User Standards for CCHMC Information Technologies

Your role in protecting CCHMC's information

June 13, 2016

INTRODUCTION

CCHMC Information Systems, and the information in those Systems, are CCHMC property. This includes all systems that support the medical center, including clinical, financial, research, and all other systems used by CCHMC. CCHMC Information Systems are a valuable resource that should only be used to support the mission and vision of CCHMC. CCHMC is committed to maintaining the confidentiality, integrity, security, and appropriate availability of its information. As a user, you have responsibilities and obligations to assure information integrity and security. All of CCHMC's policies and procedures apply to your actions within CCHMC Information Systems. The standards set forth in this manual are intended to describe further those behaviors expected from users to protect CCHMC's Information Systems and Confidential Information as defined in INFO-100. CCHMC reserves the right at all times to suspend access to CCHMC Information Systems for suspected violations, pending investigation and resolution. Electronic information (e.g. messages, metadata, access logs, etc.) can be reviewed by system administrators in audits or investigations or law enforcement and recovered from back-up media by system administrators. **YOU PLAY A CRITICAL ROLE IN MAINTAINING THE INTEGRITY OF CCHMC'S CONFIDENTIAL INFORMATION & INFORMATION SYSTEMS**.

REPORTING: Users must *immediately* report any concerns as follows:

- Potential, suspected, or actual unauthorized access or disclosure of CCHMC Confidential Information to the Integrity Helpline: 866-856-1947 or online at cchmc.ethicspoint.com.
- Loss or theft of devices to Information Services Service Desk at 513-636-4100 and the Integrity Helpline. This includes personal devices that connect to the CCHMC network (e.g., phone connecting to Exchange via Active Sync).

PROHIBITED PERSONAL USES: CCHMC Information Systems shall not be used:

- In a manner inconsistent with CCHMC Core Values, Policies, and Procedures, including INFO-102;
- For personal commercial gain; charitable solicitations, unless authorized by the appropriate CCHMC senior management; or personal political activities, such as campaigning for candidates for public office; or
- Excessively for personal use. Personal use may be excessive if it interferes with your CCHMC responsibilities, affects quantity or quality of work, becomes a distraction to patients or coworkers, or otherwise subjects CCHMC to increased operating costs (e.g. by overburdening the network or reducing capacity). Do not use CCHMC Information Systems to send unsolicited or bulk advertisements or commercial messages or CCHMC e-mail to receive promotions and information for personal purposes.

ACCOUNT MANAGEMENT

1.0 General

1.1. Access to CCHMC Information Systems will be granted only as needed to perform CCHMC work and when specifically authorized by the user's direct manager and approved by the owner for that Information System.

1.2. Users are responsible for ensuring that they only have access to the resources they need to fulfill their CCHMC responsibilities. If you have access to an application or system you do not need, contact IS Help Desk and request that the access be removed.

1.3. Managers are responsible for immediately updating user account and access privileges upon changes to job responsibilities and employment status such as termination, promotion, or internal transfer or any other occurrence or event that warrants such change. **Every job change must include an analysis of system access needs.**

2.0 Standards

2.1. ACCOUNT SET-UP: Please refer to the System Access page on Centerlink for further information.

2.2. ACCOUNT TRANSFER: Outgoing managers should work with incoming managers and the Service Desk to ensure that access to applications and resources that need to follow employee remain in place and that access to applications and resources that do not need to follow employee are removed. Outgoing and incoming managers of a transferred employee or badged non-employee must complete the System Access Form within 3 business days of the transfer or change.

2.3. ACCOUNT TERMINATION: Managers must ***immediately*** fill out the employee termination form for voluntary and non-voluntary terminations. Upon resignation, termination or any other action that discontinues an individual or organization's business relationship with CCHMC, active email accounts maintained and supported by CCHMC will be disabled. After a period of 30 days, associated email accounts, mailboxes and other information maintained by CCHMC email systems will be deleted. Outgoing employees and managers must ensure that all records are retained or deleted in accordance with MCP-G-119.

ACCOUNT CREDENTIALS: USER IDS & PASSWORDS

1.0 General

1.1. Users who have been assigned user IDs/passwords to work with systems that generate, store or manage Confidential Information bear the responsibility for preserving the confidentiality and integrity of such credentials to ensure against unauthorized use by any other person.

1.2. Employees who negligently or intentionally share their system passwords or accounts with anyone else for any reason will be held responsible for resulting misuse of the system by others. Users who have any reason to believe or suspect that someone else is using their unique credentials must immediately notify their supervisor, the IS Service Desk, and the Integrity Helpline.

