UNIVERSITY of MARYLAND
SCHOOL OF MEDICINE

Policy # & Policy Title: ***UMSOM-A-001***
Acceptable use of Email and Confidential Data

Published Date: 10/01/2016

Effective Date: 10/01/2016

Revision Date: ***5/6/2019***

Approved: E. Albert Reece .

POLICY: SOM – Acceptable use of Email and Confidential Data

I. All Workforce Members (faculty, staff, students, residents) are required to use the SOM email domain (@som.umaryland.edu) as their primary email address for all business communications.

Where legacy email addresses ending in "umaryland.edu" or "umm.edu" exist they will be forwarded in perpetuity to allow incoming mail to be delivered to the SOM email address.

II. All SOM email account names will be created in the following order. If a name collision occurs at step one, the email administrator will proceed down the list until the account name provides a unique email address.

1. First Initial of the first name followed by the full last name@som.umaryland.edu
2. First initial of the first name, middle initial, full last name@som.umaryland.edu
3. Full first name.full last name@som.umaryland.edu
4. Full first name.middle initial.full last name@som.umaryland.edu
5. First initial of the first name followed by the full last name and an incremental number@som.umaryland.edu

III. All SOM email accounts will appear in the directory and display in the format **Last Name, First Name**. Middle Initial and/or Middle/Other name can appear to further distinguish the person.

IV. The use of personal email accounts (AOL, Comcast, Verizon, Hotmail, Yahoo, Gmail, etc.) to email any SOM-related information is not permitted. Creation of Outlook/Exchange rules for the automatic forwarding of SOM email to a personal email account is strictly prohibited. Only emails that are personal in nature may be forwarded to a personal email account. Personal email accounts may be used as an alternate email for campus emergency notifications.

V. FPI/SOM has adopted the Policy/Procedures described below to apply to all emails that contain sensitive information such as PHI and credit card information.

VI. *Proceed with Caution.* Email containing confidential information such as PHI, PII, and credit card information should be used with caution and must follow the procedures described in section VIII of this Policy.

VII. *Proceed with Caution.* Avoid sending confidential information such as a Social Security Number (SSN) and/or credit card Primary Account Numbers (PAN) by email unless absolutely necessary for a work-related function and must follow the procedures described in section VIII of this Policy.

VIII. Procedure - General emails that contain confidential information

1. Email containing confidential information such as PHI, PII, or client credit card information must be encrypted when sent to an external recipient. An external recipient is any recipient who does not have an email address of any variation (e.g. @som) ending in "umaryland.edu" or "umm.edu".

2. ***ALL*** email will contain the following disclaimer at the bottom of the message :

****CONFIDENTIALITY NOTICE****

This message, including any attachments, is intended only for the use of the individual(s) to whom it is addressed, and may contain information that is privileged, confidential and prohibited from disclosure under applicable law. If you are not the intended recipient, please delete/destroy all electronic and hard copies of this message immediately and notify the sender that the message was sent in error. Thank you.

3. ***ALL*** email communications which contain confidential information such as PHI must contain an email "signature", which includes, at a minimum, the sender's full name (first and last), academic title, Practice/Department, telephone number and any other pertinent contact details.

4. As a general practice, workforce members should ***not*** send group emails containing confidential information such as PHI to distribution lists or multiple recipients. For unique circumstances that may require group emails, please contact your local IT support group for instructions.

5. Workforce members must avoid the use of confidential information such as PHI in the subject of an email because email subjects are more susceptible to potential viewing by unauthorized individuals. Use generic or non-specific phrases such as "patient record request" instead of "Patient John Jones record request" or "patient information" instead of "Patient Jones, SSN 555-55-5555".

6. If sending either an SSN or PAN is required, only send the last four digits and encrypt the email.

IX. *Proceed with Caution.* All workforce members must consider the inherent risks in communications among workforce members, patients, outside clients, and others as outlined below.

A. *Communication with outside clients.* Electronic communications, such as email, with patients and other clients pose additional risks and challenges.

Electronic communications can foster improved patient relations, improve timely communication with patients, provide a record of contacts, and save time on both sides where a telephone or personal interaction might otherwise be required. At the same time, however, email can create unreasonable expectations. Patients may feel that email inquiries should lead to an immediate response or to diagnosis and treatment decisions without the need for personal interaction. This can potentially lead to delays in appropriate treatment and inefficient use of physician or other provider time. Patients also may not appreciate the confidentiality and security inadequacies of commercial email providers.

B. *Risks.* While the use of email may be convenient and can increase the level of communication among workforce members, patients and others (*e.g.* referring or other treating providers, research colleagues or collaborators), email containing sensitive or confidential information, such as PHI, has potential risks, which include but are not limited to the following:

1. Once sent, there is no control over where an email may be forwarded.
2. Someone who is not an intended recipient may receive and/or intercept the email.
3. The identity of the sender or receiver may be changed.
4. The content of the message may be altered.
5. An email can be broadcast to many unauthorized recipients.
6. An email can transport malicious software or phishing scams that might compromise computer systems or confidential information.
7. Email is not easily indexed by patient identifier, which makes it difficult to account for email disclosures of PHI for a specific patient.
8. Email communications between a physician or other provider and patients can create false expectations regarding diagnosis, treatment, or response time.
9. Email communications between a physician or other provider and patients require the additional step of including the communication in the patient's medical record. Critical clinical information may be lost if this additional step is not followed.
10. There can be no assurance of confidentiality, especially if the email transmission is not on an approved secure email system.
11. Electronic communication with patients/potential patients should only occur at the explicit request and with consent of the patient.
12. Workforce members should not forward any patient email communications outside of the University of Maryland system without the consent of the patient.
13. Workforce members should redirect patients who request electronic communication to MyPortfolio.

Please contact your local IT support group or the SOM/FPI Information Security Office for further assistance or information.

References:

Committee Review:	UMSOM ITAAC- 09/14/2016
Other References:	Federal Law: 45 CFR §§ 164.312(e)
Review Cycle:	Annual
Document Owner:	SOM/FPI ISO