Title: Practitioner System Access Policy	No. :IM 5.18
	Effective: 2/01/2004
	Revised:
Approved By: Rich Rogers, VP/CIO, Health First	Page 1 of 5

Entity: Health First

I.

II. OBJECTIVE

To preserve the integrity and reliability of Health First's information systems and all data and information contained within the information systems; and to ensure that patient confidentiality obligations are observed by all physicians and allied health professionals ("**practitioner**") having access to and use of Health First information technology systems.

III. DEFINITION

Health First, Inc. **("Health First"),** has acquired and developed a sophisticated, state-of-the-art computer and voice system **(the "System")** that is comprised of both software products **("Software")** and hardware components **("Hardware").** The System supports the information technology requirements of Health First and related and supported entities and individuals.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), section 164.501 defines Individually Identifiable Health Information (IIHI) to include 19 data elements that are considered Protected Health Information (PHI). This includes, patient name, address, date of birth, social security number, system specific account numbers, e-mail addresses, web addresses and other individually recognizable identifiers. Health First is committed to protecting patient privacy and following legislative directives.

Protected Health Information - individually identifiable health information that is transmitted by electronic media, transmitted or maintained in any other form or medium. Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and is created or received by a health care provider, health plan, employer, or health care clearinghouse, and relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual and that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Medical Staff Physicians and Allied Health Professionals – practitioners in a Health First facility granted privileges to practice medicine by the Board of Directors of the specific facilities.

Telnet – System transfer protocol

IV. POLICY

ACCESS AND USE OF THE SYSTEM

Practitioners acknowledge that the ability to access and use the System is a privilege and not a right, and that Health First shall have the right at any time and without notice to terminate practitioner's ability to access and use the System.

All practitioners requiring access to the system must adhere to the following requirements for Health First Health Information Technology system use:

1. Restrictions on Right to Access and Use the System

a) Practitioners agree not to give or allow others to use their password and/or user log-on ID. Practitioners acknowledge that their password and user log-on ID are the equivalent of their signature. In general passwords should not be disclosed to anyone. HIT personnel will not ask for a user's password when troubleshooting a system unless it is absolutely necessary to fix a specific problem. If HIT support personnel need to ask for a user's password, the user will be asked to change his or her password immediately after the problem is resolved.

b) Practitioners will, upon becoming aware of any unauthorized disclosure of their password and/or user log-on ID, immediately notify the HIT Support desk and log a call for the Health Information Privacy and Security Officer notifying them of the unauthorized disclosure and thereafter change their password and/or user log-on ID.

c) Practitioners will log off the System or lock their Health First owned PC computer screen to ensure that any other person cannot use their user log-on ID when left unattended after they have logged onto the System.

d) Practitioners will not give or loan any software application or grant access to the System to any individual not authorized to have such software application or access to the System.

e) Practitioners may not install software on Health First Information Systems, without written approval by the Health Information Technology Department. This includes, but is not limited to executable files, screensavers, media players, FTP Clients, file sharing applications, or gadgets.

f) Practitioners agree to exercise extreme caution to ensure that they do not introduce into the System any virus, worm, trap door, back door, timer, clock, counter or other limiting routine, instruction or design that would erase data or programming or otherwise cause the System to become inoperable (a "***Malicious Code***"). In particular, practitioners agree to use Health First-provided virus-detection software to scan any external data files before loading such data files onto the System. Practitioners further agree not to load such external data files onto the System if Health First's virus-detection software identifies the existence of a Malicious Code. In addition, practitioners agree not to load or introduce any software not supplied by Health First onto their Health First owned PC or onto the System including, without limitation, "instant messaging," audio/video/photo disks/programs, encryption programs and any screen saver software, without the prior authorization of the Health Information Technology Department.

g) Practitioners understand that there is no expectation of individual privacy to any of the information they create and that Health First shall have the right to review or inspect any and all information created by them that resides on the Health First System.

2) Electronic Mail and Voicemail

a) The transmission of PHI, passwords and other sensitive data by electronic mail must be secure. Within the Health First Wide Area Network (WAN), such information is secure, and therefore the transmission is allowed. Outside the Health First Inc. network, such information is not protected and should not be transmitted over an open line.

b) Health First has created a GroupWise group named "Everyone at Health First" for convenience in sending messages to all Health First Groupwise accounts. Practitioners will send messages through Groupwise to this group only when the message has a business need to be addressed to all associates. The Groupwise system may not be used for solicitation or distribution purposes that do not have a business need.

c) Practitioners will not use profanity or any graphic, picture, image or statement in an Groupwise or Voice Mail message that would violate any Health First policy including, without limitation, Health First's non-discrimination and non-sexual harassment policies.

d) Practitioners will not use the Groupwise system for purposes of accessing the files or communications of others for any reason other than Health First business purposes.

e) Practitioners must not create or forward electronic mail messages that are defamatory, harassing or sexually explicit. Messages must not contain profanity, obscenities, or derogatory remarks related to employees, patients, or others. Remarks of this nature, even if made in jest, are prohibited. Practitioners also prohibited from sending or forwarding messages or images via systems that would offend on the basis of race, gender, national origin, religion, political beliefs, or disability.

f) Practitioners understand that they do not have a right of privacy with respect to Groupwise and Voice Mail messages and that Health First reserves the right to access, review, disclose and/or delete any inappropriate material from the contents of Groupwise and Voice Mail communications. Practitioner use of the Groupwise and Voice Mail system constitutes consent to such review by Health First, and practitioners acknowledge that they may not be aware that such review has occurred. Every reasonable effort will be made to notify the associate before such an action.

