SECTION 5: SECURITY OF PHI AND OTHER RESTRICTED DATA

5.2. Electronic Mail

POLICY

1. E-mail may be used by University of Florida (UF) workforce members to transmit Protected Health Information (PHI) and other restricted data, except Social Security Numbers, under specific conditions and for limited purposes. Social Security Numbers, even in a truncated form, must be encrypted when transmitted either within or outside the ufl.edu system.
2. UF electronic mail may not be automatically forwarded to a non-university provided or approved service.
3. University business must be conducted using an assigned ufl.edu email address.
4. Emails on the university mail system have the following default retention settings:
    a. Inbox and Sent Items: 3 years from creation or receipt
    b. Deleted Items: Purged after 30 days.
5. The Minimum Necessary Rule applies to e-mails containing PHI.
6. This policy applies to all electronic mail sent or received in the scope of employment at UF, or with the intention to conduct university business. It applies to all e-mail users including, but not limited to, faculty, staff, students, and volunteers. However, this policy does not supersede or replace any UF IT email policies.

GENERAL REQUIREMENTS

1. UF workforce members are reminded that a UF e-mail account is provided as part of a person's employment, clinical, educational, and/or professional relationship with UF. As such, individuals should use their E-mail account to support their employment, clinical, educational and/or professional duties.
2. Generally speaking, "E-mails are forever." Therefore, individuals should not send e-mail that they would not want another person, their employer, an attorney or a jury to read.
3. E-mails containing PHI or other Restricted Data may be sent from one ufl.edu address to another ufl.edu address. The sender of any such e-mail is responsible for ensuring that the recipient's address is within the ufl.edu e-mail system.
    a. UF business-related e-mail may not be auto-forwarded or otherwise transferred to non-ufl.edu accounts, including but not limited to, e-mail services such as Gmail, Yahoo, Hotmail, etc.
    b. No distribution lists, personal e-mail groups, or other multi-recipient lists may be used to send e-mail that contains PHI or other restricted data.
4. Communicating PHI and other Restricted Data (see also PHI in Email section further below)
    a. PHI may be communicated securely by e-mail when both the sender and recipient(s) have a professional Need-to-Know the PHI shared and when the amount of PHI shared is limited to what is minimally necessary to accomplish the task.
    b. PHI and other sensitive information must be shared by a secured method (e.g. between "ufl.edu" users, encrypted, etc.) per UF Information Security and related policies.

c. E-mails containing PHI or other Restricted Data must be encrypted if sent outside the UF domain (i.e., to an email address that does not end in "ufl.edu").

d. Individuals should refrain from sending Social Security numbers by E-mail.

e. E-mail authors should limit the amount and type of PHI placed in the subject line of an e-mail.

f. Individuals may not e-mail credit card information.

g. Clinicians and other individuals who communicate with UF Health patients should encourage patients who want to communicate electronically with caregivers to use the patient portal associated with Epic (e.g. MyUFHealth)

5. Patients and Research Participants

   a. The UF IRBs and/or certain research protocols may require extra safeguards when e-mailing PHI or other Restricted Data (i.e., the data must be encrypted in transit).

   b. Contact the applicable IRB for additional requirements.

DEFINITIONS

1. ***E-mail:*** A means or system for transmitting written messages electronically (as between terminals linked by telephone lines, cable networks, or other relays).
2. ***Restricted Data:*** Data in any format collected, developed, maintained or managed by or on behalf of the university, or within the scope of university activities that are subject to specific protections under federal or state law or regulations or under applicable contracts. Examples include, but are not limited to medical records, social security numbers, credit card numbers, Florida driver licenses, non-directory student records and export controlled technical data.

PRIVACY REQUIREMENTS

1. Patients have the right to request communication by alternative means; however, UF is not obligated to agree to the request.
2. PHI must be safeguarded against unauthorized use or disclosure at all times.
3. Requirements for Data Security: Each covered entity, governmental entity, or third-party agent shall take reasonable measures to protect and secure data in electronic form containing personal information. (FS 501.171)

PROCEDURES – PHI IN E-MAIL

1. Patient Communications: Encourage patients who want to communicate electronically with caregivers about healthcare issues to use the on-line communications portal associated with UF's current electronic health record system. Where this is not possible, assist the patient to complete an *Authorization to Use or Disclose PHI via Electronic Means* (see Forms). Be sure to provide the patient with the correct e-mail address of the person with whom they will be communicating. Signed forms may be delivered to the caregiver by mail, fax, or e-mail.
2. Alert Patients and Research Subjects of E-mail Hazards: Verbally address all of the following issues with patients/subjects or personal representatives who want to communicate by e-mail, before they sign an authorization.

   a. E-mail at UF can be forwarded, intercepted, printed and stored by others.

   b. E-mail communication is a convenience and not appropriate for emergencies or time-sensitive issues.

