BULLHOOK
Community Health Center

521 4th Street Havre Montana 59501 • Phone: 406-395-4305 • Fax: 406-395-5643 • www.bullhook.com

POLICY

HIPAA SECURITY PLAN **2005**
HEALTH INFORMATION PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

Finally released in February of 2003, the HIPAA Security Rules are intended to accomplish four major functions:

1. Ensure the confidentiality, integrity, and availability of all electronic protected health information (PHI) the covered entity creates, receives, maintains or transmits;
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
3. Protect against any reasonably anticipated uses or disclosures of such information not otherwise allowed by law;
4. Ensure compliance by its workforce

In determining whether a covered entity has complied with the rule, the Department of Justice will take into account the size of the office, its technical infrastructure, the potential cost of security measures, and the potential threat to the security of the information. In other words, a "reasonable approach" is what is required. In order to show Compliance, Bullhook Community Health Center will document that we have addressed the following 18 standards, many of which may already have been addressed while complying with the Privacy Rule.

A. Administrative Safeguards

1. Security Management Process
    a. Risk Analysis and Information System Review: The checklist found in Appendix A will be utilized to perform a risk analysis and information system review initially and on an annual basis. Upon completion, the HIPAA Security Officer will meet with the Management Team to note deficiencies and create appropriate responses.
    b. Risk Management: Based upon the Risk Analysis and Information System Review, the Board of Directors will adopt any additional standards required to ensure the security of its Protected Health Information (PHI).
    c. Sanction Policy: Violations of the Practice's Security Policies will be dealt with in the following manner:
        i. Mistakes made in Good Faith (no knowing violations)
            1. First offense: Verbal warning
            2. Second offense: Written warning plus required education
            3. Third offense: Probation
            4. Fourth offense: Two week suspension without pay and report to Licensing Board and the Center for Medicare and Medicaid Services (CMS)
            5. Fifth offense: Termination and report to Licensing Board and CMS.
        ii. Knowing Violations

1. First offense: Written warning plus required additional education
2. Second offense: Two week suspension without pay and report to Licensing Board and CMS
3. Third offense: Termination and report to licensing board and CMS

2. Assigned Security Responsibility: The Patient Accounts Manager will serve as the HIPAA Security Compliance Officer. The CEO will serve as the HIPAA Privacy Compliance Officer.
3. Workforce Security Standard: The Practice has determined who should have access to PHI and under what circumstances and will ensure that such access is terminated upon termination of an employment.
    a. Access determinations are on a need to know basis
    b. All keys, hardware and software will be returned upon termination of employment.
    c. User access will be deactivated upon termination of employment.
4. Information Access Management Standard: Bullhook Community Health Center has established data security policies and procedures to ensure that only authorized personnel have access to PHI.
5. Security Awareness and Training Standard: Annual training for Bullhook Community Health Center staff will be conducted in conjunction with Privacy Rule training.
6. Security Incident Procedures Standard:
    a. Business Associate contracts require business associates to disclose unauthorized releases.
    b. Upon discovery of any unauthorized disclosure, the HIPAA Security Officer shall be notified immediately.
    c. The HIPAA Security Officer will, if possible, contact the person responsible for the disclosure and ascertain the recipients of any such disclosure.
    d. The HIPAA Security Officer will then take such actions as are necessary to authorize the disclosure or ensure that the PHI involved is not forwarded, is returned to the Practice, and/or is destroyed immediately. All such efforts shall be documented.
    e. In the event that the PHI cannot be secured, the patient involved shall be so notified.
7. Contingency Plan Standard:
    a. All electronic PHI Files shall be backed up no less than monthly. Back up files shall be stored off-site in the possession of a trusted agent of Bullhook Community Health Center.
    b. In the event of the loss of PHI through fire or other catastrophe, the patients will be notified immediately and be given the opportunity to resubmit personal histories and other relevant information. Any patient file so recreated will be marked as a recreation, noting the date the original was lost, the cause of the loss, and the date of the reconstruction.
    c. No less than quarterly, back up files shall be tested for completeness.
8. Evaluation Standard: Bullhook Community Health Center will annually evaluate itself using the format in Appendix A to determine if it is in compliance with the Security Regulations. The results of the audit will be presented to the Board of Directors and any necessary corrective action will be taken no later than 30 days after such a finding is made.
9. Business Associates Standard: As in the Privacy Rule, Business Associates guarantee that they will provide security for PHI.

