Great Rivers Behavioral Health
Administrative Services Organization

Policy Title:	**Security and Confidentiality**	Policy No. **3010.01**
Category:	Information Services	Date Adopted: 01/10/2020 Date Revised: 12/6/2022 Date Reviewed: 12/6/2022
Reference:	Great Rivers Internal Policy, HCA Agreements	

Policy:

Great Rivers Behavioral Health Administrative Services Organization (Great Rivers) and its contractors shall protect and maintain all Confidential Information. The information that is defined as confidential under state or federal law or regulation, or Data that HCA and Great Rivers has identified as confidential, against unauthorized use, access, disclosure, modification or loss. This duty requires the Contractors and Great Rivers to employ reasonable security measures, which include restricting access to the Confidential Information by allowing access only to staff that have an authorized business requirement to view the Confidential Information and physically securing any computers, documents, or other media containing the Confidential Information.

Procedure:

Data Security Requirements

1. Data Transmitting
    a. When transmitting Data electronically, including via email, the Data must be encrypted using NIST 800-series approved algorithms (http://csrc.nist.gov/publications/PubsSPs.html). This includes transmission over the public internet.
    b. When transmitting Data via paper documents a Trusted System must be used.
2. **Protection of Data.** Great Rivers and its contractors shall store data and protect the data as described:

    a. Data at Rest

        i. Data will be encrypted with NIST 800-series approved algorithms. Encryption keys will be stored and protected independently of the data. Access to the Data will be restricted to Authorized Users through the use of access control lists, a Unique User ID, and a Hardened Password, or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. Systems that contain or provide access to Confidential Information must be located in an area that is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

b. Data stored on Portable/Removable Media or Devices

i. Confidential Information provided by Great Rivers on Removable Media will be encrypted with NIST 800-series approved algorithms. Encryption keys will be stored and protected independently of the Data.

ii. Great Rivers Data must not be stored by the Contractor on Portable Devices or Media unless specifically authorized within the Contract. If so authorized, the Contractor must protect the Data by:

1. Encrypting with NIST 800-series approved algorithms. Encryption keys will be stored and protected independently of the data;

2. Controlling access to the devices with a Unique User ID and Hardened Password or stronger authentication method such as a physical token or biometrics;

3. Manually lock devices whenever they are left unattended and set devices to lock automatically after a period of inactivity, if this feature is available. Maximum period of inactivity is 20 minutes.

4. Physically protect the portable devices(s) and/or media by keeping devices in locked storage when not in use;

5. Using check-in/check-out procedures when devices are shared;

6. Maintaining an inventory of devices; and

7. Ensuring that when being transported outside of a Secured Area, all devices containing Data are under the physical control of an Authorized User.

iii. Paper Documents. Any paper records containing Confidential Information must be protected by storing the records in a Secured Area that is accessible only to authorized personnel. When not in use, such records must be stored in a locked container, such as a file cabinet, locking drawer, or safe, to which only authorized persons have access.

3. Data Segregation.

a. Great Rivers data must be segregated or otherwise distinguishable from non-Great Rivers data. This is to ensure that when no longer needed by the contractor, all Great Rivers data can be identified for return or destruction.

It also aids in determining whether Great Rivers data has or may have been compromised in the event of a security breach.

b. Great Rivers data will be kept in one of the following ways:

   i. On media (e.g. hard disk, optical disc, tape, etc.) that will contain no non- Great Rivers data;

   ii. In a logical container on electronic media, such as a partition or folder dedicated to Great Rivers data;

   iii. In a database that contains only Great Rivers data;

   iv. within a database and will be distinguishable from non-Great Rivers data by the value of a specific field or fields within database records

   v. Physically segregated from non-Great Rivers data in a drawer, folder or other container as paper documents

c. When it is not feasible or practical to segregate Great Rivers data from non-Great Rivers data, then both the Great Rivers data and the non-Great Rivers data with which it is commingled must be protected as described in this policy.

