERENCES

45 CFR 164.314(e)(1), "HIPAA" - Health Insurance Reform: Security Standards (Transmission Security)

45 CFR 164.314(e)(2)(i), "HIPAA" - Health Insurance Reform: Security Standards (Transmission Security – Integrity Controls)

45 CFR 164.314(e)(2)(ii), "HIPAA" - Health Insurance Reform: Security Standards (Transmission Security - Encryption)

SJHS/CHS Policy HI413 Minimum Necessary Standard

6.0 DEFINITIONS

Confidential Information	financial data, proprietary reports, human resources information, marketing and sales information, and other similar privileged "need to know" information
Information Technology	any computer, telephone, messaging system (i.e. voicemail or e-mail), electronic media, application, protocol, or other equipment utilized on a public or private internetwork)
Protected Health Information (PHI)	individually identifiable information relating to the past, present, or future physical or mental health or condition of an individual



DIVISION: (HR, Finance, etc.) IS
LAST DATE REVISED: 02/23/2005
LAST DATE REVIEWED: 02/23/2005
ORIGINAL DATE ADOPTED: 02/23/2005
PAGE NUMBER: 51 of 71
POLICY/PROCEDURE: IS414
APPROVED BY: Security Task Force
CHS REVIEW DATE: 01/18/2006,
 4/12/2007
REVIEWED BY: CHS Compliance
 Committee

TRANSMISSION SECURITY POLICY

	or can be used to identify an individual
Role-Based Access	A type of access which fulfills the principle of least privilege, where a User is given no more privileges that reasonably necessary to fulfill a role. Ensuring least privilege requires defining a category or categories of information required to fulfill the role, determining the reasonable and appropriate minimum set of privileges required to access the electronic PHI commensurate to the defined role, and implementing reasonable and appropriate methods to restrict the user to the defined category or categories of information.
SJHS/CHS IT	Members of the SJHS/CHS Information Technology staff, other SJHS/CHS employees performing IT-specific tasks, Perot Systems associates performing IT services on behalf of SJHS/CHS, and other contractors of SJHS/CHS performing IT-specific tasks
Users	members of the SJHS/CHS workforce including its employees, volunteers, and trainees. Independent Contractors and vendors are considered Business Associates of an SJHS/CHS entity, and thus not members of its workforce.



CONTINGENCY PLANNING POLICY

1.0 PURPOSE

Information Technology is intended to improve access to information, enhance efficiency, and facilitate communication. The purpose of this policy is to define the methods of contingency planning for information technology resources utilized in support of SJHS/CHS.

2.0 SCOPE

This policy applies to all Users, and the information covered in this policy includes Protected Health Information (or PHI) and confidential information.

3.0 POLICY

It is SJHS/CHS policy to respond to contingencies (emergencies or other occurrences), which affect systems that contain electronic PHI, confidential information, and other enterprise system data.

Performance of these activities should be consistent with pertinent policies and procedures.

4.0 PROCEDURE

- 4.30. Each SJHS/CHS entity should identify and assess the relative criticality of specific applications and data in support of contingency mode planning.
- 4.31. Each SJHS/CHS entity should implement policies and procedures for continuing critical business processes while in a contingency mode of operation, and provide for the adequate protection of the security of electronic PHI, confidential information, and other enterprise system data.
- 4.32. Each SJHS/CHS entity should implement policies and procedures that control electronic access to electronic PHI, confidential information, and other enterprise system data while in contingency mode.
- 4.33. Each SJHS/CHS entity should control facility access in support of the restoration of lost data while in contingency mode
- 4.34. Each SJHS/CHS entity should implement policies and procedures for restoring electronic PHI, confidential information, and other enterprise system data.



CONTINGENCY PLANNING POLICY

4.35. Each SJHS/CHS entity should periodically test the policies and procedures referenced above, and revise as necessary.

