	Lower Providence Emergency Medical Service Standard Operating Guidelines	
	Subject: *Administration*- Station Computer & Information Systems	**SOG #100-007** **Initiated:** July 2023
	Approved: Chief Christopher J. Reynolds	**Revised:** N/A

Description: This process provides the guidelines for appropriate use of LPEMS computer equipment.

Purpose: LPEMS is presented with many concerns with the increasing use of computers, and the computer network(s) which allow member access to almost an unlimited amount of information/data in the workplace. These concerns can be effectively addressed through the following process, which establishes rules governing member use of computers. This process includes, but is not limited to, any computer, e-mail, and/or Internet service that is provided by LPEMS and/or is accessed on or from any organization computer.

Procedure:

Use and Ownership of Computer Equipment

a. All data created or recorded using any computer equipment owned, controlled, or used for the benefit of Lower Providence Emergency Medical Service is always the property of Lower Providence Emergency Medical Service. Due to the need to protect the Lower Providence Emergency Medical Service computer network, the company cannot guarantee the confidentiality of information stored on any network device belonging to LPEMS, except that it will take all steps necessary to secure the privacy of all protected health information in accordance with all applicable laws.

b. Members are responsible for exercising good judgment regarding the reasonableness of personal use and must follow operational guidelines for personal use of Internet/Intranet/Extranet systems and any computer equipment.

c. At no time may any pornographic or sexually offensive materials be viewed, downloaded, saved, or forwarded using any LPEMS computer equipment or Internet Service.

i. Refer to Member Handbook Section on Preventing Sexual and Other Harassment for further information.

d. For security and network maintenance purposes, authorized individuals within Lower Providence Emergency Medical Service may monitor equipment, systems, and network traffic at any time, to ensure compliance with all procedures.

Security and Proprietary Information

a. Confidential information should be always protected, regardless of the medium by which it is stored. Examples of confidential information include but are not limited to: individually identifiable health information concerning patients, company financial and business information, patient lists and reports, and research data. Members should take all necessary steps to prevent unauthorized access to this information.

b. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly, and user level passwords should be changed every 30 days.

c. All PCs, laptops, workstations, and remote devices should be secured with a password-protected screensaver, wherever possible, and set to deactivate after being left unattended for 10 minutes or more, or by logging-off when the equipment will be unattended for an extended period.

d. All computer equipment used by staff, whether owned by the individual staff member or LPEMS, shall regularly run approved virus-scanning software with a current virus database in accordance with this procedure.

e. Staff members must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses.

Unacceptable Use

a. Under no circumstances is a member of Lower Providence Emergency Medical Service authorized to engage in any activity that is illegal under local, state, or federal law while utilizing Lower Providence Emergency Medical Service computer resources.

b. The lists below are by no means exhaustive but attempt to provide a framework for activities that fall into the category of unacceptable use.

System and Network Activities

a. The following activities are strictly prohibited, with no exceptions:

i. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Lower Providence Emergency Medical Service.

ii. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Lower Providence Emergency Medical Service or the end user does not have an active license is strictly prohibited.

iii. Exporting system or other computer software is strictly prohibited and may only be done with express permission of management.

iv. Introduction of malicious programs into the network or server (e.g., viruses, etc.).

v. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

vi. Using a Lower Providence Emergency Medical Service computer device to actively engage in procuring or transmitting material that is in violation of the Company's prohibition on sexual and other harassment.

vii. Making fraudulent statements or transmitting fraudulent information when dealing with patient or billing information and documentation, accounts, or other patient information, including the facsimile or electronic transmission of patient care reports and billing reports and claims.

viii. Causing security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the member is not an intended recipient or logging into a server or account that the member is not expressly authorized to access, unless these duties are within the scope of regular duties.

ix. Providing information about, or lists of, Lower Providence Emergency Medical Service members or patients to parties outside LPEMS.

E-mail and Communications Activities

i. Sending unsolicited e-mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (e-mail spam).

ii. Any form of harassment via e-mail, telephone, or paging, whether through language, frequency, or size of messages.

iii. Unauthorized use, or forging, of e-mail header information.

iv. Solicitation of e-mail for any other e-mail address, other than that of the poster's account, with the intent to harass or to collect replies.

v. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

vi. Use of unsolicited e-mail originating from within Lower Providence Emergency Medical Service networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Lower Providence Emergency Medical Service or connected via Lower Providence Emergency Medical Service's network.

Use of Remote Devices

i. The appropriate use of Laptop Computers, Personal Digital Assistants (PDAs), and remote data entry devices is of utmost concern to Lower Providence Emergency Medical Service. These devices, collectively referred to as "remote devices" pose a unique and significant patient privacy risk because they may contain confidential patient, member or company information and these devices can be easily misplaced, lost, stolen, or accessed by unauthorized individuals.

ii. Remote devices will not be purchased or used without prior approval of LPEMS Executive Director.

iii. Management must approve the installation and use of any software used on the remote device.

iv. Remote devices containing confidential or patient information must not be left unattended.

v. If confidential or patient information is stored on a remote device, access controls must be employed to protect improper access. This includes, where possible, the use of passwords and other security mechanisms.

vi. Remote devices should be configured to automatically power off following a maximum of 10 minutes of inactivity.

vii. Remote device users will not permit anyone else, including but not limited to user's family and/or associates, patients, patient families, or unauthorized members, to use company-owned remote devices for any purpose.

viii. Users of company-owned remote devices will immediately report the loss of a remote device to Management.