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

Adopted: 1/1/2019
Last Reviewed: 2/16/2023
Retired: _____

Revisions: 2/28/2020

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 both to 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 optimize the security of the removal of PHI from office.

DEFINITIONS

I. Protected Health Information (PHI): Individually identifiable information relating to past, present or future physical, substance use, mental health or condition of an individual, provision of health care to an individual, or the past, present or future payment for health care provided to an individual.

II. Workforce Members: Employees, contractors, volunteers, trainees, and other persons whose conduct, in the performance of work for GCBH BH-ASO, its offices, programs or facilities, is under the direct control of GCBH BH-ASO, office, program or facility, regardless of whether they are paid by GCBH BH-ASO.

POLICY

A. In general, all PHI (Protected Health Information) must remain at the office. In certain circumstances, with the approval of the Director or HIPAA Officer, PHI may be taken out of the office. This may take the form of traveling employees or employees working from home. Remote access of PHI is covered in PS609 - Remote Access Procedure.

PROCEDURE

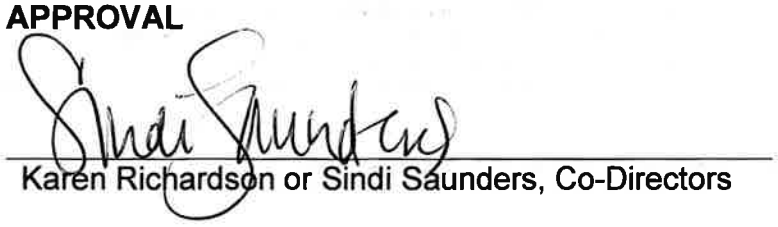
1. Originals are not taken off site. Copies are made for transport. Paper copies are shredded when no longer needed. Electronic copies are deleted.
2. PHI must only be accessed by business agency devices (including business phones, tablets, laptops, computers, etc.).
3. A log is kept of PHI taken off site.
4. All PHI taken off site is locked in a suitable container such as a locking file box or briefcase. When not in use, PHI removed from the office is protected from access by unauthorized persons using locking containers or software encryption if PHI is stored on removable storage media.
5. The above items apply to PHI in paper files, laptops, and electronic removable storage media such as computer disks, tape back-up media, and USB jump drives.

[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.

6. All PHI on electronic removable storage media and laptops are encrypted and password protected.
7. Penalties for violation of the Removal of PHI from Office Policy vary depending on the nature and severity of the specific violation. Any employee who violates the Removal of PHI from Office Policy is subject to discipline up to and including termination from employment in accordance with GCBH BH-ASO's Sanction Policy.

APPROVAL



Karen Richardson or Sindi Saunders, Co-Directors

2/16/23
Date