10.08 Internet, Social Media and E-mail

10.08.010 Purpose

The Cambria Community Healthcare District's ("District") computer systems, including all hardware and software, are the exclusive property of the District and are provided for creating and transmitting business-related information. The District treats all computer files, including electronic mail (e-mail), whether sent or received, as business information. The purpose of this policy is to:

(1) Ensure that the computer systems are used for appropriate District business;
(2) Notify employees that they have no right to privacy in the use of the computer systems, including e-mail or Internet; and
(3) Notify employee that the District reserves the right, with or without notice, to access, monitor, review, copy and/or delete any computer files, including e-mail sent or received, and all website communications are transactions.

10.08.050 E-Mail Use

(1) All e-mail business communications to non-District employees should use an appropriate professional tone, correct spelling, and proper grammar.
(2) The District reserves the rights to access, monitor, copy and/or delete any e-mail communications made on the District computer systems.
(3) There should be no expectation of privacy in the use of e-mail. Employees should not use District e-mail facilities to create or transmit information they wish to keep private.
(4) When transmitting messages via e-mail, employees should be aware that e-mail messages can be read by persons other than the addressee, and that messages may be later disclosed to outside parties. E-mail messages, including but not limited to, information relative to public projects or policy decisions may be subject to disclosure under the California Public Records Act (Government Code Section 6250 *et seq*.). E-mail messages may also be subject to disclosure in litigation or administrative proceedings in the same manner as other District records.
(5) E-mail messages sent to and received from attorneys representing the District are privileged communications. Such e-mail communications shall not be distributed or copied to unauthorized individuals.

10.08.075 Social Media Use

The purpose of this policy is to protect public data, private personnel (employee) data, ambulance patients, the public, the operations of the District, and public confidence in the District and its employees and the Board of Directors. This policy is not intended to limit the right to freedom of speech or expression, but is intended to protect the rights of the District, its members, and the public the District is committed to protect. Employees and Board Directors are advised that their speech, directly or by means of instant technology either on or off duty and in the course of their official duties that has a connection to their professional duties and responsibilities, may not be protected speech under the First Amendment. Speech that impairs or impedes the performance of the District, undermines discipline and harmony among coworkers, or negatively affects the public perception of the District may be sanctioned.

1. Ownership of Work-Related Images. Upon request, copies of work related of images taken on personal equipment will be provided to the District.

2. Permission to Take Work-Related Images.

Work-related images shall not be taken of any emergency response except as permitted by policy or as directed by the Operations Manager or Administrator. All work-related images shall be taken using District-issued equipment during emergency calls.

3. Reasons for Taking Work-Related Images.

Photos or other recordings may be taken to assist in the diagnosis or treatment of patients, if allowed by protocol or law. Such images should be forwarded to the appropriate medical care provider as an attachment to the electronic patient care record.. Work-related images, including recordings showing possible evidence of a crime, must be forwarded to law enforcement by the Administrator, when requested by law enforcement. Other work-related images used for internal, departmental purposes such as training or publicity shall be taken in a manner that removes the possibility of identifying patients.

4. Control and Dissemination of Work-Related Images.

All work-related images shall be stored in the District's computer system and be governed by the District's records management policies and procedures. Work-related images shall not be stored, retained, or disseminated in any manner by anyone other than the persons appointed to review all images and approve retention, release, or dissemination and cannot be used for personal profit or business interests or to participate in personal political activity.

5. Professionalism and Public Confidence.

The appearance of professionalism is important to public safety and the public's confidence and trust. In order to maintain the appearance of professionalism and public confidence, no employee shall post any material on any social media that is detrimental to the District's effective operation. Employees shall not disseminate protected, private, nonpublic, or confidential information including, but not limited to, the following:

(a) Matters that are under investigation

(b) Patient and employee information protected by HIPAA/medical confidentiality laws

(c) Personnel matters/data that are protected from disclosure by law.

6. Definition of Social Media.

"Social media" shall be defined for purposes of this policy as any publicly shared medium where users post content or share files. Examples of social

media include, but are not limited to, Facebook, Twitter, Snapshot, and Instagram.

