UNIVERSITY OF SOUTH CAROLINA SCHOOL OF MEDICINE GREENVILLE INFORMATION TECHNOLOGY POLICY

10/21/11 • Version 1.0

INFORMATION SECURITY POLICY

University of South Carolina School of Medicine Greenville

Last Revision Date

October 29, 2016

TABLE OF CONTENTS

University of South Carolina School of Medicine Greenville **Policy and Procedure**	
Title: INTRODUCTION	**P&P #:** IS-1.0
Approval Date: 10/29/2014	**Review: Annual**
Effective Date: 10/29/2014	**Information Technology (TVS001)**

1 Introduction

1.1 PURPOSE

This policy defines the technical controls and security configurations users and Integrated Technology (IT) administrators are required to implement in order to ensure the integrity and availability of the data environment at the University of South Carolina School of Medicine Greenville, hereinafter, referred to as the USCSOM Greenville. It serves as a central policy document with which all students, employees and contractors must be familiar, and defines actions and prohibitions that all users must follow. The policy provides IT managers within the USCSOM Greenville with policies and guidelines concerning the acceptable use of USCSOM Greenville technology equipment, e-mail, Internet connections, voice-mail, facsimile, future technology resources and information processing.

The policy requirements and restrictions defined in this document shall apply to network infrastructures, databases, external media, encryption, hardcopy reports, films, slides, models, wireless, telecommunication, conversations, and any other methods used to convey knowledge and ideas across all hardware, software, and data transmission mechanisms. This policy must be adhered to by all USCSOM Greenville students, employees or temporary workers at all locations and by contractors working with the USCSOM Greenville as subcontractors.

1.2 SCOPE

This policy document defines common security requirements for all USCSOM Greenville personnel and systems that create, maintain, store, access, process or transmit information. This policy also applies to information resources owned by others, such as contractors of the USCSOM Greenville, entities in the private sector, in cases where USCSOM Greenville has a legal, contractual or fiduciary duty to protect said resources while in USCSOM Greenville custody. In the event of a conflict, the more restrictive measures apply. This policy covers the USCSOM Greenville network system which is comprised of various hardware, software, communication equipment and other devices designed to assist the USCSOM Greenville in the creation, receipt, storage, processing, and transmission of information. This definition includes equipment connected to any USCSOM Greenville domain or VLAN, either hardwired or wirelessly, and includes all stand-alone equipment that is deployed by the USCSOM Greenville at its various locations.

1.3 ACRONYMS / DEFINITIONS

Common terms and acronyms that may be used throughout this document.

Encryption – The process of transforming information, using an algorithm, to make it unreadable to anyone other than those who have a specific 'need to know.'
External Media –i.e. CD-ROMs, DVDs, floppy disks, flash drives, USB keys, thumb drives, tapes
Firewall – a dedicated piece of hardware or software running on a computer which allows or denies traffic passing through it, based on a set of rules.
FTP – File Transfer Protocol
HIPAA - Health Insurance Portability and Accountability Act
IT - Information Technology/Integrated Technology
LAN – Local Area Network – a computer network that covers a small geographic area, i.e. a group of buildings, an office.
Malware – Short for malicious software is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems.
SOW - Statement of Work - An agreement between two or more parties that details the working relationship between the parties and lists a body of work to be completed.
User - Any person authorized to access an information resource.
Privileged Users – system administrators and others specifically identified and authorized by USCSOM Greenville management.
Users with edit/update capabilities – individuals who are permitted, based on job assignment, to add, delete, or change records in a database**.**
Users with inquiry (read only) capabilities – individuals who are prevented, based on job assignment, from adding, deleting, or changing records in a database. Their system access is limited to reading information only.
VLAN – Virtual Local Area Network – A logical network, typically created within a network device, usually used to segment network traffic for administrative, performance and/or security purposes.
VPN – Virtual Private Network – Provides a secure passage through the public Internet.
WAN – Wide Area Network – A computer network that enables communication across a broad area, i.e. regional, national.
Virus - a software program capable of reproducing itself and usually capable of causing great harm to files or other programs on the computer it attacks. A true virus cannot spread to another computer without human assistance.

University of South Carolina School of Medicine Greenville	**Policy and Procedure**
Title: USER RESPONSIBILITIES	**P&P #:** IS-1.1
Approval Date: 10/29/2014	**Review: Annual**
Effective Date: 10/29/2014	**Information Technology (TVS002, TVS003)**

2 Responsibilities

2.1 USER REQUIREMENTS

The first line of defense in data security is the individual USCSOM Greenville user. USCSOM Greenville users are responsible for the security of all data which may come to them in whatever format. The USCSOM Greenville is responsible for maintaining ongoing training programs to inform all users of these requirements.

Wear Identifying Badge so that it may be easily viewed by others **-** In order to help maintain building security, all students, faculty and staff should prominently display their identification badge. Contractors who may be in USCSOM Greenville facilities are provided with different colored identification badges. Other people who may be within USCSOM Greenville facilities may be wearing visitor badges and should be chaperoned.

Challenge Unrecognized Personnel **-** It is the responsibility of all USCSOM Greenville personnel to take positive action to provide physical security. If you see an unrecognized person in a restricted USCSOM Greenville location, you should challenge them as to their right to be there. All visitors to USCSOM Greenville offices must sign in at the front desk. In addition, all visitors must wear a visitor/contractor badge. All other personnel must be employees of the USCSOM Greenville. Any challenged person who does not respond appropriately should be immediately reported to supervisory staff.

Secure Laptop **-** When out of the office all laptop computers must be secured. Most USCSOM Greenville computers will contain sensitive data either of a medical, personnel, or financial nature, and the utmost care should be taken to ensure that this data is not compromised. Laptop computers are unfortunately easy to steal, particularly during the stressful period while traveling. Many laptop computers are stolen in snatch and run robberies, where the thief runs through an office or hotel room and grabs all of the equipment he/she can quickly remove.

Unattended Computers **-** Unattended computers should be locked by the user when leaving the work area. USCSOM Greenville policy recommends that all computers will have the automatic screen lock function set to automatically activate upon fifteen (15) minutes of inactivity. Employees are not allowed to take any action which would override this setting.

Home Use of USCSOM Greenville Corporate Assets - Only computer hardware and software approved by the USCSOM Greenville is permitted to be connected to or installed on USCSOM Greenville network. Only software that has been approved for use by the USCSOM Greenville or the Greenville Health System, hereinafter referred to as GHS, may be installed on USCSOM Greenville equipment. Personal computers supplied by the USCSOM Greenville are to be used solely for business or educational purposes. All users must read and understand the list of prohibited activities that are outlined below. Modifications or configuration changes are not permitted on computers supplied by the USCSOM Greenville for home use. Check with Integrated Technologies to see if your personal software is approved for use.

Retention of Ownership - All software programs and documentation generated or provided to employees, students, consultants, or contractors for the benefit of the USCSOM Greenville are the property of the USCSOM Greenville unless covered by a contractual agreement. Nothing contained herein applies to software purchased by USCSOM Greenville students, faculty and staff at their own expense.

2.2 PROHIBITED ACTIVITIES

Personnel are prohibited from the following activities. The list is not inclusive. Other prohibited activities are referenced elsewhere in this document.

- Crashing an information system. Deliberately crashing an information system is strictly prohibited. Users may not realize that they caused a system crash, but if it is shown that the crash occurred as a result of user action, a repetition of the action by that user may be viewed as a deliberate act.
- Attempting to break into an information resource or to bypass a security feature. This includes running password-cracking programs or sniffer programs, and attempting to circumvent file or other resource permissions.
- Introducing, or attempting to introduce, computer viruses, Trojan horses, peer-to-peer (“P2P”) or other malicious code into an information system.
- Exception: Authorized information system support personnel, or others authorized by the USCSOM Greenville, may test the resiliency of a system. Such personnel may test for susceptibility to hardware or software failure, security against hacker attacks, and system infection.
- Browsing. The willful, unauthorized access or inspection of confidential or sensitive information to which you have not been approved on a "need to know" basis is prohibited. The USCSOM Greenville and GHS have access to patient level health information which is protected by HIPAA regulations which stipulate a "need to know" before approval is granted to view the information. The purposeful attempt to look at or access information to which you have not been granted access by the appropriate approval procedure is strictly prohibited.
- Personal or Unauthorized Software. Use of personal software is prohibited. All software installed on USCSOM Greenville computers must be approved by the USCSOM Greenville IT Department.
- Software Use. Violating or attempting to violate the terms of use or license agreement of any software product used by the USCSOM Greenville is strictly prohibited.
- System Use. Engaging in any activity for any purpose that is illegal or contrary to the policies, procedures or business interests of the USCSOM Greenville is strictly prohibited.