3) External Network and Internet Access

a) The Internet is a useful research and communication resource that is provided to Health First associates for uses related to Health First business. Access to the Internet provides e-mail capabilities for contacting non-Health First resources and access to databases for research and informational purposes. This policy is intended to prevent the misuse of Internet access, specifically as it pertains to the following unacceptable practices:

1. Downloading files that contain malicious code that may contaminate Health First's information systems and databases;

2. Accessing objectionable or improper material;

3. Misrepresenting an individual's opinion as Health First policy.

b) PHI must never be sent over the Internet. Practitioners understand that the transfer of information via external networks *may not* be secure. Practitioners will not use such external networks for transmitting clinical patient data or other sensitive or highly confidential information, *unless the application being accessed utilizes a Health First approved information security solution.*

c) Practitioners may include protected health information (PHI) in e-mails if the recipient is within the Health First Groupwise e-mail system. However, care should be taken to limit the amount of PHI included in the e-mail.

d) Practitioners using information systems who discover they have connected with a web site that contains sexually explicit, racist or other potentially offensive material must immediately disconnect from that site. The ability to connect with a specific web site does not in itself imply that workers are permitted to visit that site. Practitioners should notify Health Information Technology immediately of the improper site.

e) Care must be taken to properly structure comments and questions posted to electronic bulletin boards, electronic mailing lists, on-line news groups, and related forums on public networks like the Internet.

f) Practitioners will not use external network access for any illegal, improper or illicit purposes in violation of any federal, state or local laws or of any Health First policy. Practitioners will not use Health First's equipment to attempt any unauthorized use, nor interfere with other users' legitimate use, of any internal or external computer.

g) Practitioners understand that a wide variety of information is available on external networks and that some individuals may find some information on such networks to be offensive or otherwise objectionable. Associates understand that Health First has no control over, and therefore cannot be responsible for, the content of information available on such external networks.

h) Telnet connections over the Internet are prohibited unless these connections are established using approved user authentication technology.

1) Health First Rights Upon Violation of Policies.

Practitioners understand that any unauthorized deviation from the terms of this system access policy will be carefully reviewed and will, if substantiated, result in appropriate action. Appropriate action may include but is not limited to, request for corrective action and inclusion in the practitioner's peer review file, termination of system access privileges, possible termination of any contract in force, and any other rights and remedies that may be available to Health First, in accordance with Medical Staff by-laws, Medical Staff Rules and Regulations, Departmental Rules and Regulations, and Health First policies and procedures. Users of the System understand that any willful or intentional deviation from the terms of this policy may result in both civil and criminal liabilities. See attachment A for Inappropriate Access Guidelines and level of offenses.

Copy of Data Upon Termination.

Upon termination of a practitioner's system access privileges for any reason, Health First shall use its reasonable efforts to provide such practitioner with a copy of data pertaining to his or her patients, subject to applicable patient consent requirements. It is expressly acknowledged that Health First's System may make it impractical to reproduce patient data in an electronic format, in which instance Health First shall use its reasonable efforts to produce such data in written or printed format.

2) ***Health First's Disclaimer Of All Warranties.***

Practitioners understand and agree that access and use of the system is on an "AS IS" basis and that Health First makes no warranties, whether express, implied or statutory, with respect to the system, its continued service or performance including, without limitation, the implied warranties of merchantability and fitness for a particular purpose and non-infringement.

3) Limitation of Liability.

Practitioners agree that Health First shall not have any liability to the practitioner or to any third party for any direct, indirect, incidental, special, punitive, exemplary or consequential damages including, without

limitation, damages for loss of profits, loss of revenue, loss of data, loss of savings, business interruption, downtime, loss of use of hardware or software, or for cover and the like, even if health first has been advised of the possibility of the occurrence of such damages**.**

Developed: 07/2003
Revised:
Reviewed:
Owned by: Information Privacy and Security Office

Attachment A

Health First

MEDICAL STAFF OFFICE
INAPPROPRIATE ACCESS GUIDELINES

Purpose: This document is to serve as a guideline to the Practitioner System Access policy provided by the Medical Staff Offices. The intention is to present the Vice President of Medical Affairs with examples of inappropriate access violations and the appropriate disciplinary level. These are minimum guidelines.

Level One Offense	C. Level Two Offense	Level Three Offense
Letter to be sent by the Vice President of Medical Affairs. *General description:* *Accidental access and/or lack of proper education*	D. A letter is sent to the Medical Staff Chairman of the offenders department and Medical Executive Committee. *General description:* *Unintentional break in the terms of the Confidentiality Agreement / HF Privacy Policies or an unacceptable number of previous violations*	Loss of admitting privileges or request for corrective action from the Practitioner. *General description:* *Purposeful break in the terms of the Confidentiality Agreement / HF Privacy Policies which result in reckless disclosure or an unacceptable number of previous violations*
Examples	**Examples**	**Examples**
Failing to sign off the computer when not using the system	Using another practitioner's or office staff access code	Disclosure of confidential patient / member information to individuals who do not have the need to know
Not disposing of Protected Health Information appropriately	Intentional access of records of patients not actively cared for by the practitioner looking at the records.	Accessing the record of a patient /member with intention to harm
Participating in an inappropriate release of Protected Health Information	Multiple violations of a Level One Offenses	Multiple violations of a Level One or Two Offense
Accessing own or family members records without a legitimate reason to do so		
Allowing another user to utilize the computer applications via his/her access code (password) without proper authorization to do so		
Requesting another employee to access clinical information outside of his/her access		

The above situations are examples of breeches only. No list can be all-inclusive. The above examples should be used as a general guideline. No list can anticipate every nuance or variable of unique situations.