

GREATER COLUMBIA BEHAVIORAL HEALTH Policies and Procedures

Category: Privacy and Security
Approved On: 03/27/2003
Approved By: The Board of Directors
Revised: 00/00/00
Effective Date: 15 days from approval/ the last revision

No: PS624.00

Title: Privacy and Security Plan

I. Background:

The use of computers and computer networks has become an integral part of the behavioral health and human services industry. These technologies have brought and will continue to bring enormous advantages to our industry and will continue to enable us to innovate in the means of delivering service to consumers. These technologies have also brought significant risks regarding consumer confidentiality and privacy. Many organizations have opted to establish security and privacy policies that give specific guidelines on an employee's use of these technologies, in all locations. The requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) require that such policies be established, enforced, and audited.

II. Policy:

It is the policy of Greater Columbia Behavioral Health (GCBH) that all employees must preserve the integrity and the confidentiality of health and other sensitive information pertaining to our consumers. The purpose of this policy is to ensure that GCBH employees have the necessary information to carry out its responsibilities while protecting the confidentiality of consumer information. To that end, GCBH employees will:

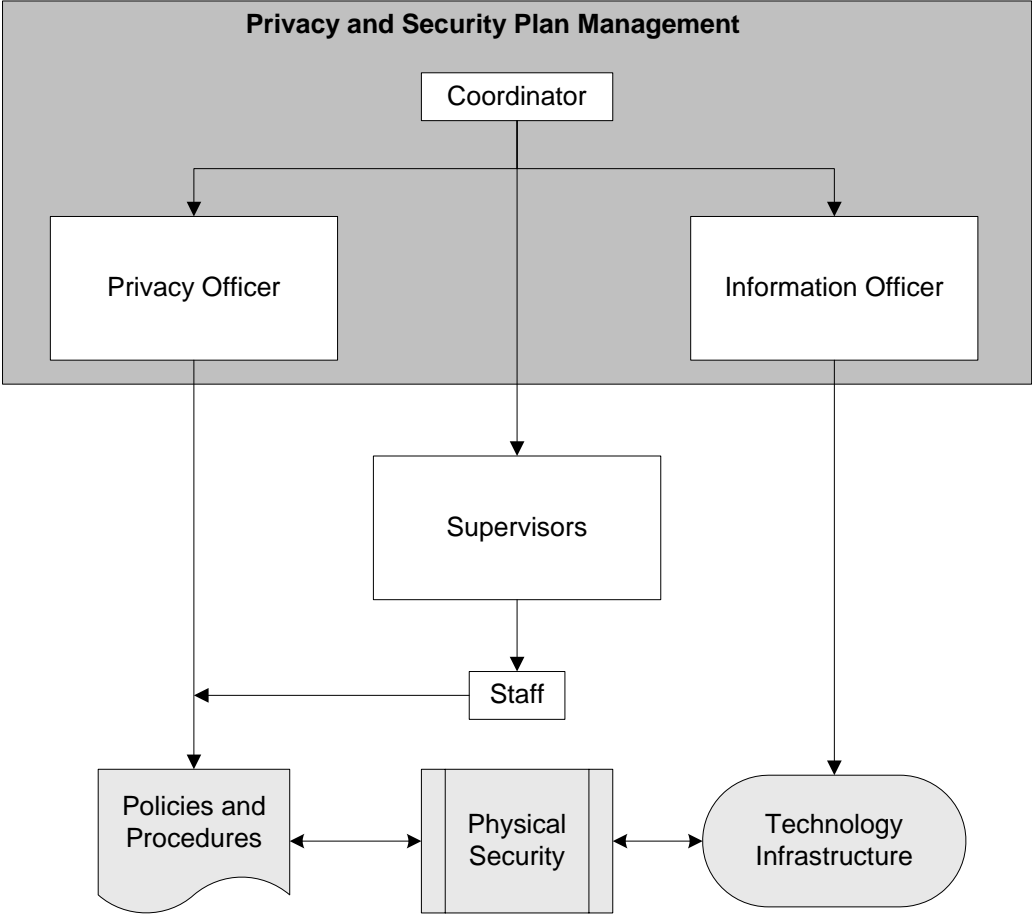
- A. Collect and use protected health information only for the purposes of supporting the delivery, payment, integrity, and quality of mental health services. GCBH employees and agents will not use or supply protected health information for non-health care uses, such as direct marketing, employment, or credit evaluation processes.
- B. Collect and use individual health information only:
 - 1. As a basis for required reporting of health information.
 - 2. To receive reimbursement for services provided.

3. For research and similar purposes designed to improve the quality and to reduce the cost of health care.
- C. Recognize that protected health information collected about consumers must be accurate, timely, complete, and available when needed. GCBH employees will:
1. Use their best efforts to ensure the accuracy, timeliness, and completeness of data to ensure that authorized personnel can access it when needed.
 2. Maintain records for the retention periods required by law and professional standards.
 3. Implement reasonable measures to protect the integrity of all data maintained about consumers.
 4. Recognize that consumers have a right of privacy. GCBH employees will respect consumers' individual dignity at all times. GCBH employees will respect consumers' privacy to the extent consistent with providing the highest quality health care possible and with the efficient administration of the facility.
- D. Act as responsible information stewards and treats all consumer data and related financial, demographic, and lifestyle information as sensitive and confidential. Consequently, GCBH employees will:
1. Treat all consumer data as confidential in accordance with professional ethics and legal requirements.
 2. Not divulge protected health information unless the consumer (or his or her personal representative) has properly authorized the disclosure or the disclosure is otherwise authorized by law.
 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 consumer authorization or as allowed by law.
 4. Implement reasonable measures to protect the confidentiality of information maintained about consumers.
 5. Remove consumer identifiers when appropriate, such as in statistical reporting and in research studies.
 6. Not disclose financial or other consumer information except as necessary for billing or authorized purposes as authorized by law and professional standards.
- E. Recognize that mental health information is particularly sensitive, as is HIV/AIDS information, developmental disability information, alcohol and drug abuse information, and other information about sexually transmitted or communicable diseases and that disclosure of such information could severely harm consumers, such as by causing loss of employment opportunities and insurance

coverage, as well as the pain of social stigma. Consequently, GCBH employees will treat such information with additional confidentiality protections as required by law, professional ethics, and accreditation requirements.

