IT Security Rules of Behavior

The Cook County Health & Hospitals System's Information Technology (IT) Security Rules of Behavior are a guide to **all** Cook County Health & Hospitals System (CCHHS) personnel, including officers, directors, members of committees with Board-delegated authority, employees, and members of the CCHHS medical staff or house staff, researchers, students and agency personnel with access to any CCHHS IT resources. This policy also affects independent contractors, consultants and other business partners (vendors) who are not employees but are working at CCHHS.

Use the Rules of Behavior as a guide and as a reminder to uphold

- Honest and ethical behavior,
- Compliance with applicable laws, regulations, and system policies, and
- Your responsibilities, as an important part of the CCHHS team.

Compliance with the CCHHS IT Security Rules of Behavior is required.

A. ACCEPTABLE USE

1. I shall:
   a. Ensure that software, including downloaded software, is properly licensed, free of malicious code, and authorized before installing and using it on CCHHS systems;
   b. Log-off or lock systems when leaving them unattended;
   c. Sanitize or securely destroy electronic media and papers that contain sensitive data when no longer needed, or as otherwise directed by management;
   d. Only access sensitive information necessary to perform job functions (i.e., need to know);
   e. Protect CCHHS information assets (CCHHS assets include but are not limited to hardware, software, and EPHI records) from unauthorized access, use, modification, destruction, theft, or disclosure and shall treat such assets in accordance with any information handling policies;
   f. Immediately report to the Information Security Officer (ISO) all: lost or stolen CCHHS equipment; known or suspected security incidents; known or suspected information security policy violations or compromises; or suspicious activity in accordance with CCHHS policies and procedures.
2. I shall not:
   a. Use another person's account, identity, or password;
   b. Access or Use sensitive information for anything other than the purpose for which it has been authorized;
   c. Violate, direct, or encourage others to violate CCHHS policies or procedures;
   d. Circumvent security safeguards including violating security policies or procedures or reconfigure systems except as authorized (i.e., violation of least privilege);
   e. Remove computers or equipment from the CCHHS premises without proper authorization;
   f. Store sensitive information in public folders or other insecure physical or electronic storage locations;
   g. Share or disclose sensitive information except as authorized and with formal agreements that ensure third parties will adequately protect it;
   h. Transport, transmit, email, remotely access, or download sensitive information unless such action is explicitly permitted by the manager or owner of such information and appropriate safeguards are in place per CCHHS policies concerning sensitive information;
   i. Store sensitive information on mobile devices such as laptops, personal digital assistants (PDAs), iPADs, universal serial bus (USB) drives, or on remote/home systems without authorization and/or appropriate safeguards (i.e., CCHHS approved encryption);
   j. Knowingly or willingly conceal, remove, mutilate, obliterate, falsify, or destroy information for personal use for myself or others;
   k. Copy or distribute intellectual property—including music, software, documentation, and other copyrighted materials—without permission or license from the copyright owner;
   l. Modify or install software without prior management approval;
   m. Load unapproved software from unauthorized sources on Department systems or networks;
   n. Use a personal email system (i.e., Gmail, Yahoo, Hotmail) to transmit sensitive information; and
   o. Use systems without the protections advised by the CCHHS HIS IT department.

IT Security Rules of Behavior

B. PERSONAL AND INCIDENTAL USE

1. Personal use of CCHHS Information Technology resources is discouraged.
2. As a convenience to CCHHS user community, incidental use of information resources is permitted. Only brief and occasional use is considered to be incidental.
3. CCHHS provided computer equipment is not intended to be used as a backup or storage device for personal use. This includes, but is not limited to files, pictures, videos or other digitally stored information or data.
4. The following are prohibited:
   a. Unethical or illegal conduct;
   b. Sending or posting obscene or offensive material in messages or forums;
   c. Sending or forwarding chain letters, email spam, inappropriate messages, or unapproved newsletters and broadcast messages;
   d. Sending messages supporting political activity restricted under the Hatch Act;
   e. Conducting any commercial or "for-profit" activity;
   f. Creating and/or operating unapproved Web sites;
   g. Incurring more than minimal additional expense, such as using non-trivial amounts of storage space or bandwidth for personal files or photos;
   h. Using the Internet or CCHHS workstation to play games, visit chat rooms, or gamble.

C. PASSWORDS

   a. Are complex, and contain a minimum of eight alphanumeric characters and at least one uppercase and one lowercase letter, one number, and one special character;
   b. Do not contain or consist of common words, names, or user IDs;
   c. Are changed immediately in the event of known or suspected compromise, and immediately upon system installation (e.g., default or vendor-supplied passwords);
   d. Are not reused until at least five other passwords have been used; and
   e. Are committed to memory, or stored in a secure place.

D. INTERNET USE

1. All software used to access the Internet must be part of CCHHS standard software suite. This software must incorporate all vendor-provided security patches.
2. Non-business-related purchases or sales made over the Internet are prohibited.
3. All user activity on the Internet is subject to logging and review

E. E-MAIL USE

1. E-mail users must not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of CCHHS.
2. Individuals must not send, forward, or receive confidential or sensitive CCHHS information through non-CCHHS email accounts. Examples include, but are not limited to, Hotmail, Yahoo mail, AOL mail.
3. Only authorized email software may be used. All CCHHS business is to be conducted using official CCHHS email. No 3rd party email or other non HIS directed email systems should be used to conduct CCHHS business
4. Individuals must not send, forward, receive, or store confidential or sensitive CCHHS information utilizing non CCHHS accredited mobile devices.
5. Report suspicious emails to the Information Systems department. Do not open them.

F. MOBILE DEVICES

1. Only CCHHS approved portable computing devices may be used to access CCHHS information resources.
2. Approved portable computing devices will require mobile device management software install on them by the Help Desk.
3. Portable computing devices must be password-protected.
4. CCHHS data should not be stored on portable computing devices. However, if there is no alternative to local storage, all sensitive CCHHS data must be encrypted using approved encryption techniques.
5. All computer systems accessing CCHHS resources from an external location must conform to CCHHS standards for configuration and connectivity.
6. Unattended portable computing devices must be physically secure. This means they must be locked in an office, locked in a desk drawer or filing cabinet, or attached to a desk or cabinet via a cable lock system.

Special Notes: Smart Devices – Mobile Phones

Pictures**: It is not permissible to use your portable computing device to take pictures of patient data.**

IT Security Rules of Behavior

Texting**: It is not permissible to transmit patient data using any form of texting.**

By signing this policy, you agree to adhere to the CCHHS IT Security Rules of Behavior. CCHHS HIS ISO reserves the right to modify these rules as needed.

Signature/Date: _____
Printed Name: _____