Policy Name: Electronic Communications Acceptable Use	
Originating Officer (Title), Council, or Committee: System Privacy and Information Security Officers	**Effective Date:** 11/04/2015
Approved By: System Leadership Council	**Last Reviewed Date:** 11/04/2015
Page 1 of 11	

1.0 Scope:

1.1 Applicable Entities:
This policy applies to Texas Health Resources and its member entities, Texas Health Group Health Plans, Users of Texas Health Electronic Communication Systems, and excludes Texas Health joint venture entities.

1.2 Applicable Departments:
This policy applies to all departments.

2.0 Purpose:

2.1 To provide consistent guidelines and direction for the acceptable use of Texas Health Electronic Communication Systems including Email, Texas Health's Intranet, the Internet and voicemail for Confidential Information, Protected Health Information (PHI) and Sensitive Personal Information (SPI).

3.0 Policy Statement(s):

3.1 Use of Texas Health Electronic Communication Systems must comply with the guidelines established in this policy.

4.0 Policy Guidance:

4.1 Guidelines for Electronic Communication Systems Acceptable Use.

4.1.1 Texas Health maintains Electronic Communication Systems to assist in the conduct of business within the company. These systems, including the equipment and the data stored in the systems, are and remain at all times the property of Texas Health whether they are located in the employee's home, at a remote location, or on the premises of any Texas Health clinical facility or business location. All messages created, sent, received, posted or stored in the Texas Health system as well as all information and materials downloaded in the Texas Health computers are and remain the property of Texas Health.

4.1.2 Users of these Electronic Communication Systems are encouraged to make use of the systems while maintaining a diligent and professional working environment.

4.1.3 Electronic Communication Systems are provided primarily for the conduct of Texas Health business. Employees may send and receive personal electronic communications during nonworking times, including breaks, meal periods and other times when they are not expected to be performing job functions. Non-work related electronic communications may not interfere with work-related activities and may not violate Texas Health policies regulating employee conduct.

4.1.4 Abuse of the Electronic Communication Systems is a violation of this policy.

4.1.5 Electronic Communication Systems and the products they produce, such as E-mail messages, may not contain offensive content that could contribute to a hostile work environment on the basis of race, sex, disability, religion or any other protected classification, or threats of violence or similar inappropriate or unlawful conduct.

4.1.6 Individuals who use the Texas Health Electronic Communication System Email to communicate externally with others (in the course of their job or on behalf of Texas Health), must adhere to the Texas Health Email Signature Protocol available on the Intranet.

4.1.7 Users are expected to adhere to all Texas Health policies including the Confidentiality, Privacy, Information Security and Social Media policies.

4.2 Texas Health Rights.

4.2.1 Texas Health reserves the right to override an individual's passwords and/or codes to facilitate access by Texas Health to Electronic Communication Systems.

4.2.2 Texas Health retains the right to access and review the User's Electronic Communication Systems, including E-mail, at any time for any reason without notice to the employee. Such reasons include, but are not limited to, determining and/or preventing abuse of Electronic Communication Systems, assuring compliance with Texas Health policies, conducting Texas Health business and/or investigating conduct or behavior that may be illegal or adversely affect Texas Health Users or customers.

4.2.3 By using Texas Health Electronic Communication Systems, all Users knowingly and explicitly consent to the monitoring of such use and acknowledge Texas Health's right to conduct such monitoring.

4.3 Additional guidelines on use of Voicemail.

4.3.1 Reasonable efforts should be taken to protect confidentiality of Confidential Information, PHI or SPI when leaving, retrieving or forwarding voicemail that may contain such information.

4.3.2 Voicemail containing Confidential Information, PHI or SPI should only be left for those with a legitimate need-to-know, using the minimum amount necessary.

a. When leaving a message, you should verify that you are leaving the message for the intended recipient. (Verify that the greeting for the mailbox is that of the intended recipient.)

b. Care should be taken when forwarding messages to confirm they are forwarded to the intended recipient.

