

Employee Computer Users Agreement

I. Introduction

The use of computers at RMCHCS is an important part of nearly every employee's work day. Computers are used primarily to improve our ability to serve patients, enhance communications, and to track revenue, expenses and other data. As such, it is imperative that every employee utilize computers in an efficient, effective manner. This document outlines the manner in which computers should be used and details what is considered improper computer use. As an employee of the organization, you are expected to abide by the guidelines outlined below.

II. Accounts

- A. There are several types of computer accounts available based on an employee's need:
 - 1. An NT account gives you access to printers and files on our NT network and to e-mail.
 - 2. Meditech accounts are primarily for the purpose of accessing the RMCHCS patient care system, for performing various patient-care related tasks, for managing human resources and for managing the finances of the organization.
 - 3. There are other miscellaneous accounts used for specific purposes by various departments throughout the organization.
- B. Accounts are established by the MIS Department based on an employee's need as determined by his or her supervisor.
- C. Sharing of a computer account with other persons is prohibited, unless specifically authorized by the MIS Department. You will be assigned an account belonging only to you.
- D. Passwords must be protected. You must not leave a machine logged on when not present unless the machine is in a secure area, such as a private office.

III. General Usage

- A. Access of or attempts to access another person's directory, files, or mail, whether protected or not, without permission of the owner is prohibited.
- B. Attempts to access unauthorized machines via the computer network, to decrypt encrypted materials, or to obtain privileges to which you are not entitled are prohibited.
- C. The organization has signed software licenses for much of the software that is available on the computer systems; removal or transfer of such software without authorization is prohibited.

- D. Non-employees are prohibited from using the organization's computers for personal use unless a supervisor has authorized such use. Non-employees may not gain access to the patient care system, unless they have been officially authorized by the MIS Department.
- E. All documents and files residing on any organization computer are the property of Rehoboth McKinley Christian Health Services.

IV. Internet Access

- A. The Internet is available for your use based on your immediate supervisor's permission.
- B. Internet usage is governed by your need to access information important to the performance of your job duties.
- C. Internet usage that wastes time is strictly prohibited. Users are not necessarily restricted from occasionally using the Internet for personal purposes, however, this must be done during breaks or lunch periods, or when the person is not actively engaged in the performance of his/her job responsibilities.
- D. Accessing pornographic, lewd or excessively violent material utilizing RMCHCS computers is prohibited.
- E. Accessing sites that waste network bandwidth resources, such as Internet radio and TV broadcasts, are strongly discouraged. Using the Internet to play streaming songs and videos is also strongly discouraged.
- F. Game playing on the Internet is prohibited.
- G. Accessing Internet chat rooms for entertainment purposes is prohibited.
- H. The Internet is used for support purposes by the MIS department. Files and documents from various software and hardware vendors are frequently downloaded throughout a typical workday. Downloading other large files that would slow down access by the MIS Department, particularly during peak periods, is strongly discouraged.

V. E-mail Usage

- A. E-mail is an important method of communication for RMCHCS employees. It is used for intra-office communication as well as for communication with outside organizations. While personal e-mail may be received, as in Internet usage, it should be managed judiciously and on your own time.
- B. The sending of e-mail messages containing pornographic, lewd or excessively violent content is prohibited.
- C. Using e-mail for the harassment of other individuals, the promotion of goods and services for material gain and the promotion of political candidates is prohibited.
- D. Using e-mail for "spamming" or for distributing chain letters or other large, non-essential mailings is prohibited.
- E. In order to limit inadvertent network problems, users are discouraged from sending mail to the "allusers" account, unless the mail is an important or urgent message necessary to the overall functioning of the organization. Mail sent to the "allusers" account should be limited to relatively small messages and should not contain large attachments.

