Purpose:

West Des Moines EMS is committed to protecting our staff members, the patients we serve and the City of West Des Moines from illegal or damaging actions by individuals and the improper release of protected health information and other confidential or proprietary information.

The purpose of this policy is to outline the acceptable use of computer equipment at WDMEMS. These rules are in place to protect the employee and patients of WDMEMS. Inappropriate use, exposes WDMEMS to risks including virus attacks, compromise of network systems and services, breach of patient confidentiality and other legal claims.

Scope:

This policy applies to employees, volunteers, contractors, consultants, temporary employees, students, and others at WDMEMS who have access to computer equipment, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by WDMEMS.

Procedure:

Use and Ownership of Computer Equipment.

1. All data created or recorded using any computer equipment owned, controlled or used for the benefit of WDMEMS is at all times the property of WDMEMS. Because of the need to protect the WDMEMS computer network, the company cannot guarantee the confidentiality of information stored on any network device belonging to WDMEMS,
except that it will take all steps necessary to secure the privacy of all protected health information in accordance with all applicable laws.

2. Staff 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.

3. At no time may any pornographic or sexually offensive materials be viewed, downloaded, saved, or forwarded using any Company computer equipment.

4. For security and network maintenance purposes, authorized individuals within WDMEMS may monitor equipment, systems and network traffic at any time, to ensure compliance with all West Des Moines policies.

Security and Proprietary Information

1. Confidential information should be protected at all times, 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, WDMEMS financial and business information, patient lists and reports, and research data. Staff members should take all necessary steps to prevent unauthorized access to this information.

2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.

3. 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.

4. All computer equipment used by staff, whether owned by the individual staff member or WDMEMS, shall regularly run approved virus-scanning software with a current virus database in accordance with company policy.

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

Unacceptable Use

1. Under no circumstances is a staff member of WDMEMS authorized to engage in any activity that is illegal under local, state, or federal law while utilizing West Des Moines computer resources.

2. 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

The following activities are strictly prohibited, with no exceptions:

1. 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 WDMEMS.

2. 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 WDMEMS or the end user does not have an active license is strictly prohibited.

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

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

5. 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.

6. Using an WDMEMS computer device to actively engage in procuring or transmitting material that is in violation of the Company’s prohibition on sexual and other harassment.

7. 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.

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

9. Providing information about, or lists of, WDMEMS staff members or patients to parties outside WDMEMS.

E-mail and Communications Activities

1. 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).

2. Any form of harassment via e-mail, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of e-mail header information.

4. 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.

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

6. Use of unsolicited e-mail originating from within West Des Moines’s networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by West Des Moines or connected via West Des Moines’s network.

Use of Remote Devices

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

1. Remote devices will not be purchased or used without prior West Des Moines E.M.S. approval.

2. West Des Moines E.M.S. must approve the installation and use of any software used on the remote device.

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

4. 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.

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

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

7. Remote device users will not install any software onto any PDA owned by Dallas County and/or WDMEMS except as authorized by the City of West Des Moines.

8. Users of West Des Moines -owned remote devices will immediately report the loss of a remote device to a supervisor or the Privacy Officer.