2.0 Standards

2.1. Users are prohibited from sharing individual account credentials or logging into CCHMC Information Systems with their unique credentials and then permitting another person to access information in those databases and/or systems.

2.2. Users must access only those resources to which they have been explicitly authorized access.

2.3. Users must not have more than one account on any given system or resource.

2.4. Users who have become locked out of an application as a result of too many incorrect username/password attempts must notify the IS Service Desk or application administrator promptly so the event can be logged as a user error, rather than as an unauthorized access attempt. The Service Desk/application administrator must not reset any such accounts until the identity of the user can be positively established. Where technically supported, user IDs will be automatically disabled as a result of entering too many consecutively incorrect user ID/password combinations.

2.5. When prompted to remember a password by a browser, program, or application (e.g., Internet Explorer, Mozilla etc.), users should always select "no". Passwords must not be hard-coded (whether readable or not) into applications and programs.

2.6. USER IDs:

2.6.1. User IDs will be created only by following the approved System Account setup process.

2.6.2. Remote network and/or sensitive application access to CCHMC Information Systems may require additional (i.e. multi-factor) authentication. Authentication devices (e.g., SecurID tokens/keyfobs/PINs/Security question answers) must be managed to ensure their security. It is each user's responsibility to maintain the physical security of tokens in your possession at all times. This includes ensuring that it is either physically or electronically within your control or locked in an area where it cannot be accessed by unauthorized users.

2.7. PASSWORDS:

2.7.1. Users are individually responsible for maintaining the confidentiality, security and integrity of their chosen passwords.

2.7.2. **Under no circumstances should users provide a password to anyone. No legitimate activity, even internal support, would require that you communicate your password.** If you have forgotten your password, go to mypassword.cchmc.org or call the Service Desk to reset your password. Only Service Desk personnel and system administrators shall have the privileges to reset passwords. Service Desk personnel and system administrators do not need your current password in order to reset a password.

2.7.3. Users are required to change their password every 120 days and immediately change the default passwords of any newly-assigned or reset accounts. Users will be reminded to change their password 30 days before their password will expire. Where technically capable, CCHMC will control and regulate the use of temporary passwords.

2.7.4. Users who suspect that their passwords have been compromised must immediately report the suspected compromise to the IS Service Desk and the Integrity Helpline and change or reset all passwords in question.

2.7.5. Passwords must not be stored in plain text or readily accessible formats (paper, email, share drives, personal phones).

2.7.6. Passwords must comply with current standards to ensure appropriate strength of password and have the following characteristics (where supported by the application):

- Different from your previous five passwords;
- At least 6 characters in length;
- Containing a mix of alpha, numeric, and special characters; and
- Not be based on easily guessed or available information (example: user name, names of children, spouse, pets, etc.).

PHYSICAL & ENVIRONMENTAL SECURITY

1.0 Standards

1.1. Users are responsible for securing areas with CCHMC Information Systems and Confidential Information in order to prevent unauthorized access, damage, or interference. Ensure that Confidential Information is not visible in an unattended work area or workstation, log off systems after access, do not post passwords in visible areas, do not tamper with the automated screen savers, and lock cabinets/rooms containing systems that access or store Confidential Information.

1.2. Protection of equipment (including computer equipment that is used off-site) is necessary to reduce the risk of unauthorized access to CCHMC Information Systems and to protect against loss or damage. Depending on the size of the system or device, physical access to areas where systems reside must be restricted to personnel specifically authorized to operate or maintain the systems or as authorized by the Chief Information Officer (CIO). Please contact the Information Services Service Desk for more information.

MALWARE, SPAM, AND SOCIAL ENGINEERING

1.0 General

1.1. Malicious software, social engineering acts and hoaxes are designed to disrupt computer systems, gather information that leads to loss of privacy or exploitation, or gain unauthorized access to system resources.

2.0 Standards

2.1. CCHMC Information Systems have an automated anti-malware management system. Disabling, altering, deleting, or preventing these programs or other security settings from updating is strictly prohibited.

2.2. The deliberate creation, use, storage, distribution, and/or possession of malware is expressly prohibited. The intentional storage, distribution, and/or possession of malware may be construed as failure to safeguard CCHMC Information Systems.

2.3. REMOVAL OF UNAUTHORIZED SOFTWARE: Unauthorized, malicious or nuisance software can be installed on a computer without the knowledge of the User. If you discover unauthorized software installed or suspect it of being on any CCHMC system, you must contact the Information Services immediately. Information Services may remove, with or without prior notification any malicious or unauthorized software.

