Current Status: *Active*	**PolicyStat ID:** *9753110*
Origination:	*02/2017*
Effective:	*09/2021*
Last Approved:	*09/2021*
Last Revised:	*09/2021*
Next Review:	*09/2022*
Owner:	*Amy Porwoll: CCH CHIEF INFORMATION OFFICER SVP EX*
Area:	*Information Systems*
Regulatory Tags:	*Communications Decency Act of 1996, Copyright Act of 1976, Digital Millennium Copyright Act of 1998, Electronic Communications Privacy Act 1986 (2001), Health Insurance Portability Accountability 1996, MN 2012 Use of Wireless Devices While Driving, Telecommunications Act of 1934, Telecommunications Act of 1996*
Applicability:	*CC/CH Systemwide*

Digital Device Management

PURPOSE

A. CentraCare (CC) recognizes the need to allow remote access to the network and resource and will establish mechanisms to allow the access while applying safeguards to protect CC data and affiliates.

1. Establish an authorized method for controlling desktop, mobile, and storage devices that contain or access CC information and resources to ensure the security of information stored on and/or accessed.
2. Provide guidance to minimize the risks associated to loss of program functionality, exposure of sensitive information, malicious threats, and legal concerns.

CentraCare adopts the following Policy/Procedure for:

Carris Health - Clinic
Carris Health - Redwood
Carris Health - Rice
Carris Health - Willmar Surgery Center

CentraCare – Clinic
CentraCare – Employees
CentraCare - Long Prairie
CentraCare – Melrose

CentraCare – Monticello
CentraCare – Paynesville
CentraCare - Plaza Surgery Center
CentraCare - Sauk Centre
CentraCare - St. Benedict's Community
CentraCare - St. Cloud Hospital

POLICY

A. CentraCare (CC) is committed to providing a stable and secure environment for all patients, customers, employees, volunteers, other affiliates, and CC network infrastructure to provide the best quality care living the CC Mission and Vision.

B. NO EXPECTATION OF PRIVACY

1. Electronic communications sent and received using company equipment or CC-provided Internet access, including web-based messaging systems used with such systems or access are not private and are subject to viewing, downloading, inspection, release, and archiving by CC Information Systems staff.
2. CC maintains the right to inspect any and all files stored on the network, individual computers, or storage media as well as any personal devices used with CC resources. An authorized employee with justification may access another employee's computer, computer files, or electronic communications without prior authorization from either the employee or an appropriate IS official.
3. Information Systems (IS) staff may audit any IS computer device at any time. If IS staff discover an individual has used e-communication resources inappropriately, they will notify the appropriate manager and designated Human Resource personnel to ensure an appropriate investigation.
4. Information Systems will comply with reasonable requests from law enforcement and regulatory agencies for logs, diaries, archives, or files on individual Internet activities, e-mail use, or computer use.

DEFINITIONS

Affiliates or Users: Anyone approved for employment, contract, educational reasons, volunteer, etc.

CC Data or Information: Confidential, restricted, personally identifiable, or proprietary data.

Critical Care Equipment: Included but is not limited to, infusion pumps, infant incubators, ventilators, ECG monitors, apnea monitors, defibrillators/monitors, blood warmer, dialysis units.

Digital Device: Electronic devices including but not limited to laptops, desktops, tablets, various mobile devices such as iPads, iPhones, smartphones, mobile storage devices, etc. Also known as mobile device.

Encryption: is the process of transforming data using an algorithm to make it unreadable to anyone except the intended recipients.

Logon Credentials: CC user ID and password combination that allows one to connect to the

CC network.

Malicious Threats: Program codes designed to damage electronic systems or to steal critical information. Activities including but not limited to computer hacking, spyware, malware, viruses, adware, etc

Mobile Storage Device: Includes but is not limited to, mobile devices, diskettes, magnetic tapes, external/removable hard drives, flash cards, thumb drives (USB sticks), CD/DVD, Zip drives, CD Burners, back-up units, etc.

Network Infrastructure: An interconnected group of computer systems linked by various parts of telecommunications architecture. Individual networked computers to routers, cables, wireless access points, switches, backbones, network protocols, and network methodologies.

P2P Networking: a peer-to-peer (P2P) network is created when two or more PCs are connected and share resources (files) without going through a separate server computer.

Remote Access: Use of VPN to connect to the CC network to gain access to CC resources and data

Radio Frequency (RF): Transmitting devices include, but are not limited to, cell phones, walkie talkies, HAM radios, and hand-held inventory terminals.

Secure Point to Point Tunnel: Secure access to the IS via an encrypted tunnel over the Internet. This type of connection is generally an “always on” connection

Shared Drive: A drive/folder on a computer that is configured to allow access to the contents of the drive/folder from other computer’s across the network.