2.3 ELECTRONIC COMMUNICATION, E-MAIL, INTERNET USAGE

As a productivity enhancement tool, The USCSOM Greenville encourages the business use of electronic communications. However, all electronic communication systems and all messages generated on or handled by USCSOM Greenville owned equipment are considered the property of the USCSOM Greenville or GHS– not the property of individual users. Consequently, this policy applies to all USCSOM

Greenville and GHS employees and contractors, and covers all electronic communications including, but not limited to, telephones, e-mail, voice mail, instant messaging, Internet, fax, personal computers, and servers.

USCSOM Greenville and GHS provided resources, such as individual computer workstations or laptops, computer systems, networks, e-mail, and Internet software and services are intended for business purposes. However, incidental personal use is permissible as long as:

1) it does not consume more than a trivial amount of employee time or resources,
2) it does not interfere with staff productivity,
3) it does not preempt any business activity,
4) it does not violate any of the following:

    a) Copyright violations – This includes the act of pirating software, music, books and/or videos or the use of pirated software, music, books and/or videos and the illegal duplication and/or distribution of information and other intellectual property that is under copyright.
    b) Illegal activities – Use of USCSOM Greenville information resources for or in support of illegal purposes as defined by federal, state or local law is strictly prohibited.
    c) Commercial use – Use of USCSOM Greenville information resources for personal or commercial profit is strictly prohibited.
    d) Political Activities – All political activities are strictly prohibited on USCSOM Greenville premises. The USCSOM Greenville encourages all of its employees to vote and to participate in the election process, but these activities must not be performed using USCSOM Greenville assets or resources.
    e) Harassment – The USCSOM Greenville strives to maintain a workplace free of harassment and that is sensitive to the diversity of its employees. Therefore, the USCSOM Greenville prohibits the use of computers, e-mail, voice mail, instant messaging, texting and the Internet in ways that are disruptive, offensive to others, or harmful to morale. For example, the display or transmission of sexually explicit images, messages, and cartoons is strictly prohibited. Other examples of misuse includes, but is not limited to, ethnic slurs, racial comments, off-color jokes, or anything that may be construed as harassing, discriminatory, derogatory, defamatory, threatening or showing disrespect for others.
    f) Junk E-mail - All communications using IT resources shall be purposeful and appropriate. Distributing “junk” mail, such as chain letters, advertisements, or unauthorized solicitations is prohibited. A chain letter is defined as a letter sent to several persons with a request that each send copies of the letter to an equal number of persons. Advertisements offer services from someone else to you. Solicitations are when someone asks you for something. If you receive any of the above, delete the e-mail message immediately. Do not forward the e-mail message to anyone.

Generally, while it is **NOT** the policy of the USCSOM Greenville to monitor the content of any electronic communication, the USCSOM Greenville is responsible for servicing and protecting the USCSOM Greenville’s equipment, networks, data, and resource availability and therefore may be required to access and/or monitor electronic communications from time to time. Several different methods are employed to accomplish these goals. For example, an audit or cost analysis may require reports that monitor phone numbers dialed, length of calls, number of calls to / from a specific handset, the time of day, etc. Other examples where electronic communications may be monitored include, but are not limited to, research and testing to optimize IT resources, troubleshooting technical problems and detecting patterns of abuse or illegal activity.

The USCSOM Greenville reserves the right, at its discretion, to review any employee's files or electronic communications to the extent necessary to ensure all electronic media and services are used in compliance with all applicable laws and regulations as well as USCSOM Greenville policies.

Employees should structure all electronic communication with recognition of the fact that the content could be monitored, and that any electronic communication could be forwarded, intercepted, printed or stored by others.

2.4 INTERNET ACCESS

Internet access is provided for USCSOM Greenville users and is considered a great resource for the organization. This resource is costly to operate and maintain, and must be allocated primarily to those with business, administrative or contract needs. The Internet access provided by the USCSOM Greenville should not be used for entertainment, listening to music, viewing the sports highlight of the day, games, movies, etc. Do not use the Internet as a radio or to constantly monitor the weather or stock market results. While seemingly trivial to a single user, the company wide use of these non-business sites consumes a huge amount of Internet bandwidth, which is therefore not available to responsible users.

Many Internet sites, such as games, peer-to-peer file sharing applications, chat rooms, and on-line music sharing applications, have already been blocked by the USCSOM Greenville and GHS routers and firewalls. This list is constantly monitored and updated as necessary. Any person visiting pornographic sites may be disciplined and may be terminated.

2.5 REPORTING SOFTWARE MALFUNCTIONS

Users should inform the appropriate USCSOM Greenville Integrated Technology personnel when the user's software does not appear to be functioning correctly. The malfunction - whether accidental or deliberate - may pose an information security risk. If the user, or the user's manager or supervisor, suspects a computer virus infection, the USCSOM Greenville computer virus policy should be followed, and these steps should be taken immediately:

- Stop using the computer
- Do not carry out any commands, including commands to <Save> data.
- Do not close any of the computer's windows or programs.
- Do not turn off the computer or peripheral devices.
- If possible, physically disconnect the computer from networks to which it is attached.
- Inform the appropriate USCSOM Greenville IT Personnel as soon as possible. Write down any unusual behavior of the computer (screen messages, unexpected disk access, unusual responses to commands) and the time when they were first noticed.
- Write down any changes in hardware, software, or software use that preceded the malfunction.
- Do not attempt to remove a suspected virus!

2.6 REPORT SECURITY INCIDENTS

It is the responsibility of each USCSOM Greenville student, employee or contractor to report perceived security incidents on a continuous basis to the appropriate supervisor or security person. A User is any person authorized to access an information resource. Users are responsible for the day-to-day, hands-on security of that resource. Users are to formally report all security incidents or violations of the security policy immediately should report any perceived security incident to either their immediate supervisor, or to their department head, or to any member of the USCSOM Greenville IT Department.

Reports of security incidents shall be escalated as quickly as possible. Each member of the USCSOM Greenville IT must inform the other members as rapidly as possible. Each incident will be analyzed to determine if changes in the existing security structure are necessary. All reported incidents are logged and the remedial action indicated. It is the responsibility of the IT department to provide training on any procedural changes that may be required as a result of the investigation of an incident.

Security breaches shall be promptly investigated. If criminal action is suspected, the USCSOM Greenville shall contact the appropriate law enforcement and investigative authorities immediately, which may include but is not limited to the police or the FBI.

2.7 TRANSFER OF SENSITIVE/CONFIDENTIAL INFORMATION

When confidential or sensitive information from one individual is received by another individual while conducting official business, the receiving individual shall maintain the confidentiality or sensitivity of the information in accordance with the conditions imposed by the providing individual. All employees must recognize the sensitive nature of data maintained by the USCSOM Greenville and hold all data in the strictest confidence. Any purposeful release of data to which an employee may have access is a violation of USCSOM Greenville policy and will result in personnel action, and may result in legal action.

2.8 TRANSFERRING SOFTWARE AND FILES BETWEEN HOME AND WORK

Personal software shall not be used on USCSOM Greenville computers or networks. If a need for specific software exists, submit a request to your supervisor or department head. Users shall not use USCSOM Greenville purchased software on home or on non-USCSOM Greenville computers or equipment.

USCSOM Greenville proprietary data, including but not limited to patient information, IT Systems information, financial information or human resource data, shall not be placed on any computer that is not the property of the USCSOM Greenville without written consent of the respective supervisor or department head. It is crucial to the USCSOM Greenville to protect all data and, in order to do that effectively we must control the systems in which it is contained. In the event that a supervisor or department head receives a request to transfer USCSOM Greenville data to a non-USCSOM Greenville Computer System, the supervisor or department head should notify the IT department or appropriate personnel of the intentions and the need for such a transfer of data.

The USCSOM Greenville Wide Area Network ("WAN") is maintained with a wide range of security protections in place, which include features such as virus protection, e-mail file type restrictions, firewalls, anti-hacking hardware and software, etc. Since the USCSOM Greenville does not control non-USCSOM Greenville personal computers, the USCSOM Greenville cannot be sure of the methods that may or may not be in place to protect USCSOM Greenville sensitive information, hence the need for this restriction.

2.9 INTERNET CONSIDERATIONS

Special precautions are required to block Internet (public) access to USCSOM Greenville information resources not intended for public access, and to protect confidential USCSOM Greenville information when it is to be transmitted over the Internet.

The following security and administration issues shall govern Internet usage.