5.0 REFERENCES

45 CFR 164.308(a)(7)(i), "HIPAA" - Health Insurance Reform: Security Standards (Contingency Planning)

45 CFR 164.308(a)(7)(ii)(B), "HIPAA" - Health Insurance Reform: Security Standards (Contingency Planning – Disaster Recovery Plan)

45 CFR 164.308(a)(7)(ii)(C), "HIPAA" - Health Insurance Reform: Security Standards (Contingency Planning – Emergency Mode Operation Plan)

45 CFR 164.308(a)(7)(ii)(D), "HIPAA" - Health Insurance Reform: Security Standards (Contingency Planning – Testing and Revision Procedures)

45 CFR 164.308(a)(7)(ii)(E), "HIPAA" - Health Insurance Reform: Security Standards (Contingency Planning – Applications and Data Criticality Analysis)

45 CFR 164.310(a)(2)(i), "HIPAA" - Health Insurance Reform: Security Standards (Facility Access Controls – Contingency Operations)

45 CFR 164.314(e)(2)(i), "HIPAA" - Health Insurance Reform: Security Standards (Access Control – Emergency Access Procedure)

SJHS/CHS Policy IS405 Facility Security and Access Control Policy

SJHS/CHS Policy IS406 Data Backup Policy

SJHS/CHS Policy IS409 Identity Management and Workforce Security Policy

JCAHO IM Standard 2.30 (Continuity of Information)

6.0 DEFINITIONS

Confidential Information	financial data, proprietary reports, human resources information, marketing and
--------------------------	---



ST. JOSEPH HEALTH SYSTEM

DIVISION: (HR, Finance, etc.)	IS
LAST DATE REVISED:	02/23/2005
LAST DATE REVIEWED:	02/23/2005
ORIGINAL DATE ADOPTED:	02/23/2005
PAGE NUMBER:	54 of 71
POLICY/PROCEDURE:	IS415
APPROVED BY:	Security Task Force
CHS REVIEW DATE:	01/18/2006, 4/12/2007
REVIEWED BY:	CHS Compliance Committee

CONTINGENCY PLANNING POLICY

	sales information, and other similar privileged “need to know” information
Information Technology	any computer, telephone, messaging system (i.e. voicemail or e-mail), electronic media, application, protocol, or other equipment utilized on a public or private internetwork)
Protected Health Information (PHI)	individually identifiable information relating to the past, present, or future physical or mental health or condition of an individual or can be used to identify an individual
SJHS/CHS IT	Members of the SJHS/CHS Information Technology staff, other SJHS/CHS employees performing IT-specific tasks, Perot Systems associates performing IT services on behalf of SJHS/CHS, and other contractors of SJHS/CHS performing IT-specific tasks
Users	members of the SJHS/CHS workforce including its employees, volunteers, and trainees. Independent Contractors and vendors are considered Business Associates of an SJHS/CHS entity, and thus not members of its workforce.



DATA MOBILITY POLICY

25.0PURPOSE

Information Technology is intended to improve access to information, enhance efficiency, and facilitate communication. The purpose of this policy is to define the procedures for securing data on mobile systems.

26.0SCOPE

This policy applies to all Users, and the information covered in this policy includes Protected Health Information (or PHI) and confidential information.

27.0POLICY

It is SJHS/CHS policy to guard against unauthorized access to or modification of electronic PHI that resides on a mobile system.

Performance of these activities should be consistent with pertinent policies and procedures

28.0PROCEDURE

- 28.1.** Mobile system configurations should conform to as many pertinent policies, procedures, and standards as allowed by the mobile system and operating system architecture. Examples of these include, but are not limited to: anti-virus configurations (outlined in the Protection From Malicious Software Policy), the backing up of pertinent data (outlined in the Data Backup Policy), and the general maintenance of the confidentiality and security of any Information Technology access to PHI (outlined in the Information Technology Access and Usage Policy).
- 28.2.** Reasonable precautions should be made to prohibit unauthorized entities from viewing, accessing, or acquiring information on mobile systems. These include, but are not limited to: exercising care during use of the mobile device, implementing inactivity timers or automatic shutdown mechanisms, implementing locking cables or other similar locking mechanisms, and maintaining possession of the mobile system while in transit.
- 28.3.** Mobile systems are not intended for, and should not be used for, the storage of information as would a desktop workstation or other similar system.
- 28.4.** As appropriate, mobile systems should implement a form of encryption for protecting the data. Encryption mechanisms implemented to comply with this policy should support a minimum of, but not limited to, a 128-bit level of encryption.



