CATEGORY: Clinical
DOCUMENT NAME: Privacy and Confidentiality of Patient Information
APPROVED: 08/1/2024
LAST REVIEW: 08/1/2024

PURPOSE: To ensure patient PHI is maintained in compliance with HIPAA laws regarding all Communication.

POLICY: It is Baptist Community Health Services (BCHS) policy that all employees shall regard information about BCHS's patients, clients, staff, or associates as confidential. Information regarding any patient's medical records, telephone conversations, family histories and diseases or illnesses shall be restricted to BCHS's professional and paraprofessional personnel appropriate business associates or relatives that directly participate in the care of the patient. Employees who violate this policy are subject to disciplinary action, including termination from employment. Mobile, SMS Messaging, opt-in data will not be shared with third parties.

PROCEDURE:

1. BCHS complies with the Federal and state laws that govern privacy, security, and confidentiality of patient health information (PHI) and what BCHS may possess, control, or access in the normal course of business.

2. BCHS ensures that all types of documents are properly maintained in accordance with applicable laws and guidelines.

3. All patient records and information will be stored in a location that will provide convenient and quick access and which will best protect the records from decay and exposure to natural elements.

4. Patient records that are paper and related information shall be retained by BCHS in accordance with applicable law and guidelines.

   a. After the retention period has expired, record destruction shall comply with all BCHS policies and procedures and applicable federal and state laws, rules and regulations and requirements of third party payors.

5. Patient information and medical records should be secured against loss, destruction, unauthorized access, unauthorized reproduction, corruption, or damage.

6. BCHS employees must maintain the confidentiality of patient information in compliance with all applicable laws and regulations.

7. BCHS employees shall refrain from revealing any personal or confidential information concerning patients unless supported by legitimate patient care purposes, authorized by the patient or otherwise required by law.

8. Any request for a patient’s medical record, financial and/or billing information must be accompanied by a release signed by the patient authorizing release of the records to the person who is requesting the records.

9. BCHS intends to comply with all of the requirements of the HIPAA law and regulations, including regulatory standards.

10. All BCHS employees are required to review, and be familiar with BCHS’s HIPAA and privacy policies.

11. This policy is applicable to, but is not limited to:

- Non-routine disclosures of individually identifiable health information, including, but not limited to disclosures to employers, life insurance companies, mortgage lenders, drug or medical device manufacturers, etc.

- Patient inquiries regarding their ability to access, review, restrict and/or amend their medical records

12. Upon a patient's request, BCHS’s compilation and preparation of a summary of all of the disclosures involving a patient’s medical records and individually identifiable health information.

13. The HIPAA Security Rule generally requires that providers, such as BCHS, safeguard all electronic patient health information (EPHI) by:

a. Ensuring the confidentiality, integrity, and availability of all EPHI the provider creates, receives, maintains, or transmits

b. Protecting against reasonably anticipated threats or hazards to the security or integrity of such information

c. Protecting against any reasonably anticipated use of disclosures of such information that are not permitted under the Security Rule

d. Ensuring compliance with the Security Rule by its workforce

14. BCHS employees will transfer patient information over electronic communication functionalities according to HIPAA regulations, namely

- To the minimum extent necessary to support and carry out quality patient care

- On secure, HIPAA compliant functionalities only

15. For email and document sharing, covered functionalities of Google may be used.

16. BCHS entered into a HIPAA Business Association Amendment agreement with Google for the following HIPAA included functionalities:

a. *As of March 9, 2017, the following functionality within the G Suite Services is Included Functionality under the G Suite HIPAA Business Associate Amendment*

b. Gmail, Google Calendar, Google Drive (including Docs, Sheets, Slides and Forms), Google Hangouts (chat messaging feature only), Hangouts Meet, Google Keep, Cloud Search, Google Sites, and Google Vault (if applicable).

17. Within these functionalities, BCHS employees may transfer PHI only within the BCHS domain.

18. Transferring PHI outside of a BCHS domain requires the exchange be encrypted, and this modality should be used only when deemed necessary for quality patient care.

19. Within the electronic health record, PHI may be transferred via Athena's secure IM functionality or by other notifications within the EHR

20. The Security Rule includes two types of specifications: those that are "required" and those that are "addressable." All required specifications must be implemented. However, HIPAA allows covered entities to look at addressable specifications and determine whether each one is workable and makes sense for their particular setting.

21. When implementing the specification is not reasonable and appropriate, the provider must:

- Document why it would not be reasonable and appropriate; and
- Implement an equivalent alternative measure, if reasonable and appropriate.

22. HIPAA regulations also require covered entities, such as BCHS, to notify each individual whose unsecured PHI has been, or is reasonably believed to have been accessed, acquired, used, or disclosed following a breach of that unsecured PHI. A "breach" is defined as the unauthorized acquisition, access, use or disclosure of PHI which compromises the security or privacy of such information.

23. "Unsecured" PHI is defined as PHI that is not secured through the use of a technology or methodology required in Health and Human Services (HHS) guidance to render PHI "unusable, unreadable, or indecipherable to unauthorized individuals." HHS issued guidance on April 17, 2009, identifying two methods for securing PHI: encryption and destruction. Covered entities that take the steps specified in the HHS guidance to secure PHI will not be required to provide the notifications required by the breach notification regulations in the event of a breach.