Title: Using the Facility's Information System
Manual: Administrative
Number: GA056 **Chapter: General Administration**

Highlights

Policy Statement

Only authorized personnel shall have access to our facility's computer information system.

Policy Interpretation and Implementation

Purpose of Facility's Information System

1. Our facility's information system is provided for the sole purpose of facilitating resident care and business processes.

Accountability for Computer Information

2. All personnel who have access to our computer information system are accountable for all computing activities they perform.

Responsibility for Monitoring/Enforcement of Policies

3. The HIPAA Compliance Officer and management personnel at all levels are responsible for monitoring the actions of their staff and enforcing the policies of this facility relative to the protection of health and financial information.

Prohibited Activities

4. The following activities are prohibited by facility personnel:

    a. Using facility computers or data for personal business or gain;
    b. Interfering with the operation of any of our computers, systems, applications, programs, or data;
    c. Using any computer to disrupt any external computing system;
    d. Altering or deleting data or software, except as permitted by the Information Systems Manager or Administrator;
    e. Unauthorized browsing of resident clinical or financial information, employee information, or other facility/resident data;
    f. Installing unauthorized or illegally-copied software or data;
    g. Downloading/transferring resident/facility data for the purpose of personal gain or with the intent to improperly disclose such information;
    h. Unauthorized access to internet sites; or
    i. Any other activity that violates the intent of our facility's policies governing the protection of information.

Monitoring Actions of Computer Users

5. The facility's HIPAA Compliance Officer, Administrator, or other facility management personnel may monitor actions of computer users.

Breach of Security

6. Violations of breach of security or misuse of our facility's computer information system must be reported to the HIPAA Compliance Officer or to the Administrator immediately. Such violations may warrant immediate revocation of access privileges and/or termination of employment.

Leaving Workstations or Terminals Unattended

7. Workstations and terminals may not be left unattended unless the user logs off or shuts down his/her system before leaving his/her workstation or terminal.

Title: Using the Facility's Information System
Manual: Administrative
Number: GA056 **Chapter: General Administration**

continues on next page

Unauthorized Use of Resident or Facility Information

8. Any person who uses resident or facility information for non-business purposes may be subject to termination and civil or criminal legal action.

Passwords and User ID Codes

9. Passwords and user ID codes may not be shared.

References	
OBRA Regulatory Reference Numbers	See the Health Insurance Portability and Accountability Act (HIPAA) regulations at: http://www.hhs.gov/ocr/hipaa/finalreg.html
Survey Tag Numbers	n/a
Related Documents	Computer Terminals/Workstations Passwords and User ID Codes
Policy Revised	Date:____06/01/2016___ By:____M. Carey_____ Date:_____ By:_____ Date:_____ By:_____ Date:_____ By:_____