c. Highly sensitive health or Personal Information should not be communicated by e-mail (i.e., HIV status, mental illness, chemical dependency, worker compensation issues, financial account information, Social Security numbers, etc.)

d. Employers generally have the right to access any e-mail received or sent by an employee at work.

e. Staff other than the health care provider may read and process e-mail.

f. Clinically relevant messages and responses will be documented in the patient's health record.

g. Communication guidelines must be defined between the clinician/researcher and the patient/subject, including,

   i. How often e-mail will be checked,

   ii. Instructions for when and how to escalate to phone calls and office visits, and

   iii. Types of transactions appropriate for e-mail.

h. E-mail message content must include:

   i. The subject of the message in the subject line, i.e., Prescription Refill, Appointment Request, etc., and

   ii. Clear patient/subject identification including name, telephone number and record identification number in the body of the message.

i. UF will not be liable for information lost or misdirected due to technical errors or failures.

3. Retain the completed Authorization form in either the patient/subject's health record or a separate file maintained by the clinician/researcher. Give a completed copy to the patient, if necessary.

4. E-mail Disclaimer Notice: Include the following or a similar confidentiality disclaimer statement in all e-mails that are sent from UF:

   NOTE: This communication may contain information that is legally protected from unauthorized disclosure. If you are not the intended recipient, please note that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this message in error, you should notify the sender immediately by telephone or by return e-mail and delete this message from your computer.

PROCEDURES – OTHER RESTRICTED DATA IN E-MAIL

1. This section applies to all use of e-mail systems within UF where the correspondence contains restricted data. It applies to e-mail that either originates from or is forwarded into a computer or network used for UF mission or business purposes. It applies to all e-mail users including, but not limited to, faculty, staff, students, and volunteers.

   a. Electronic mail (e-mail) may be used by University of Florida (UF) workforce members to transmit restricted data, except Social Security Numbers, under specific conditions and for limited purposes. Social Security Numbers, even in a truncated form, must be encrypted when transmitted either within or outside the ufl.edu system.

2. Conditions: All applicable conditions below must be met in order to include restricted data in e-mails:

   a. Student UFIDs may only be included in E-mail communications that are directly related to official University records and to perform authorized business transactions where unique identification of students is necessary.

b. Internal E-mails may only be sent from one ufl.edu address to another ufl.edu address. The sender of any e-mail containing PHI is responsible for ensuring that the recipient's address is within the ufl.edu e-mail system.

c. UF business-related e-mail may not be auto-forwarded or otherwise transferred to non-ufl.edu accounts, including but not limited to, e-mail services such as Gmail, Yahoo, Hotmail, etc.

d. No distribution lists, personal e-mail groups, or other multi-recipient lists may be used to send e-mail that contains restricted data.

e. Access to ufl.edu e-mail accounts through the Internet must be by secure (SSL) connections.

f. Authorized external e-mail communications containing restricted data (i.e., sent outside the ufl.edu domain) must be protected by encryption.

3. When replying to e-mail containing restricted data from senders outside the ufl.edu system, the restricted data may not be re-sent in the e-mail reply; that is, the response from UF may not contain the restricted data that was included in the sender's original e-mail.

4. E-mail messages relevant for documentation purposes must be printed or otherwise preserved in full and included in the appropriate UF business or academic record.

5. Sending internal e-mails containing restricted data:

   a. Always double-check to be sure the recipient's e-mail address is within the ufl.edu e-mail system.

   b. Do not include a student UFID with the student's name in the subject line of e-mails. Limited student names with associated UFIDs may be included in the body of the email. Place lists of student UFIDs (more than 3) in an electronically secured (at least password protected) attachment to your e-mail message.

6. E-mail Encryption and protections may be accomplished in either of the following ways:

   a. Encrypt the connection(s) between sender and receiver (i.e., through SSL, TLS or VPN), or

   b. Place restricted data in a word or data file, protect the file using a strong password/code, and communicate the password/code to the recipient in a secure fashion. DO NOT include the pass code in the email with the file.

7. Include the following confidentiality statement or a comparable statement in all e-mails that are sent from the University of Florida:

   NOTE: This communication may contain information that is legally protected from unauthorized disclosure. If you are not the intended recipient, please note that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this message in error, you should notify the sender immediately by telephone or by return email and delete this message.

REFERENCES

1. HIPAA: 45 CFR §164.306 Security standards: General rules, §164.522 Right to Request Privacy Protections
2. Florida Statutes: 501.171(g) Security of confidential personal information
3. UF IT Data Security Standards at https://it.ufl.edu/policies/information-security/
4. UF Regulations: 1.0103 Policies on Restricted Data: 4.007 Confidentiality of Student Records and Applicant Records

EXHIBITS

1. UF Email Policies at, https://it.ufl.edu/policies/email/
2. UF Privacy *Authorization to Use or Disclose PHI via E-mail* form at, http://privacy.ufl.edu/uf-health-privacy/forms/.