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

Adopted: 1/1/2019
Last Reviewed: 3/2/2026
Retired: _____

Revisions: 2/28/2020, 1/27/2021, 4/11/2022, 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 set forth the necessary information for Greater Columbia Behavioral Health (GCBH BH-ASO) employees to carry out their responsibilities while protecting the confidentiality of individuals' information. The requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), 42 CFR Part 2, or Health Information Technology for Economic and Clinical Health 04/27/09 (HITECH) require that such policies be established, enforced, and audited.

DEFINITIONS

I. None

POLICY

A. All employees preserve the integrity and the confidentiality of health and other sensitive information pertaining to individuals.

PROCEDURE

GCBH BH-ASO Employees:

1. Collect and use protected health information only for the purposes of supporting the delivery, payment, integrity, and quality of behavioral health services. GCBH BH-ASO employees and agents do not use or supply protected health information for non-health care uses, such as direct marketing, employment, or credit evaluation processes.
2. Collect and use individual health information only:
   - 2.1. As a basis for required reporting of health information.
   - 2.2. To receive reimbursement for services provided.
   - 2.3. For research and similar purposes designed to improve the quality and to reduce the cost of health care.
3. Recognize that protected health information collected about individuals must be accurate, timely, complete, and available when needed.
   - 3.1. Use their best efforts to ensure the accuracy, timeliness, and completeness of data to ensure that authorized personnel can access it when needed.

[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.

3.2. Maintain records for the retention periods required by law and professional standards.

3.3. Implement reasonable measures to protect the integrity of all data maintained about individuals.

3.4. Recognize that individuals have a right of privacy. GCBH BH-ASO employees respect individuals' dignity at all times. GCBH BH-ASO employees respect individuals' privacy to the extent consistent with providing the highest quality health care possible and with the efficient administration of the facility.

4. Act as responsible information stewards and treat all individual data and related financial, demographic, and lifestyle information as sensitive and confidential.

4.1. Treat all individuals' data as confidential in accordance with professional ethics and legal requirements.

4.2. Not divulge protected health information unless the individual (or their personal representative) has properly authorized the disclosure or the disclosure is otherwise authorized by law.

4.3. When releasing protected health information, take appropriate steps to prevent unauthorized re-disclosures, such as specifying that the recipient may not further disclose the information without individual authorization or as allowed by law.

4.4. Implement reasonable measures to protect the confidentiality of information maintained about individuals.

4.5. Remove individual identifiers when appropriate, such as in statistical reporting and in research studies.

4.6. Not disclose financial or other individual information except as necessary for billing or authorized purposes as authorized by law and professional standards.

4.7. Recognize that mental health information is particularly sensitive, as is HIV/AIDS information, developmental disability information, alcohol and drug abuse information, other information about sexually transmitted or communicable diseases, and that disclosure of such information could severely harm individuals, such as by causing loss of employment opportunities and insurance coverage, as well as the pain of social stigma. Consequently, GCBH BH-ASO employees treat such information with additional confidentiality protections as required by law, professional ethics, and accreditation requirements.

4.8. Recognize that, although GCBH BH-ASO owns the health record, the individual has a right of access to information contained in the record.

4.8.1. Permit individuals access to their records except when access would be detrimental to the individual under "therapeutic exception" to individual access. In such cases, GCBH BH-ASO and its employees provide an authorized representative access to the individual records in accordance with professional ethics and laws.

4.8.2. Provide individuals an opportunity to request correction of inaccurate data in their records in accordance with the law and professional standards.

4.9. GCBH BH-ASO does not tolerate violations of this policy. Violation of this policy is grounds for disciplinary action, up to and including termination of employment and criminal or professional sanctions in accordance with GCBH BH-ASO's sanction policy and personnel rules and regulations.

4.10. The management structure for this Plan is outlined below. These individuals have primary responsibility for the development, deployment, and ongoing management of the Plan and all associated policies and procedures.

5. Reporting Security Problems:

5.1. If sensitive GCBH BH-ASO information is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties, the HIPAA Officer is notified immediately.

5.2. If any unauthorized use of GCBH BH-ASO's information systems has taken place, or is suspected of taking place, the IS Manager and HIPAA Officer is likewise notified immediately. Similarly, whenever passwords or other system access control mechanisms are lost, stolen, or disclosed, or are suspected of being lost, stolen, or disclosed, the IS Manager and HIPAA Officer are notified immediately.

