General Policy F.2 **WORKSTATION/COMPUTER USE**

Introduction

Catholic Charities, Inc. has adopted this Policy on Workstation (computer) use to comply with HIPAA, with the draft regulations requirement for such a policy as well as with our duty to protect the confidentiality and integrity of confidential treatment information as required by law, professional ethics, and accreditation requirements.

Assumptions

- ❖ Every computer workstation in the facility is vulnerable to environmental threats, such as fire, water damage, power surges, and the like.

- ❖ Any computer workstation in the facility can access confidential patient information if the user has the proper authorization.

- ❖ All computer screens visible to individuals who do not have access to confidential information that may appear on the screen.

Preventative Measures

a. All computer users will monitor the computer's operating environment and report potential threats to the computer and to the integrity and confidentiality of data contained in the computer system. For example, if air conditioning fails and the temperature around the computer could exceed a safe level, the user must immediately notify their immediate supervisor for corrective action.

b. All computers plugged into an electrical power outlet will use a surge suppressor.

c. All personnel using computers will familiarize themselves with and comply with the facility's disaster plans and take appropriate measures to protect computers and data from disasters.

d. Personnel using computers will not eat nor drink at the terminal to prevent damage due to spills and so forth.

e. Personnel logging onto the system will ensure that no one observes the entry of their password. Passwords must be changed monthly and shared with your immediate supervisor only. Personnel using the computer system will not write down their password and place it at or near the terminal, such as by putting their password on a yellow "sticky" on the screen or a piece of tape under the keyboard.

f. Personnel will neither log onto the system using another's password nor permit another to log on with their password. Nor will personnel enter data under another person's password.

g. After three failed attempts to log on, the system will refuse to permit access and generate a notice to the system administrator.

h. Each person using the facility's computers is responsible for the content of any data he or she inputs into the computer or transmits through or outside the facility's system. No person may hide his or her identity as the author of the entry or represent that someone else entered the data or sent the message. All personnel will familiarize themselves with and comply with the facility's e-mail policy.

i. No employees may access any confidential patient or other information that they do not have a need to know. No employee may disclose confidential patient or other information unless properly authorized (see the Confidentiality Policy and the Disclosure Policy).

j. Employees must not leave printers unattended when they are printing confidential patient or other information. This rule is especially important when two or more computers share a common printer or when the printer is in an area where unauthorized personnel have access to the printer.

k. Employees may not use the facility's system to solicit for outside business ventures, organizational campaigns, or political or religious causes. Nor may they enter, transmit, or maintain communications of a discriminatory or harassing nature or materials that are obscene or x-rated. No person shall enter, transmit, or maintain messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes, sexual preference, or health condition. No person shall enter, maintain, or transmit any abusive, profane, or offensive language.

l. Each computer will be programmed to generate a screen saver when the computer receives no input for five minutes. The screen saver must prompt the user for a password before allowing the use to view the screen or inter data. The screen saver password should be different from your log on password.

m. Users must log off or "lock" the system if he or she leaves the computer for any period of time. All computers must be shut down at the end of each work day provided that another user will not need access to the same computer.

n. Each program must develop a policy and procedure that will ensure the accuracy of data its personnel enter into the system. For example, a designated employee will be assign to review data on a weekly bases for accuracy.

o. Each program must develop a policy and procedure on hard-copy printouts, including who may generate such printouts, what may be done with the printouts, how to dispose of the unwanted printouts, and how to maintain confidentiality of hard-copy printouts.

p. No personnel may download data from the facility's system onto diskette, CD, hard drive, fax, scanner, any network drive or any other hardware, software, or paper without the express permission of the program director or immediate supervisor.

q. No personnel may download any software without express written permission. The program director must approve any software that an employee wishes to download. This rule is necessary to protect against the transmission of computer viruses into the facility's system.

r. Every computer as well as each server must have an up-to-date virus protection program loaded on their computer and have it scheduled to run at a minimum of once a week. The virus protection program should be able to provide continued protection from viruses as long as the computer is turned on.

s. Computer users who use the internet for work related research should also have a "spy ware" blocking program to prevent third parties from access to your computer. This program should also be scheduled to run weekly.