Submission ID:
For CEO's Office Use Only

USF Health Care

New:	☐	Revised:	☒	Supersedes:	07/15/20

Internal Guideline and Procedure Name:	**Email Communications Containing Protected Health Information**		
Responsible Office:	Privacy & Healthcare Civil Rights Compliance Program (PHCR)		
Submitted By:	Barbara Wolodzko	**Title:**	Privacy Officer

Review/Approvals:	***Committee Name and/or CEO Name:***	**Date Approved:**
Oversight Committee ***(if applicable):***		
Sr. Assoc. Vice President, USF Health Chief Operating Officer, USF Health CEO, UMSA	Renee Dubault	
USFHC Finance, EMC or CLB ***(if applicable)*****:**		

OBJECTIVES AND PURPOSES:

To establish standards regarding email communications containing individually identifiable health information considered Protected Health Information (PHI) under the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules. (See 45 CFR § 164.530(c).) This addresses only email communications.

STATEMENT OF INTERNAL GUIDELINES.

The best practice for communications containing PHI should be the use of the secure patient portal, MyChart. Utilizing MyChart also complies with the requirement that all treatment decisions are documented in the patient's electronic medical record.

However, if a patient contacts a provider by email communication, the provider should respond by email to the patient in accordance with the procedures outlined below advising the patient, in her or his sole discretion, whether he or she will communicate with a patient via email. A provider may deny a patient's request to communicate via email and instead direct the patient to communicate via telephone or through the secure patient portal, MyChart. If the provider agrees to accept email communications, a copy of each consent given by a patient to communicate via email must be secured in the electronic medical record.

In accordance with HIPAA regulations, any external email communication containing personally identifiable information or confidential data should be encrypted. However, email communications between USF Health (@usf.edu) email, USF Tampa General Physicians (USFTGP) (@usftgp.org) email, and Tampa General Hospital (@tgh.org) email is transmitted within an encrypted tunnel so individual email encryption is not required by the workforce member.

However, encryption is required for external email communications to other entities and emails to non-USF Health email addresses, non-USFTGP email addresses, and non-TGH email addresses. For example, an email sent from a USF Health email address (@usf.edu) to a Gmail account, a Yahoo account or other institutions without a secure connection must be encrypted. All internal email between USF Health email addresses (@usf.edu) USFTGP email addresses (@usftgp.org) and TGH email addresses (@TGH.org) are

protected by the firewall and do not require encryption. For more information on how to encrypt an email please reach out to Information Security.

Email communications containing PHI should be treated with the same degree of privacy and confidentiality as the patient's medical record. All email communications, sent or received, concerning the treatment of a patient, are to be considered part of the patient's medical record and are to be secured in the patient's medical record.

AREAS OF RESPONSIBILITY FOR IMPLEMENTATION.
In response to email communications from patients containing or related to PHI, inform the patient of the availability of the online patient portal, MyChart, for secure communications.

If a patient insists on email communications with their physician, the physician in his or her sole discretion, should inform the patient that he or she:

- does not communicate with patients via email and instruct the patient to either communicate via telephone or through the secure patient portal, MyChart, or
- does communicate with patients via email and add the following statement:

  "USF Health cannot and does not guarantee the privacy or security of any messages being sent over the internet. There is a potential that emails sent over the internet can be intercepted and read by others. If this concerns you, you should not communicate with me through email. By responding to this email, you consent to email communications."

RESPONSIBLE OFFICE
The preceding was developed by the Privacy Officer, USF Health Privacy & Healthcare Civil Rights Compliance Program (PHCR). Any questions or concerns should be directed to PHCR at privacy@usf.edu or their helpline at (813) 974-2222.

Prior approval: Revised for name change and contact updates 02/27/24; PSAC 08/24/20 and Practice Leadership Team 10/21/20; 5/12/17 Updated Electronic Messaging to address only email communications; CPO 07/12/16, 07/06/17, AVP of QSR 07/06/16, 07/16/17 and by USF Health PSAC 4/19/16, 04/18/17.