4.4 Additional guidelines on use of Internet.

4.4.1 Reasonable efforts should be taken to protect confidentiality and prevent unauthorized disclosure of Confidential Information, PHI or SPI when using the Internet.

4.4.2 If using the Internet to input Confidential Information, PHI or SPI, the User should verify the site is secure. (This could be accomplished by observing the security lock in the lower right hand corner of the browser or reviewing the address in the address bar to verify it begins with "https".) If the site does not appear to be secure, the information should not be entered.

4.5 Additional guidelines on use of Email.

4.5.1 Reasonable efforts will be taken to protect confidentiality of Email containing Confidential Information, PHI or SPI. Email containing Confidential Information, PHI or SPI should be distributed only to those with a legitimate need-to-know using the minimum amount necessary.

4.5.2 Use of large Email distribution lists by individuals (in the course of their job or on behalf of Texas Health) during work time, will be limited to the following approved senders: directors and above, Human Resources Officers and their designees, Security, Emergency Management, Texas Health Resources University, and Communications & Image. Entity triads in collaboration with the ITS Help Desk may approve others as appropriate.

4.5.3 Storing and viewing of Confidential Information within Email system calendaring must be restricted to authorized individuals.

4.5.4 Sending Email Containing Confidential Information, PHI or SPI.

a. Reasonable efforts will be taken to verify the identity of the requestor/recipient prior to the transmission.

b. Email containing Confidential Information, PHI or SPI that is sent via Internal Email is permissible using the following guidelines:

1) The Texas Health Email address book should be used to select the recipients of the Email.

2) The sender should verify that they are sending to the correct individual by viewing detailed description of the individual within the Email address book.

3) Confidential Information, PHI or SPI may be distributed to multiple recipients; however, the use of distribution lists is not recommended.

4) The word “Secure” should be added to the subject line of the e-mail, to indicate the confidential nature of the information to the recipient.

c. Email containing Confidential Information, PHI or SPI should only be sent to Internet Mail (Email external to our systems) if the following guidelines are met:

1) Auto forwarding of Email to an external Email address is not authorized.

2) Encryption tools or other secured methods of Email delivery that are approved by Texas Health should be used to protect the information during transmission. If encryption or other secure method of Email delivery cannot be used, Confidential Information, PHI or SPI should not be sent externally by Email (except PHI as permitted by the Patient Access to Health Information Policy).

i. The word “Secure” must be added to the subject line of the e-mail. This will encrypt the message to the external party.

3) Storing of Email or attachments containing Confidential Information, PHI or SPI on unencrypted systems or systems not managed by Texas Health is not authorized.

4) Confirm the external Email address prior to sending the Confidential Information, PHI or SPI using one or more of the following methods:

i. Confirm the correct spelling and punctuation of the address with the intended recipient, or

ii. Send a test Email message to the recipient and confirm receipt.

iii. When a request for Confidential Information, PHI or SPI is made via Email, the reply button should be used to reply to the message.

5) This statement should be included in all external Email communications that contain Confidential Information, PHI or SPI.

i. The information in this Email is confidential, sensitive personal or protected health information intended only for the addressee(s) use to accomplish the intended purpose. Any other person, including anyone who believes s/he might have received this message in error, is requested to notify the sender immediately by return Email, and to delete it without further reading or retention.

d. When a User becomes aware of sending Email containing Confidential Information, PHI or SPI to an incorrect or misdirected Email address:

1) Attempt to electronically recall the Email. (This can only be done for internal messages).

2) Contact the recipient by phone and/or Email. Inform the recipient that the information was sent in error and request that the documents be deleted and/or destroyed.

3) Notify your immediate supervisor of any internal misdirected Email.

4) Notify the entity privacy officer or information security officer regarding the circumstances of any external misdirected Email containing PHI or SPI.

5) Notify HR about misdirected Email containing Confidential Information.