- F. Recognize that, although GCBH owns the health record, the consumer has a right of access to information contained in the record. GCBH and its employees will:
 - 1. Permit consumers access to their records except when access would be detrimental to the consumer under the so-called “therapeutic exception” to consumer access. In such cases, GCBH and its employees will provide an authorized representative access to the consumer records in accordance with professional ethics and laws.
 - 2. Provide consumers an opportunity to request correction of inaccurate data in their records in accordance with the law and professional standards.
- G. All employees of GCBH must adhere to this policy. GCBH must adhere to this policy. GCBH will 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 clinical information sanction policy and personnel rules and regulations.
- H. The management structure for this Plan is outlined on the following page. These individuals have primary responsibility for the development, deployment, and ongoing management of the Plan and all associated policies and procedures.

**Greater Columbia Behavioral Health
Privacy and Security Plan Management
Chain of Responsibility**



III. Reporting Security Problems:

- A. If sensitive GCBH information is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties, the Information Officer (IO) and Privacy Officer (PO) must be notified immediately.
- B. If any unauthorized use of GCBH's information systems has taken place, or is suspected of taking place, the IO and PO must likewise be 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 IO and PO must be notified immediately.

IV. Additional Responsibilities:

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

- A. Information Systems will establish an Internet security infrastructure consisting of hardware, software, policies, and standards, and department staff will provide technical guidance on PC security to all GCBH staff. The IS Department will respond to virus infestations, hacker intrusions, and similar events.
- B. IS staff will monitor compliance with Internet security requirements, including hardware, software, and data safeguards. Program directors must ensure that their staffs are in compliance with the Internet security policy established in this document. IS staff will also provide administrative support and technical guidance to management on matters related to Internet security.
- C. IS staff will periodically, and no less than annually, conduct a risk assessment of each production information system they are responsible for to determine both risks and vulnerabilities.
- D. IS staff will check that appropriate security measures are implemented on these systems in a manner consistent with the level of information sensitivity.
- E. IS staff will check that user access controls are defined on these systems in a manner consistent with the need-to-know.
- F. GCBH information owners will see to it that the sensitivity of data is defined and designated on these systems in a manner consistent with in-house sensitivity classifications.
- G. GCBH supervisors will ensure that:
 - 1. Employees under their supervision implement security measures as defined in this document.
 - 2. Employees under their supervision delete sensitive (confidential) data from their disk files when the data is no longer needed or useful.

3. Employees under their supervision who are authorized to use personal computers are aware of and comply with the policies and procedures outlined in all GCBH documents that address information security.
4. Employees and contractor personnel under their supervision complete the pre-exit clearance process upon their official termination of employment or contractual agreement.
5. Employees and contractor personnel under their supervision make back-up copies of sensitive, critical, and valuable data files as often as is deemed reasonable.

H. Users of GCBH Internet connections must:

1. Know and apply the appropriate GCBH policies and practices pertaining to Internet security.
2. Not permit any unauthorized individual to obtain access to GCBH Internet connections.
3. Not use or permit the use of any unauthorized device in connection with GCBH personal computers.
4. Not use GCBH Internet resources (software/hardware or data) for other than authorized company purposes.
5. Maintain exclusive control over and use of his/her password, and protect it from inadvertent disclosure to others.
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)
7. Ensure that data under his/her control and/or direction is properly safeguarded according to its level of sensitivity.
8. Report to the CIO or IS staff any incident that appears to compromise the security of GCBH information resources. These include missing data, virus infestations, and unexplained transactions.
9. Access only the data and automated functions for which he/she is authorized in the course of normal business activity.
10. Obtain IS Manager authorization for any uploading or downloading of information to or from GCBH multi-user information systems if this activity is outside the scope of normal business activities.
11. Make backups of all sensitive, critical, and valuable data files as often as is deemed reasonable by the IS Manager.

V. Contact Point:

Questions about this policy may be directed to the Information Officer.

VI. Disciplinary Process:

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

VII. Related Policies:

- | | |
|--|---|
| A. Computer and Information Usage | B. Employee Training |
| C. Confidentiality and Disclosures of Protected Health Information | D. Privacy Officer Job Responsibilities |
| E. Confidentiality and Security Agreement | F. Sanctions |
| G. E-Mail and Internet Usage | H. Telefacsimiles |

VIII. Scheduled Review of this Policy:

The review of the GCBH policies and procedures manual is on a two year cycle. The GCBH policy review and revision approval process is a three month process. This policy is scheduled to be reviewed every second year:

- A. by GCBH staff by April of odd years,
- B. by the Regional Advisory Board (RAB) by May of odd years,
- C. by the GCBH Board of Directors by June of odd years, and
- D. outside of the schedule if required.