HEALTHQUEST

Title: *Acceptable Use of E-Mail and Voice Mail Policy*	**Number/Type**: *HQ. 5.11*
Owner: John Schwartz, CISO	**Effective Date**: 05/19/2016
For use at: All HQ locations and its affiliates	

PURPOSE:

This policy defines the terms of acceptable use for Health-Quest E-Mail and Voice-Mail uses. Unauthorized and/or inappropriate use of E-Mail and Voice-Mail can expose the Health-Quest Organization, its employees and patients to undue an unacceptable risks. These risks are not acceptable to Health-Quest management, its employees and patients. This policy defines what is and is NOT acceptable to Health-Quest as well as some key controls.

PROCEDURE:

1.1 Statement

As part of its normal operations, Health-Quest makes E-Mail and Voice-Mail accounts available to staff, contractors, and privileged/HQ credentialed clinicians. These accounts are to be used to perform the business and/or clinical functions of the Health-Quest organization and other use is prohibited.

1.2 Applicability

The policy applies to all E-Mail and Voice-Mail accounts maintained by Health-Quest and the personnel it was issued to.

For E-Mail, this includes all accounts ending with “@health-quest.org” as well as any other E-mail accounts setup by and for Health-Questions functions and/or its employees when performing business and clinical operations. *Personal E-Mail accounts are not in the scope of the policy however, it should be noted that when using personal E-Mail accounts, employees should understand and agree that as Health-Quest employee their actions (e.g. forwarding emails) reflect on the organization and are required to follow the Health-Quest code of ethical behavior and the HIPAA Security & Privacy Rules.*

For Voice-Mail, this includes all Voice-Mail accounts maintained on Health-Quest hardware for the use of its staff as well as all accounts provided with mobile devises with voice technologies such as cell phones and iPads, etc. As with personal E-Mail, when using personal Voice-Mail, Health-Quest employees are required to follow the Health-Quest code of ethical behavior and the HIPAA Security & Privacy Rules.

Health-Quest employees are *prohibited from using personal E-Mail* and Voice-Mail in their routine discharge of their responsibilities. If they are faced with unusual circumstances and employees find themselves using these personal accounts, they must notify their manager and conduct themselves in accordance to Health-Quest code of ethical behavior and adhere to HIPAA Security & Privacy Rules.

1.3 Ownership and Privacy

Health-Quest E-Mail and Voice-Mail account and the hardware and internal networks that they run on are all to be considered the property of Health-Quest regardless of whether they are purchased or leased. In addition, any leased communication devices and Health-Quest loaded software which are paid for by Health-Quest are to be treated as they property of the Health-Quest organization.

- Private and public networks and the equipment which are not owned by Health-Quest are to be treated as such for the purposes of this policy when and if they are used by Health-Quest staff in the performance of their jobs.

- Any information created, store and/or transmitted using the equipment referenced above are, without exception except as defined by law, the property of Health-Quest. No one, regardless of their employee status with Health-Quest, using this equipment for E-Mail or Voice-Mail should have any expectation of privacy or ownership of such information.

- Health-Quest reserves the right to inspect any messages, voice, or data created, stored and/or transmitted using its equipment. This right is entirely at the discretion of Health-Quest management for business and clinical purposes and may only be restricted as prohibited by applicable law.

- To ensure that the interrogation of E-Mail and Voice-Mail is performed for authorized business and clinical purposes the following controls are to be maintained:

    - Anyone wishing to have access to an E-Mail or Voice-Mail account will open a service request (Infopoint Ticket). The request will specify a business purpose for the request, the name of the individual whose accounts the requestor wishes to access, the data range and whether or not the individual is a current employee or not.

    - Approval of the request will require sign-off from an HR representative, and one or more of the following: the Chief Information Officer, The Chief Information Security Officer and/or the Chief Compliance Officer. The number of choices available is deliberate so that the appearance of any conflict of interest can be avoided.

    - In the event that the requestor deems that the interrogation of an account represents a matter so sensitive that they are not comfortable having it recorded in a service request, then they are to make their request through a Human Resource representative who will manage the process in a confidential manner.

- In the event that the interrogation of an account is required by a court order, then the legal department will be consulted to ensure that all applicable laws and legal procedures are followed.

1.4 Acceptable and Unacceptable Use

Health-Quest E-Mail and Voice-Mail accounts are to be used for business and/or clinical purposes only.

