CRYSTAL RUN HEALTHCARE LLP

Policy / Procedure

MANUAL: ADMINISTRATIVE
SECTION: Information Management - Information Technology

<table>
<tr><td colspan="2">POLICY STATEMENT: Technology Acceptable Use</td></tr>
<tr><td>IMPLEMENTATION: 01/1/06</td><td rowspan="4">CONCURRENCES:
All Departments</td></tr>
<tr><td>REVIEWS:</td></tr>
<tr><td>REVISIONS: 02/09/2010</td></tr>
<tr><td>INITIATOR:
Director of Information Technology</td></tr>
<tr><td colspan="2">APPROVAL: Chief Operating Officer / Chief Medical Officer</td></tr>
</table>

PURPOSE:

To outline the acceptable use of computer equipment, Internet access, e-mail, and other Information Technology (IT) at Crystal Run Healthcare

These rules are in place to protect the employees and Crystal Run Healthcare. Inappropriate use exposes Crystal Run Healthcare to risks including virus attacks, compromise of network systems and services, and possible legal issues.

PROCEDURE:

This policy applies to employees, contractors, consultants, temporaries, vendors, and other workers at Crystal Run Healthcare, including all personnel affiliated with third parties. This policy applies to all equipment that connects to Crystal Run Healthcare's internal networks.

General Use and Ownership:

1. Users should be aware that the data they create on the practice systems remains the property of Crystal Run Healthcare.

2. Crystal Run Healthcare reserves the right to audit networks and systems (including data/internet usage/email usage /etc.) on a periodic basis to ensure compliance with this policy.

3. All personnel who use the practice's systems have an obligation to use the systems in a manner that is appropriate, effective and efficient for official business only use. Personnel must be aware that workstations display sensitive and confidential information for the purpose of patient healthcare and transacting business. Therefore all personnel must use discretion and apply security measures while performing day to day activities.

Security and Proprietary Information:

1. Employees should take all necessary steps to prevent unauthorized access to Protected Health Information (PHI) information.

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

3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by locking out user account when the system is unattended for 10 minutes.
   NOTE: A locked machine can only be unlocked by the user or a System Administrator (IT Staff).

4. Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the *"Portable Device Security Tips"* (See Attachment A).

5. Under no circumstances is an employee of Crystal Run Healthcare authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Crystal Run Healthcare-owned resources.

Internet and E-mail Usage

1. Crystal Run Healthcare's Internet access and email systems shall not be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, national origin, or that may be in violation of the sexual harassment or hostile workplace laws. Employees who receive any emails or website links with this content from any Crystal Run Healthcare employee or external entity should report the matter to their supervisor immediately.

2. Using Crystal Run Healthcare's Internet access or email system for personal and/or non-work related purposes is not an acceptable practice and is prohibited. Sending chain letters, jokes or any other frivolous misuse of email from a Crystal Run Healthcare email account is prohibited.

3. Crystal Run Healthcare employees shall have **no expectation of privacy** in anything they store, send or receive on the organizations Internet access or email systems. Crystal Run Healthcare will monitor Internet usage and email communication without prior notice.

4. Broadcasting of e-mail to multiple Distribution Lists or more than 10 employees is prohibited without prior authorization. If an employee requires information to be disseminated throughout a department they must receive prior approval from the departments Manager.

5. For e-mail distribution to multiple departments, or to Distribution Lists such as "Physicians, Providers, Alert Broadcast or any other organization wide email Distribution Lists, explicit permission is required. Authorization of these types of emails requires employees to send a draft to the Distribution List **Broadcast E-mail Request** for review.

   If the content is approved, it will be emailed by designated individuals with the appropriate authority.

6. Upon termination/resignation of any Crystal Run Healthcare employee, the Information Technology Department will terminate all email privileges of such employee.

7. Upon termination/resignation of any Crystal Run Healthcare employee, archiving of the employee's mailbox must be requested by the department Director or by the request of the Human Resources Department.

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 Crystal Run Healthcare (e.g. Instant Messaging, MP3 Rippers, USB jump drives, Digital Music, Music Streaming etc).

2. Personal software installation and usage onto Crystal Run Healthcare equipment is prohibited. The use of USB portable storage devices to introduce or remove data from Crystal Run Healthcare equipment is prohibited.

3. Authorized users are prohibited from sharing or revealing their passwords or user accounts with others. This includes family and other household members when work is being done at home.

4. Making fraudulent offers of products, items, or services originating from any Crystal Run Healthcare account.

5. Providing information about, or lists of, Crystal Run Healthcare employees to parties outside Crystal Run Healthcare.

6. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals on the Crystal Run Healthcare messaging system (email spam).

7. Creating or forwarding "chain letters" of any type.

8. Using Crystal Run Healthcare's Internet and Email Services for personal use or in a manner that is inappropriate, is not acceptable and is prohibited.

9. Only equipment authorized by IT Management shall be utilized on Crystal Run Healthcare's infrastructure.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

REFERENCES:

CROSS REFERENCES:

ATTACHMENT:

Attachment A: Portable Device Security Tips

Acceptable Use Attachment A: Portable Device Security Tips

Portable Device Security Tips

- Do not store information such password, pins numbers patient health information or any other type of sensitive information on notebook computers or PDA'S as these devices are high risk for theft.
- Password protect all portable devices.
- While using portable devices, if there is a need to leave the device to perform other duties, lock or enable a password protected screen saver.
- Do not leave portable devices in unsecured areas.
- Do not leave portable devices in a locked or unlocked car, unlocked offices or desks.
- Do not leave portable devices in high volume patient areas, keep close proximity or carry the device with you.
- Crystal Run Healthcare's owned equipment while not in use should be stored in a secure area.
- Use caution when utilizing public Internet Access Points or "Hot Spots" as these public services are usually not secure and are a common ground for hacker and security breeches.
- Utilizing Internet services that is in a manner deemed inappropriate by the guidelines that Crystal Run Healthcare has put in place even outside the practice is strictly prohibited.
- Failure to comply with Crystal Run Healthcare's usage policies, introduces risk and potential security threats or breeches to the practice's network infrastructure. Compliance Policies and Procedures must be followed while using the practice's owned equipment.
- If personnel feel that their portable device or password has been compromised in any way please contact the Information Technology department immediately.
- Please report all thefts to the Human Resources department.