4.5.5 Receiving Email Containing Confidential Information, PHI or SPI.

a. Texas Health will take reasonable precautions to protect Email containing Confidential Information, PHI or SPI. (See Section 8.0 – Related Documentation and/or Attachments)

b. Once the intended purpose of the Confidential Information, PHI or SPI has been accomplished, the Email should be purged.

c. When a User becomes aware of receiving misdirected Email:

1) Notify the sender that an Email was received in error.

2) Delete the Email without further reading of the contents.

3) Do not use or disclose the content of the Email that was received in error.

4.6 Sanctions.

4.6.1 Violations of this policy will be processed according to applicable Texas Health policies including the Progressive Corrective Action policy.

4.6.2 Any employee who observes anyone violating this policy should promptly notify his or her supervisor, a representative of Human Resources, the entity privacy or information security officer, or the Texas Health Compliance Hotline at 1-800-381-4728.

4.7 Nothing contained in this policy shall be construed to restrict employees' rights to discuss the terms and conditions of their employment, working conditions, and other protected activity as provided under applicable law.

5.0 Definitions:

5.1 Confidential Information - Information including patient information, protected information of participants of Texas Health benefit plans and programs, customer information, physician credentialing, peer review, quality review, business intelligence, privileged committee records, logon and password information,

employee health records, protected health information, social security numbers, financial account information or credit card information.

Confidential Information also includes trade secrets and other similar confidential business information related to internal business affairs and operations of Texas Health (such as information regarding the development of systems, processes, policies, know-how, and technology, as well as internal reports, procedures, or other internal business-related confidential communications) that is not generally available to the public. Any information which has potential to jeopardize Texas Health's marketplace competitiveness is considered Confidential Information.

Furthermore, employees may use or disclose information learned or acquired through his/her association with Texas Health only for the performance of his or her job or as otherwise permitted by law.

This definition does not restrict employees from discussion their wages and terms and conditions of employment as permitted by law.

5.2 Contractor - Any non-Workforce person or entity including its employees or agents that provides services to Texas Health or any of its wholly owned or controlled entities and whose employees or agents may encounter Confidential Information while providing services under the Contractor's agreement with Texas Health.

5.3 Electronic Communication Systems - These systems include, but are not limited to, Texas Health Intranet, Internet and Voicemail.

5.4 Email - A corporate information asset used to transmit and communicate information electronically to conduct Company business.

5.5 Group Health Plan - Texas Health-sponsored group health plan (GHP) providing for medical, dental, vision or health care spending reimbursement. Certain functions of the GHP may be delegated to Third Party Administrators.

5.6 Health Information - Any information, including Genetic Information, whether oral or recorded in any form or medium, that is created or received by a provider, plan, employer or clearinghouse; and that relates to the past, present, or future health condition of an Individual as well as the provision of healthcare to the Individual.

5.7 Individual - The subject of Health Information. This includes patients, Group Health Plan participants and their covered dependents. Legally Authorized Representatives will be accorded the same rights regarding Uses and Disclosures of Health Information as the Individual.

5.8 Individually Identifiable Health Information (IIHI) - Health Information that identifies the Individual or provides a reasonable basis for doing so, by virtue of containing one or more of the eighteen identifiers specified by the Privacy Rule.

5.9 Internal Email - Email sent and/or received from Texas Health's internal closed network such as the Intranet.

5.10 Internet - The worldwide "network of networks" forming connections using Internet protocol. The Internet provides file transfer, remote login, Email, news and other services. For the purposes of this policy, Internet will be considered to be both specific and generic to electronic pathways connecting private and public information processing and storage facilities.

5.11 Internet Email - Email sent and/or received across the Internet. Texas Health Workforce members with Email on their PC also have Internet mail.

