ELLIOT
HEALTH SYSTEM

Summary of Policies on Appropriate Use of Information Systems

Applicability

These policies apply to all persons who use the computer systems and network of Elliot Health System, including but not limited to employees, contractors, students and volunteers. (These persons are collectively referred to herein as "Users".)

Use for Business Purposes

The computers, network, Internet connections, software applications and electronic mail systems (collectively referred to as "computer systems") made available to Users are intended for use to support the business of EHS and to help Users do their work.

Incidental personal use of our computer systems is permissible so long as: (a) it does not consume more than a trivial amount of resources, (b) does not affect User productivity, and (c) does not interfere with any business activity.

Confidential Information

Our information systems include confidential information, including proprietary information, personnel records, and individually identifiable health information. We have a legal and ethical obligation to safeguard the privacy of that information.

Users are required to follow the Privacy and Security Policies and Procedures of EHS with regard to their use and disclosure of confidential information.

Users are not permitted to seek access to confidential information if access to that information is not required to enable the user to perform his or her work for EHS.

Use of Computer System

Users will be authorized to access our computer system and records stored on that system to the extent necessary to enable them to perform their work.

Authentication of User Identity

Each person authorized to use our computer systems will be issued a user identity. User identities are confidential, and should not be shared with other people.

In almost all circumstances, when Users log onto our computer system, they will be asked to enter a User Identity.

Passwords and password management

Users are expected to follow these guidelines when creating passwords when technically feasible:

- Passwords must be at least 6 characters in length.
- Mix letters with numbers and symbols if possible.
- Avoid use of words.
- Avoid use of names of family members, pets, favorite sports teams or other obvious passwords.
- Never use the word "password" as your password.

Consider use of a Passphrase. Make up a sentence, then use the first letter of each word in the sentence to create your password. For example:

Next Winter I'm Going To Hawaii To Golf = NWIG2H2G

Passwords are confidential. They should not be shared with other people.

Passwords should not be written down and left in obvious places, such as under a keyboard, on a "sticky" note on a monitor, on a blotter, etc.

Passwords must be changed every ninety days. Users will not be allowed to switch back and forth between two or three passwords.

Automatic logoff

Where possible, our computer system will automatically logoff users whose identity and right of access cannot be authenticated. Users who have difficulty logging onto the computer system should report the problem to the Information Services help desk at extension 2800.

Where possible and appropriate, users will be logged off the computer system if they are inactive for thirty minutes.

Access Control

Permission for individual access to protected health information will be based on the work each person performs and the records the person needs to perform that work. An individual's user identity and password will determine their access to records.

Workstation Use

EHS will determine the hardware and software to be installed on each workstation, including portable computers. Users are not permitted to install additional hardware or software without the permission from the Information Services and Technology Department. This includes free software or shareware downloaded from the Internet.

Patches

The Information Services and Technology Department will download and install patches to update operating system and application software to reduce security risks. Users are encouraged to install current security patches to any portable computer or home computer used for business purposes.

Protection against Malicious Software

All computers provided by EHS are installed with software tools to reduce the security risks caused by malicious software, including computer viruses, Trojan horses, spyware, etc. All anti-virus software definitions must be kept current. Any portable computer or home computer used for business purposes are encouraged to have anti-virus protection software, and kept updated for current virus definitions.

Firewalls

The EHS computer system includes firewalls and intrusion detection software to prevent access by unauthorized persons. In addition, EHS utilizes web filtering software to prevent access to sites deemed inappropriate or harmful. Portable computers and home computers used for business purposes are encouraged to use personal firewalls and other commercially available security products to reduce the risks of unauthorized access.

Reporting security incidents

Users must report any suspicious, unauthorized or malicious activity that might affect the security of the computer system or the confidentiality, availability or integrity of confidential information to the EHS Compliance Department or Information Services and Technology Department as soon as it is discovered.

Disposal of electronic media

All computers that are the property of EHS will be disposed of by ITSG and the data stored on these devices will be erased using software tools designed for this specific purpose. PDA, floppy disk, CD-R, CD-RW, tape or other electronic media used to store confidential information must be either physically destroyed or “wiped clean” in accordance with EHS security policies.

Equipment control (into and out of site)

Users must “sign-out” any computer equipment they wish to remove from the operating locations of EHS.

Users should not connect any non-EHS provided computer or network equipment(hubs, switches, wireless access points, etc.) to the Elliot network for any reason.

