Icahn
School of
Medicine at
Mount
Sinai

Acceptable Use of Technology Policy (Updated April 6th, 2015) v.3.5

Overview

The Icahn School of Medicine at Mount Sinai (ISMMS) expects that all persons who use school computing hardware, software, networking services, or any property related or ancillary to the use of these facilities will abide by the following policy statement:

School information technology resources are provided with the expectation that the school community will use them in a spirit of mutual cooperation. Resources are limited and must be shared. Everyone will benefit if users avoid activities that cause problems for others who use the same system.

Any access to or sharing of protected or confidential information must comply with Mount Sinai Health System policies, including HIPAA, the Family Education Rights and Privacy Act, and the appropriate use of technology guidelines defined in this document. Remember that compliance begins *by being aware whether your communication could contain protected or other confidential data and by taking the appropriate steps to secure such content. Your responsibilities within the Mount Sinai Health System extend to a variety of other forms of daily communication, including public areas, telephone use, texting, and social media technologies.*

All hardware, software, and related services are supplied by the school for the sole purpose of supplementing and reinforcing the school's educational, research, and clinical goals as set forth in the student and faculty handbooks and other mission statements of the school. These documents may be found (and not limited to) these locations:

ISMMS medical and graduate student handbooks
http://www.mssm.edu/education/student-resources/student-handbooks

ISMMS faculty handbook
http://icahn.mssm.edu/about-us/services-and-resources/faculty-resources/handbooks-and-policies/faculty-handbook

HIPAA policies and procedures
http://policies.mountsinai.org/web/hipaa/policies

Social media guidelines
http://icahn.mssm.edu/about-us/services-and-resources/computer-services/policies/social networking-guideline

Use of Hardware and Software

We expect that all students, faculty, and employees will use only the provided hardware, software, or services which they are authorized to use.

All hardware devices using school or hospital email, file, or collaboration services, including personal laptops, must be encrypted, while AirWatch Mobile Device Management (MDM) must be

enabled for personal smartphones. Thumb drives or any storage devices that contain protected health information (PHI) or other confidential information must also be encrypted. For more information or support, please contact the Academic IT Support Center (1.212.241.7091, email: ASCIT@mssm.edu).

Individuals may not extend their use of the resources described for any purpose beyond their intended use or beyond those activities sanctioned in school policy statements.

In particular, no one may use hardware and software:

- To acquire personal profit or gain
- To harass, threaten, or otherwise invade the privacy of others
- To initiate or forward email chain letters
- To cause breaches or disruptions of computer, network, or telecommunications systems
- To initiate activities which unduly consume computing or network resources
- To transmit sensitive or proprietary information to unauthorized persons or parties

It is a specific violation of these guidelines to provide account passwords to individuals who are not the owners of the accounts or to obtain passwords to or use others' accounts.

It is against this policy to copy or reproduce any licensed software or media, except as expressly permitted by the license. Unauthorized use or distribution of software, media, or digital content is a violation of this policy.

Individuals who violate the aims of this policy will be subject to disciplinary action or to referral to law enforcement authorities without prior notification of those who have sent or received such messages. ISMMS IT personnel are authorized to monitor suspected violations and to examine items stored on any school storage medium by individuals suspected of violating this policy.

Web and Data Storage

Access to the Internet is provided as a communications tool and an information resource to facilitate the performance of job- or academic-related functions. This policy applies to any Internet service accessed on or from a Mount Sinai Health System facility, provided by the school, accessed using school-owned equipment, or used in a manner that identifies the individual with the ISMMS or Mount Sinai Health System. The Mount Sinai Health System reserves the right to review any information, files, or communications sent, stored, or received on its computer systems.

Inappropriate use of the Internet may result in loss of access privileges and in disciplinary action up to and including dismissal. Students, faculty, and employees are prohibited from using Mount Sinai Health System-provided Internet services in connection with any of the following activities:

- Engaging in illegal, fraudulent, or malicious conduct
- Working on behalf of organizations without a professional or business affiliation with the Mount Sinai Health System
- Sending, receiving, or storing offensive, obscene, or defamatory materials
- Obtaining unauthorized access to any computer system
- Using another individual's account or identity without explicit, written authorization
- Attempting to test, circumvent, or defeat the security or crediting systems of the Mount Sinai Health System or any other organization without prior authorization from Information Management Systems and Services/Security and Corporate Data Administration (IMSS/SACDA) or ISMMS IT
- Any use or activity that impedes Mount Sinai Health System operations

Cloud Storage

Users of school-provided cloud services, such as Google Apps for Education and Box.com, have the ability to share files with colleagues within or outside the Mount Sinai Health System for academic collaboration purposes. Students, faculty, and employees must not, under any circumstances, share unencrypted files containing PHI or other confidential information with colleagues outside the Mount Sinai Health System. As mentioned, compliance begins by being aware of the data that you are generating and by following appropriate steps to secure such content if it contains protected or other confidential information.