Prior approval of the USCSOM Greenville Integrated Technology or appropriate personnel authorized by the USCSOM Greenville shall be obtained before:

- An Internet, or other external network connection, is established;
- USCSOM Greenville information (including notices, memoranda, documentation and software) is made available on any Internet-accessible computer (e.g. web or ftp server) or device;
- Users may not install or download any software (applications, screen savers, etc.). If users have a need for additional software, the user is to contact their supervisor;
- Use shall be consistent with the goals of the USCSOM Greenville. The network can be used to market services related to the USCSOM Greenville, however use of the network for personal profit or gain is prohibited.
- Confidential or sensitive data - including credit card numbers, telephone calling card numbers, logon passwords, and other parameters that can be used to access goods or services - shall be encrypted before being transmitted through the Internet.
- The encryption software used, and the specific encryption keys (e.g. passwords, pass phrases), shall be escrowed with the USCSOM Greenville IT department or appropriate personnel, to ensure they are safely maintained/stored. The use of encryption software and keys, which have not been escrowed as prescribed above, is prohibited, and may make the user subject to disciplinary action.

2.10 DE-IDENTIFICATION OF PERSONAL HEALTH INFORMATION (PHI)

As directed by HIPAA, all personal identifying information is removed from all data that falls within the definition of PHI before it is stored or exchanged.
De-identification is defined as the removal of any information that may be used to identify an individual or of relatives, employers, or household members.

PHI includes:

- Names
- Addresses
- Geographic subdivisions smaller than a state
- All elements of dates directly related to the individual (Dates of birth, marriage, death, etc.)
- Telephone numbers

- Facsimile numbers
- Driver’s license numbers
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers, certificate/license numbers
- Vehicle identifiers and serial numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers
- Full face photographic images and any comparable images

University of South Carolina School of Medicine Greenville	**Policy and Procedure**
Title: IDENTIFICATION and AUTHENTICATION	**P&P #:** IS-1.2
Approval Date: 10/29/14	**Review: Annual**
Effective Date: 10/29/14	**Information Technology** **(TVS008, TVS015, TVS016, TVS023)**

3 Identification and Authentication

3.1 USER LOGON IDS

Individual users shall have unique logon IDs and passwords. An access control system shall identify each user and prevent unauthorized users from entering or using information resources. Security requirements for user identification include:

- Each user shall be assigned a unique identifier.
- Users shall be responsible for the use and misuse of their individual logon ID.

All user login IDs are audited and all inactive logon IDs are revoked. The USCSOM Greenville Human Resources Department notifies the IT Director or appropriate personnel upon the departure of all employees and contractors, at which time login IDs are revoked.

The logon ID is locked or revoked after a maximum of three (3) unsuccessful logon attempts which then require the passwords to be reset by the appropriate Administrator.

3.2 PASSWORDS

User Account Passwords
User IDs and passwords are required in order to gain access to all USCSOM Greenville networks and workstations. All passwords are restricted by a corporate-wide password policy to be of a "Strong" nature. This means that all passwords must conform to restrictions and limitations that are designed to make the password difficult to guess. Users are required to select a password in order to obtain access to any electronic information both at the server level and at the workstation level. When passwords are reset, the user will be automatically prompted to manually change that assigned password.

Password Length – Passwords are required to be a minimum of eight characters.

Content Requirements - Passwords must contain a combination of upper and lower case alphabetic characters, numeric characters, and special characters.

Change Frequency – Passwords should be changed every 180 days. Compromised passwords shall be changed immediately.

Reuse - The previous eight passwords cannot be reused.

Restrictions on Sharing Passwords - Passwords shall not be shared, written down on paper or stored within a file or database on a workstation and should be kept confidential.

Restrictions on Recording Passwords - Passwords are masked or suppressed on all online screens, and are never printed or included in reports or logs. Passwords are stored in an encrypted format.

3.3 CONFIDENTIALITY AGREEMENT

Users of USCSOM Greenville information resources may be required to sign, as a condition for use or access to USCSOM Greenville and GHS systems, an appropriate confidentiality agreement. The agreement shall include the following statement, or a paraphrase of it:

> *I understand that any unauthorized use or disclosure of information residing on the USCSOM Greenville or GHS information resource systems may result in disciplinary action consistent with the policies and procedures of federal, state, and local agencies.*

Temporary workers and third-party employees not already covered by a confidentiality agreement shall sign such a document prior to accessing USCSOM Greenville information resources.

Confidentiality agreements shall be reviewed when there are changes to contracts or other terms of employment, particularly when contracts are ending or employees are leaving an organization.

3.4 ACCESS CONTROL

Information resources are protected by the use of access control systems. Access control systems include both internal (i.e. passwords, encryption, access control lists, constrained user interfaces, etc.) and external (i.e. port protection devices, firewalls, host-based authentication, etc.).

Rules for access to resources (including internal and external telecommunications and networks) have been established by the information/application owner or manager responsible for the resources.

This guideline satisfies the "need to know" requirement of the HIPAA regulation, since the supervisor or department head is the person who most closely recognizes a person’s need to access data. Users may be added to the information system, network, or EHR **only** upon approval by GHS or appropriate personnel who are responsible for adding the employee to the network in a manner and fashion that ensures the employee is granted access to data only as specifically requested.

Online banner screens, if used, shall contain statements to the effect that unauthorized use of the system is prohibited and that violators will be subject to criminal prosecution.

Identification and Authentication Requirements

The host security management program shall maintain current user application activity authorizations. Each initial request for a connection or a session is subject to the authorization process previously addressed.

3.5 USER LOGIN ENTITLEMENT REVIEWS

If an employee changes positions at the USCSOM Greenville, employee’s new supervisor or department head shall promptly notify the Information Technology (“IT”) Department of the change of both the roles or access that need to be added and the roles or access that need to be removed so that employee has access to the minimum necessary data to effectively perform their new job functions. The effective date of the position change should also be noted so that the IT Department can ensure that the employee will have appropriate roles, access, and applications for their new job responsibilities.

Annually, the IT Director shall facilitate entitlement reviews with department heads to ensure that all employees have the appropriate roles, access, and software necessary to perform their job functions effectively while being limited to the minimum necessary data to facilitate compliance and protect data.

3.6 TERMINATION OF USER LOGON ACCOUNT

Upon termination of an employee, whether voluntary or involuntary, employee’s supervisor or department head shall promptly notify the IT Department. If employee’s termination is voluntary and employee provides notice, employee’s supervisor or department head shall promptly notify the IT Department of employee’s last scheduled work day so that their user account(s) can be configured to expire. The employee’s department head shall be responsible for insuring that all keys, ID badges, and other access devices as well as USCSOM Greenville equipment and property is returned to the USCSOM Greenville prior to the employee leaving the USCSOM Greenville on their final day of employment.

University of South Carolina School of Medicine Greenville	**Policy and Procedure**
Title: NETWORK CONNECTIVITY	**P&P #:** IS-1.3
Approval Date: 10/29/2014	**Review: Annual**
Effective Date: 10/29/2014	**Information Technology**

4 Network Connectivity

4.1 TELECOMMUNICATION EQUIPMENT

Certain direct link connections may require a dedicated or leased network line. These facilities are authorized only by USCSOM Greenville, GHS or appropriate personnel and ordered by the appropriate personnel. Communication equipment and services include but are not limited to the following:

- phone lines
- fax lines
- phone head sets
- software type phones installed on workstations
- conference calling contracts
- cell phones
- Smart Phone type devices
- call routing software
- call reporting software
- phone system administration equipment
- Network lines
- long distance lines
- 800 lines
- local phone lines
- PRI circuits
- telephone equipment

University of South Carolina School of Medicine Greenville **Policy and Procedure**	
Title: MALICIOUS CODE	**P&P #:** IS-1.4
Approval Date: 10/24/2014	**Review: Annual**
Effective Date: 10/24/2014	**Information Technology (TVS018)**

5 Malicious Code

5.1 ANTIVIRUS SOFTWARE INSTALLATION

Antivirus software is installed on all USCSOM Greenville personal computers and servers. Virus update patterns are updated daily on the USCSOM Greenville servers and workstations. Virus update engines and data files are monitored by appropriate administrative staff that is responsible for keeping all virus patterns up to date.

Configuration **-** The antivirus software currently implemented by the USCSOM Greenville is Kaspersky Antivirus. Updates are received directly from Kaspersky which is scheduled daily.

Remote Deployment Configuration **-** Through an automated procedure, updates and virus patches may be pushed out to the individual workstations and servers on an as needed basis.

Monitoring/Reporting – A record of virus patterns for all workstations and servers on the USCSOM Greenville network may be maintained. Appropriate administrative staff is responsible for providing reports for auditing and emergency situations as requested by the appropriate personnel.

5.2 NEW SOFTWARE DISTRIBUTION

Only software approved by the IT Department or appropriate personnel will be used on internal computers and networks. All new software will be tested by appropriate personnel in order to ensure compatibility with currently installed software and network configuration. In addition, appropriate personnel must scan all software for viruses before installation. This includes shrink-wrapped software procured directly from commercial sources as well as shareware and freeware obtained from electronic bulletin boards, the Internet, or on disks (magnetic or CD-ROM and custom-developed software).