DATA MOBILITY POLICY

- 28.5. As appropriate, mobile systems should natively include, or be located behind, a network isolation mechanism such as a firewall when not connected to the SJHS/CHS network.
- 28.6. Events that reveal a known, suspected, or reasonably anticipated security incident should be reported in accordance with pertinent policies. Examples of these events include, but are not limited to: computer virus outbreaks, unauthorized access, theft of a physical asset that contains information such as a database or mailing list, or the unauthorized transmission or disclosure of electronic information.
- 4.5.1 Detail regarding the definition and reporting requirements of a possible security incident are located in SJHS/CHS Policy IS404, Security Incident Response and Reporting Policy.

29.0 REFERENCES

45 CFR 164.312(a)(2)(iv): "HIPAA" – Health Insurance Reform: Security Standards (Access Control – Encryption and Decryption)

SJHS/CHS Policy IS404 Security Incident Response and Reporting Policy

30.0 DEFINITIONS

Confidential Information	financial data, proprietary reports, human resources information, marketing and sales information, and other similar privileged "need to know" information
Information Technology	any computer, telephone, messaging system (i.e. voicemail or e-mail), electronic media, application, protocol, or other equipment utilized on a public or private internetwork)
Mobile System	Information technology that is designed to be connected in an intermittent manner to the SJHS/CHS network (i.e. laptop computer, mobile phone, PDA, etc.)



ST. JOSEPH HEALTH SYSTEM

DIVISION: (HR, Finance, etc.) IS
LAST DATE REVISED: 02/23/2005
LAST DATE REVIEWED: 02/23/2005
ORIGINAL DATE ADOPTED: 02/23/2005
PAGE NUMBER: 57 of 71
POLICY/PROCEDURE: IS416
APPROVED BY: Security Task Force
CHS REVIEW DATE: 01/18/2006, 4/12/2007
REVIEWED BY: CHS Compliance Committee

DATA MOBILITY POLICY

Protected Health Information (PHI)	individually identifiable information relating to the past, present, or future physical or mental health or condition of an individual or can be used to identify an individual
SJHS/CHS IT	Members of the SJHS/CHS Information Technology staff, other SJHS/CHS employees performing IT-specific tasks, Perot Systems associates performing IT services on behalf of SJHS/CHS, and other contractors of SJHS/CHS performing IT-specific tasks
Users	members of the SJHS/CHS workforce including its employees, volunteers, and trainees. Independent Contractors and vendors are considered Business Associates of an SJHS/CHS entity, and thus not members of its workforce.
Workstation	an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment



DATA INTEGRITY POLICY

31.0PURPOSE

Information Technology is intended to improve access to information, enhance efficiency, and facilitate communication. The purpose of this policy is to define the procedures for protecting electronic health information from improper alteration or destruction.

32.0SCOPE

This policy applies to all Users, and the information covered in this policy includes Protected Health Information (or PHI) and confidential information.

33.0POLICY

It is SJHS/CHS policy to guard against the improper alteration or destruction of electronic protected health information.

Performance of these activities should be consistent with pertinent policies and procedures

34.0PROCEDURE

34.1. Information technology purchased for use by SJHS/CHS should conform to existing standards. These standards include technical features that guard against the improper alteration or destruction of electronic health information.

34.1.1. Examples of technical features that guard against the improper alteration or destruction of electronic health information may include, but are not limited to: error detection and correction for hard drives, error-correcting memory, operating systems, software, and configuration methods for each.

34.2. SJHS/CHS IT has no obligation to provide support for SJHS/CHS-purchased assets that do not conform to established standards.

34.3. Each SJHS/CHS Information Services Planning Council (ISPC) should be advised of and/or approve and document exceptions as necessary.

