I. PURPOSE

This policy applies to all SUNY Downstate Medical Center (SUNY DMC) employees, faculty, staff, residents, students, contractors, consultants, temporary workers, other authorized third party entities and personnel (herein referred to as “workforce members”). This policy establishes standards for the electronic transmission of Protected Health Information (“PHI”) controls that SUNY DMC will employ to protect the security and privacy of electronic PHI. This policy applies to email, instant messaging, voice mail, file transfer, and any other technology that transmits health information electronically.

II. POLICY

PHI that is to be transmitted will be transmitted in a manner that protects against unauthorized access and ensures its integrity. Accommodate the need to protect the PHI and the need for efficient communication of PHI in support of patient care. PHI may be transmitted electronically only when the use or disclosure is permitted...
in accordance with other existing policies, and when the circumstances described herein are met. When electronic transmission of PHI reasonable and appropriate security measures shall be implemented. Effective security of PHI communicated electronically is a team effort, involving the participation and support of every SUNY DMC workforce member and affiliate user of SUNY DMC PHI. It is the responsibility of every user to know these guidelines and to conduct their activities accordingly.

III. DEFINITIONS

None

IV. PROCEDURES/GUIDELINES

Patient/Provider Electronic Communications

The following are industry guidelines/ legal standards, compiled by the Office of Compliance and Audit Services (OCAS), which should be utilized when customizing a procedure section to DMC’s Electronic Communication of Health Related Information Policy.

I. Administrative Recommendations

A. Eligible Patients / Patient Authorization

1. An approved consent form must be used to obtain patient authorization to communicate protected health information electronically with a patient.
2. The following criteria should be considered before enrolling patients for electronic communications:
   a. The provider and patient have a prior established relationship;
   b. The patient has been seen at DMC within a specified time period;
   c. The patient’s health literacy and language literacy level are adequate for communication;
   d. The patient knowledge of the electronic application is appropriate;
   e. The patient is capable of complying with DMC’s electronic messaging policies and guidelines.
3. Prior to enrollment, patients must be informed that failure to comply with the agreement may result in physician termination of the electronic messaging relationship.

B. Email Template- DMC Departments utilizing email communications should have a standardized template for email in place to ensure that the appropriate information is communicated and captured.

1. A banner should be displayed prominently at the beginning of the email message. Suggested language includes:

   “THIS CONFIDENTIAL COMMUNICATION CONTAINS INFORMATION PROTECTED BY PROVIDER PATIENT PRIVILEGE.”
2. A standard block of text should be posted in the body, at the end of email messages to patients. It should include the following:
   a. The provider’s full name;
   b. The provider’s contact information;
   c. Established response time;
   d. Instructions for when response time is not met;
   e. Instructions for urgent communications and patient emergencies;
   f. Statement that patients may, at any time, escalate communication to a phone call or office visit;
   g. Statement that the use of email is not a substitute for clinical evaluation;
   h. Reminder about security risks.
3. A statement of confidentiality should be posted on the bottom of all email correspondence. Suggested language includes:

“The contents of this email message and any attachments are confidential and are intended solely for the addressee. The information may also be legally privileged. This transmission is sent in trust, for the sole purpose of delivery to the intended recipient. If you have received this transmission in error, any use, reproduction or dissemination of this transmission is strictly prohibited. If you are not the intended recipient, please immediately notify sender by reply email or by (718) 270- XXXX.”

C. Response Timeframes – a maximal turnaround time for patient initiated messages should be established and communicated with the patient. Timeframes should include:
   a. Priority for different types of messages (Test results, side effects of medications);
   b. Identification of what may require urgent, emergent handling;
   c. Instructions for when turnaround time is not met.
D. What DMC Will Communicate - the types of transactions permitted / not permitted via electronic communications should be generally established.

Permitted examples include:
   a. Non- urgent referrals/ consultations;
   b. Prescription renewals;
   c. Non-urgent medical advice;
   d. Test results, based on professional judgment;
   e. Insurance inquiries;
   f. Benefit information;
   g. Provider network information;
   h. Billing information;
   i. Scheduling/ canceling/ rescheduling appointments;
   j. Clinic/ provider changes;
   k. Release of records.

Prohibited examples include:
   a. HIV information;
   b. Mental health information;
   c. Alcohol and substance abuse information;
   d. Genetic testing;
e. Worker’s compensation injuries and disabilities;
   f. Confusing or abnormal test results;
   g. New diagnoses;
   h. Bad news;
   i. Urgent information (such information should specifically be defined);
   j. Information pertaining to legal liability.