Although shareware and freeware can often be useful sources of work-related programs, the use and/or acquisition of such software must be approved by the IT Department or appropriate personnel. Because the software is often provided in an open distribution environment, special precautions must be taken before it is installed on USCSOM Greenville computers and networks. These precautions include determining that the software does not, because of faulty design, “misbehave” and interfere with or damage USCSOM Greenville hardware, software, or data, and that the software does not contain viruses, either originating with the software designer or acquired in the process of distribution.

All data and program files that have been electronically transmitted to a USCSOM Greenville computer or network from another location must be scanned for viruses immediately after being received. Contact the appropriate USCSOM Greenville personnel for instructions for scanning files for viruses.

Every diskette, CD-ROM, DVD and USB device is a potential source for a computer virus. Therefore, every diskette, CD-ROM, DVD and USB device must be scanned for virus infection prior to copying information to a USCSOM Greenville computer or network.

Computers shall never be “booted” from a CD-ROM, DVD or USB device received from an outside source. Users shall always remove any CD-ROM, DVD or USB device from the computer when not in use. This is to ensure that the CD-ROM, DVD or USB device is not in the computer when the machine is powered on. A CD-ROM, DVD or USB device infected with a boot virus may infect a computer in that manner, even if the CD-ROM, DVD or USB device is not “bootable”.

5.3 RETENTION OF OWNERSHIP

All software programs and documentation generated or provided by employees, consultants, or contractors for the benefit of the USCSOM Greenville are the property of the USCSOM Greenville unless covered by a contractual agreement. Nothing contained herein applies to software purchased by USCSOM Greenville employees at their own expense.

University of South Carolina School of Medicine Greenville **Policy and Procedure**	
Title: ENCRYPTION	**P&P #:** IS-1.5
Approval Date: 10/29/2014	**Review: Annual**
Effective Date: 10/29/2014	**Information Technology (TVS012, TVS015)**

6 Encryption

6.1 DEFINITION

Encryption is the translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text*;* encrypted data is referred to as cipher text**.**

6.2 ENCRYPTION KEY

An encryption key specifies the particular transformation of plain text into cipher text, or vice versa during decryption.

If justified by risk analysis, sensitive data and files shall be encrypted before being transmitted through networks. When encrypted data are transferred between agencies, the agencies shall devise a mutually agreeable procedure for secure key management. In the case of conflict, the USCSOM Greenville shall establish the criteria in conjunction with the IT Director or appropriate personnel. The USCSOM Greenville employs several methods of secure data transmission.

6.3 FILE TRANSFER PROTOCOL (FTP)

Files may be transferred to secure FTP sites through the use of appropriate security precautions. Requests for any FTP transfers should be directed to the IT department or appropriate personnel. FTP by its very nature is not secure. Consult with Integrated Technologies to determine the best and most secure solution before transferring files.

6.4 SECURE SOCKET LAYER (SSL) WEB INTERFACE

Any EHR hosted system, if applicable, will require access to a secure SSL website. Any such access must be requested using GHS Help Desk and have appropriate approval from the supervisor or department head or appropriate personnel before any access is granted.

University of South Carolina School of Medicine Greenville	**Policy and Procedure**
Title: BUILDING SECURITY	**P&P #:** IS-1.6
Approval Date: 10/29/2014	**Review: Annual**
Effective Date: 10/29/2014	**Information Technology (TVS009, TVS010)**

7 Building Security

It is the policy of the USCSOM Greenville and GHS to provide building access in a secure manner. Each site, if applicable, is somewhat unique in terms of building ownership, lease contracts, entranceway access, fire escape requirements, and server room control. However, the USCSOM Greenville and GHS strive to continuously upgrade and expand its security and to enhance protection of its assets and medical information that has been entrusted to it. The following list identifies measures that are in effect at the USCSOM Greenville and GHS. All other facilities, if applicable, have similar security appropriate for that location.

Health Sciences Education, Administration and ESC Buildings

- Entrance to the buildings during non-working hours is controlled by an ID badge system.
- Only specific personnel are given entrance. Loan of the ID badge to non-approved personnel is strictly prohibited.
- The USCSOMG reception area is staffed at all times during the hours of 7:00 AM to 12:00 AM.
- Any unrecognized person in a restricted location should be challenged as to their right to be there. All visitors should register at the front desk, wear a visitor badge if required and be accompanied by a USCSOM Greenville staff member. In some situations, non-USCSOM Greenville personnel do not need to be accompanied at all times.
- Swipe cards control access to all other doors. Each card is coded to allow admission to specific areas based on each individual’s job function or need to know.
- The building is equipped with security cameras to record activities in the parking areas, within buildings and the area encompassing all entrances. All activities in these areas are recorded on a 24 hour a day 365 day per year basis.
- Fire Protection: Use of local building codes will be observed. Manufacturer’s recommendations on the fire protection of individual hardware will be followed.

University of South Carolina School of Medicine Greenville	
Title: TELECOMMUTING	**P&P #:** IS-1.7
Approval Date: 10/29/2014	**Review: Annual**
Effective Date: 10/29/2014	**Information Technology**

8 Telecommuting

With the increased availability of broadband access and VPNs, telecommuting has become more viable for many organizations. The USCSOM Greenville may consider telecommuting to be an acceptable work arrangement in certain circumstances. This policy is applicable to all employees and contractors who work occasionally outside of the USCSOM Greenville office environment. It applies to users who work from their home, to employees on temporary travel, to users who work from a remote office location, and to any user who connects to the USCSOM Greenville and GHS network and/or GHS hosted EHR, if applicable, from a remote location.

While telecommuting can be an advantage for users and for the organization in general, it presents new risks in the areas of confidentiality and security of data. Workers linked to the USCSOM Greenville and GHS networks become an extension of the wide area network and present additional environments that must be protected against the danger of spreading Trojans, viruses, or other malware. This arrangement also exposes the corporate as well as patient data to risks not present in the traditional work environment.

8.1 GENERAL REQUIREMENTS

Telecommuting workers are required to follow all corporate, security, confidentiality, HR, or Code of Conduct policies that are applicable to other employees/contractors.

- **Need to Know:** Telecommuting Users will have the access based on the same ‘need to know’ as they have when in the office.
- **Password Use:** The use of a strong password, changed at least every 180 days, is even more critical in the telecommuting environment. Do not share your password or write it down where a family member or visitor can see it.
- **Training:** Personnel who telecommute must complete the same annual privacy training as all other employees.
- **Contract Specific:** There may be additional requirements specific to the individual contracts to which an employee is assigned.

8.2 REQUIRED EQUIPMENT

Employees approved for telecommuting must understand that the USCSOM Greenville will not provide all equipment necessary to ensure proper protection of information to which the employee has access; however, the following lists define the equipment and environment required:

USCSOM Greenville Provided:

USCSOM Greenville supplied workstation.
If using Citrix, a USCSOM Greenville/GHS issued access is required.
If approved by your supervisor, a USCSOM Greenville supplied phone.

Employee Provided:

Broadband connection and fees,
Secure office environment isolated from visitors and family,
A lockable file cabinet to secure documents when away from the home office.

8.3 HARDWARE SECURITY PROTECTIONS

Virus Protection**:** Home users must never stop the update process for Virus Protection. Virus Protection software is installed on all USCSOM Greenville personal computers and is set to update the virus pattern on a daily basis. This update is critical to the security of all data, and must be allowed to complete.

VPN and Firewall Use**:** Established procedures must be rigidly followed when accessing USCSOM Greenville or GHS information of any type. The USCSOM Greenville requires the use of VPN software and a firewall device. Disabling a virus scanner or firewall is reason for termination.

Lock Screens**:** No matter what location, always lock the screen before walking away from the workstation. The data on the screen may be protected by HIPAA or may contain confidential information. Be sure the automatic lock feature has been set to automatically turn on after 15 minutes of inactivity.

8.4 DATA SECURITY PROTECTION

Data Backup**:** Backup procedures have been established that encrypt the data being moved to an external media. Use only that procedure – do not create one on your own. If there is not a backup procedure established, or if you have external media that is not encrypted, contact the appropriate USCSOM Greenville personnel for assistance. Protect external media by keeping it in your possession when traveling.

Transferring Data to the USCSOM Greenville**:** Transferring of data to the USCSOM Greenville requires the use of an approved VPN connection to ensure the confidentiality and integrity of the data being transmitted. Do not circumvent established procedures, nor create your own method, when transferring data to the USCSOM Greenville.

External System Access: If you require access to an external system, contact your supervisor or IT department and appropriate personnel will assist in establishing a secure method of access to the external system.

