Issued By :- Medical Advisory Committee
Reference:- Health Records Services

Title:- **APPROPRIATE MEANS OF COMMUNICATING CONFIDENTIAL INFORMATION**

Reviewers: Health Records and Communications Committee
Medical Advisory Committee, Privacy Officer

Distribution: Mount Sinai Intranet/General Manual/Policy & Procedures

Purpose

The purpose of this Policy is to protect the confidentiality of information when communicating it through various means.

Definitions

"Confidential information" is information of a sensitive nature in any format which is created or received by the hospital in the course of its business, which is not otherwise available to the public, and includes, but is not limited to, financial, human resources, human rights, administrative and patient health information.

"Sending" when used in reference to email, includes "forwarding".

Policy

All disclosures and releases of confidential information must conform to the Confidentiality and Release of Information policy, the Confidentiality of Patient Health Information policy and Information Systems Security policy and any other applicable policies.

A fully executed Consent to the Disclosure of Patient Health Information form or other appropriate authorization transmitted by FAX shall be acceptable as proof of Consent, provided that the originally signed authorization is forwarded to Mount Sinai Hospital by mail and that the authorization meets all criteria for validity (see Section VI of the Confidentiality and Release of Information policy).

Faxing

The following policy statements must be considered prior to faxing any confidential information:

1. Personal and confidential information should only be transmitted by fax when no other more secure and practical means of communicating the confidential information is available.

2. Confidential information must be transmitted from and received on machines located in a secure area where it can be monitored and operated by authorized persons only in order to ensure confidentiality.

3. The sender of the information shall be responsible for ensuring security of the health information being transmitted.

4. Patient identification should not be removed from reports to be faxed, since it is in the best interest of patient care. However, when sending other forms of confidential information, de-identifying the information should be considered.

Issued By :- Medical Advisory Committee
Reference:- Health Records Services

Title:- **APPROPRIATE MEANS OF COMMUNICATING CONFIDENTIAL INFORMATION**

Reviewers: Health Records and Communications Committee
Medical Advisory Committee, Privacy Officer

Distribution: Mount Sinai Intranet/General Manual/Policy & Procedures

5. Only pertinent confidential information deemed necessary is to be faxed. For example, in the case of personal health information, the entire record should generally not be faxed.

The following procedures should be followed when faxing confidential information:

1. The release of all health information by fax must be documented appropriately in the health record, including maintaining a copy of the confirmation of transmission form.

2. When sending confidential information, the Mount Sinai Hospital Fax Cover Sheet must be used. The name of both the sender and his/her department and the intended recipient, along with a notation indicating the total number of pages faxed must be indicated on the Fax Cover Sheet.

3. When practical and particularly when the location of the recipient machine is unknown, senders should telephone ahead to alert the recipient that a fax containing confidential information is on its way.

4. When master lists of fax numbers or numbers pre-programmed into a fax machine are used, they should be regularly checked to ensure their accuracy.

5. Prior to sending the fax, the entered fax number must be reviewed to ensure that this number corresponds with the intended recipient's fax number.

6. The sender of each fax should confirm the success of a transmission by checking the confirmation report after the fax has been sent.

7. Some departments utilize auto-fax technology included in their clinical applications as a means of transmitting confidential information to referring caregivers and other authorized persons. Departments relying on this technology must implement quality control processes and appropriate procedures to ensure confidentiality is maintained. Quality control must include periodic verification that all speed dialled numbers are current and valid and that all recipients receiving confidential information are intended.

8. When a fax has been mistakenly sent to the wrong number, the unintended recipient should be asked to return or destroy the confidential information. The sender is responsible for notifying the owner of the confidential information of the unauthorized disclosure and the sender must notify the Corporate Privacy Officer. For more information, please reference the sections of the the Confidentiality of Patient Health Information policy dealing with breaches of privacy/confidentiality.

Issued By :- Medical Advisory Committee
Reference:- Health Records Services

Title:- **APPROPRIATE MEANS OF COMMUNICATING CONFIDENTIAL INFORMATION**

Reviewers: Health Records and Communications Committee
Medical Advisory Committee, Privacy Officer

Distribution: Mount Sinai Intranet/General Manual/Policy & Procedures

9. Upon receipt of a fax, the designated individual should check the number of pages of the fax to ensure that it matches the number listed on the cover sheet. If a fax is received in error, the sender should be notified.