E. **Electronic Communication Triage** - Providers may triage received patient electronic communications to ensure the fastest response time. Guidelines for how received communications will be opened and answered must be established.

F. **Privacy guidelines:**
   a. Providers may not communicate with patients using personal email accounts (Ex: AOL, Earthlink, Gmail).
   b. Providers may not initiate electronic messages to patients.
   c. Password protected screen savers and automatic log off mechanisms must be utilized on desktop workstations in the office and at home.
   d. Electronic messages containing patient identifiable information must be encrypted, including wireless communications.

G. **Filing and Retention** - all clinically relevant electronic messages from provider to provider and provider to patient must be made a permanent part of the patient’s medical record (including messages, replies and confirmations of receipt).
   a. The full text of the patient's query should be included in the electronic communication's reply.
   b. For email communications, the provider’s email address should be copied in the reply to the patient. Which now includes both the original message and the provider's reply, the message should be printed. The paper copy is then filed in the chart.

II. **Provider Communication Guidelines**
This section may be used to develop a provider handout. Documentation that a provider has received the electronic communication guidelines should be filed in Departmental records.

A. **Provider Communication Guidelines**
   1. Providers should not communicate with patients unless a signed consent form is on file.
   2. Providers should not initiate any electronic communication to a patient.
   3. Providers should use discretion in outgoing message titles. For example, "About Your HIV Test" is not an acceptable subject header.
   4. Providers should electronically copy and paste e-mail addresses and/ or use the reply button to minimize mistyped e-mail addresses.
   5. Providers should always double-check all "To:" fields prior to sending messages.
   6. Providers should provide information in the clearest possible manner. Language should be clear, easy to read and appropriate for the intended recipient.
7. Providers should avoid anger, sarcasm, harsh criticism, and libelous references to third parties in messages. The impersonal nature and ambiguity of electronic messages often results in real or imagined exaggeration of animosity toward the recipient. Providers must realize that sick, anxious, or angry patients might indeed express stronger sentiments with electronic messages than they would face-to-face or over the phone. Providers should make an effort to restrain their language despite their own stress or fatigue.

8. Providers should notify patients to come in to discuss their care or to call them if electronic messages become too lengthy or the correspondence is prolonged.

9. Providers should configure automatic reply to acknowledge receipt of messages. Replies should be “Your message has been received by Dr. John Smith. I will attempt to process your request—within one business day. If you need immediate assistance, please call Pat, my nurse, at 718-270-xxxx.”

10. Providers should send a new message to inform the patient of completion of request (for prescription refills, records transfer, and other transactions).

11. Providers should activate out-of-the-office replies on any electronic message account that will not be serviced by staff or covering physicians during an absence that exceeds the established electronic communication response time. Such messages should include the provider's estimated date of return and instructions on whom to contact for immediate assistance.

12. Providers should never use group addressing, where those in the group see each other’s names, when sending electronic messages to patients. Providers should use the blind copy feature in the email software.

13. Providers or designee(s) should print all messages, with replies and confirmation of receipt, and place in patient's paper chart. When patient acknowledgment of receipt of the electronic message is expected, the printed (chart) copy should not be filed until this confirmation is received. In the absence of such confirmation, it cannot be assumed that the patient has much less read, important instructions. When in doubt, providers should confirm delivery by telephone.

14. Providers should never forward patient-identifiable information to a third party without the patient's express authorization. Text forwarding to a colleague for the purpose of consultation should not contain the patient's name or email address.

15. Providers should never use patient's e-mail address/ texting number in a marketing scheme or supply such addresses/ numbers to third parties for advertising or any other use.

16. Providers should never share professional electronic messaging accounts/ passwords with family members, friends or non- medical coworkers. If providers answer electronic messages from home, they must take special precautions to prevent other household members from intercepting messages from patients.

17. Providers should always utilize appropriate privacy and security safeguards.

B. Provider Ethical Guidelines
1. Electronic correspondence should not be used to establish a patient physician relationship. Rather, electronic communications should supplement other, more personal encounters and provide support to the existing patient physician relationship.

2. When using electronic communications, providers hold the same ethical responsibilities to their patients as they do during other encounters. Whenever communicating medical information, providers must present the information in a manner that meets professional standards and the same expectation of quality as in the traditional medical care process.