Electronic Mail Policy

Users have an obligation to use e-mail appropriately, effectively, and efficiently.

Users should not share their electronic mail identity and password with anyone else.

Electronic mail can be forwarded, intercepted, printed and stored by others. Users must use even greater discretion with regard to the information that they include in electronic mail than they apply to written documents.

Any electronic mail message sent outside EHS that includes any information that could be used to identify an individual as a patient, or any information about the health or well being of a patient must be encrypted.

Any electronic mail message that includes confidential information should include a subject header or “flag” to indicate that the communication is personal and confidential.

All messages originated or transported within or received into EHS’s electronic mail system are the property of EHS.

Users should have no expectation of privacy relating to their use of our e-mail system. EHS reserves the right to access the electronic mail system and to read any User’s electronic mail to ensure that it is being used for legitimate business purposes.

Most electronic mail messages are temporary communications, which are non-vital and may be discarded routinely. Messages that may be important to the treatment of an individual patient or the operation of EHS’s business should be retained in accordance with practices that apply to paper records. Any such electronic mail pertaining to an individual receiving services from EHS should be filed in the individual’s electronic or paper clinical record.

Use of electronic mail to communicate with patients may improve communications and help in treatment. Due to the inherent risks involved in electronic communications, patients who wish to communicate by e-mail should be informed of the following:

- E-mail is not appropriate for emergencies or time-sensitive issues.
- Highly sensitive or personal information should not be communicated via e-mail unless the communication is encrypted.
- Any electronic mail from EHS that includes protected health information will be encrypted.
- Staff other than the clinical professional treating the individual may read and process the mail.
- No one can guarantee the security and privacy of e-mail messages.
- Any e-mail message from a patient must include (1) the category of the communication in the subject line, i.e., prescription refill, appointment request, etc., and (2) clear patient identification including patient name, telephone number and patient identification number in the body of the message.

Internet Access

Users may access the Internet through EHS’s network. Except for incidental personal use, access to the Internet should be primarily for EHS business purposes. Users should not access the Internet using dial-up modems, except as authorized by the Information technology Department.

Remote Access Policy

EHS will allow a limited number of Users the right to access the computer system from remote locations. Remote access rights must be approved by User's supervisor and the Security Officer.

In order to ensure the security of our computer system and safeguard confidential information, the following policies apply:

Access to the EHS computer system from outside of its defined network perimeter must be controlled by Virtual Private Network (VPN) or RAS technology in accordance with organization Security Policies. The System Administrator will work with persons authorized to access the system remotely to set up a VPN or authorized RAS connection.

Persons authorized to work at home or otherwise have remote access to EHS's computer system are encouraged to install and maintain current definitions on anti-virus software, update software patches, and install intrusion detection software on computers used for those purposes.

Prohibited Uses of EHS Computer System

Users are expressly prohibited from using EHS's computer systems for any of the following purposes:

- Copying or transmission of any document, software or other intellectual property protected by copyright, patent or trademark law, without proper authorization by the owner of the intellectual property.

- Engaging in any communication that is threatening, defamatory, obscene, offensive, or harassing.

- Political activities including sending political messages and solicitation of funds.

- Gambling.

- Viewing, downloading, or exchanging pornography.

- Illegal activities of any kind.

- Disclosure of protected health information in a manner inconsistent with our Privacy Policies and Procedures.

- Use of e-mail addresses for marketing purposes without explicit permission from the target recipient.

- Forwarding of e-mail from in-house or outside legal counsel, or the contents of that mail, to individuals outside of the company without the express authorization of counsel.

- Misrepresenting, obscuring, suppressing, or replacing a user's identity on an electronic communication.

- Obtaining access to the files or communications of others with no substantial company business purpose.

- Attempting unauthorized access to data or attempting to breach any security measure on any electronic communication system, or attempting to intercept any electronic communication transmissions without proper authorization.

Enforcement

Employees of EHS who violate any part of this policy are subject to disciplinary action up to and including dismissal.

EHS reserves the right to immediately terminate for cause any contract or business relationship with any User who violates any part of this policy.

EHS will report to appropriate authorities any violation of this policy that is a violation of the law.

Questions about this Policy

Questions about this policy for use of information systems should be directed to:

Information Technology Customer Service Center at 603-663-2800, or
Corporate Compliance Department at 663-2970

Policy Approval and Acceptance

This policy is effective as of April 20, 2005.

I have read this Summary of Elliot Health System’s Policy on Appropriate Use of Information Systems and agree to abide by its terms.

____