5.12 Intranet - Communications architecture similar to the Internet but constructed for internal organizational use.

5.13 Legally Authorized Representative - (1) A parent or legal guardian, if the patient is a Minor; (2) a legal guardian, if the patient has been found by a court to be incapable of managing the patient's personal affairs; (3) an agent of the patient authorized under a Medical Power of Attorney for the purpose of making a health care decision when the patient is incompetent; (4) an attorney ad litem and/or guardian ad litem appointed for the patient by a court; (5) A person authorized to consent to medical treatment on behalf of the patient under Chapter 313 of the Texas Consent to Medical Treatment Act (6) a personal representative or heir of the patient, if the patient is deceased; (7) an attorney retained by the patient or by the patient's legally authorized representative; (8) a person exercising a power granted to the person in the person's capacity as an attorney-in-fact or agent of the patient by a Statutory Durable Power of Attorney that is signed by the patient as principal. (See Texas Health's Policy on Health Information Uses and Disclosures for full definition).

5.14 Medical Staff - Includes all members, however classified (active, courtesy, etc.) of entity medical staffs.

5.15 Privacy Rule - The Health Insurance Portability and Accountability Act of 1996 Final Privacy Rule.

5.16 Protected Health Information (PHI) - Individually Identifiable Health Information that is protected by the requirements of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and Texas state law.

5.17 Sensitive Personal Information (SPI) - means:

5.17.1 A person's first name or first initial and last name in combination with any one or more of the following items, if the names and items are not encrypted. For this purpose, person means anyone with this type of information maintained by Texas Health, such as employee, patient, physician, volunteer information, etc. (Sensitive Personal Information does not include publicly available information that is lawfully made available to the general public from the federal, state or local government.)

a. Social security number;

b. Driver's license number or government-issued identification number; or

c. Account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to a person's financial account; or

5.17.2 Information that identifies an individual and relates to:

a. The physical or mental health or condition of the individual;

b. The provision of health care to the individual; or

c. Payment for the provision of health care to the individual.

5.18 Trustee/Director - Refers to a person who serves as a member of the governing board of Texas Health Resources or any of its wholly owned or controlled corporations pursuant to the bylaws of the respective corporation.

5.19 Users - Texas Health Workforce members, members of Texas Health facility Medical Staff, Trustees/Directors, contractors, vendors or others who use the Texas Health Electronic Communication Systems.

5.20 Workforce - Employees, volunteers, persons involved in Texas Health training programs or those sponsored by its wholly owned or wholly controlled entities, and other persons whose conduct, in the performance of work for an entity, is under the direct control of such entity, whether or not they are paid by the entity.

6.0 **Responsible Parties:**

6.1 Entity Privacy Officer

6.1.1 Responsible for implementation and oversight of this policy and Privacy policies to maintain compliance with federal and state laws as it applies to an Individual's PHI or SPI.

6.2 Entity Information Security Officer

6.2.1 Responsible for implementation and oversight of this policy and IT Security policies and standards to maintain compliance with regulations and industry best practices as it applies to Confidential Information, PHI or SPI.

6.3 Communications & Image department

6.3.1 Responsible for implementation and oversight of this policy as it pertains to the Texas Health Email signature protocol and large Email distribution lists.

6.4 Entity Human Resources Officer

6.4.1 Responsible for implementation and oversight of this policy and HR policies as it applies to Confidential Information.

6.5 This policy applies to all Users as defined in this policy.

7.0 **External References:**

7.1 HIPAA Administration Simplification 45 C.F.R. Parts 160 and 164.

8.0 **Related Documentation and/or Attachments:**

8.1 Acceptable Workstation Use - THR System Policy

8.2 Confidentiality - THR System Policy

8.3 Encryption - THR System Policy

8.4 Health Information Uses and Disclosures - THR System Policy

8.5 Information Privacy and Security Sanctions - THR System Policy

8.6 Minimum Necessary Use and Disclosure of Health Information Policy - THR System Policy

8.7 Mobile Security, Photography and Secure Text Messaging ITP-14 - THR System Policy

8.8 Password Management - THR System Policy

8.9 Patient Access to Health Information - THR System Policy

8.10 Payment Card Data Security ITP-10 - THR System Policy

8.11 Progressive Corrective Action - THR System Policy

8.12 Social Media - THR System Policy

9.0 **Required Statements:**

Not Applicable