7. Reporting Violations.

Any employee becoming aware of or having knowledge of a posting or of any web site or web page in violation of this policy may anonymously report possible violations to the Administrator.

8. Penalties for Violation of Policy.

Violation of this policy may be considered an extraordinary breach of the public's expectation of privacy and of the District's policies and regulations regarding the use of social media and may subject the offender to discipline and possible termination of employment.

10.08.100 Internet Use

(1) Employees may access the Internet so long as it does not adversely affect the ability to perform work duties.
(2) Employees have no right to privacy in the use of the Internet on District computer systems.
(3) The District reserves the right, with or without notice, to access, monitor, review, copy and/or delete any computer files, including any and all website communications and/or transactions by District employees. The District further reserves the right to monitor any employee's Internet use for the purposes of determining whether such use is appropriate or acceptable.

10.08.150 Prohibited Uses of E-mail and the Internet

Prohibited uses of e-mail and/or the Internet on District computer systems include, but are not limited to, the following:

(1) To access any materials that are obscene, pornographic, or in poor taste;
(2) To transmit sexually explicit images, messages, and/or cartoons; ethnic or racial slurs, or anything that may be construed as harassment or disparaging of others based on their race, national origin, ethnic group identification, religion, age, sex, sexual orientation, marital status, color or physical or mental disability;
(3) To play games;
(4) To conduct illegal activities, such as, but not limited to, gambling, commit a crime or fraud, or violate any federal, state or local law;
(5) To use the user-name or password of another person to gain access to his/her e-mail or any other computer file or account without that person's permission;
(6) To transmit sensitive or privileged information to unauthorized persons or organizations;
(7) To download or otherwise acquire software without prior consent of the District Administrator, or his/her designee; and
(8) To use the Internet in any manner that causes confidential or sensitive information to be subject to eavesdropping or interception by unauthorized individuals.

10.08.200 Computer Systems - Hardware and Software

Prohibited activities with regard to employee use of District computer systems - hardware and software - include, but are not limited to, the following:

(1) Installing programs on District computer systems without prior consent of the District Administrator, or his/her designee;
(2) Copying any District computer program for the purpose of using it on any other computer without the prior consent of the District Administrator, or his/her designee;
(3) Connecting computers, including laptops and personal computers not owned by the District, to the District's information systems network without prior consent of the District Administrator, or his/her designee;
(4) Disclosing an employee's account or e-mail password, or otherwise making such account available to others;
(5) Infringing on other employee's access and use of District computer systems, including, but not limited to:
    a. Sending excessive messages, either locally or offsite;
    b. Unauthorized modification of system facilities, operating systems, or disk partitions;
    c. Attempting to crash or tie up a computer or network;
    d. Damaging or vandalizing District computing facilities, equipment, software, or computer files;
    e. Intentionally using or developing programs that disrupt other computer users or which assess private or restricted portions of the system and/or damage the software or hardware components of the system; or
    f. Introducing or allowing the spread of any virus or destructive information, file, or other item.

10.08.250 Connection of Personal Computer and Internet Capable Devices to District Internet/network Connections

Personnel may, with written consent of the Administrator, connect personal computers to the District's Internet connection under the following conditions:

(1) Connection may be made by either cable or "WIFI".
(2) Personnel may not access District computer systems to access or download files or programs through the network system
(3) The provisions of policy 10.08 shall apply to use of personal computers while on District premises.

10.08.300 Violation of Policy

Any violation of this policy, or other inappropriate use of the District's computer systems, including e-mail and Internet activities, is considered a serious violation of District policies and may result in disciplinary action as outlined in Section 10.05 of this manual.

10.09 SEIU Employee use of Social Media

The District acknowledges the right of SEIU Local 620 to maintain its own social media outlets and to control the contents thereof. Local 620, however agrees:

- That it will identify all of its postings as being from Local 620 and not being representative of the Cambria Community Health Care District.
- It will post nothing that compromises patient confidentiality, including names and pictures.
- It will not post license plate numbers, house numbers or identifiable buildings.