CareNu		Effective Date:	11/10/2023
Policy Title:	Electronic Communications Systems, Acceptable Use	Last Review Date:	11/10/2023
Issuing Department:	Systems	Last Revision Date:	11/10/2023
Policy Number:	HE.02.08	Next Review Date:	11/10/2024
Applies to:	☐ ACO ☐ MSO ☐ TPA ☒ ALL		

Policy

It is the Policy of the above Organization(s) to ensure proper use of all electronic communications systems.

Purpose

To ensure proper use of all electronic communications systems.

Scope

This process applies across the organization.

Definitions

N/A

Procedure

1. Business Purpose and Use

a. Computers, computer-related equipment, electronic files, the e-mail system, internet access, telephone, cellular phones and software furnished to employees are Company property, primarily intended for business use. Cell phone usage for personal reasons is expected to occur during meal and rest periods. Information-processing resources are tools to be used for performing business functions sanctioned by Company in a manner consistent with all regulations, policies and procedures and laws.

b. Much of the information collected, stored, and managed by the Company is protected information under Health Insurance Portability and Accountability Act (HIPAA) implementing regulations and other statutory directives. Company managed information and data must also be used for business purposes only, in accordance with all applicable laws and corporate regulations, policies and procedures.

c. The Company, at its sole discretion, specifies what materials, files, information, hardware, software, and communications are permitted. All other material, files, information, hardware, software, and communications are prohibited.

d. Use of Company's systems is a privilege that may be withdrawn at the sole discretion of management. In addition, these privileges are automatically revoked upon termination of employment or of contract with Company. By their use, all

users of Company's systems agree to comply with the rules prescribed in this policy.

e. The Company does not allow text messaging services (SMS/MMS) on Company provided phones for patient facing employees. At the sole discretion of the Company, this may be temporarily granted for a documented use case after approval by senior Compliance and/or IT Security leadership.

f. The Company, at its sole discretion, defines the authorized business purpose of each computer communication system, or information system.

2. Sensitivity and Diversity

a. The Company is sensitive to the diversity of its employees and strives to maintain a workplace free of harassment. Therefore, the Company expects professional, appropriate language and conduct at all times and prohibits the use of computers, networks, Internet, electronic messaging or any other Company systems in ways that are disruptive, offensive to others, harmful to morale, unethical, actionable or illegal.

b. Displaying or transmitting sexually explicit images, messages, and cartoons is not allowed. The list of other misuses of Company's systems includes, but is not limited to, racial slurs, gender-specific comments, or any other comments or images that could reasonably offend someone on the basis of race, age, sex, religious or political beliefs, national origin, disability, sexual orientation, or any other characteristic protected by law.

3. Access to CareNu Network, Systems, Information and Data

a. All persons and entities are required to be authorized according to an established, auditable process before gaining logical and physical access to any electronic information managed by Company. Access to Company networks, systems, information, and data is granted on business need basis.

b. Any user account with 30 days of inactivity will be disabled.

4. Software and Computer Configurations

a. All software installed on workstations and all other systems must be approved and licensed by the CareNu IT Department. All of the computers provided by CareNu are already loaded with software applications deemed necessary to accomplish most jobs.

b. Any software that is not part of IT Department's standard desktop(s) or system configurations is to be approved by the IT Leadership before being installed.

c. Each employee with a desk phone assigned is responsible for changing his/her voicemail greeting on the first week of employment or when out of the office for an extended period of time. In the event of an unexpected or prolonged absence, the department manager or employee supervisor should contact the IT department to request access to and change the message after all attempts to have the employee do so have been exhausted.

5. Copyright, Trademark, Patent and Other Intellectual Property

a. The unauthorized use, installation, copying, or distribution of copyrighted, trademarked, or patented material on the Internet\Web, in e-mail and by other media, is expressly prohibited. As a general rule, if a user did not create the material, does not own the rights to it, or has not gotten authorization for its use, it should not be distributed on the

Internet\Web, in e-mail, or through other media.

b. Users are also responsible for ensuring that the person providing them any material over the Internet\Web, e-mail, or by other media has the appropriate distribution rights, before using or distributing it themselves.

