



TITLE: ACCEPTABLE USE OF HCHD INTERNET AND EMAIL SYSTEM

PURPOSE: To establish the guidelines for the use of the Harris County Hospital District's Internet and email system.

POLICY STATEMENT:

In order to conduct Harris County Hospital District (HCHD) business in the most efficient manner possible, HCHD systems' Users shall be permitted to use HCHD's Internet and email system. Use of the HCHD's Internet and email system must be limited to business purposes and done in a professional, lawful, and ethical manner. Violations of this policy shall include discipline up and including termination.

POLICY ELABORATION:

I. DEFINITIONS:

- A. ELECTRONIC MEDIA:** Storage media including memory devices in computers (hard drives) or any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, compact flash drive, or digital memory card.
- B. ELECTRONIC PROTECTED HEALTH INFORMATION (ePHI):** Protected Health Information that is created, received, maintained, or transmitted by electronic means.
- C. HCHD'S INTERNET AND EMAIL SYSTEM:** Any computing device, including any personal device that is owned, subsidized, or provided by the HCHD that is used to store, view, or manipulate HCHD data, including email, whether connected directly to or indirectly the HCHD's authorized Internet or email server. Examples include, but are not limited, to personal computers, netbooks, laptops, personal digital assistants (PDA), digital cameras, cellular phones, Smartphone, or personal tablet computers owned, subsidized, or provided by the HCHD.
- D. INTERNET:** An international network of independent computer systems. The World Wide Web is one of the most recognized means of using the Internet.



- E. MALICIOUS SOFTWARE AND EMAIL:** Programs designed to damage or disrupt an information system (e.g., a virus); and/or emails such as phishing or emails that appear strange or suspicious
- F. OBJECTIONABLE INFORMATION OR MATERIAL:** Anything that is offensive, defamatory, obscene, or harassing, including, but not limited to, sexual images, jokes and comments, racial or gender-specific slurs, or any other comments, jokes, or images that would be expected to offend someone based on their physical or mental disability, age, religion, marital status, sex, sexual orientation, gender identity/expression, political beliefs, veteran status, national origin, or ancestry, or any other category protected by federal, state, or local laws.
- G. PROTECTED HEALTH INFORMATION (PHI):** Individually identifiable Health Information of a patient in any form that is created or received by a healthcare provider, and relates to the patient's healthcare condition, provision of healthcare, or payment for the provision of healthcare.
- H. SPAM/JUNK EMAIL:** Bulk solicited or unsolicited email, which can be either commercial (such as an advertisement) or noncommercial (such as a chain letter from a friend) and which does not serve a HCHD purpose.
- I. SUBSIDIZED DEVICE:** Any device whose use is subsidized by the HCHD.
- J. UNAPPROVED SOFTWARE:** Any application that has not undergone testing and approval by HCHD Information Services.
- K. USER:** Any person who uses or accesses the HCHD's Internet or email system to read, enter, update, send, copy or print information regardless of the medium.
- L. VIOLATION:** An infraction of this policy or any other policy, procedure or safeguard that may result in damage to the HCHD or exposure to liability, whether such damage or liability actually occurs.
- M. SYSTEM:** Includes computers portable and stationary, emails, wireless devices, and e.g., EPIC, ASAP, PACS, etc., systems.



II. BUSINESS USE:

- A. HCHD Internet and email system is to be used for legitimate business purposes and the HCHD reserves the right to monitor, review, audit, intercept, access, and disclose all information that a user creates, receives, sends, or stores while using the HCHD's Internet or email system. Users may be granted access to the HCHD's Internet and email system to assist them in the performance of their jobs. All users have a responsibility to use the HCHD's Internet and email system in a professional, lawful and ethical manner. Users may access the HCHD's Internet and email system for incidental or de minimis personal use. Users of the HCHD's Internet and email system who commit violations shall subject to disciplinary action, up to and including termination.
- B. Access to and disclosure of PHI and e-PHI are governed by the state and federal laws and regulations as referenced in HCHD privacy and security, and Health Information Portability and Accountability policies.

III. PERSONAL USE:

- A. While incidental or de minimis personal use of the HCHD's Internet and email system may occur when it does not interfere with the User's productivity or work performance, such use is a privilege that may be revoked at any time at management's discretion. An example of incidental or de minimis personal use of the HCHD's Internet and email system is a quick search of current weather or traffic conditions. This small exception does not authorize any User to operate a commercial or personal business by using the HCHD's Internet or the email system. A User has no expectation of privacy in any communication, message, data, or information on or transmitted as a result of his/her personal use of the HCHD's Internet or email system. Incidental or de minimis personal use of the HCHD's Internet and email system is monitored by HCHD and must not interfere (1) with the User's productivity or work performance or (2) the performance of HCHD's computer system. All electronic communications, including emails and instant messages, created, sent, received or stored on the HCHD's Internet or email system are and remain the property of the HCHD. They are not the private property of any User and are subject to viewing, downloading, inspection, release, and archiving by the HCHD at all times. In addition, this information is subject to disclosure to the User's supervisors, law enforcement, government officials, or to other third parties as authorized by law.



