

Document Type:¹

☒ 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

Document Scope: (applies to Policy & Procedure only)

- 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 providers².
- The requirements herein apply both to GCBH BH-ASO and its network providers². 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 provide guidance to Greater Columbia Behavioral Health (GCBH BH-ASO) staff when there is a breach involving an individual's unsecured protected health information. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that GCBH BH-ASO notify individuals whose unsecured PHI has been compromised by such a breach. In certain circumstances involving 500 or more individuals, in addition to notifying Washington State Health Care Authority (HCA) and the Secretary of the U.S. Department of Health and Human Services (HHS), GCBH BH-ASO must also report such breaches to the media. GCBH BH-ASO's breach notification process will be carried out in compliance with the Health Information Technology for Economic and Clinical Health (HITECH) Act, as part of the American Recovery and Reinvestment Act of 2009.

DEFINITIONS:

- I. **Breach:** The acquisition, access, use, or disclosure of Protected Health Information in a manner not permitted under HIPAA, which compromises the security or privacy of the protected health information. Breach excludes:
 - I.1. Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or business associate if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under HIPAA.
 - I.2. Any inadvertent disclosure by a person who is authorized to access protection health information at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under HIPAA.
 - I.3. A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

- II. Protected Health Information (PHI): Protected health information is individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium.
- III. Unsecured Protected Health Information (Unsecured PHI): Any PHI which has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of technology or methodology, such as encryption or destruction, as specified by the HSS Secretary.
- IV. Workforce/Staff: Employees, volunteers, trainees, and other persons under the direct control of GCBH BH-ASO, whether or not they are paid by GCBH BH-ASO.

POLICY:

- A. GCBH BH-ASO adheres to HIPAA's requirements that covered entities notify individuals whose unsecured protected health information has been impermissibly accessed, acquired, used, or disclosed, compromising the security or privacy of the protected health information. The notification requirements only apply to breaches of unsecured PHI. In other words, if PHI is encrypted or destroyed in accordance with the HIPAA guidance, there is a "safe harbor" and notification is not required.
- B. GCBH BH-ASO complies fully with the Washington State Health Care Authority (HCA) contract which specifies that GCBH BH-ASO will notify the HCA in event of a breach.

PROCEDURE:

- 1. Discovery of Breach: A breach is treated as discovered as of the first day on which such breach is known to GCBH BH-ASO or, by exercising reasonable diligence, would have been known to GCBH BH-ASO or any person, other than the person committing the breach, who is a workforce member or agent of GCBH BH-ASO.
 - 1.1. Workforce members who believe that an individual's information has been used or disclosed in any way that compromises the security or privacy of that information will immediately notify their manager and GCBH BH-ASO's HIPAA officer.
 - 1.2. Following the discovery of a potential breach, GCBH BH-ASO's HIPAA officer will begin an investigation, conduct a risk assessment, and, based on the results of the risk assessment, begin the process of notifying each individual whose PHI has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed as a result of the breach. GCBH BH-ASO shall also begin the process of determining what notifications are required or should be made, if any, to the Secretary of the U.S. Department of Health and Human Services (HHS), media outlets, and Washington State Health Care Authority (HCA).
- 2. Breach Investigation: GCBH BH-ASO's HIPAA Officer is responsible for the management of the breach investigation, completion of the risk assessment, and

coordinating with other GCBH BH-ASO and Provider staff as appropriate (e.g., administration, security incident response team, human resources, risk management, public relations, legal counsel.) All GCBH BH-ASO and Provider staff are expected to assist in this investigation as requested. As the principle investigator, GCBH BH-ASO's HIPAA Officer will also be the key facilitator for all breach notification processes.

3. Risk Assessment: For breach response and notification purposes, a breach is presumed to have occurred unless GCBH BH-ASO can demonstrate that there is a low probability that the PHI has been compromised based on, at minimum, the following risk factors:
 - 3.1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification. Consider:
 - 3.1.1. Social security or ProviderOne numbers
 - 3.1.2. Identifying clinical details, diagnosis, treatment, medications
 - 3.1.3. Demographic information
 - 3.2. The unauthorized person who used the PHI or to whom the disclosure was made.
 - 3.2.1. Does the unauthorized person have obligations to protect the PHI's privacy and security?
 - 3.2.2. Does the unauthorized person have the ability to re-identify the PHI?
 - 3.3. Whether the PHI was actually acquired or viewed.
 - 3.3.1. Does analysis of a stolen and recovered device show that PHI stored on the device was never accessed?
 - 3.4. The extent to which the risk to the PHI has been mitigated.
 - 3.4.1. Can GCBH BH-ASO obtain the unauthorized person's satisfactory assurances that the PHI will not be further used or disclosed or will be destroyed?

The evaluation should consider these factors, or more, in combination to determine the overall probability that PHI has been compromised. The risk assessment should be thorough and completed in good faith, and the conclusions should be reasonable.

Based on the outcome of the risk assessment, GCBH BH-ASO's HIPAA Officer will determine the need to move forward with breach notification. The HIPAA Officer must document the risk assessment and the outcome of the risk assessment process.