6. Personal Gain

The Organization specifically prohibits the use of Company resources for the purposes of conducting a private business, running a lottery or pool, engaging in a hobby; operating a website, Bulletin Board, listserv, blog; and any other activity not sanctioned in writing as an authorized use by Company.

7. Personal Responsibility and Accountability

Users are held personally accountable for any violations of this policy, including but not limited

to the following:

a. Sending or posting discriminatory, harassing, or threatening messages or images

b. Sending or posting messages or material that could damage Company's image, reputation, or financial well-being or passing off personal views as representing those of Company

c. Sending or posting messages that defame or slander other individuals

d. Sending or posting messages that disparage another organization's products or services

e. Sending anonymous e-mail messages

f. Sending PHI or PII over SMS/MMS on BYOD or Company provided phones.

g. Taking photos or storing image of PHI or PII on BYOD devices.

h. Sending unencrypted emails with patient or credit card information

i. Attempting to access, or view, or exchange pornography or obscene materials

j. Attempting to access, or view, or exchange materials related to unethical or illegal activities (such as, drugs, espionage, hacking, sabotage, terrorism, theft, violence, etc.)

k. Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities

l. Using company system resources for political causes or activities, religious activities, or any sort of gambling

m. Sending or posting confidential material, trade secrets, or proprietary information outside of Company

n. Stealing, using, or disclosing someone else's user ID or password without authorization

o. Copying, pirating, or downloading software and electronic files without permission

p. Violating copyright law; failing to observe licensing agreements

q. Engaging in unauthorized transactions that may incur a cost to Company or initiate unwanted Internet & e-mail services and transmissions

r. Attempting to break into the computer system of another entity or person

s. Refusing to cooperate with an internal security investigation or with law enforcement in an investigation

t. Jeopardizing the security of Company's electronic communications systems

u. Intentionally introducing a virus, harmful component, corrupted data into the Company's information resources or maliciously tampering with any of Company computer systems

v. Engaging in any other illegal, unethical, actionable, or unprofessional activities

w. Not exercising sound judgment or not asking for guidance where the application of this policy is unclear or questionable.

8. Equipment Care & Accountability:

a. Each staff person is responsible for handling the equipment with reasonable care.

b. Company provided equipment must be kept in a secure place when not in use for client visit or documentation.

c. Staff will notify the IT Department to report any issues, loss or theft of any company-owned equipment. Any reported damage, loss or theft of the equipment should be documented in an Ethics Point ticket by the employee who reported the incident. Each employee is responsible for returning back any company equipment to his manager when no longer with the company or will be on a leave of absence for an extended period of time, managers are responsible to collect equipment prior to the leave, if they are able to. Human Resources will assist with obtaining any equipment from employees who leave suddenly or who have been out on long-term leave of absence.

9. Privacy

a. Company's network resources are business systems that require monitoring to ensure the availability, integrity, and confidentiality of the information and data created, processed, transferred, and stored therein. Consequently, users of the Company's network resources have no expectation of privacy when using these resources and should conduct themselves accordingly. (This includes building security information systems.)

b. For Manager requests to access specific employee data, please see "Policy: Security Video, Access Control Logs, & Email Archive Access".

10. Sanctions

Non-compliance with the provisions for acceptable use may result in disciplinary action up to and including termination of employment. In addition, non-compliance that constitutes a violation of the law may result in referral to law enforcement or governing regulatory authority.

References

[Reference any law, regulation or standard that applies to this policy. **For Example**: 42 C.F.R. §§ 422.564 and 423.564]

Approval/Revision History

Version Number	Change Date; (Original/ Reviewed/ Revised)	First Level Approval	Second Level Approval
V1	11/10/2023 Original	Name: Matthew Strohhacker Title: Sr. Director, Systems 11/10/2023 Date	Name: Maya Kaczmarek Title: Sr. Director, Operations 11/10/2023 Date
V2	MM/DD/YYYY Revised	Name: Title: [MM/DD/YYYY] Date	Name: Title: [MM/DD/YYYY] Date