3. When using electronic communications, there must be some form of identification/certification that the provider is the licensed, currently registered provider that s/he purports to be. The qualifications of the author should, therefore, be clearly indicated.

4. Providers should not communicate with patients that are outside of the state in which the provider holds a license.

5. Information provided via electronic communications should be supported by clear references to source data. It should be indicated as to whether information is based on scientific studies, expert consensus and/or professional/personal experience or opinion.

6. Good faith efforts should be made to present controversial issues in a fair and balanced manner, presenting all reasonable sides.

7. Any claims relating to the benefits/performance of a specific treatment, product or service should be supported by appropriate, balanced and best available evidence.

8. Any financial relationships related to the recommendation of a specific treatment, product or service should be clearly identified.

9. New diagnosis and treatment should not be addressed exclusively via electronic communications.

10. The privacy and confidentiality of personal data submitted by the patient via electronic messaging must be respected, in accordance with Federal and State law.

C. Patient Guidelines – This section may be used to develop a patient handout. Documentation that a patient has received electronic communication guidelines should be filed in the medical record.

1. Patients should be instructed on what information must be included in the electronic message:
   a. Patient name and identification number, if any- suggested patient identifiers include:
      i. Date of birth;
      ii. Phone number.
   b. Name of the healthcare provider;
   c. Appropriate use of the subject line to identify the type of message in order to facilitate response time (Prescription refill, appointment, billing question).

2. Patients should be advised as to the hours of electronic messaging operations and expected response time.
GUIDELINES FOR PATIENT/PROVIDER ELECTRONIC COMMUNICATIONS

3. Patients should be instructed to contact the office by phone if they do not receive a response to an electronic message within the expected time frame.

4. Patients should be informed that messages should be concise.

5. Patients should be educated about the appropriate types of transactions for electronic communications. Examples of when electronic communication is appropriate include:
   a. Prescription renewals;
   b. Non-urgent medical advice;
   c. Test results, based on professional judgment;
   d. Insurance inquiries;
   e. Benefit information;
   f. Provider network information;
   g. Billing information;
   h. Scheduling/canceling/rescheduling appointments;
   i. Clinic/provider changes;
   j. Other non-urgent communication.

6. Patients should be educated that sensitive information may not be discussed via electronic communications. Examples include:
   a. HIV;
   b. Mental health;
   c. Alcohol and substance abuse;
   d. Genetic testing;
   e. Worker’s compensation injuries and disabilities;
   f. Urgent health conditions.

7. Patients should be informed that they are required to acknowledge receipt of electronic communications.

8. Patients should be advised of the privacy/security risks associated with the use of electronic communications:
   a. Electronic messages may be intercepted, altered and/or forwarded;
   b. Email address/text number may be entered incorrectly and delivered to the wrong recipient;
   c. Sender may assume that a message was sent when it was not;
   d. Inability of some computers to open attachments;
   e. Possibility of misinterpretation of electronic communications due to nonverbal feedback;
   f. Attachments saved to the hard drive may present a risk for unauthorized access and breach of confidentiality.

9. Patients should be informed about indemnity for information loss due to technical failures.

10. Patients should be advised of general electronic communication practices, such as:
   a. Electronic messages may be forwarded to other hospitals or providers (referrals).
   b. Electronic messages will become part of the patient’s permanent medical record and are discoverable for legal purposes.
c. Office/ nursing personnel will be screening/ responding to electronic messages.

11. Patients should be educated regarding the need to develop his/ her own privacy practices. Patients must be charged with the responsibility to handle their information in a secure manner.

12. Patients should be referred to DMC’s Notice of Privacy Practices for additional information regarding uses and disclosures of patient information.

13. Patients should be informed that electronic correspondence will be terminated for patients who repeatedly do not adhere to the written electronic communication guidelines.

III. ATTACHMENTS

None

IV. REFERENCES

HIPAA Standards for Privacy of Individually Identifiable Health Information.

Joint commission Standards

<table>
<thead>
<tr>
<th>Date Reviewed</th>
<th>Revision Required (Circle One)</th>
<th>Responsible Staff Name and Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/2014</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>6/2016</td>
<td>Yes [No]</td>
<td>Michael Burns, Associate Administrator/ Clinical Information Systems</td>
</tr>
</tbody>
</table>