

	<b>Technology Management Services</b>	
	<b>Name:</b>	<b>E-mail Policy</b>
	<b>Start Date:</b>	<b>01/01/1996</b>
	<b>Approval Date:</b>	<b>3/29/2017</b>
	<b>Approved By:</b>	<b>Kyle Peoples</b>

## E-mail Policy

### **Purpose:**

To protect the integrity and functioning of the SMCS (Springfield Medical Care Systems) email system. The SMCS email system is an operational and business resource. There is a level of responsibility that all users need to maintain. Inappropriate use can compromise the system's integrity, availability and compliance with applicable laws. This policy is designed to clarify the use, ownership, confidentiality, security, eligibility and account management of the system.

### **Scope:**

This policy establishes requirements for SMCS employees, students and volunteers.

### **Policy:**

The SMCS email system will be managed by the Technology Management Services Department (TMS) to ensure that there is a level of access control for the system which is commensurate with the sensitivity and criticality of the system and the Organizational Data contained within it, and to ensure that inappropriate use does not compromise the system's integrity and availability.

### **Responsibilities:**

#### **Compliance:**

Electronic mail (E-mail) system customers must comply with all Springfield Medical Care Systems' conduct and confidentiality policies as they apply to the e-mail environment. Non-compliance with any of these policies may result in termination of your e-mail account as well as any penalties defined by other institutional policies.

#### **Ownership:**

SMCS is the sole owner of the e-mail system. The data files therein, are the sole property of the institution, and may be viewed by Administration if deemed necessary. Users should have no expectation of privacy. Users do not own or have rights to files outside of day to day business use. All Springfield Medical Care Systems employees and Springfield Hospital employees are required to use the e-mail system provided to them by SMCS.

#### **Email Use:**

The SMCS email system is for business related use only and should not be used for purposes of solicitation. Employees may not send mass mailings to all

employees or to large groups of employees without approval from their department manager. Users should delete chain and junk email messages without forwarding or replying to them. Electronic chain letters and other forms of non-business related mass mailings are prohibited. It is a violation of policy to use the email system for the generation of personal income or to initiate unsolicited mass mailings.

Appropriate use of the email system should be followed. It is a violation of this policy to send fraudulent, obscene, or harassing email to anyone.

Do not send patient identifiable information via e-mail to any non-SMCS affiliated provider and/or entity. Additionally, you can only transmit patient/employee information via e-mail, internally, if you have the consent of your department manager and it is related to your job specific duties. Only authorized employees that have the proper consent to send patient information via the ZixCorp Encryption system may send confidential patient information. See attached email encryption procedure.

Users should not use personal texting accounts to send sensitive information, PHI, or other SMCS business information.

Users should not forward email containing sensitive information or protected health information (PHI) to public email systems such as Hotmail.com, gmail.com, or other public email system services. In addition, users should not forward to their personal email accounts. Personal email accounts should not be used for official SMCS business.

Users should delete suspicious email that they are not expecting. They may contain viruses or malware. Never not open attached files or web links unless you are certain the email is from a legitimate source.

E-mail may be inadvertently sent to unauthorized recipients at the touch of a button. Exercise every caution in making sure that the e-mail transmittal is addressed to the right party and only to that party.

Delete all large or outdated messages. The e-mail system has physical limits on the amount of messages that can be stored on the server's hard drive. All large messages should be saved to your personal computer's hard drive and then deleted. Normally you can cut your storage- requirements in half by removing the largest 5% of your files.

Please use the email signature feature to include your name, title, organization name and phone number as a signature at the bottom of every email sent.

Users are responsible for reporting any suspected or confirmed violations of this policy to their department manager or the Corporate Compliance Officer.

Contact the Help Desk at 885-7635 or the Director of Technology Management Services at 885-7638 if you have any questions concerning this policy.

### **Account Deletion:**

The e-mail account will be disabled upon termination of employment or non-compliance with e-mail policy. The e-mail of terminated employees is subject to review by the Director of Human Resources, Chief Compliance Officer, Security Officer and/or CEO.

**Enforcement:**

Any user found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or assignment, depending on the severity of the infraction. In addition, SMCS may report the matter to civil and criminal authorities as may be required by law.