Virtual Private Network (VPN): is a network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network.

GUIDELINES

(For loss of a CC digital device - Please refer to the Stolen or Missing Computing Device Policy)

A. Software Purchases for CC Devices
    1. All software purchases must be approved by Information Systems prior to purchase.
    2. All software installs must be performed by Information Systems (IS) Desktop Support. Please contact IS Help Desk ext. 54540 for assistance.

B. Computer Shares and Data Storage Options
    1. Shared Drives
        a. All shared folders must be set up by Information Systems.
        b. The shares will be created only at the point that files will need to be accessed by multiple staff.
        c. Will be set-up per management approval and User Access request.
    2. Data Storage

a. All storage devices must be approved by IS. The requesting department director is responsible for use and security of the device.

b. Storage devices cannot be used to create copies of patient information, business, or human resource information without authorization from the CIO.

c. Storage devices cannot be used to create copies of licensed software or media for employee's personal use.

d. Protected Health Information (PHI) cannot be stored on the hard drive of the PC unless using OneDrive to sync to a CC managed device.

e. Under no circumstances may CC owned private or proprietary data be stored within social media sources or cloud based storage offerings including but not limited to Google, MyPC Backup, Carbonite, Just Cloud.com, DropBox, etc.

f. Users are required to work with Information Systems for cloud based needs to assure appropriate security measures are in place.

g. All data needed to backed up must reside on CC secured approved storage.

C. Digital Devices CC Owned: (also known as mobile devices)

1. Personal Communication Devices (PCDs) will be issued only to CC personnel with duties that require them to be in immediate and or frequent contact when they are away from their normal work locations. Distribution is limited to persons for whom the productivity gained is appropriate in relation to the costs incurred.
2. Users must exercise extreme caution with a CC owned digital device while in public places, meeting rooms and other unprotected areas. Do not leave these devices unattended and protect them from unauthorized physical access, tampering, loss or theft.
3. With a user's permission, IS staff may connect to the user's computer with full control. This will facilitate troubleshooting of problems on the user's device.
4. With authorization from the CIO and the user's supervisor, Information Systems staff may monitor a user's activity for attempts to change settings or circumvent computer security.
5. Users will not attempt to alter computer configuration settings that might compromise the security or performance of a CC managed computer system.
6. IS will maintain a hardware address (MAC address) that can be registered and tracked.
7. CC Information Systems will configure CC digital devices to allow only the minimum features, functions, and services needed to carry out CC business requirements.
8. Users should not rely on the data storage on their computers. Information Systems will not be responsible for recovery of data stored on the physical computer in the event of a computer system's failure
9. All computers will have their Screen Savers set to lock after 3 minutes of no use and the computer is set to lock after 15 minutes of no activity.
10. CC users are required to immediately report any intentional form of malicious abuse and or threats made to a CC computer device or network infrastructure by contacting

the Information Systems Help Desk at extension 54540.

11. Users needing to connect external devices including but not limited to thumb drives, external disc storage devices, or other digital device to a computer on the CC network must first bring them to the IS Help Desk for acceptance. The Digital Device Management form must be completed and security software installed by the user for the protection of the CC network.
12. Securing the CC network infrastructure include but not limited to, Windows updates/ critical patches, virus/malware protection with daily DAT updates, firewalls, IDS/IPS, encryption protection for devices and data sensitive emails, spam filtering, Data Loss Prevention (DLP), various monitoring/auditing tools, policies, enforced configuration settings for devices, etc.

D. Digital Devices (Personal or CC owned): (Also known as mobile devices)

1. Wireless/Cell Phone use... please see the E-Communications policy for phone and voice-mail use.
2. All personal owned digital devices used on the CC network must be approved.
3. All digital devices connecting to the CC network must have anti-theft and anti-virus protection installed and up to date where applicable.
4. Use of digital devices while driving is prohibited. Handless devices are acceptable under necessary circumstances.
5. All digital devices are prohibited from being used for sharing, communicating, or storing confidential information regarding residents, patients, employees, or other affiliates of CC, excluding direct calls to the care team and usage of approved CC mobile device applications.
6. Employees are prohibited from taking any photos or videos of patients, their families, or CC proprietary using a digital device, cell phone or other personal device that is capable of taking photos or videos throughout the facilities.
7. It is recommended to not use cell phones, walkie talkies or other RF transmitting devices within three feet of the following equipment:
    a. any critical care equipment located in areas such as patient rooms, critical care units, emergency department, operating rooms, diagnostic and treatment areas, and clinical laboratories, or
    b. power wheelchairs, because it may cause erratic uncontrolled movements. Cisco wireless phones transmit on a different frequency, therefore are not limited in use by critical care equipment.
8. When in a location that will not interfere with critical care equipment, employees will place cell phones or other RF transmitting devices on silent/vibrate mode.
9. In the event utilization of secure remote access methods to stored CC data are not possible; the affiliate must adhere to the following restrictions and requirements:
    a. Authorized CC Information Systems security personnel must authorize and certify in writing, in advance, that the storing of restricted and confidential data on the electronic device is necessary to conduct CC business operations.