E-mail: Do not send any individual-identifiable information (PHI or PII) via e-mail unless it is encrypted. If you need assistance with this, contact the IT department or appropriate personnel to ensure an approved encryption mechanism is used for transmission through e-mail.

Non-USCSOM Greenville Networks: Extreme care must be taken when connecting USCSOM Greenville equipment to a home or external network. Although the USCSOM Greenville actively monitors its security status and maintains organization wide protection policies to protect the data within all contracts, the USCSOM Greenville has no ability to monitor or control the security procedures on non-USCSOM Greenville networks.

Protect Data in Your Possession: View or access only the information that you have a need to see to complete your work assignment. Regularly review the data you have stored to ensure that the amount of patient level data is kept at a minimum and that old data is eliminated as soon as possible. Store electronic data only in encrypted work spaces. If your laptop has not been set up with an encrypted work space, contact the IT department or appropriate personnel for assistance.

Hard Copy Reports or Work Papers: Never leave paper records around your work area. Lock all paper records in a file cabinet at night or when you leave your work area.

Data Entry When in a Public Location: Do not perform work tasks which require the use of sensitive or patient level information when you are in a public area, i.e. airports, airplanes, hotel lobbies. Computer screens can easily be viewed from beside or behind you.

Sending Data Outside the USCSOM Greenville**:** All external transfer of data must be associated with an official contract, non-discloser agreement, or appropriate Business Associate Agreement. Do not give or transfer any patient level information to anyone outside the USCSOM Greenville without the written approval of your supervisor.

8.5 DISPOSAL OF PAPER AND/OR EXTERNAL MEDIA

Shredding: All paper which contains sensitive information that is no longer needed must be shredded before being disposed. Do not place in a trash container without first shredding. All employees working from home, or other non-USCSOM Greenville work environment, MUST have direct access to a shredder.

Disposal of Electronic Media: All external media must be sanitized or destroyed in accordance with HIPAA compliant procedures.

- Do not throw any media containing sensitive, protected information in the trash.
- Return all external media to your supervisor
- External media must be wiped clean of all data. The IT department or appropriate personnel have very definitive procedures for doing this – so all external media must be sent to them.
- The final step in this process is to forward the media for disposal by a certified destruction agency.

University of South Carolina School of Medicine Greenville	**Policy and Procedure**
Title: SPECIFIC PROTOCOLS AND DEVICES	**P&P #:** IS-1.8
Approval Date: 10/29/2014	**Review: Annual**
Effective Date: 10/29/2014	**Information Technology (TVS009)**

9 Specific Protocols and Devices

9.1 WIRELESS USAGE STANDARDS AND POLICY

Due to an emergence of wireless access points in hotels, airports, and in homes, it has become imperative that a Wireless Usage policy be developed and adopted to ensure the security and functionality of such connections for USCSOM Greenville employees. This policy outlines the processes and procedures for acquiring wireless access privileges, utilizing wireless access, and ensuring the security of USCSOM Greenville and GHS laptops and mobile devices.

<u>Approval Procedure</u> **-** In order to be granted the ability to utilize the wireless network interface on your USCSOM Greenville or GHS laptop or mobile device you will be required to gain the approval of your immediate supervisor or department head and the IT department or appropriate personnel.

<u>Software Requirements</u> **-** The following is a list of minimum software requirements for any USCSOM Greenville laptop that is granted the privilege to use wireless access:

- Windows 7 (Firewall enabled)
- Antivirus software
- Appropriate VPN Client, if applicable

If your laptop does not have all of these software components, please notify your supervisor or department head so these components can be installed.

9.2 USE OF TRANSPORTABLE MEDIA

Transportable media included within the scope of this policy includes, but is not limited to, SD cards, DVDs, CD-ROMs, and USB devices.

The purpose of this policy is to guide employees/contractors of the USCSOM Greenville in the proper use of transportable media when a legitimate business requirement exists to transfer data to and from USCSOM Greenville networks. Every workstation or server that has been used by either USCSOM Greenville students, employees or contractors is presumed to have sensitive information stored on its hard drive. Therefore procedures must be carefully followed when copying data to or from transportable media to protect sensitive USCSOM Greenville data. Since transportable media, by their very design are easily lost, care and protection of these devices must be addressed. Since it is very likely that transportable media will be provided to a USCSOM Greenville user by an external source for the exchange of information, it is necessary that everyone has guidance in the appropriate use of media from other companies.

The use of transportable media in various formats is common within the USCSOM Greenville. All users must be aware that sensitive data could potentially be lost or compromised when moved outside of USCSOM Greenville networks. Transportable media received from an external source could potentially pose a threat to USCSOM Greenville and GHS networks. ***Sensitive data*** includes all human resource data, financial data, USCSOM Greenville proprietary information, and personal health information ("PHI") protected by the Health Insurance Portability and Accountability Act ("HIPAA").

USB devices are handy devices which allow the transfer of data in an easy to carry format. They provide a much improved format for data transfer when compared to previous media formats, like CD-ROMs, or DVDs. The software drivers necessary to utilize a USB device are normally included within the device and install automatically when connected. They now come in a rugged titanium format which connects to any key ring. These factors make them easy to use and to carry, but unfortunately easy to lose.

Rules governing the use of transportable media include:

- No ***sensitive data*** should ever be stored on transportable media unless the data is maintained in an encrypted format.
- All USB devices used to store USCSOM Greenville, GHS data or sensitive data must be an encrypted USB device. The use of a personal USB device is strictly prohibited.
- Users must never connect their transportable media to a workstation that is not issued by the USCSOM Greenville or GHS.
- Non-USCSOM Greenville and GHS workstations and laptops may not have the same security protection standards required by the USCSOM Greenville and GHS, and accordingly virus patterns could potentially be transferred from the non-USCSOM Greenville or GHS device to the media and then back to the USCSOM Greenville or GHS workstation.

  Example: Do not copy a work spreadsheet to your USB device and take it home to work on your home PC.

- Data may be exchanged between USCSOM Greenville workstations/networks and workstations used within the USCSOM Greenville. The very nature of data exchange requires that under certain situations data be exchanged in this manner.

  Examples of necessary data exchange include:

  Data provided to auditors via USB device during the course of the audit.

- It is permissible to connect transferable media from other businesses or individuals into USCSOM Greenville workstations or servers as long as the source of the media in on USCSOM Greenville approved devices.
- Copy ***sensitive data*** only to the encrypted space on the media. Non-sensitive data may be transferred to the non-encrypted space on the media.
- Report all loss of transportable media to your supervisor or department head. It is important that the IT department is notified either directly from the employee or contractor or by the supervisor or department head immediately.

When no longer in productive use, all USCSOM Greenville laptops, workstation, or servers must be wiped of data in a manner which conforms to HIPAA regulations. All transportable media must be wiped according to the same standards. Thus all transportable media must be returned to the IT department or appropriate personnel for data erasure when no longer in use.

University of South Carolina School of Medicine Greenville **Policy and Procedure**	
Title: DISPOSAL OF EXTERNAL MEDIA / HARDWARE	**P&P #:** IS-1.10
Approval Date: 10/29/2014	**Review: Annual**
Effective Date: 10/29/2014	**Information Technology (TVS020, TVS021)**

10 Disposal of External Media / Hardware

10.1 DISPOSAL OF EXTERNAL MEDIA

It must be assumed that any external media in the possession of an employee is likely to contain either protected health information ("PHI") or other sensitive information. Accordingly, external media (CD-ROMs, DVDs, USB drives) should be disposed of in a method that ensures that there will be no loss of data and that the confidentiality and security of that data will not be compromised.

The following steps must be adhered to:

- It is the responsibility of each employee to identify media which should be shredded, erased or destroyed.
- External media should never be thrown in the trash.
- When no longer needed all forms of external media are to be sent to the IT department or appropriate personnel for proper disposal.
- The media will be secured until appropriate destruction methods are used.
- Requirements Regarding Equipment

All equipment to be disposed of will be wiped of all data, and all settings and configurations will be reset to factory defaults. No other settings, configurations, software installation or options will be made. Asset tags and any other identifying logos or markings will be removed.

10.2 DISPOSITION OF EXCESS EQUIPMENT

As the older USCSOM Greenville computers and equipment are replaced with new systems, the older machines are held in inventory for a wide assortment of uses:

- Older machines are regularly utilized for spare parts.
- Older machines are used on an emergency replacement basis.
- Older machines are used for testing new software.
- Older machines are used as backups for other production equipment.
- Older machines are used when it is necessary to provide a second machine for personnel who travel on a regular basis.