VI. Patient Data

- A. Anyone who works with and within the organization serving patients and clients has a right to access sensitive data for the exclusive purpose of accomplishing a particular job or task. You and all users must thus abide by the following:
1. As a user of critical patient data, you may read the information, print it out, convey the information to third party insurers and other individuals within the scope of your job position and the laws that protect access to such information.
 2. You must take reasonable care to insure that such sensitive information is not carelessly conveyed or allowed to be accessed by individuals not having authorization to access such information.
 3. Files that are to be transmitted electronically must be encrypted for transmission using a process developed by the MIS department.
 4. Persons working with and within the organization do not have the right to convey patient information to other organizations, family members or friends or anyone else who does not have a right to such information, without the proper legal authorizations.
 5. When viewing patient data on a computer monitor or terminal in a public area such as an admitting or reception desk, the screen must be angled such that viewing is restricted to authorized individuals only.
 6. You should set screen savers to automatically lock screens after no more than 15 minutes of no keyboard activity.
 7. Care must be taken so that printouts are not inadvertently sent to the wrong printer where unauthorized individuals might have access to the information.
 8. The RMCHCS computer system is for the exclusive use of authorized employees and users only in the performance of their job duties. Permission to utilize the patient care system is not granted to friends, family members, vendors or other non-authorized persons
 9. Files that are to be transmitted electronically must be encrypted for transmission using a process developed by the MIS department.
 10. You may not utilize patient or client data for personal gain, retribution, gossip or other unauthorized or illicit purposes.
 11. Electronic data is, in some respects easier to gain access to than more traditional forms of patient data. However, you should exercise the same amount of care with electronic data that they would use with written data such as patient charts.

VII. Organizational Resources

Organizational Resources Users of organizational computers shall not consume unreasonable amounts of limited resources. Resources that are in limited supply include laser printing, disk space and, in some cases, machine access itself. Laser printing should be used judiciously; it should not be used for unnecessary multiple copies. Picture files or other large files should not be stored on disk unless they are relevant to a person's job duties. In areas where multiple users utilize one machine, users should complete their work in a timely fashion in order to allow others access. At no time should such a machine be utilized for personal purposes when there are others waiting to use it.

VIII. Sanctions

Failure to abide by the above procedures or to compromise the security of confidential data could result in verbal or written reprimands, suspension or termination, depending on the severity of the infraction. It could also result in criminal or civil prosecution if any applicable laws are broken as a result of the infraction. Individuals using the computer system without authority, or in excess of their authority, are subject to similar sanctions.

IX. Agreement (Please return page 4 to MIS)

I understand and agree to abide by the principles and procedures outlined above.

Print Name

Signature of Authorized User

Immediate Supervisor's Signature

Date

MIS Office Director or Designee

X. Comments:

MIS Use Only		
<u>Date Set Up</u>	Meditech Username:	
	ApplDB:	Desktop:
Meditech ____/____/____		
NT & Email ____/____/____		
Hire Date ____/____/____		
Term Date ____/____/____		

Revised May, 2002

Glossary

- ❑ RMCHCS - Rehoboth McKinley Christian Health Services. Any references to “the organization” or “organizational” apply to the RMCHCS organization and all of its components.
- ❑ Spamming – to deliberately send large amounts of unsolicited “junk mail” to a list of users.
- ❑ Computer – any computer device belonging to the organization. This can include desktop computers, laptop and notebook computers, small CE devices, computer servers or any other electronic device capable of accessing RMCHCS files and data.
- ❑ E-mail – an electronic means for sending and receiving mail.
- ❑ Patient care system – largely implies Meditech, however, various departments have other patient data collection systems in place and this term applies to any of them.
- ❑ Chat room – an Internet “meeting place” where various individuals simultaneously “converse” by typing messages that others in the chat room can see and respond to.
- ❑ Network – the sum total of all the computers, printers and other devices within the organization connected for the purpose of sharing information and files. Synonymous with “intranet.”
- ❑ Internet – a global network for sharing information and files with other organizations not tied to our network.