Email

The following policy statements must be considered prior to emailing confidential information in recognition of the fact that email is a means of communication that increases the ease with which information can be circulated, forwarded and broadcast:

1. Email messages are not encrypted on the MSH-email system. Internal users are contained within the MSH firewall. However, since the emails are not encrypted, MSH cannot guarantee the confidentiality and security of messages users send to or receive from others.

2. Email communication sent using eHealth Ontario's ONE Mail is automatically encrypted and therefore can be used to send confidential and personal health information (PHI) to users at other organizations that are also participating in ONE Mail.

3. Confidential information, including patient health information, may be emailed internally to addresses on the global list for appropriate purposes on a need to know basis only.

4. Because email can be intercepted, altered, forwarded, or used without authorization or detection outside of the MSH firewall or ONE Mail system, confidential information may only be emailed externally (i.e. to an account not on the global list which includes @utoronto.ca accounts) if:

    - The patient or other person to whom the confidential information belongs consents to the use of external email to communicate their health information and that consent is appropriately documented;
    - The confidential information has been stripped of all personal identifiers rendering the confidential information anonymous; OR
    - Provided there is no personal health information contained anywhere in the email or any attachment, the other confidential information is contained in an email attachment that is password protected. If communicating the password by email, it should be sent to the intended recipient in a separate email from the one with the password protected document attached to it.

5. Emails concerning a patient's treatment are considered part of the legal health record and should be printed and included in the patient's health record.

Issued By :- Medical Advisory Committee
Reference:- Health Records Services

Title:- **APPROPRIATE MEANS OF COMMUNICATING CONFIDENTIAL INFORMATION**

Reviewers: Health Records and Communications Committee
Medical Advisory Committee, Privacy Officer

Distribution: Mount Sinai Intranet/General Manual/Policy & Procedures

6. All users of email are reminded that email can be used as evidence in court and patients may have a right to access all emails concerning them.

7. As the owner of the email system, MSH reserves the right to audit and monitor email usage and content, subject to the specific conditions outlined in this policy. When appropriate, a manager or supervisor will obtain the employee's consent to access an employee's email account. However, a manager or supervisor may be given short-term view-only access to an employee's email account, without the employee's consent, in order to support hospital business activities in an employee's absence, to investigate suspected misconduct / violation of a hospital policy or to support a legal investigation. Afterwards, where appropriate, the employee will be notified of the manager's access as soon as possible.

8. eHealth Ontario reserves the right to investigate suspected breaches of the ONE Mail system as per the Acceptable Use Policy. For further details, refer to eHealth Ontario's web site: http://www.ehealthontario.on.ca/solutions/communitycare.asp

The following procedures must be followed in connection with sending confidential information via email:

1. Always check the email address(es) set out in the "To" field to ensure it belongs to the intended recipient(s).

2. Never include identifying information in the "Subject" field of an email like a person's name, MRN, OHIP Number, Social Insurance Number etc.

3. Use the "Reply All" function sparingly. Consider if everyone actually needs to be copied on the emailed response prior to sending it.

4. Use of a Confidentiality Notice is not mandatory; however, if the user chooses to use one, the following Notice must be used:

   The information in this email may be confidential. This email is intended to be reviewed only by the individual(s) or organization named above. If you are not the intended recipient or an authorized representative of the intended recipient, please be notified that any review, dissemination or copying of this email and its attachments (if any) is strictly prohibited. If you have received this email in error, please immediately notify the sender by return email and delete this email from your system, including from the deleted items folder. Thank you for your cooperation.

5. Patient consent to the communication of his/her confidential information must be documented in one of two ways:

Issued By :- Medical Advisory Committee
Reference:- Health Records Services

Title:- **APPROPRIATE MEANS OF COMMUNICATING CONFIDENTIAL INFORMATION**

Reviewers: Health Records and Communications Committee
Medical Advisory Committee, Privacy Officer

Distribution: Mount Sinai Intranet/General Manual/Policy & Procedures

(i) Patient consent may be obtained via email by the care provider sending the following message to a patient and the patient sending a positive response by return email:

Dear Patient: Your Mount Sinai Hospital care provider is pleased to communicate with you through email. However, you should know that email messages are not encrypted on the hospital email system, and therefore, the hospital cannot guarantee the security of messages that you send to or receive from your care providers. Please do not use email to communicate emergency or urgent health matters since email messages can be delayed for technical reasons beyond the control of your care provider.

Your care provider may make decisions about your treatment based on information you provide through email. This information will also form part of your health record if it is relevant to your care.