University of South Carolina School of Medicine Greenville	**Policy and Procedure**
Title: CHANGE MANAGEMENT	**P&P #:** IS-1.11
Approval Date: 10/29/2014	**Review: Annual**
Effective Date: 10/29/2014	**Information Technology (TVS024)**

11 Change Management

Statement of Policy

To ensure that USCSOM Greenville is tracking changes to networks, systems, and workstations including software releases and software vulnerability patching in information systems that contains electronic protected health information (“ePHI”). Change tracking allows the Integrated Technology (“IT”) Department to efficiently troubleshoot issues that arise due to an update, new implementation, reconfiguration, or other change to the system.

Procedure

1. The IT staff or other designated USCSOM Greenville employee who is updating, implementing, reconfiguring, or otherwise changing the system shall carefully log all changes made to the system.
    a. When changes are tracked within a system, i.e. Windows updates in the Add or Remove Programs component they do not need to be logged on the change management tracking log; however, the employee implementing the change will ensure that the change tracking is available for review if necessary.
2. The employee implementing the change will ensure that all necessary data backups are performed prior to the change.
3. The employee implementing the change shall also be familiar with the rollback process in the event that the change causes an adverse effect within the system and needs to be removed.

University of South Carolina School of Medicine Greenville	**Policy and Procedure**
Title: INFORMATION SYSTEM ACTIVITY REVIEW	**P&P #:** IS-1.13
Approval Date: 10/29/2014	**Review: Annual**
Effective Date: 10/29/2014	**Information Technology** **(TVS014, TVS017, TVS019)**

12 Information System Activity Review

Statement of Policy

To establish the process for conducting, on a periodic basis, an operational review of system activity including, but not limited to, user accounts, system access, file access, security incidents, audit logs, and access reports. USCSOM Greenville shall conduct on a regular basis an internal review of records of system activity to minimize security violations.

Procedure

1. The Integrated Technology shall be responsible for conducting reviews of USCSOM Greenville's information systems' activities. Such person(s) shall have the appropriate technical skills with respect to the operating system and applications to access and interpret audit logs and related information appropriately.

2. The IT Director shall develop a report format to capture the review findings. Such report shall include the reviewer's name, date and time of performance, and significant findings describing events requiring additional action (e.g., additional investigation, employee training and/or discipline, program adjustments, modifications to safeguards). To the extent possible, such report shall be in a checklist format.

3. Such reviews shall be conducted annually. Audits also shall be conducted if USCSOM Greenville has reason to suspect wrongdoing. In conducting these reviews, the Information Technology Services shall examine audit logs for security-significant events including, but not limited to, the following:

    a. Logins – Scan successful and unsuccessful login attempts. Identify multiple failed login attempts, account lockouts, and unauthorized access.

    b. File accesses – Scan successful and unsuccessful file access attempts. Identify multiple failed access attempts, unauthorized access, and unauthorized file creation, modification, or deletion.

c. Security incidents – Examine records from security devices or system audit logs for events that constitute system compromises, unsuccessful compromise attempts, malicious logic (e.g., viruses, worms), denial of service, or scanning/probing incidents.

d. User Accounts – Review of user accounts within all systems to ensure users that no longer have a business need for information systems no longer have such access to the information and/or system.

All significant findings shall be recorded using the report format referred to in Section 2 of this policy and procedure.

1. The Information Technology Services shall forward all completed reports, as well as recommended actions to be taken in response to findings, to the appropriate personnel for review if required. The IT Director shall consider such reports and recommendations in determining whether to make changes to USCSOM Greenville's administrative, physical, and technical safeguards. In the event a security incident is detected through such auditing, such matter shall be addressed via appropriate security protocols.

University of South Carolina School of Medicine Greenville **Policy and Procedure**	
Title: DATA INTEGRITY	**P&P #:** IS-1.14
Approval Date: 10/29/2014	**Review: Annual**
Effective Date: 10/29/2014	**Information Technology (TVS012, TVS013)**

13 Data Integrity

Statement of Policy

The purpose of this policy is to protect USCSOM Greenville’s data from improper alteration or destruction.

Procedure

To the fullest extent possible, USCSOM Greenville shall utilize applications with built-in intelligence that automatically checks for human errors.

USCSOM Greenville shall acquire appropriate network-based and host-based intrusion detection systems. The Integrated Technology department shall be responsible for installing, maintaining, and updating such systems.

To prevent transmission errors as data passes from one computer to another, USCSOM Greenville will use encryption, as determined to be appropriate, to preserve the integrity of data.

USCSOM Greenville will check for possible duplication of data in its computer systems to prevent poor data integration between different computer systems.

To prevent programming or software bugs, USCSOM Greenville will test its information systems for accuracy and functionality before it starts to use them. USCSOM Greenville will update its systems when IT vendors release fixes to address known bugs or problems.

1. USCSOM Greenville will install and regularly update antivirus software on all workstations to detect and prevent malicious code from altering or destroying data.

2. To prevent exposing magnetic media to a strong magnetic field, workforce members shall keep magnetic media away from strong magnetic fields and heat. For example, computers should not be left in automobiles during the summer months.

University of South Carolina School of Medicine Greenville	**Policy and Procedure**
Title: CONTINGENCY PLAN	**P&P #:** IS-1.15
Approval Date: 10/29/2014	**Review: Annual**
Effective Date: 10/29/2014	**Information Technology (TVS026)**

14 Contingency Plan

Statement of Policy

To establish and implement policies and procedures for responding to an emergency or other occurrence (e.g., fire, vandalism, system failure, natural disaster) that damages systems that contain data.

USCSOM Greenville is committed to maintaining formal procedures for responding to an emergency or other occurrence that damages systems containing data. USCSOM Greenville shall continually assess potential risks and vulnerabilities to protect health information in its possession, and develop, implement, and maintain appropriate administrative, physical, and technical security measures in accordance with the HIPAA Security Rule.

Procedure

1. Data Backup Plan

    a. USCSOM Greenville, under the direction of the IT Director, shall implement a data backup plan to create and maintain retrievable exact copies of all data.

    b. The IT department shall monitor storage and removal of backups and ensure all applicable access controls are enforced.

    c. The IT department shall test backup procedures on an annual basis to ensure that exact copies of all data can be retrieved and made available. To the extent such testing indicates need for improvement in backup procedures, the IT department shall identify and implement such improvements in a timely manner.

2. Disaster Recovery and Emergency Mode Operations Plan

    a. The IT Director shall be responsible for developing and regularly updating the written disaster recovery and emergency mode operations plan for the purpose of:

        i. Restoring or recovering any loss of data and/or systems necessary to make data available in a timely manner caused by fire, vandalism, terrorism, system failure, or other emergency; and

        ii. Continuing operations during such time information systems are unavailable. Such written plan shall have a sufficient level of detail and explanation that a person unfamiliar with the system can implement the plan in case of an emergency or disaster. Copies of the plan shall be maintained on-site and at the off-site locations at which backups are stored or other secure off-site location.

b. The disaster recovery and emergency mode operation plan shall include the following:

   i. Current copies of the information systems inventory and network configuration developed and updated as part of USCSOM Greenville's risk analysis.

   ii. Current copy of the written backup procedures developed and updated pursuant to this policy.

   iii. An inventory of hard copy forms and documents needed to record clinical, registration, and financial interactions with patients.

   iv. Identification of an emergency response team. Members of such team shall be responsible for the following:

      1. Determining the impact of a disaster and/or system unavailability on USCSOM Greenville's operations.

      2. In the event of a disaster, securing the site and providing ongoing physical security.

      3. Retrieving lost data.

      4. Identifying and implementing appropriate "work-a-rounds" during such time information systems are unavailable.

      5. Taking such steps necessary to restore operations.

   v. Procedures for responding to loss of electronic data including, but not limited to retrieval and loading of backup data or methods for recreating data should backup data be unavailable. The procedures should identify the order in which data is to be restored based on the criticality analysis performed as part of USCSOM Greenville's risk analysis

   vi. Telephone numbers and/or e-mail addresses for all persons to be contacted in the event of a disaster, including the following:

      1. Members of the immediate response team,

      2. Facilities at which backup data is stored,

      3. Information systems vendors, and

      4. All current workforce members.

c. The IT team shall meet on at least an annual basis to:

   i. Review the effectiveness of the plan in responding to any disaster or emergency experienced by USCSOM Greenville;

   ii. In the absence of any such disaster or emergency, plan drills to test the effectiveness of the plan and evaluate the results of such drills.

University of South Carolina School of Medicine Greenville **Policy and Procedure**	
Title: SECURITY MANAGEMENT PROCESS	**P&P #:** IS-1.17
Approval Date: 10/29/2014	**Review: Annual**
Effective Date: 10/29/2014	**Information Technology**

15 Security Management Process

Statement of Policy

To ensure USCSOM Greenville conducts an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic data held by USCSOM Greenville.