2.4. SPAM, SOCIAL ENGINEERING, AND HOAX MESSAGES: Social engineering and hoax messages pose serious threats to CCHMC Information Systems. Users must recognize and avoid social engineering attempts. Do not engage in actions requested in a suspicious or unexpected e-mail. Creation or forwarding of hoax messages is expressly prohibited. Do not open unexpected, questionable, or suspicious mail without due caution. Call the IS Service Desk for assistance before opening any questionable e-mail or if receiving virus-relating warnings from sources other than IS, and forward the e-mail to SPAMHELP@cchmc.org.

ELECTRONIC MESSAGING

1.0 General

1.1. Electronic messaging refers to systems that transmit messages between users, including email, instant messaging, texting, listservs, blogs, social media, and other electronic forums.

1.2. The following disclaimer should be used when sending an email with Confidential Information:

> *The information contained in this electronic mail message is Confidential and Protected Information intended only for the use of the individual or entity named above. As the recipient of this information you may be prohibited by State and Federal law from disclosing this information to any other party without specific written authorization from the individual to whom it pertains. If the reader of this message is not the intended recipient, or the employee or agent responsible for delivering it to the intended recipient, you are hereby notified that any disclosure, dissemination, distribution, copying, or action taken in reliance on the contents of this communication is strictly prohibited. If you have received this communication in error, please notify us immediately by telephone and destroy the message and its attachments.*

2.0 Standards

2.1. SENDING CCHMC CONFIDENTIAL INFORMATION TO RECIPIENTS EXTERNAL TO CCHMC:

2.1.1. ZIX: Email messages sent to an external address containing CCHMC Confidential Information, including Protected Health Information, must only be sent using the ZIX secure email system.

2.1.2. CCHMC Confidential Information should not be contained in the body or subject line of email sent externally.

2.1.3. Emailing files greater than 50MB requires significant system resources, slows overall network traffic, and should be avoided. File Transfer Protocol (FTP) or Secure File Transfer Protocol (SFTP) can be utilized to send or transfer large files to recipients external to CCHMC. SFTP should be utilized for files containing Confidential Information. Please contact the Information Services Service Desk for further information. Mailing portable devices, such as external hard drives or thumb drives, may not be used unless approved by IS Security and encrypted.

2.2. LISTSERVS: Subscriptions to email listservs shall be limited to essential, CCHMC-related uses.

2.3. FORWARDING MESSAGES: Users should not create or forward messages that are not related to a CCHMC purpose. Users must not *automatically* forward internal electronic mail to any address outside the CCHMC network.

2.4. FORGERY: Forgery of personal email or newsgroup message headers is prohibited. This includes account identification, reply-to addresses, and host-of-origin information in either the message headers or message body.

2.4.1. Exception: Spam-avoidance alteration of email addresses in the message body or reply-to line in externally sent mail is permitted, as long as the identification is human-readable (e.g., john@NOSPAM.cchmc.org or "John at cchmc dot org").

2.5. ELECTRONIC MESSAGING & TEXTING: Instant messaging and texting may not provide a secure vehicle to transmit CCHMC Confidential Information. Do not instant message and/or text CCHMC Confidential Information unless you are using a specific program or CCHMC cell phone issued for that purpose and that encrypts the message.

2.5.1. Secure texting via Voalte© technology: CCHMC issues Voalte phones and offers the VoalteMe and VoalteMessenger applications for secure, HIPAA-compliant texting. Access is requested via a System Access Form. Issued devices must be stored by each unit/department in a secure location and signed in and out at the start and close of the user's shift with the Voalte Inventory Process Form. CCHMC policies and procedures must be followed when using Voalte technology. For example, critical lab results must be communicated verbally and in accordance with CPC-I-227, and orders must be communicated in accordance with CPC-I-122 and I-123. When communicating patient information via Voalte technology, patient name and room number must be identified.

2.6. MEDICAL ADVICE & EDUCATION: Patient-specific medical advice should not be given over the internet. When communicating medical information to an email address external to CCHMC, use appropriate safeguards and ensure that medical information is communicated in a general manner.

SOFTWARE & HARDWARE: REQUESTS & INSTALLATION

1.0 General

1.1. IS provides standard hardware and software to support overall CCHMC functions. Additional hardware and software for individual users may be requested via the Information Services Service Desk (513-636-4100) and may be subject to additional approval and costs. Requests for enterprise-wide, departmental, or area-specific hardware or software solutions require review and approval by the IT Steering Committee via the Project Request process and also may have additional costs. This includes custom-built applications.