4. Notification – Individuals Affected: If it is determined that breach notification must be sent to affected individuals, a standard breach notification letter (as modified for the specific breach) will be sent out to all affected individuals. GCBH BH-ASO also has the discretion to provide notification following an impermissible use or disclosure of PHI without performing a risk assessment, if deemed appropriate. Notice to affected individuals shall be written in plain language and must contain the following information:
 - 4.1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.

- 4.2. 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, or other types of information were involved).
- 4.3. Any steps the individuals should take to protect themselves from potential harm resulting from the breach.
- 4.4. A brief description of what GCBH BH-ASO is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches.
- 4.5. Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, email address, website, or postal address.
 - 4.5.1. This letter will be sent by first-class mail to the individual at the last known address of the individual or, if they agree 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 GCBH 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.
 - 4.5.2. If there is insufficient or out-of-date contact information that precludes direct written or electronic notification, a substitute form of notice reasonably calculated to reach the individual shall be provided. If 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, by telephone, or by other means. If 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 GCBH BH-ASO's website, or a conspicuous notice in major print or broadcast media in GCBH 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 their PHI may be included in the breach.
 - 4.5.3. Notice to affected individuals shall be made without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach. If GCBH 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. It is the responsibility of GCBH BH-ASO to demonstrate that all notifications were made as required, including evidence demonstrating the necessity of any delay.

5. Notification – Health Care Authority: GCBH BH-ASO must notify Washington State Health Care Authority (HCA) within five (5) business days of discovery. If GCBH BH-ASO does not have full details regarding the potential breach, it will report what is available, and then provide full details within fifteen (15) business days of discovery. If it

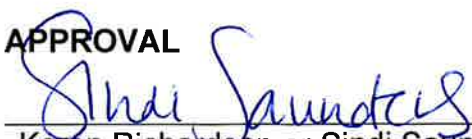
is determined that breach notification must be sent to affected individuals, GCBH BH-ASO must notify HCA in writing within two (2) business days after determining notification must be sent to individuals.

6. Notification – U.S. Department of Health and Human Services: In the event a breach of unsecured PHI affects 500 or more individuals, HHS will be notified at the same time notice is made to the affected individuals, in the manner specified on the HHS website. If fewer than 500 individuals are affected, GCBH BH-ASO's HIPAA officer may report them to HHS at the time of client notification or shall maintain a log of the breaches to be submitted annually to the Secretary of HHS no later than 60 days after the end of each calendar year, in the manner specific on the HHS website. The submission shall include all breaches discovered during the preceding calendar year.
7. Notification – Media: In the event the breach affects more than 500 residents of a state, prominent media outlets serving the state and regional area will be notified without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach. The notice shall be provided in the form of a press release.
8. Delay of Notification Authorized for Law Enforcement Purposes: If a law enforcement official states to GCBH BH-ASO or a business associate that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, after consulting with in-house legal counsel, GCBH BH-ASO shall:
 - 8.1. If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or
 - 8.2. 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.
 - 8.3. This applies to notices made to individuals, the media, HHS, HCA, and by business associates.
9. Maintenance of Breach Information: GCBH BH-ASO's HIPAA officer 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 for each breach:
 - 9.1. A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of individuals affected, if known.
 - 9.2. A description of the types of unsecured protected health information involved in the breach.
 - 9.3. A description of the action taken with regard to notification of patients regarding the breach.
 - 9.4. Steps taken to mitigate the breach and prevent future occurrences.
10. Business Associate / Contracted Provider Responsibilities: Greater Columbia Behavioral Health's business associates, or contracted providers, shall, without unreasonable delay notify GCBH BH-ASO in writing of such breach within five (5) business days of discovery,

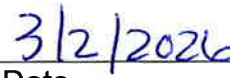
as well as two (2) business days after determining notifications must be sent to individuals. Such notice shall include the identification of each individual whose unsecured PHI has been, or is reasonably believed by the business associate to have been, accessed, acquired, used, or disclosed during the breach. The business associate shall provide GCBH BH-ASO with any other available information that 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 business associate of discovery of a breach, the business associate will be responsible for notifying affected individuals, HHS, and HCA.

11. Workforce Training: As described in GCBH BH-ASO policy PS620, GCBH BH-ASO staff shall receive HIPAA training annually. All staff members are trained to identify and report breaches within GCBH BH-ASO.
12. Complaints: As described in GCBH BH-ASO policy PS615, individuals also have the right to complain about the GCBH BH-ASO's patient privacy policies and procedures, its compliance with such policies and procedures, and breach notification processes.
13. Sanctions: GCBH BH-ASO staff who fail to comply with this policy shall be subject to disciplinary action, up to and including termination.
14. Retaliation / Waiver: GCBH BH-ASO may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for exercising his or her privacy rights. Individuals shall not be required to waive their privacy rights as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.
15. Burden of Proof: If a breach occurs at Greater Columbia Behavioral Health, GCBH BH-ASO has the burden of proof for demonstrating that all notifications were made as required or that the use or disclosure did not constitute a breach.
 - 15.1. If a contracted provider experiences a breach, the contracted provider has the burden of proof for demonstrating that all notifications were made as required or that the use or disclosure did not constitute a breach.

APPROVAL



Karen Richardson or Sindi Saunders, Co-Directors



Date