USCSOM Greenville shall conduct an accurate and thorough risk analysis to serve as the basis for USCSOM Greenville's HIPAA Security Rule compliance efforts. USCSOM Greenville shall re-assess the security risks to its data and evaluate the effectiveness of its security measures and safeguards as necessary in light of changes to business USCSOM Greenville's and technological advancements.

Procedure

a. The IT Director shall be responsible for coordinating USCSOM Greenville's risk analysis. The Director shall identify appropriate persons within the organization to assist with the risk analysis.

b. The risk analysis shall proceed in the following manner:

   i. Document USCSOM Greenville's current information systems.

      a) Update/develop information systems inventory. List the following information for all hardware (i.e., network devices, workstations, printers, scanners, mobile devices) and software (i.e., operating system, various applications, interfaces): date acquired, location, vendor, licenses, maintenance schedule, and function. Update/develop network diagram illustrating how organization's information system network is configured.

      b) Update/develop facility layout showing location of all information systems equipment, power sources, telephone jacks, and other telecommunications equipment, network access points, fire and burglary alarm equipment, and storage for hazardous materials.

      c) For each application identified, identify each licensee (*i.e.,* authorized user) by job title and describe the manner in which authorization is granted.

      d) For each application identified:

i) Describe the data associated with that application.

ii) Determine whether the data is created by the organization or received from a third party. If data is received from a third party, identify that party and the purpose and manner of receipt.

iii) Determine whether the data is maintained within the organization only or transmitted to third parties. If data is transmitted to a third party, identify that party and the purpose and manner of transmission.

iv) Define the criticality of the application and related data as high, medium, or low. Criticality is the degree of impact on the organization if the application and/or related data were unavailable for a period of time.

v) Define the sensitivity of the data as high, medium, or low. Sensitivity is the nature of the data and the harm that could result from a breach of confidentiality or security incident.

vi) For each application identified, identify the various security controls currently in place and locate any written policies and procedures relating to such controls.

e) Identify and document threats to the confidentiality, integrity, and availability (referred to as "threat agents") of data created, received, maintained, or transmitted by USCSOM Greenville. Consider the following:

i) Natural threats, e.g., earthquakes, storm damage.

ii) Environmental threats, e.g., fire and smoke damage, power outage, utility problems.

iii) Human threats

a. Accidental acts, e.g., input errors and omissions, faulty application programming or processing procedures, failure to update/upgrade software/security devices, lack of adequate financial and human resources to support necessary security controls

b. Inappropriate activities, e.g., inappropriate conduct, abuse of privileges or rights, workplace violence, waste of corporate assets, harassment

c. Illegal operations and intentional attacks, e.g., eavesdropping, snooping, fraud, theft, vandalism, sabotage, blackmail

d. External attacks, e.g., malicious cracking, scanning, virus introduction

iv) Identify and document vulnerabilities in USCSOM Greenville's information systems. A vulnerability is a flaw or weakness in security policies and procedures, design, implementation, or controls that could be accidentally triggered or intentionally exploited, resulting in unauthorized access to data, modification of data, denial of service, or repudiation (*i.e.,* the inability to identify the source and hold some person accountable for an action). To accomplish this task, conduct a self-analysis utilizing the standards and implementation specifications to identify vulnerabilities.

f) Determine and document probability and criticality of identified risks.

    i) Assign probability level, i.e., likelihood of a security incident involving identified risk.

        a. "Very Likely" (3) is defined as having a probable chance of occurrence.

        b. "Likely" (2) is defined as having a significant chance of occurrence.

        c. "Not Likely" (1) is defined as a modest or insignificant chance of occurrence.

    ii) Assign criticality level.

        a. "High" (3) is defined as having a catastrophic impact on the medical USCSOM Greenville including a significant number of medical records which may have been lost or compromised.

        b. "Medium" (2) is defined as having a significant impact including a moderate number of medical records within the USCSOM Greenville which may have been lost or compromised.

        c. "Low" (1) is defined as a modest or insignificant impact including the loss or compromise of some medical records.

    iii) Determine risk score for each identified risk. Multiply the probability score and criticality score. Those risks with a higher risk score require more immediate attention.

g) Identify and document appropriate security measures and safeguards to address key vulnerabilities. To accomplish this task, review the vulnerabilities you have identified in relation to the standards and implementation specifications. Focus on those vulnerabilities with high risk scores, as well as specific security measures and safeguards required by the Security Rule.

h) Develop and document an implementation strategy for critical security measures and safeguards.

    i) Determine timeline for implementation.

    ii) Determine costs of such measures and safeguards and secure funding.

    iii) Assign responsibility for implementing specific measures and safeguards to appropriate person(s).

    iv) Make necessary adjustments based on implementation experiences.

v) Document actual completion dates.

i. Evaluate effectiveness of measures and safeguards following implementation and make appropriate adjustments.

c. The IT Director shall be responsible for identifying appropriate times to conduct follow-up evaluations and coordinating such evaluations. The IT Director shall identify appropriate persons within the organization to assist with such evaluations. Such evaluations shall be conducted upon the occurrence of one or more of the following events: changes in the HIPAA Security Regulations; changes in technology, environmental processes, or business processes that may affect HIPAA Security policies or procedures; or the occurrence of a serious security incident. Follow-up evaluations shall include the following:

i. Inspections, reviews, interviews, and analysis to assess adequacy of administrative and physical safeguards. Such evaluation shall include interviews to assess employee compliance; after-hours walk-through inspections to assess physical security, password protection (i.e., not posted), and workstation sessions terminated (i.e., employees logged out); review of latest security policies and procedures for correctness and completeness; and inspection and analysis of training, incident, and media logs for compliance.

ii. Analysis to assess adequacy of controls within the network, operating systems and applications. As appropriate, USCSOM Greenville shall engage outside vendors to evaluate existing physical and technical security measures and make recommendations for improvement.

University of South Carolina School of Medicine Greenville **Policy and Procedure**	
Title: Sanction Policy Security Violations and Disciplinary Action	**P&P #:** IS-4.0
Approval Date: 10/29/2014	**Review: Annual**
Effective Date: 10/29/2014	**Human Resources (TVS001)**

16 Sanction Policy

Policy

It is the policy of the USCSOM Greenville that all workforce members must protect the confidentiality, integrity, and availability of sensitive information at all times. The USCSOM Greenville will impose sanctions, as described below, on any individual who accesses, uses, or discloses sensitive information without proper authorization.

The USCSOM Greenville will take appropriate disciplinary action against employees, contractors, or any individuals who violate the USCSOM Greenville's information security and privacy policies or state, or federal confidentiality laws or regulations, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Purpose

To ensure that there are appropriate sanctions that will be applied to workforce members who violate the requirements of HIPAA, USCSOM Greenville's security policies, Directives, and/or any other state or federal regulatory requirements.

Definitions

Workforce member means employees, students, volunteers, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity. This includes full and part time employees, affiliates, associates, volunteers, and staff from third party entities who provide service to the covered entity.

Sensitive information, includes, but not limited to, the following:

- Protected Health Information (PHI) – Individually identifiable health information that is in any form or media, whether electronic, paper, or oral.
- Electronic Protected Health Information (ePHI) – PHI that is in electronic format.
- Personnel files – Any information related to the hiring and/or employment of any individual who is or was employed by the USCSOM Greenville.
- Payroll data – Any information related to the compensation of an individual during that individuals' employment with the USCSOM Greenville.
- Financial/accounting records – Any records related to the accounting USCSOM Greenville's or financial statements of the USCSOM Greenville.
- Other information that is confidential – Any other information that is sensitive in nature or considered to be confidential.

Availability refers to data or information is accessible and useable upon demand by an authorized person.

Confidentiality refers to data or information is not made available or disclosed to unauthorized persons or processes.
Integrity refers to data or information that have not been altered or destroyed in an unauthorized manner.

Violations
Listed below are the types of violations that require sanctions to be applied. They are stated at levels 1, 2, and 3 depending on the seriousness of the violation.

Level	Description of Violation
1	• Accessing information that you do not need to know to do your job. • Sharing computer access codes (user name & password). • Leaving computer unattended while being able to access sensitive information. • Disclosing sensitive information with unauthorized persons. • Copying sensitive information without authorization. • Changing sensitive information without authorization. • Discussing sensitive information in a public area or in an area where the public could overhear the conversation. • Discussing sensitive information with an unauthorized person. • Failing/refusing to cooperate with the GHS Information Security Office, Chief Information Officer, USCSOM Greenville IT Director and/or authorized designee.
2	• Second occurrence of any Level 1 offense (does not have to be the same offense). • Unauthorized use or disclosure of sensitive information. • Using another person's computer access code (user name & password). • Failing/refusing to comply with a remediation resolution or recommendation.
3	• Third occurrence of any Level 1 offense (does not have to be the same offense). • Second occurrence of any Level 2 offense (does not have to be the same offense). • Obtaining sensitive information under false pretenses. • Using and/or disclosing sensitive information for commercial advantage, personal gain, or malicious harm.