Email and Collaboration Technology Usage

Email and collaboration technologies, including Google Apps for Education, are provided to assist and facilitate scholarly communication and collaboration. These technologies are provided for official business and educational use in the course of assigned duties. The school reserves the right to access and disclose all messages sent over its electronic mail systems for the purposes of monitoring security breaches and investigating inappropriate usage as defined in this policy. The Mount Sinai Health System is obligated to comply with legal subpoenas, court orders, and similar lawful requests from external regulators or authorities.

Inappropriate use of email and/or collaboration technology may result in loss of access privileges and disciplinary action up to and including dismissal. Inappropriate use includes but is not limited to:

- Unauthorized attempts to access others' email accounts
- Transmission of protected and/or confidential information to unauthorized persons or other organizations
- Transmission of obscene or harassing messages to any other individual
- Transmission of offensive material, solicitations, or proselytization for commercial ventures, religious or political causes, or other non-job related solicitations
- Any illegal, unethical, or other activity that could adversely affect the Mount Sinai Health System

Protected Health Information, FERPA, and Other Confidential Information

All hardware devices, including bring your own devices and personal laptops, on which school email, file, or collaboration services are used must be encrypted. AirWatch MDM must be enabled for personal smartphones. Thumb drives or any storage devices that contain PHI data must also be encrypted. For more information or support, please contact the Academic IT Support Center (1.212.241.7091, email: ASCIT@mssm.edu). Students, faculty, and employees are responsible for ensuring that their devices are password enabled and encrypted.

The key points of the above policies are as follows:

- You may use only your ISMMS email account to communicate protected or confidential information. Emails containing PHI, financial information, or other confidential ISMMS information and/or social security numbers may not be sent or redirected to non-ISMMS email accounts.
- The minimum necessary amount of PHI should be disclosed via email. When at all possible, use the Medical Record number, rather than the patient name, as the patient identifier.
- Messages that leave the Mount Sinai Health System network and contain PHI or other confidential information must be encrypted using the ISMMS IT-approved solution described as follows.
- Messages sent within the Mount Sinai Health System network are automatically encrypted.
- Encryption will not prevent misdirection or unintended forwarding of a previous string of

emails. Extreme caution must be exercised to prevent such risks. Be aware of the content that you generate.

Secure Messaging and Encryption

In addition to ensuring that your device is encrypted (see above), you must select an email encryption option if you are sending PHI or other confidential information to an external recipient.

Activating the email encryption option:

- For Microsoft Exchange users, include the word [secure] within square brackets in the subject line of the message. The recipient will be asked to self-enroll when the message is opened. The secure send mechanism can be used in any email client (e.g., Outlook, Outlook Web Access, smartphone).
- For Google Apps users, install the Virtru add-on to the browser and/or device (go to http://www.virtru.com for instructions). When composing a message, select the "Virtru Protection is on" option.

Spam and Inappropriate Use of Messaging Tools

ISMMS systems, including email, are intended for official business use. Inappropriate use may result in disciplinary actions and loss of access privileges. Unsolicited mass emailing of materials not related to school business is considered spam and may result in the loss of access privileges.

Student Privacy, Secure Email, and Phishing

Please remember to take care when opening attachments or following links contained in email messages. Verify with the sender of the message if you receive an unexpected attachment or an email that contains suspicious links. Be especially cautious of emails that have been quarantined. Unless a quarantined message is correspondence that you are expecting, do not release the email.

Please also take care with any messages that ask you to provide private information (e.g., birthdays, social security number, credit card numbers, user account passwords). These messages might actually be phishing attempts by persons pretending to be from legitimate companies or organizations. If you have any doubts, contact the party requesting the information for confirmation. Users should not rely on the contact information contained in the email but use the contact information typically found on the company website or on the back of a bank or credit card.

Attestation

I understand that by receiving ISMMS network and Internet access to email and library resources, I agree to abide by all institutional policies related to use of the ISMMS systems to access the Internet, email, and all other computer and network resources.

I acknowledge receipt of these policies and understand that they might be changed, and I will abide by these changes as reflected on the ISMMS website or received via other forms of communication.

I understand that I am responsible for all actions performed from my computer account. I further understand that, in the course of my work, I may be given or otherwise gain access to confidential or privileged information related to this or other institutions, ISMMS students or employees, or other individuals or groups. I will respect the confidentiality of all information to which I have access and neither divulge information without appropriate consent nor seek to obtain access to confidential information to which I am not entitled.

For more information or support, please contact the Academic IT Support Center (1.212.241.7091, email: ASCIT@mssm.edu)