B. Physical Safeguards

10. Facility Access Controls Standards:
    a. Only authorized staff shall have keys to the facility.
    b. Only authorized staff members shall have access to PHI passwords.
    c. Only authorized staff shall have access to PHI and such access shall be restricted to a need to know basis. Should a staff member be found to have violated this policy, disciplinary action will be taken in accordance with this manual.
    d. Any unauthorized release of PHI shall be deemed a cause for discipline as otherwise set forth in the manual.
11. Workstation Security Standard: Bullhook Community Health Center policies set forth appropriate use of internet and email functions. Particular emphasis items are:
    a. Internet access is for business use. Employees may not download data from the internet without the clearance of the Chief Information Officer.
    b. At the close of each work day, workstations shall be secured.
12. Workstation Security Standard:
    a. Computers shall have screen savers that are enacted upon no more than five minutes of inactivity.
    b. Workstation computers shall be located in such a way so that the screens may not be regularly visible by patients or guests.
13. Device and Media Controls Standard:
    a. All hardware drives shall be erased before being removed from the building for disposal.
    b. Off-site backup data will be handled only by trusted agents of BCHC.
    c. All paper charts shall be shredded upon being discarded.

C. Technical Safeguards

14. Access Control Standard:
    a. All electronic PHI shall be accessible only through a password.
15. Audit Controls Standard: The actual systems that house PHI will be audited/inspected at least annually to ensure the integrity of electronic PHI.
16. Integrity Standard:
    a. Any change to PHI may only be performed upon the request of a treating health care professional
    b. Any change to PHI must be recorded (either electronically or manually).
17. Person or Entity Authentication Standard:
    a. Each staff member allowed access to PHI will be assigned a password, which must be used before electronic PHI may be retrieved.
    b. This password will be changed upon termination of employment.
18. Transmission Security Standard:
    a. In order to minimize the chance of unauthorized access to electronic transmissions of PHI business associate letter will include the provision that no PHI will be transmitted email to or from this facility.
    b. All payment transmission will be appropriately encrypted.
    c. All computers will maintain an updated version of the VIPRE antivirus program.

Date: 9-12-2017

CHIEF EXECUTIVE OFFICER

Date: 9-11-17

CHAIR, BOARD OF DIRECTORS

Date first adopted	04/13/2011
Date Revised/QI Board approval	04/13/2011
New date adopted/Board of Directors approval	04/27/2011, 09/11/2017

APPENDIX A
SECURITY RULE ASSESSMENT CHECKLIST

1. Individual in Charge of HIPAA Compliance:
   Name _____

2. How Are Paper Medical Records Kept? (Note All Which Apply.)
   a. Open Shelves Accessible to All: _____
   b. Open Shelves Accessible to Staff Only: _____
   c. Open Shelves in Locked Room: _____
   d. Filing Cabinets with No Locks: _____
   e. Shelves/Filing Cabinets with Locks: _____
   f. Off-Site Storage, No Security: _____
   g. Off-Site Secure Storage: _____

3. How Is Paper Claims and Billing Information Kept? (Note All Which Apply.)
   a. Open Shelves Accessible to All: _____
   b. Open Shelves Accessible to Staff Only: _____
   c. Open Shelves in Locked Room: _____
   d. Filing Cabinets with No Locks: _____
   e. Shelves/Filing Cabinets with Locks: _____
   f. Off-Site Storage, No Security: _____
   g. Off-Site Secure Storage: _____

4. How Is Other Patient Information on Paper Kept? (Note All Which Apply.)
   a. Open Shelves Accessible to All: _____
   b. Open Shelves Accessible to Staff Only: _____
   c. Open Shelves in Locked Room: _____
   d. Filing Cabinets with No Locks: _____
   e. Shelves/Filing Cabinets with Locks: _____
   f. Off-Site Storage, No Security _____
   g. Off-Site Secure Storage: _____

5. How Is Electronic Patient Information Kept? (Note All Which Apply.)
   a. Personal Computer(s), No Network Connections: _____
   b. Personal Computers, Internal Network: _____
   c. Personal Computers, Internet Connection: _____
   d. Off-Site Personal Computers/Laptops Permitted Remote Access (Dial-In, Internet, etc.): _____
   e. Floppy Disks/CDs/Backup Tapes: _____
   f. Handheld Devices (Palm Pilot, Jornada, etc.): _____

