GREATER COLUMBIA BEHAVIORAL HEALTH, LLC. BH-ASO

Computer and Information Security

No: PS606

Document Type:[1] ___ Policy & Procedure _X_ Process Guideline ___ Plan ___ System Description

Adopted: 1/1/2019
Last Reviewed: 7/8/2024
Retired: _____

Revisions: 10/14/19, 2/28/2020, 1/22/2021, 1/24/2022, 2/16/2023, 7/8/2024

Document Scope: (applies to Policy & Procedure only)

X The requirements herein apply only to the GCBH BH-ASO Central Office and its functions.

– The requirements herein apply, verbatim, to GCBH BH-ASO and its network providers[2].

– The requirements herein apply to both GCBH BH-ASO and its network providers[2]. Additionally, network providers must have internal documents outlining their processes for implementing the requirements, insofar as they relate to actions for which network providers are responsible.

PURPOSE: To comply with the requirements that GCBH BH-ASO shall establish and maintain, and shall require contracted providers to maintain, a health information system that complies with the requirements of OCIO Security Standard 141.10, the HCA contract, and provides the information necessary to meet GCBH BH-ASO's obligations under the HCA contract. OCIO Security Standards are available at https://watech.wa.gov. GCBH BH-ASO shall have in place mechanisms to verify the health information received from contracted providers. This policy shall also outline how GCBH BH-ASO will comply with the requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, and 42 CFR Part 2.

DEFINITIONS

I. None

POLICY

A. Much of GCBH BH-ASO's confidential information is stored in electronic computer networks and devices. GCBH BH-ASO takes great care to ensure that access to those computers, networks, and devices is strictly limited to staff with a need to know and/or view that information. The key elements of GCBH BH-ASO computer and information use are included in the following procedures:

   a. Workstation and Portable Computer

   b. Password Protection

   c. Remote Access

B. GCBH BH-ASO makes use of access codes and passwords. The Password Protection Procedure PS610 outlines the specific policies and procedures for management of those codes and passwords. All users are familiar with and comply with this procedure.

C. GCBH BH-ASO staff using desktop computers, laptops, or other electronic appliance either standalone or networked are familiar with and follow the contents of the Workstation and Portable Computer Procedure.

[1]See definitions of document types in AD100, "Development, Approval & Review of Formal GCBH BH-ASO Documents"
[2]"Network Provider" – An organization with which GCBH BH-ASO is contracted for the provision of direct services.

PROCEDURE

1. Workstation Use Assumptions:
    1.1. Every desktop computer in GCBH BH-ASO is vulnerable to environmental threats, such as fire, water damage, power surges, and the like.
    1.2. Any desktop computer in GCBH BH-ASO can access confidential information if the user has the proper authorization.
    1.3. All computer screens can be visible to individuals who do not have access to confidential information that may appear on the screen.
2. Portable Computer Assumptions:
    2.1. Portable computers pose a significant security risk because they may contain confidential information and, being mobile, are more at risk for loss, theft, or other unauthorized access than GCBH BH-ASO's stationary workstations.
    2.2. Portable computers may be more vulnerable to viruses and security threats since they are used as a mobile device. Public or private networks other than GCBH BH-ASO's network may not regularly provide a virus or security protected environment like GCBH BH-ASO's network.
    2.3. Portable computer use is more difficult for GCBH BH-ASO to audit; thus, security breaches may be more difficult to identify and correct.
3. Preventative Measures for Workstations and/or Portable Computers:
    3.1. GCBH BH-ASO staff 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, slow response times of accessing data, error messages, and unexpected reboots of the computer/laptop, computer/laptop system halts, virus messaging, or other such attacks.
    3.2. All portable computer hard drives will be encrypted.
    3.3. All computers plugged into an electrical power outlet will use a desktop uninterrupted power supply (ups) unit with surge suppressing approved by the Information Services Manager.
    3.4. GCBH BH-ASO staff shall take reasonable precautions to protect computers and data from loss, damage, or destruction such as being cautious and discerning about opening links and attachments in emails, navigating to websites that may be deemed as suspicious or unsafe, keeping computers away from liquids, safe from unstable heights that would risk it to drop/break,etc.
    3.5. GCBH BH-ASO staff will maintain a record of the movements of hardware and electronic media and any person responsible therefore.
    3.6. GCBH BH-ASO staff will not connect unknown removable storage devices to GCBH equipment unless necessary for business and it has been vetted and approved by the IS Manager.
4. Remote Access:
    4.1. Remote access is meant to be an alternative method of support for GCBH BH-ASO office functions. By using GCBH BH-ASO hardware, software, and/or network

systems, staff assumes personal responsibility for their appropriate use. Staff reads and complies with the Remote Access Procedure, and understands the following:

4.1.1. That any software and hardware devices provided to staff by GCBH BH-ASO remain the property of the Agency.

4.1.2. There is no modifying, altering, or upgrading any software programs or hardware devices provided to staff by GCBH BH-ASO without the permission of the Information Services Department.

4.1.3. The need to take maximum precautions to prevent unauthorized access and/or viewing of an individual's protected health information.

4.1.4. All staff is strictly prohibited from downloading, copying, or keeping in any form protected health information (PHI) on personal computer(s).

4.1.5. There is no copying, or duplicating (except for backup purposes as part of your job), or allowing anyone else to copy or duplicate any software.

4.1.6. If staff leave GCBH BH-ASO for any reason, they immediately return the original and/or copies of any and all software, computer materials, or computer equipment received from GCBH BH-ASO that is either in immediate possession or otherwise directly or indirectly under their control.

4.1.7. All staff agree that reasonable efforts to protect all GCBH BH-ASO provided software and hardware devices from theft and physical damage must be taken.

5. Confidentiality and Security Agreement:

5.1. The Confidentiality and Security Agreement is used to acknowledge receipt of, and compliance with, this policy. A signed and dated Confidentiality and Security Agreement is placed in each employee's personnel file.

APPROVAL

Sindi Saunders

Karen Richardson or Sindi Saunders, Co-Directors

7/8/24

Date