4. **Data Disposition.**

a. Upon request by Great Rivers, at the end of the Contract term, or when no longer needed, Confidential Information/Data must be returned to HCA or disposed of as set out below, except as required to be maintained for compliance or accounting purposes.

b. Media are to be destroyed using a method documented within NIST 800-88 (http://csrc.nist.gov/publications/PubsSPs.html).

c. For Data stored on network disks, deleting unneeded Data is sufficient as long as the disks remain in a Secured Area and otherwise meet the requirements listed in this policy. Destruction of the Data as outlined in this section of this policy may be deferred until the disks are retired, replaced, or otherwise taken out of the Secured Area.

5. Data Confidentiality

a. The Contractor will not use, publish, transfer, sell or otherwise disclose any Confidential Information gained by reason of this Contract for any purpose that is not directly connected with the purpose of this Contract, except:

   i. as provided by law; or

ii. with the prior written consent of the person or personal representative of the person who is the subject of the Confidential Information.

b. Non-Disclosure of Data

i. The Great Rivers and Contractors will ensure that all employees or Subcontractors who will have access to the Data described in this Policy (including both employees who will use the Data and IT support staff) are instructed and aware of the use restrictions and protection requirements of this policy before gaining access to the Data identified herein. The Contractor will ensure that any new employee is made aware of the use restrictions and protection requirements of this Exhibit before they gain access to the Data.

ii. The Contractor will ensure that each employee or Subcontractor who will access the Data signs a non-disclosure of confidential information agreement regarding confidentiality and non-disclosure requirements of Data under this Contract. The Contractor must retain the signed copy of employee non-disclosure agreement in each employee's personnel file for a minimum of six years from the date the employee's access to the Data ends. The Contractor will make this documentation available to HCA upon request.

c. Penalties for Unauthorized Disclosure of Data

i. The Contractor must comply with all applicable federal and state laws and regulations concerning collection, use, and disclosure of Personal Information and PHI. Violation of these laws may result in criminal or civil penalties or fines.

ii. The Contractor accepts full responsibility and liability for any noncompliance with applicable laws or this Contract by itself, its employees, and its Subcontractors.

6. Cloud Storage

a. Contractor has written procedures in place governing use of the Cloud

b. storage and Contractor attests in writing that all such procedures will be uniformly followed.

c. (b) The Data will be Encrypted while within the Contractor network.

d. (c) The Data will remain Encrypted during transmission to the Cloud.

e. (d) The Data will remain Encrypted at all times while residing within the Cloud storage solution.

f. (e) The Contractor will possess a decryption key for the Data, and the decryption key will be possessed only by the Contractor and/or Great Rivers.

g. (f) The Data will not be downloaded to non-authorized systems, meaning

h. systems that are not on either the Great Rivers or Contractor networks.

i. (g) The Data will not be decrypted until downloaded onto a computer within the control of an Authorized User and within either the Great Rivers or Contractor's network.

j. (2) Data will not be stored on an Enterprise Cloud storage solution unless either:

k. (a) The Cloud storage provider is treated as any other Sub-Contractor, and agrees in writing to all of the requirements within this exhibit; or, (b) The Cloud storage solution used is FedRAMP certified.

l. (3) If the Data includes protected health information covered by the Health Insurance Portability and Accountability Act (HIPAA), the Cloud provider must sign a Business Associate Agreement prior to Data being stored in their Cloud solution.

7. **System Protection**. To prevent compromise of systems which contain Great Rivers Data or through which that Data passes:

   a. Systems containing Great Rivers Data must have all security patches or hotfixes applied within 3 months of being made available.

   b. The Contractor will have a method of ensuring that the requisite patches and hotfixes

   have been applied within the required timeframes.

   c. Systems containing Great Rivers Data shall have an Anti-Malware application, if available, installed.

   d. Anti-Malware software shall be kept up to date. The product, its anti-virus engine, and any malware database the system uses, will be no more than one update behind current.

POLICY SIGNATURE

DocuSigned by:
Vickie L. Raines
2EC90BCF63204FC...

12/13/2022

Vickie L. Raines, Chair
Great Rivers Governing Board

Date