At any time, you or your care provider can decide that you no longer wish to communicate through email. If you decide to stop communicating through email, you must inform your care provider in writing or at your next appointment. If your care provider cannot continue email communications with you, he or she will inform you in writing and/or notify you about this at the time of your next appointment. By replying to this message, you have read and agree to these terms. If you have any questions or comments about your privacy, please refer to http://www.mtsinai.on.ca/Patients/patprivacy.htm.

The patient's positive reply must be included in the patient's health record.

(ii) Patient signs a Patient Consent for Email Communications form and an executed copy is kept in the patient's health record.

6. All emails **concerning a patient's care** must be printed off and included in the patient's health record.

7. Emails regarding the care of an inpatient, day surgery, medical daycare, or emergency patient are to be included in the "Correspondence" section of the paper record or alternatively, they may be forwarded to the Health Records Services department for inclusion in the patient's record, provided a MRN is included with the email.

8. Email correspondence must be retained in paper format for as long as other aspects of the patient's health record are maintained and in no circumstances for less than health record retention legal requirements (10 years for adults or 10 years past the patient's eighteenth birthday).

Issued By :- Medical Advisory Committee
Reference:- Health Records Services

Title:- **APPROPRIATE MEANS OF COMMUNICATING CONFIDENTIAL INFORMATION**

Reviewers: Health Records and Communications Committee
Medical Advisory Committee, Privacy Officer

Distribution: Mount Sinai Intranet/General Manual/Policy & Procedures

9. All requests for access to a user's email account must be approved by the Corporate Privacy Officer. Under no circumstances will a manager or supervisor be provided with a user's password.

10. When an email is sent to an unauthorized recipient, the unintended recipient should be asked to destroy the confidential information. To destroy an email, at minimum, it must be deleted from the unintended recipient's in-box, as well as the deleted items folder. The sender is responsible for notifying the owner of the confidential information of the unauthorized disclosure and the sender must notify the Corporate Privacy Officer. For more information, please reference the sections of the Confidentiality of Patient Health Information policy dealing with breaches of privacy/confidentiality.

Mail

1. Mail represents the most secure means of sending confidential information and is the preferred method of communicating confidential information when time permits.

2. When mail is returned to the Hospital opened, the Mail Room will stamp the mail as being "Received Open/Damaged from Carrier". In those circumstances, the sender is responsible for notifying the owner of the confidential information of the unauthorized disclosure and the sender must notify the Corporate Privacy Officer. For more information, please reference the sections of the Confidentiality of Patient Health Information policy dealing with breaches of privacy/confidentiality.

3. When returned mail is stamped as "Opened by Mail Room Staff – No return address", it is not necessary to notify the owner of the confidential information as no unauthorized disclosure has occurred.

Telephone

1. Confidential information should only be communicated over the telephone when the timely delivery of health care requires it. For example, the microbiology lab needs to communicate results to the ordering physician; time simply does not permit communicating the information any other way.

2. Care should be taken to ensure that unauthorized persons are not within earshot when communicating confidential information.

3. If regularly communicating confidential information over the telephone, minimize the number of employees fielding the telephone requests so that they can develop a familiarity with the usual inquiring parties. When possible, a log of in-coming telephone requests should be maintained or the telephone conversation should be documented in the relevant health record.

Issued By :- Medical Advisory Committee
Reference:- Health Records Services

Title:- **APPROPRIATE MEANS OF COMMUNICATING CONFIDENTIAL INFORMATION**

Reviewers: Health Records and Communications Committee
Medical Advisory Committee, Privacy Officer

Distribution: Mount Sinai Intranet/General Manual/Policy & Procedures

4. When forced to leave messages on answering machines or voicemail, for example to confirm an appointment, limit the amount of information disclosed as much as practical as individual(s) other than the patient may have access to the messaging system. For example, consider leaving only the care provider's name and number and other information necessary to confirm an appointment, or simply ask the individual to call back.

5. Patient requests that messages not be left must be respected.

6. Cell phones should not be used to store or transmit confidential information.

References

- *Guidelines on Facsimile Transmission Security*, Information and Privacy Commissioner / Ontario, Revised January 2003;
- *The College Answers Physicians' Questions about PHIPA*, College of Physicians and Surgeons of Ontario, Dialogue Online, November/December 2004;
- *Documentation Practice Standard*, College of Nurses of Ontario, 2004;
- *Hospital Privacy Toolkit: Guide to the Ontario Personal Health Information Protection Act*, September 2004
- *Faxing Personal Information Fact Sheet*, Office of the Privacy Commissioner of Canada, Last Updated 2004-03-01.