b. The department management must determine and certify in writing that reasonable alternative means to provide the user with secure access to CC business data do not exist.

c. The department management must assess the sensitivity of the data to reside on a secure digital device and determine that the business need necessitating storage on the digital device outweigh(s) the associated risk(s) of loss or compromise.

d. The department management must authorize, in writing, the storage of specific CC business data on a secure digital device and the acceptance of all associated risk(s).

10. CC business data that has been authorized to be stored on a secure digital device shall be:

    a. the minimum data necessary to perform the business function necessitating storage on the digital device.

    b. stored only for the time needed to perform the business function

    c. encrypted using at least 256 bit encryption technology

    d. protected from any and all forms of unauthorized access and disclosure

    e. stored only on secured digital devices with up to date anti-theft and anti-virus protection

11. Any authorized CC business data placed on a digital device shall be documented, tracked, and audited by the Information Systems Security department. The information tracked shall include the identification of the individual authorizing storage of the data on the digital device, the authorized user of the digital device, the asset tag of the digital device, information about the stored data, and the final disposition of that data.

12. Personal devices may have network authorization removed if found in violation of this policy until proof of protection is presented.

E. Network

1. The Director of the requesting department must approve remote access for VPN

2. All modern connections out of the IS network or inbound directly to servers, PC's, or network attached devices must be approved by the IT Director, secured, and monitored by Information Systems.

3. For a Secure Point to Point Tunnel, the CIO must approve access.

4. Information Systems will not troubleshoot home wireless access issues to the IS network.

5. P2P networking - peer to peer file sharing is restricted to CC approved applications only such as Sharepoint.

6. Applications/websites of sexually explicit, offensive, or illegal in nature is not permitted while connected to the CC network via VPN, or secure point-to-point tunnel. This includes personal owned computers using the CC network.

7. Exceptions to our web filtering will be permitted for appropriate business reasons. Refer requests via the IS User Access form.

8. All managed Windows PCs will have patch management controlled by a Windows Update and Group Policy.

F. VIOLATION OF LAW AND POLICY

1. Theft and Abuse
   Federal and state laws prohibit the theft and abuse of computers and other electronic resources such as electronic communication resources, systems, and services. Abuses include (but not limited to) unauthorized entry, use, transfer, tampering with the communications of others, and interference with the work of others and with the operations of electronic communication resources, systems, and services. The law classifies certain types of offenses as felonies.
2. Copyright Material
   Use of any Copyright material without properly documented written approval is prohibited by CC including but not limited to music, software/applications, written material, videos, pictures, etc.

G. DISCIPLINE
   Failure to comply with the Digital Device Management policy will jeopardize the user's access to the CC network. Employees who have inappropriately utilized a CC Digital Device will be subject to discipline, which may include termination.

REGULATORY CITATIONS

Copyright Act 1976
Communications Decency Act 1996
Digital Millennium Copyright Act of 1998
Electronic communications Privacy Act of 1986 (amended by the USA Patriot Act of 2001)
Health Insurance Portability and Accountability Act 1996
Telecommunications Act of 1934
Telecommunications Act of 1996
Use of Wireless Communications Devices While Driving. Minnesota Law 2012.

REFERENCE CITATIONS

Facility specific, none stated

Attachments

No Attachments

Approval Signatures

Step Description	Approver	Date
Communication of Activation	Amy Porwoll: CCH CHIEF INFORMATION OFFICER SVP EX	09/2021
CCH Corporate Compliance Committee	Jessica Gotvald: CCH EXECUTIVE ASSISTANT TO VP NE	05/2021
	Amy Porwoll: CCH CHIEF INFORMATION OFFICER SVP EX	05/2021
	Amy Porwoll: CCH CHIEF INFORMATION OFFICER SVP EX	05/2021

Applicability

Carris Health - Clinic, Carris Health - Redwood, Carris Health - Rice, Carris Health - Willmar Surgery Center, CentraCare - Clinic, CentraCare - Employees, CentraCare - Long Prairie, CentraCare - Melrose, CentraCare - Monticello, CentraCare - Paynesville, CentraCare - Plaza Surgery Center, CentraCare - Sauk Centre, CentraCare - St. Benedict's Community, CentraCare - St. Cloud Hospital