5.3. Notification of Compromise or Potential Compromise. The compromise or potential compromise of HCA shared data must be reported to the HCA Contact designated on the contract within five (5) business days of discovery.

6. Additional Responsibilities:

6.1. As defined below, GCBH BH-ASO employees responsible for Internet security have been designated in order to establish a clear line of authority and responsibility.

6.1.1. Information Systems will establish an Internet security infrastructure consisting of hardware, software, policies, and standards, and department staff will provide technical guidance on workstation, laptop, and all electronic security to all GCBH BH-ASO staff. The IS Department responds to viruses, hacker intrusions, and similar events.

6.1.2. IS staff monitors compliance with Internet security requirements, including hardware, software, and data safeguards. Program directors ensure that their staff is in compliance with the Internet security policy established in this document. IS staff shall provide administrative support and technical guidance to management on matters related to Internet security.

6.1.3. IS staff periodically, no less than annually, conducts a risk assessment of each production information system they are responsible for to determine both risks and vulnerabilities.

6.1.4. IS staff check that appropriate security measures are implemented on these systems in a manner consistent with the level of information sensitivity.

6.1.5. IS staff check that user access controls are defined on these systems in a manner consistent with the users need-to-know.

6.1.6. GCBH BH-ASO information owners see to it that the sensitivity of data is defined and designated on these systems in a manner consistent with in-house sensitivity classifications.

6.2. GCBH BH-ASO supervisors ensure that:

6.2.1. Employees under their supervision implement security measures as defined in this document.

6.2.2. Employees comply with all stated GCBH BH-ASO policies that ensure data security.

6.2.3. Employees and contractor personnel under their supervision complete the pre-exit clearance process upon their official termination of employment or contractual agreement.

6.2.4. Employees and contractor personnel under their supervision make back-up copies of sensitive, critical, and valuable data files as often as is deemed reasonable.

6.3. Users of GCBH BH-ASO Internet connections:

6.3.1. Know and apply the appropriate GCBH BH-ASO policies and practices pertaining to Internet security.

6.3.2. Do not permit any unauthorized individual to obtain connect to GCBH BH-ASO Internet connections.

6.3.3. Do not use or permit the use of any unauthorized device in connection with GCBH BH-ASO workstations.

6.3.4. Do not use GCBH BH-ASO Internet resources (software/hardware or data) for any reason other than authorized business purposes.

6.3.5. Maintain exclusive control over and use of their password, and protect it from inadvertent disclosure to others.

6.3.6. Select a password that bears no obvious relation to the user, the user's organizational group, or the user's work project, and that is not easy to guess. (See Password Protection policy)

6.3.7. Ensure that data under their control and/or direction is properly safeguarded according to its level of sensitivity.

6.3.8. Report to the IS Manager or IS staff any incident that appears to compromise the security of GCBH BH-ASO information resources. These include missing data, viruses, and unexplained transactions.

6.3.9. Access only the data and automated functions for which they are authorized in the course of normal business activity.

6.3.10. Obtain IS Manager authorization for any uploading or downloading of information to or from GCBH BH-ASO information systems if this activity is outside the scope of normal business activities.

6.3.11. Make backups of all sensitive, critical, and valuable data files as often as is deemed reasonable by the IS Manager.

6.3.12. Be mindful of printing documents, and ensure that print jobs are retrieved promptly and not left in unsecured areas.

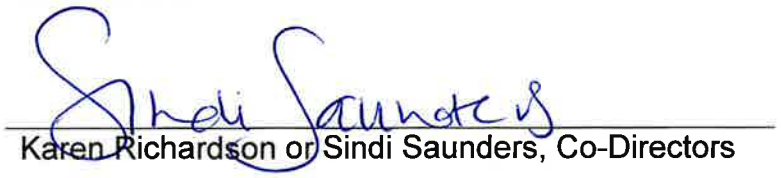
7. Contact Point:

7.1. Questions about this policy may be directed to the IS Manager and/or HIPAA Officer.

8. Disciplinary Process:

8.1. Violation of these policies may subject employees or contractors to disciplinary procedures up to an including termination.

APPROVAL



Karen Richardson or Sindi Saunders, Co-Directors

3/2/2024
Date