Use of Computer and Information Systems and Equipment

Board Approval: R M Kelley, Chairman Date: 4/26/16

1) Purpose

a) JCESA is committed to protecting our employees, the patients we serve and the company from illegal or damaging actions by individuals and the improper release of protected health information and other confidential or proprietary information.

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

2) Scope

This policy applies to employees, volunteers, contractors, consultants, temporary employees, students, and others at JCESA 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 JCESA.

3) Procedure

a) Use and Ownership of Computer Equipment

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

ii) Employees 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.

iii) At no time may any pornographic or sexually offensive materials be viewed, downloaded, saved, or forwarded using any JCESA computer equipment. Please refer to the JCESA Workplace Harassment Policy 1450 for further information.

iv) For security and network maintenance purposes, authorized individuals within JCESA may monitor equipment, systems and network traffic at any time, to ensure compliance with all Agency policies.

b) Security and Proprietary Information

i) 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, company financial and business information, patient lists and reports, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.

ii) 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.

iii) 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.

iv) All computer equipment used by employees, whether owned by the individual employee or JCESA, shall regularly run approved virus-scanning software with a current virus database in accordance with agency policy.

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

c) Unacceptable Use

i) Under no circumstances is an employee of JCESA authorized to engage in any activity that is illegal under local, state, or federal law while utilizing JCESA computer resources.

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

d) System and Network Activities

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 JCESA.

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 JCESA 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, worms, 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 JCESA computer device to actively engage in procuring or transmitting material that is in violation of the Agency'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 employee 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.

ix) Providing information about, or lists of, JCESA Employees or patients to parties outside JCESA.

e) 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 JCESA's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by JCESA or connected via JCESA's network.

f) Use of Remote Devices

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

i) Remote devices will not be purchased or used without prior Agency approval.

ii) The Agency must approve the installation and use of any software used on the remote device.

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

iv) 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.

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

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

vii) Remote device users will not install any software onto any PDA owned by JCESA except as authorized by the Agency.

viii) Users of agency-owned remote devices will immediately report the loss of a remote device to the on duty officer.

g) Enforcement

i) Any Employees found to have violated this policy may be subject to disciplinary action, up to and including suspension and termination.