1.2. STORAGE OF CCHMC CONFIDENTIAL INFORMATION: Each User is responsible for adequately safeguarding Confidential Information. CCHMC Confidential Information should only be stored on network drives secured by user name and password or in other CCHMC-approved encrypted storage/applications. The storage of CCHMC Confidential Information in unapproved external services/systems (e.g., Google documents, backup systems) should not be used. Only approved cloud storage (i.e., Microsoft One drive) should be used for CCHMC information storage off-site. Please contact the Information Services Service Desk for further information on approved storage locations.

2.0 Standards

2.1. All software and hardware purchases must receive pre-approval and follow the current IS approval process.

2.1.1. Please click here for more information on the approved process.

2.2. INSTALLATION OF UNAUTHORIZED SOFTWARE: Only properly licensed, obtained and approved software may be installed on CCHMC computers.

2.2.1. Any non-standard software not purchased or distributed by a CCHMC approved vendor is prohibited.

2.2.2. Unauthorized duplication or distribution of CCHMC-licensed software is prohibited.

2.2.3. Please check CenterLink for webpage on Purchasing Hardware or Software for more information.

2.2.4. Individual users may not acquire administrator rights to CCHMC devices without IS Security approval.

2.3. Custom-built applications must follow all CCHMC policies and procedures.

PORTABLE DEVICE MANAGEMENT

1.0 Standards

1.1. Users are responsible for ensuring optimum security, such as encryption, of computing devices (regardless of device ownership) that access, transmit, or store CCHMC Information Systems or Confidential Information.

1.2. Users shall not allow non-CCHMC users access to CCHMC devices.

1.3. Devices are prohibited from accessing the secure network of CCHMC unless access is approved.

1.4. If you choose to access CCHMC Information Systems (regardless of device ownership), it is your responsibility to ensure that the device is properly secured and protected. Take advantage of all protections the device provides.

1.5. Do not store access credentials to CCHMC Information Systems (e.g., userids, passwords) on devices.

1.6. Users are responsible for adequately destroying, erasing, or retiring devices that have been used to access and/or transmit CCHMC Information Systems or Confidential Information. Users should contact Environmental Services to arrange for the appropriate disposal of CCHMC equipment (513-636-4381).

REMOTE ACCESS

1.0 General

1.1. Remote access to CCHMC Information Systems from public and non-CCHMC private networks must be managed and protected. CCHMC personnel are provided with Extranet access. Other remote access options or VPN require specific authorization to remotely access CCHMC systems and information.

2.0 Standards

2.1. EXTRANET: Access is granted by using network user name and password.

2.2. VPN: Access will only be granted following submission of a completed Remote Access Request form that has been approved by a divisional director or higher authority. Gateway-to-gateway VPN connections (semi-permanent) will require the explicit approval of the CIO or CTO.

2.3. Remote access users should secure home wireless networks or use a wired connection when using either method to remotely access CCHMC Information systems.

SAFEGUARDS FOR NON-CCHMC DEVICES

1.0 General

1.1. CCHMC policies, procedures, and standards apply when CCHMC Information Systems and Confidential Information is accessed from devices not owned or supported by CCHMC.

1.2. It is each user's responsibility to ensure that CCHMC Information Systems and CCHMC Confidential Information, including PHI, is protected from unauthorized access, use, disclosure, modification, and/or loss, including when such systems or information is accessed from non-CCHMC devices.

2.0 Standards

2.1. Access to or use of CCHMC Information Systems and Confidential Information using non-CCHMC devices shall be either through the Extranet, VPN, or other IS-approved CCHMC access mechanism (e.g. VoalteMe). CCHMC does make some applications/websites available externally. Where applicable, access to these applications is controlled through approved system access processes.

2.2. If using a non-CCHMC device to access CCHMC Information Systems or while working with CCHMC Confidential Information, Users are responsible for the actions of non-CCHMC users (e.g., household members).

2.2.1. CCHMC discourages access to CCHMC Information Systems via shared devices.

2.3. Each User is responsible for implementing appropriate security measures on non-CCHMC devices used to access CCHMC Information Systems and/or CCHMC Confidential Information. This includes, but is not limited to:

- installation and automatic updating of anti-malware detection programs and vendor security patches;
- immediately logging off when finished accessing CCHMC Information Systems or Confidential Information (e.g., VPN);
- physical security measures, such as using locks and not leaving non-CCHMC devices visible in public places;
- implementing separate user profiles and password protecting and using encryption on the device itself; and
- maintaining current operating system and browser configurations.