35.0REFERENCES

45 CFR 164.312(c)(1): "HIPAA" – Health Insurance Reform: Security Standards (Integrity)

45 CFR 164.312(c)(2): "HIPAA" – Health Insurance Reform: Security Standards (Mechanism to Authenticate Electronic Protected Health Information)



DATA INTEGRITY POLICY

36.0 DEFINITIONS

Confidential Information	financial data, proprietary reports, human resources information, marketing and sales information, and other similar privileged “need to know” information
Information Technology	any computer, telephone, messaging system (i.e. voicemail or e-mail), electronic media, application, protocol, or other equipment utilized on a public or private internetwork)
Protected Health Information (PHI)	individually identifiable information relating to the past, present, or future physical or mental health or condition of an individual or can be used to identify an individual
SJHS/CHS IT	Members of the SJHS/CHS Information Technology staff, other SJHS/CHS employees performing IT-specific tasks, Perot Systems associates performing IT services on behalf of SJHS/CHS, and other contractors of SJHS/CHS performing IT-specific tasks
Users	members of the SJHS/CHS workforce including its employees, volunteers, and trainees. Independent Contractors and vendors are considered Business Associates of an SJHS/CHS entity, and thus not members of its workforce.



PHYSICIAN USE OF ELECTRONIC MEDICAL RECORD SYSTEMS POLICY

37.0PURPOSE

Information Technology is intended to improve access to information, enhance efficiency, and facilitate communication. The purpose of this policy is to define the procedures for physician connectivity in support of SJHS/CHS business operations.

38.0SCOPE

This policy applies to all Physicians as defined below, and the information covered in this policy includes Protected Health Information (or PHI) and confidential information.

39.0POLICY

It is SJHS/CHS policy to control the methods of connectivity for physicians that support SJHS/CHS business activities.

Performance of these activities should be consistent with pertinent policies and procedures.

40.0PROCEDURE

40.1. The principles of role-based access and minimum necessary, as well as established policies regarding vendor management, should be used for the provisioning of physician connectivity utilized in support of SJHS/CHS.

40.2. Only physicians that are on the medical staff of SJHS/CHS ministries, and after signing a user/confidentiality statement, can have access to electronic protected health information. In addition, such physicians may only access electronic protected health information in the scope of treating their patients at the hospital or in their private practice; they may not use electronic protected health information for purposes in their job function at Public Health or any other role.

40.2.1. Any information that is to be reported to Public Health should be requested through the medical record department and under the normal process for reporting to Public Health in order that the hospital can account for such disclosures pursuant to HIPAA.



PHYSICIAN USE OF ELECTRONIC MEDICAL RECORD SYSTEMS POLICY

- 40.2.2. Physicians having dual roles at the hospital and Public Health should not access electronic protected health information for public health duties or any other reason that is beyond direct treatment of their patients.
- 40.3. At a minimum, physician connectivity requests should include: confidentiality statements or contracts by all parties requesting access, acknowledgements that access is subject to monitoring and review by St. Joseph Health System/Covenant Health System, patient data accessed is to be used solely for treatment of a particular patient, an understanding that any misuse or violation will result in the loss of access, local IT approval, local compliance approval, and SJHS Corporate compliance approval.
- 40.4. Physicians should not implement automated transmission of SJHS/CHS information without explicit permission from SJHS IT. This includes automated file transfer, automated e-mail forwarding of SJHS/CHS e-mail to non-SJHS/CHS e-mail addresses, and other similar automated transmissions.
- 40.5. Remote access requests for physicians shall also conform to the SJHS Remote Access Policy.
- 40.6. SJHS/CHS IT has no obligation to provide support for physician computing devices or software installed on vendor computing devices to facilitate connectivity.
- 40.7. SJHS/CHS IT reserves the right to disconnect physician computing devices and physician-supported computing devices that do not comply with these requirements.

