Great Rivers Behavioral Health Administrative Services Organization

Policy Title:	**Breach Notification – Protected Health Information Process and Security Incident Procedures**	Policy No. **5024.00**
Category:	HIPAA Privacy & Security	Date Adopted: 02/14/2020 Date Revised:
Reference:	Washington Health Care Authority Contract with Great Rivers Behavioral Health Organization; ▪ ARRA Title XIII Section 13402 – Notification in the Case of Breach ▪ RCW 42.56.590 – Personal Information – Notice of security breaches. ▪ RCW 19.255.010 – Disclosure, notice – Definitions – Rights, remedies. 45 CFR Parts 160 and 164 – HIPAA Privacy and Security Rules; 45 CFR 164.306 and 45 CFR 164.308	

POLICY:

1.1. Breach Notification – Protected Health Information

1.1.1. Discovery of Breach: A potential breach of PHI shall be treated as "discovered" as of the first day on which such breach is known to Great Rivers Behavioral Health Administrative Services Organization (Great Rivers BH-ASO), or by exercising reasonable diligence would have been known to Great Rivers BH-ASO (includes breaches by Great Rivers BH-ASO's business associates). Great Rivers BH-ASO shall be deemed to have knowledge of a breach if such breach is known or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent (business associate) of Great Rivers BH-ASO. Following the discovery of a potential breach, Great Rivers BH-ASO shall begin an investigation, conduct a risk assessment, and, based on the results of the risk assessment, if a breach is confirmed, then begin the process to notify each individual who's PHI has been, or is reasonably believed by Great Rivers BH-ASO to have been, accessed, acquired, used, or disclosed. Great Rivers BH-ASO shall also begin the process of determining what, if any, external notifications are required or should be made [e.g., Secretary of Department of Health & Human Services (HHS), media outlets, law enforcement officials, etc.]. If a Great Rivers BH-ASO contracted business associate discovers a breach within their agency, they will notify Great Rivers BH-ASO and keep Great Rivers BH-ASO apprised of their investigation, risk assessment, and results of their investigation.

1.1.2. Breach Investigation: The Privacy Officer and Security Officer, as appropriate, shall confer and decide who will lead the investigation of the suspected or confirmed breach. The chosen investigative lead shall be responsible for the management of the breach investigation, completion of a risk assessment, and coordination with others as appropriate (e.g., Executive Team, Governing Board, etc.) The investigator(s) shall be the key facilitators for all breach notification processes to the appropriate entities (e.g., HHS, media, law enforcement officials, etc.). All documentation related to the breach investigation, including the risk assessment, shall be retained for a minimum of ten (10) years.

1.1.3. Risk Assessment: For an acquisition, access, use, or disclosure of PHI to constitute a breach, it must constitute a violation of the Privacy Rule. Three specific exceptions to the definition of a "breach" under HIPAA are recognized [see Final Omnibus Rule [45 CFR 164.402(2)]]. In addition to the three exceptions, HIPAA recognizes that a use or

disclosure of unencrypted PHI that suggests a low risk of harm based upon the following criteria is also not a "breach" by definition:

1.1.3.1. Consideration of who impermissibly used or to whom the information was impermissibly disclosed;

1.1.3.2. The nature and extent of PHI involved;

1.1.3.3. Whether the PHI was actually acquired or viewed; and

1.1.3.4. The extent to which the risk to PHI has been mitigated.

1.1.4. Timeliness of Notification: Upon determination that breach notification is required, the notice shall be made without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach by Great Rivers BH-ASO involved or the business associate involved. It is the responsibility of Great Rivers BH-ASO to demonstrate that all notifications were made as required, including evidence demonstrating the necessity of delay.

1.1.5. Delay of Notification Authorized for Law Enforcement Purposes: If a law enforcement official states to Great Rivers BH-ASO that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, Great Rivers BH-ASO shall:

1.1.5.1. If the statement is in writing, and specifies the time for which a delay is required, delay such notification, notice, or posting of the time period specified by the official; or

1.1.5.2. If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described above is submitted during that time.

1.1.6. Content of the Notice: The notice shall be written in plain language and must contain the following information:

1.1.6.1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.