- B. Users of the HCHD's Internet and email system must not use the HCHD's Internet and email system for soliciting business, selling products, or otherwise engaging in commercial activities.
- C. Users must not create, receive, send, view, or store Objectionable Information or Material on the HCHD's Internet and email system.
- D. The use of abusive, profane, or offensive language and any illegal activities including piracy, cracking, extortion, blackmail, copyright infringement, and unauthorized access to any computers on the Internet or email are prohibited.
- E. Each User is responsible for the content of all text, audio or images that he or she places or sends over HCHD's Internet and email system. No email or other electronic communications may be sent which hide the identity of the sender or represent the sender as someone else.
- F. Users must not place HCHD confidential or Protected Health Information on any computer system, which may be viewed or accessed by persons who are not authorized to access or view this information.
- G. Users must not use the HCHD's Internet or e-mail systems to distribute Junk Mail.
- H. Users must not utilize the HCHD's Internet and email system to transmit any information in violation of applicable laws or regulations, including in violation of copyright or other intellectual property laws.
- I. Unless the HCHD Legal Department has approved in advance, users are prohibited from using HCHD's Internet and email system connections to establish, operate, conduct, or further non-HCHD business channels.
- J. HCHD confidential or Electronic Protected Health Information must not be sent over the HCHD's Internet and email system unless it has first been encrypted by methods approved by Information Security.
- K. Users must not up-load or transmit software, which has been licensed from a third party, or software which has been developed by HCHD to any computer through the



HCHD's Internet and email system via e-mail unless authorized in writing by Information Security and the HCHD Legal Department.

- L. Users must not store fixed passwords in dial-up communication programs or Internet browsers at any time.
- M. HCHD's Internet and email system Users must not engage in video or audio streaming unless these have been approved in advance by the Information Security Department.
- N. Users must not use workstations to participate in any manner with sites that promote pirating software even if this participation occurs during non-working hours.
- O. Users must not download software from the Internet unless authorized in writing by Information Security.
- P. Users must not download Malicious Software or Unapproved Software.

IV. PRIVACY:

- A. **Users have no expectation of privacy in their use of Workstations.**
- B. To the extent allowed by law, HCHD officials, managers, and their designees are permitted to review a User's electronic devices which include electronic devices whose use is subsidized or provided by the HCHD, electronic files, messages, e-mail, and Internet usage to ensure that HCHD's Internet and email systems are being used in compliance with the law and HCHD policies. Violation of this policy shall lead to discipline up and including termination.

V. SYSTEM CONFIGURATION:

- A. The HCHD has the right to monitor and log any and all aspects of its computer system and Electronic Media including, but not limited to, monitoring Internet sites visited by users, monitoring chat and newsgroups, monitoring file downloads, and all electronic communications, including e-mail, sent and received by Users.
- B. The HCHD has the right to utilize software that makes it possible to identify and block access to Internet sites.



REFERENCES/BIBLIOGRAPHY:

HCHD Information Security Policy and Procedures 3.11.800 Information Security Policy.

HCHD Information Security Policy and Procedures 3.11.803 Information System User Responsibility Policy.

HCHD Policy and Procedures 6.20 Employee Discipline Policy.

Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191 (codified at 45 C.F.R. Parts 160 and 164), as amended.

Title XIII, Subtitle D of the American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, as amended (“HITECH Act”).

TEX. HEALTH & SAFETY CODE ANN. § 181.001 *et seq.*, as amended.

OFFICE OF PRIMARY RESPONSIBILITY:

Vice President, Human Resources

REVIEW/REVISION HISTORY:

Record review and revisions below:

Effective Date	Version# (If Applicable)	Review or Revision Date (Indicate Reviewed or Revised)	Reviewed or Approved by: (If Board of Managers Approved, include Board Motion#)
	1.0 Original	Reviewed 09/18/2007	Vice President, Human Resources and Director, Information Systems
		Approved 10/02/2007	HCHD Policy Review Committee
12/6/2007		Approved 12/06/2007	HCHD Board of Managers (No. 07.12-587)
	2.0	Revised/Approved 07/12/2011	HCHD Operations Policy Committee