41.0 REFERENCES

45 CFR Parts 160, 162, 164: "HIPAA" – Health Insurance Reform: Security Standards (Final Rule)

SJHS Policy IS420, Remote Access Policy

42.0 DEFINITIONS

Confidential Information	financial data, proprietary reports, human
--------------------------	--



**PHYSICIAN USE OF ELECTRONIC
 MEDICAL RECORD SYSTEMS
 POLICY**

	resources information, marketing and sales information, and other similar privileged "need to know" information
Information Technology	any computer, telephone, messaging system (i.e. voicemail or e-mail), electronic media, application, protocol, or other equipment utilized on a public or private internetwork)
Physicians	Physicians, physician/clinicians, physician staff, or other similar entities that are not SJHS/CHS employees responsible for the medical care of SJHS/CHS patients
Protected Health Information (PHI)	individually identifiable information relating to the past, present, or future physical or mental health or condition of an individual or can be used to identify an individual
SJHS IT	Members of the SJHS/CHS Information Technology staff, other SJHS/CHS employees performing IT-specific tasks, Perot Systems associates performing IT services on behalf of SJHS/CHS, and other contractors of SJHS/CHS performing IT-specific tasks
Users	Members of the SJHS/CHS workforce including its employees, volunteers, and trainees. Independent Contractors and vendors are considered Business Associates of an SJHS/CHS entity, and thus not members of its workforce



REMOTE ACCESS POLICY

1.0 PURPOSE

Information Technology is intended to improve access to information, enhance efficiency, and facilitate communication. The purpose of this policy is to define the methods for managing remote access to information technology resources utilized in support of SJHS/CHS.

2.0 SCOPE

This policy applies to members of the SJHS/CHS workforce (including its employees, volunteers, and trainees), independent contractors, vendors, physicians, clinicians, and any and all other entities that desire remote connectivity to SJHS. The information covered in this policy includes Protected Health Information (or PHI) and all other confidential information.

Of note is the expectation of SJHS/CHS to institute a higher degree of care for remote access to information.

3.0 POLICY

It is SJHS/CHS policy to manage the methods of remote access to information technology resources utilized in support of SJHS/CHS.

Performance of these activities shall be consistent with pertinent policies and procedures.

4.0 PROCEDURE

- 4.36. The principles of role-based access and minimum necessary, as well as established policies regarding identity management and workforce security, shall be used for the provisioning of remote access for applications, services, or other information technology resources utilized in support of SJHS/CHS.
- 4.37. Local IT governance at each ministry shall be advised of and/or approve remote access provisioning for applications, services, or other information technology resources utilized in support of SJHS/CHS.
 - 42.1.1. Local IT governance at each ministry shall periodically review remote access provisioning requirements and needs as appropriate.



REMOTE ACCESS POLICY

42.1.2. Specific exemptions to standardized remote access must be approved by the SJHS IT Security Task Force.

4.38. Each request for remote access to applications, services, or other information technology resources utilized in support of SJHS/CHS shall be reviewed as appropriate. Examples of items for review include, but are not limited to: authoritative approval that the request is reasonable, appropriate, and genuine; confirmation that pertinent confidentiality agreements have been tendered; confirmation that pertinent site-specific telecommuting agreements have been tendered; and confirmation that licensing costs for any required remote access licenses are approved. Additionally, each SJHS/CHS ministry shall identify a repository for the documentation of such requests as appropriate.

4.3.1 Remote access requests for physicians, physician/clinicians, physician staff, or other similar entities that are not SJHS employees shall also conform to the SJHS Physician Use Of Electronic Medical Record Systems Policy.

4.3.2 Remote access requests for vendors shall also conform to the SJHS Vendor Use Of Electronic Medical Record Systems Policy

4.3.3 Each SJHS/CHS-owned computing device configured for remote access shall conform to SJHS/CHS standards and policies, and each personally-owned computing device configured for remote access shall conform to the SJHS Personally-Owned Computing Device policy.

4.3.4 Operations and functions interacting with patient data shall conform to SJHS/CHS standards and policies, with emphasis on the policies listed in section 5.0 (References).