1.1.6.2. A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, Social Security number, date of birth, home address, record number, diagnosis, disability code, or other types of information were involved);

1.1.6.3. Any steps the individual should take to protect themselves from potential harm resulting from the breach;

1.1.6.4. A brief description of what Great Rivers BH-ASO or Business Associate is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches;

1.1.6.5. Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an email address, web site, or postal address

1.1.7. Methods of Notification: The method of notification will depend on the individuals/ entities to be notified. The following methods must be utilized accordingly:

1.1.7.1. Notice to Individual(s): Notice shall be provided promptly and in the following form:

1.1.7.1.1. Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice, and such agreement has not been withdrawn, by electronic mail. The notification shall be provided in one or more mailings as information is available. If Great Rivers BH-ASO knows that the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification by first-class mail to the next of kin or person representative shall be carried out;

1.1.7.1.2. Substitute Notice: In the case where there is insufficient or out-of-date contact information (including a phone number, email address, etc.) that precludes direct written or electronic notification, a substitute form of notice reasonably calculated to reach the individual shall be provided. A substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative;

1.1.7.1.3. In a case in which there is insufficient or out-of-date contact information for fewer than 10 individuals, then the substitute notice may be provided by an alternative form of written notice, telephone, or other means;

1.1.7.1.4. In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then the substitute notice shall be in the form of either a conspicuous posting for a period of 90 days on the home page of Great Rivers BH-ASO's website, or a conspicuous notice in a major print or broadcast media in Great Rivers BH-ASO's geographic areas where the individuals affected by the breach likely reside. The notice shall include a toll-free number that remains active for at least 90 days where an individual can learn whether his or her PHI may be included in the breach.

1.1.7.2. If Great Rivers BH-ASO determines that notification requires urgency because of possible imminent misuse of unsecured PHI, notification may be provided by telephone or other means, as appropriate in addition to the methods noted above.

1.1.8. Notice to Media: Notice shall be provided to prominent media outlets serving the state and regional area when the breach of unsecured PHI affects more than 500 patients. The Notice shall be provided in the form of a press release.

1.1.9. Notice to Secretary of HHS: Notice shall be provided to the Secretary of HHS as follows below. The Secretary shall make available to the public on the HHS Internet website a list identifying covered entities involved in all breaches in which the unsecured PHI of more than 500 patients is accessed, acquired, used, or disclosed.

1.1.9.1. For breaches involving 500 or more individuals, Great Rivers BH-ASO and/or Business Associate shall notify the Secretary of HHS as

instructed at www.hhs.gov at the same time notice is made to the individuals.

1.1.9.2. For breaches involving less than 500 individuals, Great Rivers BH-ASO and/or Business Associate will maintain a log of the breaches and annually submit the log to the Secretary of HHS during the year involved (logged breaches occurring during the preceding calendar year to be submitted no later than 60 days after the end of the calendar year). Instructions for submitting the log are provided at www.hhs.gov.

1.2. Maintenance of Breach Information/Log: As described above, and in addition to the reports created for each incident, Great Rivers BH-ASO shall maintain a process to record or log all breaches of unsecured PHI regardless of the number of patients affected. The following information should be collected/logged for each breach (see sample Breach Notification Log):

1.2.1. A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of patients affected, if known.

1.2.2. A description of the types of unsecured protected health information that were involved in the breach (such as full name, Social Security number, date of birth, home address, record number, etc.).

1.2.3. A description of the action taken with regard to notification of patients regarding the breach.

1.2.4. Resolution steps taken to mitigate the breach and prevent future occurrences.

1.3. Business Associate Responsibilities: The business associate (BA) of Great Rivers BH-ASO that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information shall, without unreasonable delay and in no case later than 60 calendar days after discovery of a breach, notify Great Rivers BH-ASO of such breach. Such notice shall include the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the BA to have been, accessed, acquired, or disclosed during such breach. The BA shall provide Great Rivers BH-ASO with any other available information that Great Rivers BH-ASO is required to include in notification to the individual at the time of the notification or promptly thereafter as information becomes available. Upon notification by the BA of discovery of a breach, Great Rivers BH-ASO will be responsible for notifying affected individuals, unless otherwise agreed upon by the BA to notify the affected individuals (note: it is still the burden of the Covered Entity to document this notification).

1.4. Workforce Training: Great Rivers BH-ASO shall train all members of its workforce on the policies and procedures with respect to PHI as necessary and appropriate for the members to carry out their job responsibilities. Workforce members shall also be trained as to how to identify and report breaches within Great Rivers BH-ASO.

1.5. Sanctions: Great Rivers BH-ASO shall have in place and apply appropriate sanctions against members of its workforce who fail to comply with privacy policies and procedures.

1.6. Retaliation/Waiver: Great Rivers BH-ASO may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by the individual of any privacy right. Great Rivers BH-ASO may not require individuals to waive their privacy rights under as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

POLICY SIGNATURE

DocuSigned by:
Edna J. Fund
3731C87058C2465

4/14/2020

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

Date