It is acknowledged that an occasional non-work related message will be sent and/or received using these systems; these must be kept to a minimum. In addition, any occasional personal use must be complaint with the Health-Quest policies, code of ethical behavior as well as all applicable laws and regulations.

Health-Quest E-Mails should have the following disclaimer at the bottom of all messages sent outside the organization:

> "The information contained in this E-Mail is intended for the use of just the named recipient only. It may contain information that is privileged, confidential and exempt from disclosure under applicable law. If you receive this message and are not the intended recipient, you are hereby notified that any use, dissemination, distribution, or copying of this communication is strictly prohibited. If you have received this communication in error, please notify me immediately by using your reply option to advise me of such error. Thank you"

Unacceptable uses include, but not limited to the following:

- The use of wallpaper, graphics, or slogans other than those approved by Health-Quest Public Relations.
- Any E-Mail or Voice-Mail that could be considered "SPAM", i.e., jokes, chain letters, unrecognized sender, attachment or other advertising material from or for unsolicited goods or services.
- Any communications that could be considered harassing or threatening.
- Any forging of signatures or credentialed to make a message appear as if it were coming from someone other than the authentic sender.
- Any communication leaving the organization which the sender has reason to believe would be made public unless communication has been approved by Health-Quest Public Relations. This includes but is not limited to letters to the editor, on-line chats, posts, news groups, and WEBINARS on the Internet.

1.5 Blogging and Instant Messaging

New technologies and practices, such as blogging and instant messaging are subject to the same restrictions as those for E-Mail and Voice-Mail noted above. Instant messaging on the Health-Quest network is only permitted with written authorization from the CIO, or CISO.

1.6 Non-Retaliation and Non-Retribution for Reporting

- “Good faith report” as defined in the Non-Retaliation and Non-Retribution for Reporting policy is not subject to the restriction listed in this policy.
- From the Non-Retaliation and Non-Retribution for Reporting policy: “Employees have a variety of reporting options; however, they are encouraged to take advantage of internal reporting mechanisms. These might include reports to Human Resources, Risk Management, Quality Improvement, Internal Audit, Compliance or the Compliance Hotline”.

1.7 Enforcement

This section of the Information Security Policy will be enforced according to the procedures outlined in HQ 5.1 and HQ Sanction Policy.

REFERENCES/SOURCES

HIPAA		**ISO 27001:2005**	
Title	**Number**	**Title**	**Number**
Workstation Use	164.310(b)	Acceptable use of assets	A.7.1.3
Workstation Security	164.310(c)	Physical security perimeter	A.9.1.1
Person or entity authentication	164.312(d)	Equipment sitting and protection	A.9.2.1
Access control	164.312(a)(1)	Security of equipment off premises	A.9.2.5
Access authorization	164.308.(a)(4)(ii)(B)	Removal of property	A.9.2.7
Automatic logoff	164.312(a)(2)(iii)	Access control policy	A.11.4.2
Security Management Process	164.308(a)(1)	Information security policy	A.5.1
Assigned security responsibility	164.308(a)(2)	Management commitment to information security	A.6.1.1
Risk analysis	164.308(a)(1)(ii)(A)	Classification guidelines	A.7.2.1
Risk Management	164.308(a)(1)(ii)(B)	Information labeling and handling	A.7.2.2
Information system activity review	164.308(a)(1)(ii)(D)	Management Responsibilities	A.8.2.1

Workforce security	164.308(a)(3)	Terms and conditions of employment	A.8.1.3
Authorization and/or supervision	164.308(a)(3)(ii)(A)	Information security awareness and training	A.8.2.2
Workforce clearance procedure	164.308(a)(3)(ii)(B)	Disciplinary process	A.8.2.3
Sanctions policy	164.308(a)(1)(ii)(C)	Termination responsibilities	A.8.3.1
Terminations policy	164.308(a)(3)(ii)(C)	Audit logging	A.10.10.1
Policies and procedures	164.316(a)	Monitoring system use	A.10.10.2
Documentation time limit	164.316(b)(2)(i)		
Documentation availability	164.316(b)(2)(ii)		
Documentation updates	164.316(b)(2)(iii)		

POLICY HISTORY:

Original implementation date: 02/20/2009
Date Reviewed: 05/20/2016
Date Revised: 05/20/2016

APPROVAL:

__John Schwartz HQ - CISO___________________________ ________05/20/2016_____________
[Policy Owner] Date