4.3.5 At a minimum, each connection should be confirmed for the type of anti-virus solution in place, the type of firewall in place, confirmation that appropriate security updates are applied, and confirmation that each of the above are updated as appropriate.



REMOTE ACCESS POLICY

4.3.6 SJHS/CHS IT has no obligation to provide support for personally-owned, third-party, or any other classification of non-SJHS/CHS computing device or software.

4.4 Events which involve remote access that reveal a known, suspected, or reasonably anticipated security incident shall be reported in accordance with pertinent policies. Examples of these events include, but are not limited to: computer virus outbreaks, unauthorized access, theft of a personally-owned computing devices that contains information such as a database or mailing list, or the unauthorized transmission or disclosure of electronic information.

4.4.1 Details regarding the definition and reporting requirements of a possible security incident are located in SJHS Policy IS404, Security Incident Response and Reporting Policy.

5.0 REFERENCES

SJHS Policy HI413 Minimum Necessary Standard Regarding the Use and Disclosure of Protected Health Information

SJHS Policy HI454 Role-Based Access Review

SJHS Policy HI516, Sanction/Disciplinary Process

SJHS Policy IS401, Information Technology Access and Usage

SJHS Policy IS402, Media Re-Use and Disposal

SJHS Policy IS404 Information Security Incident Response and Reporting Policy

SJHS Policy IS406, Data Backup

SJHS Policy IS407, Information System Activity Review

SJHS Policy IS409 Identity Management and Workforce Security

REMOTE ACCESS POLICY

SJHS Policy IS412, Protection From Malicious Software

SJHS Policy IS414, Transmission Security

SJHS Policy IS416, Data Mobility

SJHS Policy IS417, Data Integrity

SJHS Policy IS419, Physician Use of Electronic Medical Record Systems Policy

SJHS Policy IS421, Vendor Use of Electronic Medical Record Systems Policy

6.0 DEFINITIONS

Confidential Information	financial data, proprietary reports, human resources information, marketing and sales information, and other similar privileged “need to know” information
Information Technology	any computer, telephone, messaging system (i.e. voicemail or e-mail), electronic media, application, protocol, or other equipment utilized on a public or private internetwork)
Protected Health Information (PHI)	individually identifiable information relating to the past, present, or future physical or mental health or condition of an individual or can be used to identify an individual
Role-Based Access	A type of access which fulfills the principle of least privilege, where a User is given no more privileges that reasonably necessary to fulfill a role. Ensuring least privilege requires defining a category or categories of information required to fulfill the role, determining the reasonable and appropriate minimum set of privileges required to access the electronic PHI commensurate to the defined role, and implementing reasonable and appropriate



ST. JOSEPH HEALTH SYSTEM

DIVISION: (HR, Finance, etc.) IS
LAST DATE REVISED: 12/22/2006
LAST DATE REVIEWED: 12/22/2006
ORIGINAL DATE ADOPTED: 12/22/2006
PAGE NUMBER: 67 of 71
POLICY/PROCEDURE: IS420
APPROVED BY: Security Task Force
CHS REVIEW DATE: 2/21/2007; 3/6/2007
REVIEWED BY: CHS Compliance Committee;
CHS Board of Trustees

REMOTE ACCESS POLICY

	methods to restrict the user to the defined category or categories of information.
SJHS IT	Members of the SJHS Information Technology staff, other SJHS employees performing IT-specific tasks, Perot Systems associates performing IT services on behalf of SJHS, and other contractors of SJHS performing IT-specific tasks



VENDOR USE OF ELECTRONIC MEDICAL RECORD SYSTEMS POLICY

43.0PURPOSE

Information Technology is intended to improve access to information, enhance efficiency, and facilitate communication. The purpose of this policy is to define the procedures for vendor connectivity in support of SJHS/CHS business operations.

44.0SCOPE

This policy applies to all Vendors, and the information covered in this policy includes Protected Health Information (or PHI) and confidential information.

45.0POLICY

It is SJHS/CHS policy to control the methods of connectivity for vendors that support SJHS/CHS business activities.

