10. No employees may access any confidential member or other information that they do not have a need to know. No employee may disclose confidential member or other information unless properly authorized (see the Corporate Confidentiality Policy and the Disclosure Policy).
11. All documents containing and or displaying CHG member Protected Health Information (PHI) must be locked up at the end of the of the work day.
12. Employees must not leave printers unattended when they are printing confidential member 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.
13. Employees may not use CHG's system to solicit for personal 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 race, age, disability, religion, national origin, physical attributes, sexual preference, health condition or other protected class in accordance with State/Federal law. No person shall enter, maintain, or transmit any abusive, profane, or offensive language.
14. 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.
15. Each computer will be programmed to generate a screen saver when the computer receives no input for 5 minutes. Supervisors may specify an appropriate period to protect confidentiality while keeping the computer available for use in conjunction with the Information Systems Division.
16. It is recommended that each department develop a policy to ensure the accuracy of data its personnel enters into the system and provide a copy of such policy to the Information Systems Division.
17. Each department may develop a policy on hard-copy printouts, including who may generate such printouts, what may be done with the printouts, how to dispose of the printouts, and how to maintain confidentiality of hard-copy printouts. Each department must provide a copy of such policy to the Information Systems Division.
18. No personnel may download data from CHG'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 department head with notice to the Chief of Information Officer.
19. No personnel may download any software without express written permission of the Systems Manager. The Systems Manager must approve any software that an employee wishes to download. This rule is necessary to protect against the transmission of computer viruses into CHG's system.
20. No personnel may hack into CHG's computer system.
21. Personnel may access only the programs and data that they have been authorized to use.
22. No personnel may intentionally create and transmit any virus, worms, Trojan horses, or any other disruptive programs that may interfere with CHG's computer systems.
23. All computers and data remain the property of CHG. CHG has the right to access all data created with CHG's computers.
24. CHG reserves the right to monitor all programs, data entry, e-mails, and web-sites visited.
25. All Personnel will receive an annual training from the Information Systems Division on workstation use.

Community Health Group	Policy Number: 5504	Applies to Product Type: ☒ Medi-Cal ☒ CMC	Page 1 of 3
Original Effective Date: May 1, 2002		Revision Effective Date: May 1, 2017	
Policy Applies to: All Staff		Classification Series: 5500-5999 Regulatory Affairs	
Policy Title:	HIPAA Workstation Policy		

Policy Statement

It is the policy of Community Health Group (CHG) that all personnel that use computer terminals must be familiar with the contents of this policy and follow its guidance, as appropriate, when using computer equipment. Familiarity with the plan and demonstrated competence in the requirements of the plan are an important part of everyone's responsibility who uses computer terminals.

Purpose

CHG has adopted this Policy on Workstation Use to comply with Health Insurance Portability and Accountability Act of 1996 (HIPAA), as well as with our duty to protect the confidentiality and integrity of confidential medical information as required by law, professional ethics, and accreditation requirements.

Assumptions:

- Every computer workstation in CHG 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 may be visible to individuals who do not have access to confidential information that may appear on the screen.

Procedure

Preventative Measures

1. 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 the Information Systems Division and maintenance.
2. All computers plugged into an electrical power outlet will use a surge suppressor approved by the Information Systems Division.
3. All personnel using computers will familiarize themselves with and comply with the disaster plans and take appropriate measures to protect computers and data from disasters.
4. Personnel using computers should not eat nor drink at the terminal to prevent damage due to spills and so forth.
5. Personnel logging onto the system will ensure that no one observes the entry of their password.
6. 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.
7. After three failed attempts to log on, the system will refuse to permit access and generate a notice to the Systems Manager.
8. 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.
9. All personnel will familiarize themselves with and comply with CHG's e-mail policy.

Enforcement

All supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination from employment, professional discipline, or criminal prosecution in accordance with State and Federal law.

Regulatory: HIPAA and 42 CFR §422.118

NCQA: None

Attachments: None

Department Head

Title: Regulatory Affairs Manager ~~Compliance Officer~~

Signature: [signature]

Date: 4-10-18

Division Chief

Title: Associate Chief Executive Officer

Signature: [signature]

Date: 4.10.18