Recommended Disciplinary Actions
In the event that a workforce member violates the USCSOM Greenville's privacy and security policies and/or violates the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or related state laws governing the protection of sensitive and patient identifiable information, the following recommended disciplinary actions will apply.

Violation Level	Recommended Disciplinary Action
1	• Verbal or written reprimand • Retraining on privacy/security awareness • Retraining on the USCSOM Greenville's privacy and security policies • Retraining on the proper use of internal or required forms
2	• Letter of Reprimand*; or suspension • Retraining on privacy/security awareness • Retraining on the USCSOM Greenville's privacy and security policies • Retraining on the proper use of internal or required forms
• 3	• Termination of employment or contract • Civil penalties as provided under HIPAA or other applicable Federal/State/Local law • Criminal penalties as provided under HIPAA or other applicable Federal/State/Local law

•

Important Note: The recommended disciplinary actions are identified in order to provide guidance in policy enforcement and are not meant to be all-inclusive. If formal discipline is deemed necessary, the USCSOM Greenville shall consult with Human Resources prior to taking action. When appropriate, progressive disciplinary action steps shall be followed allowing the employee to correct the behavior which caused the disciplinary action.

*A Letter of Reprimand must be reviewed by Human Resources before given to the employee.

References
U.S. Department of Health and Human Services
Health Information Privacy. Retrieved April 24, 2009, from
http://www.hhs.gov/ocr/privacy/index.html

Related Policies
GHS Information Security Policy

Acknowledgment
I, the undersigned employee or contractor, hereby acknowledges receipt of a copy of the Sanction Policy for USCSOM Greenville.

Dated this ________ day of ___________________, 20____.

____
Signature of Employee/Student/Contractor

University of South Carolina School of Medicine Greenville	**Policy and Procedure**
Title: Reporting and Managing a Privacy Breach Procedure	**P&P #:** IS-6.0
Approval Date: 10/29/2014	**Review: Annual**
Effective Date: 10/29/2014	**Information Technology (TVS025)**

17 Breach Notification Procedures

Purpose
To outline the process for notifying affected individuals of a breach of protected information under the Privacy Act, unsecured protected health information (PHI) for the purposes of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Health Information Technology for Economic and Clinical Health Act (HITECH), and/or state breach notification purposes.

Scope
This applies to all students, faculty, employees, volunteers, and other individuals working under agreements with the USCSOM Greenville.

Definitions

Personal Information – Personal Information has many definitions including definitions by statute which may vary from state to state. Most generally, Personal Information is a combination of data elements which could uniquely identify an individual. Please review applicable state data breach statutes to determine what definition of Personal Information is applicable for purposes of the document.

HIPAA Breach – Unauthorized acquisition, access, use, or disclosure of unsecured PHI.

Personally Identifiable Information (PII) – Information in any form that consists of a combination of an individual's name and one or more of the following: Social Security Number, driver's license or state ID, account numbers, credit card numbers, debit card numbers, personal code, security code, password, personal ID number, photograph, fingerprint, or other information which could be used to identify an individual.

Individually Identifiable Health Information (IIHI) – PII which includes information related to the past, present or future condition, treatment, payment or provision of health care to the identified individual.

Privacy Act Breach – Unauthorized acquisition or reasonable belief of unauthorized acquisition of personal information protected by the Privacy Act. This information includes, but is not limited to Social Security Number, government issued ID numbers, financial account numbers or other information posing a risk of identity theft.

Private Information – Information protected by the Privacy Act, Personally Identifiable Information, Personal Information and Protected Health Information collectively.

Protected Health Information (PHI) – Individually identifiable health information except for education records covered by FERPA and employment records.

Procedure

Reporting a Possible Breach

1. Anyone who becomes aware of a possible breach of privacy involving Private Information in the custody or control of the USCSOM Greenville will immediately inform Integrated Technology.
2. Notification should occur immediately upon discovery of a possible breach, however, in no case should notification occur later than twenty-four (24) hours after discovery.
    a. The supervisor/manager will verify the circumstances of the possible breach and inform the Dean and the division Administrator/Director within twenty-four (24) hours of the initial report.

Containing the Breach

1. The appropriate individuals will take the following steps to limit the scope and effect of the breach.
    a. Work with department(s) to immediately contain the breach. Examples include, but are not limited to:
        i. Stopping the unauthorized access
        ii. Recovering the records, if possible
        iii. Shutting down the system that was breached
        iv. Mitigating the breach, if possible
        v. Correcting weaknesses in security
        vi. Notifying the appropriate authorities including the local Police Department if the breach involves, or may involve, any criminal activity

Investigating and Evaluating the Risks Associated with the Breach

1. To determine what other steps are immediately necessary, the appropriate individuals in collaboration with the USCSOM Greenville's Legal Counsel and affected department(s) and administration, will investigate the circumstances of the breach.
    a. A team will review the results of the investigation to determine root cause(s), evaluate risks, and develop a resolution plan.
    b. The appropriate individuals, in collaboration with the USCSOM Greenville's Legal Counsel, will consider several factors in determining whether to notify individuals affected by the breach including, but not limited to:
        i. Contractual obligations
        ii. Legal obligations – the USCSOM Greenville's Legal Counsel should complete a separate legal assessment of the potential breach and provide the results of the assessment
        iii. Risk of identity theft or fraud because of the type of information lost such as social security number, banking information, identification numbers
        iv. Risk of physical harm if the loss puts an individual at risk of stalking or harassment
        v. Risk of hurt, humiliation, or damage to reputation when the information includes medical or disciplinary records
        vi. Number of individuals affected

Notification

1. The USCSOM Greenville IT department will work with the department(s) involved, the USCSOM Greenville's Legal Counsel and appropriate leadership to decide the best approach for notification and to determine what may be required by law.
2. If required by law, notification of individuals affected by the breach will occur as soon as possible following the breach.
    a. Affected individuals must be notified without reasonable delay, but in no case later than sixty (60) calendar days after discovery, unless instructed otherwise by law enforcement or other applicable state or local laws.
        i. Notices must be in plain language and include basic information, including:
            1. What happened
            2. Types of PHI involved
            3. Steps individuals should take
            4. Steps covered entity is taking
            5. Contact Information
        ii. Notices should be sent by first-class mail or if individual agrees electronic mail. If insufficient or out-of-date contact information is available, then a substitute notice is required as specified below.
    b. If law enforcement authorities have been contacted, those authorities will assist in determining whether notification may be delayed in order not to impede a criminal investigation.
3. The required elements of notification vary depending on the type of breach and which law is implicated. As a result, the USCSOM Greenville's IT Director and Legal Counsel should work closely to draft any notification that is distributed.
4. Indirect notification such as website information, posted notices, media will generally occur only where direct notification could cause further harm, or contact information is lacking.
    a. If a breach affects five-hundred (500) or more individuals, or contact information is insufficient, the USCSOM Greenville will notify a prominent media outlet that is appropriate for the size of the location with affected individuals, and notice will be provided in the form of a press release.
5. Using multiple methods of notification in certain cases may be the most effective approach.

Business associates must notify the USCSOM Greenville if they incur or discover a breach of unsecured PHI.

1. Notices must be provided without reasonable delay and in no case later than sixty (60) days after discovery of the breach.
2. Business associates must cooperate with the USCSOM Greenville in investigating and mitigating the breach.

Notice to Health and Human Services (HHS) as required by HIPAA – If the USCSOM Greenville's Legal Counsel determines that HIPAA notification is not required; this notice is also not required.

1. Information regarding breaches involving five-hundred (500) or more individuals, regardless of location, must be submitted to HHS at the same time that notices to individuals are issued.
2. If a breach involves fewer than five-hundred (500) individuals, the USCSOM Greenville will be required to keep track of all breaches and to notify HHS within sixty (60) days after the end of the calendar year.

Prevention

1. Once immediate steps are taken to mitigate the risks associated with the breach, the IT Director will investigate the cause of the breach.
    a. If necessary, this will include a security audit of physical, organizational, and technological measures.
    b. This may also include a review of any mitigating steps taken.
2. The IT Director will assist the responsible department to put into effect adequate safeguards against further breaches.
3. Procedures will be reviewed and updated to reflect the lessons learned from the investigation and regularly thereafter.
4. The resulting plan will also include audit recommendations, if appropriate.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing these procedures. Employees who violate these procedures are subject to discipline up to and including termination in accordance with the USCSOM Greenville's Sanction Policy.