Performance of these activities should be consistent with pertinent policies and procedures.

46.0PROCEDURE

- 46.1.** The principles of role-based access and minimum necessary, as well as established policies regarding vendor management should be used for the provisioning of vendor connectivity utilized in support of SJHS/CHS.
- 46.2.** Vendor connectivity requests should include: business justification, local business department approval, local IT approval, local compliance approval, and SJHS Corporate compliance approval.
- 46.3.** Vendor use and connectivity for remote access shall also conform to the SJHS Remote Access Policy.
- 46.4.** Prior to establishing connectivity, vendor computing device configurations should be confirmed for a) updated anti-virus solutions, b) updated patch management solutions, and c) implementation of a network isolation mechanism, e.g. firewall, that supports network address translation (NAT).
- 46.5.** Vendors should not implement automated transmission of SJHS/CHS information without explicit permission from SJHS/CHS IT. This includes automated file transfer, automated e-mail forwarding of SJHS/CHS e-mail to non-SJHS/CHS e-mail addresses, and other similar automated transmissions.



VENDOR USE OF ELECTRONIC MEDICAL RECORD SYSTEMS POLICY

- 46.6.** SJHS/CHS information that may be created, received, maintained, or transmitted by a vendor is subject to as many confidentiality provisions as applicable. Examples of these include, but are not limited to: Business Associate Agreements, Contracts, and Confidentiality Agreements.
- 46.7.** SJHS/CHS IT has no obligation to provide support for vendor computing devices or software installed on vendor computing devices to facilitate connectivity.
- 46.8.** SJHS/CHS IT reserves the right to disconnect vendor computing devices and vendor-supported computing devices that do not comply with these requirements.

47.0 REFERENCES

45 CFR Parts 160, 162, 164: "HIPAA" – Health Insurance Reform: Security Standards (Final Rule)

SJHS IS420, Remote Access Policy

48.0 DEFINITIONS

Confidential Information	financial data, proprietary reports, human resources information, marketing and sales information, and other similar privileged "need to know" information
Information Technology	any computer, telephone, messaging system (i.e. voicemail or e-mail), electronic media, application, protocol, or other equipment utilized on a public or private internetwork)
Protected Health Information (PHI)	individually identifiable information relating to the past, present, or future physical or mental health or condition of an individual or can be used to identify an individual



ST. JOSEPH HEALTH SYSTEM

DIVISION: (HR, Finance, etc.) IS
LAST DATE REVISED: 12/22/2006
LAST DATE REVIEWED: 12/22/2006
ORIGINAL DATE ADOPTED: 12/22/2006
PAGE NUMBER: 70 of 71
POLICY/PROCEDURE: IS421
APPROVED BY: Security Task Force
CHS REVIEW DATES: 2/21/2007; 3/6/2007
REVIEWED BY: CHS Compliance Committee;
CHS Board of Trustees

VENDOR USE OF ELECTRONIC MEDICAL RECORD SYSTEMS POLICY

SJHS IT	Members of the SJHS/CHS Information Technology staff, other SJHS employees performing IT-specific tasks, Perot Systems associates performing IT services on behalf of SJHS/CHS, and other contractors of SJHS/CHS performing IT-specific tasks
Users	members of the SJHS/CHS workforce including its employees, volunteers, and trainees. Independent Contractors and vendors are considered Business Associates of an SJHS/CHS entity, and thus not members of its workforce



ST. JOSEPH HEALTH SYSTEM

DIVISION: (HR, Finance, etc.) IS
LAST DATE REVISED: 12/22/2006
LAST DATE REVIEWED: 12/22/2006
ORIGINAL DATE ADOPTED: 12/22/2006
PAGE NUMBER: 71 of 71
POLICY/PROCEDURE: IS421
APPROVED BY: Security Task Force
CHS REVIEW DATES: 2/21/2007; 3/6/2007
REVIEWED BY: CHS Compliance Committee;
CHS Board of Trustees

**VENDOR USE OF ELECTRONIC
MEDICAL RECORD SYSTEMS
POLICY**
