Great Rivers Behavioral Health
Administrative Services Organization

Policy Title:	**Privacy and Security**	Policy No. **5023.00**
Category:	Privacy & Security	Date Adopted: 1/10/2020 Date Revised: Date Reviewed:
Reference:	Washington Health Care Authority Contract with Great Rivers Behavioral Health	

POLICY

1.1. Great Rivers Behavioral Health Administrative Services Organization (Great Rivers BH-ASO), in an effort to be compliant with the Privacy Rules of HIPAA's Administrative Simplification provisions, sets out, in this policy, the information necessary for its employees to carry out their responsibilities while protecting the confidentiality of consumer 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.

1.1. All Great Rivers BH-ASO employees preserve the integrity and the confidentiality of health and other sensitive information pertaining to consumers.

PROCEDURE:

2.1. Great Rivers BH-ASO Employees:

- 2.1.1. Collect and use protected health information only for the purposes of supporting the delivery, payment, integrity, and quality of behavioral health services. Great Rivers 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.
- 2.1.2. Collect and use individual health information only:
  - 2.1.2.1. As a basis for required reporting of health information.
  - 2.1.2.2. To receive reimbursement for services provided.
  - 2.1.2.3. For research and similar purposes designed to improve the quality and to reduce the cost of health care.
- 2.1.3. Recognize that protected health information collected about consumers must be accurate, timely, complete, and available when needed
- 2.1.4. Use their best efforts to ensure the accuracy, timeliness, and completeness of data to ensure that authorized personnel can access it when needed.
- 2.1.5. Maintain records for the retention periods required by law and professional standards.
- 2.1.6. Implement reasonable measures to protect the integrity of all data maintained about consumers.
- 2.1.7. Recognize that consumers have a right of privacy. Great Rivers BH-ASO employees respect consumers' individual dignity at all times. Great Rivers

BH-ASO's employees respect consumers' privacy to the extent consistent with providing the highest quality health care possible and with the efficient administration of the facility.

2.1.8. Act as responsible information stewards and treats all consumer data and related financial, demographic, and lifestyle information as sensitive and confidential.

2.1.9. Treat all consumer data as confidential in accordance with professional ethics and legal requirements.

2.1.10. 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.

2.1.11. 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.

2.1.12. Implement reasonable measures to protect the confidentiality of information maintained about consumers.

2.1.13. Remove consumer identifiers when appropriate, such as in statistical reporting and in research studies.

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

2.1.15. 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, Great Rivers BH-ASO employees treat such information with additional confidentiality protections as required by law, professional ethics, and accreditation requirements.

2.1.16. Recognize that, although Great Rivers BH-ASO owns the health record, the consumer has a right of access to information contained in the record.

2.1.16.1. 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, Great Rivers BH-ASO and its employees provide an authorized representative access to the consumer records in accordance with professional ethics and laws.

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

2.1.17. Great Rivers 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 Great Rivers BH-ASO clinical information sanction policy and personnel rules and regulations.

2.2. Reporting Security Problems:

2.2.1. If sensitive Great Rivers BH-ASO information is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties, the IS Manager (IS Mgr) through the role of Security Officer (SO) is notified immediately.

2.2.2. If any unauthorized use of Great Rivers BH-ASO's information systems has taken place, or is suspected of taking place, the IS Mgr 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 Mgr is notified immediately.

2.2.3. Notification of Compromise or Potential Compromise. The compromise or potential compromise of DSHS shared data must be reported to the DSHS Contact designated on the contract within one (1) business day of discovery.

2.3. Additional Responsibilities:

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

2.3.1.1. Information Systems will establish an Internet security infrastructure consisting of hardware, software, policies, and standards, and department staff will provide technical guidance on PC security to all Great Rivers BH-ASO staff. The IS Department responds to virus infestations, hacker intrusions, and similar events.

2.3.1.2. 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 provides administrative support and technical guidance to management on matters related to Internet security.

2.3.1.3. 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.

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

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

2.3.1.6. Great Rivers 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.

2.3.2. Great Rivers BH-ASO ensures that:

2.3.2.1. Employees implement security measures as defined in this document.

2.3.2.2. Employees follow best practices of Computer, Internet, and Electronic Mail Policy standard along with complying with all stated Great Rivers BH-ASO policies that ensure data security.

2.3.2.3. Employees who are authorized to use personal computers are aware of and comply with the policies and procedures outlined in all Great Rivers BH-ASO documents that address information security.

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

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

2.3.3. Users of Great Rivers BH-ASO's Internet connections:

2.3.3.1. Know and apply the appropriate Great Rivers BH-ASO's policies and practices pertaining to Internet security.

2.3.3.2. Do not permit any unauthorized individual to obtain access to Great Rivers BH-ASO's Internet connections.

2.3.3.3. Do not use or permit the use of any unauthorized device in connection with Great Rivers BH-ASO's personal computers.

2.3.3.4. Do not use Great Rivers BH-ASO's Internet resources (software/hardware or data) for other than authorized company purposes.

2.3.3.5. Maintain exclusive control over and use of his/her password, and protect it from inadvertent disclosure to others.

2.3.3.6. 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)

2.3.3.7. Ensure that data under his/her control and/or direction is properly safeguarded according to its level of sensitivity.

2.3.3.8. Report to the IS Manager or IS staff any incident that appears to compromise the security of Great Rivers BH-ASO's information resources. These include missing data, virus infestations, and unexplained transactions.

2.3.3.9. Access only the data and automated functions for which he/she is authorized in the course of normal business activity.

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

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

2.4.1. Contact Point:

2.4.1.1. Questions about this policy may be directed to the IS Manager.

2.5.1. Disciplinary Process:

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

POLICY SIGNATURE

Edna J. Fund DIGITALLY SIGNED

Edna J. Fund, Chair
Great Rivers BH-ASO Governing Board

01/30/2020
07:57 PM EST

Date