6. Attach a List of All Policies Concerning the Following and Note the Last Date Revised/Reviewed:
   a. Access to Files Containing Patient Information
   b. Access to Rooms, Shelves, Filing Cabinets Where Patient Records Are Kept
   c. Access to or Use of Electronic Equipment on Which Patient Information is Stored

7. Attach copy of access determination sheet for employees and note any information which is out of date.

8. Attach a List of All Policies Concerning the Following and Note the Last Date Revised/Reviewed:
   a. Confidentiality of and Access to Patient Information
   b. Use and Disclosure of Patient Information by Staff
   c. Disciplinary Procedures for Breach of Patient Confidentiality

9. Attach a List of All Policies Concerning the Following and Note the Last Date Revised/Reviewed
   a. Patient Review and Copying of Records
   b. Patient Requests to Amend Records
   c. Accounting to Patients for Disclosures of Patient Information
   d. Use or Disclosure of Patient Information for Marketing or General Contact Purposes

10. Copy and Attach:
   a. Standard or Customary Patient Release of Information Forms
   b. Any Notice of Information or Privacy Practices Published or Available to Patients
   c. Any Patient Brochures You May Publish
   d. Any "Patients' Rights" Notices You May Provide

11. List and attach copies of any contracts or agreements with Individuals and Organizations to which you regularly Disclose or receive:
   a. Patient Clinical Information
   b. Patient Billings and/or Claims Information
   c. Any Other Patient Information

HIPAA Security Audit Report

Name of Reviewer: _____

Date of Audit: _____

Standard: Security Management Process
Requirement: Risk Analysis and Information System Review
Deficiencies:
Corrective Action to Be Taken:
Date Corrective Action Completed:

Standard: Assigned Security Responsibility
Requirement:
Deficiencies:
Corrective Action to Be Taken:
Date Corrective Action Completed:

Standard: Workforce Security
Requirement: Policies and Procedures with regard to who has access to PHI
Deficiencies:
Corrective Action to Be Taken:
Date Corrective Action Completed:

Standard: Workforce Security
Requirement: Access to PHI is terminated upon termination of employment
Deficiencies:
Corrective Action to Be Taken:
Date Corrective Action Completed:

Standard: Workforce Security
Requirement: All keys, hardware and software are returned upon termination of employment
Deficiencies:
Corrective Action to Be Taken:
Date Corrective Action Completed:

Standard: Workforce Security
Requirement: Passwords are deleted upon termination of employment
Deficiencies:
Corrective Action to Be Taken:
Date Corrective Action Completed:

Standard: Information Access Management
Requirement: Policies and Procedures as to how PHI is accessed
Deficiencies:
Corrective Action to Be Taken:

Date Corrective Action Completed:

Standard: Information Access Management
Requirement: Unauthorized personnel not allowed access to medical record areas or PHI
Deficiencies:
Corrective Action to Be Taken:
Date Corrective Action Completed:

Standard: Security Awareness and Training
Requirement: Staff training provided
Deficiencies:
Corrective Action to Be Taken:
Date Corrective Action Completed:

Standard: Security Incident Procedures
Requirement: Policies and Procedures provide for identification and response to unauthorized disclosures
Deficiencies:
Corrective Action to Be Taken:
Date Corrective Action Completed:

Standard: Security Incident Procedures
Requirement: Policies and Procedures provide for mitigation of harmful effects
Deficiencies:
Corrective Action to Be Taken:
Date Corrective Action Completed:

Standard: Security Incident Procedures
Requirement: Unauthorized disclosures and their outcomes are documented.
Deficiencies:
Corrective Action to Be Taken:
Date Corrective Action Completed:

Standard: Contingency Plan
Requirement: Policies are in place to deal with sudden loss of PHI
Deficiencies:
Corrective Action to Be Taken:
Date Corrective Action Completed:

Standard: Contingency Plan
Requirement: Policies include provisions for data backup
Deficiencies:
Corrective Action to Be Taken:
Date Corrective Action Completed:

Standard: Contingency Plan
Requirement: Policies have an emergency plan for PHI loss

Deficiencies:
Corrective Action to Be Taken:
Date Corrective Action Completed:

Standard: Contingency Plan
Requirement: Policies have a provision for testing contingency plan and revision procedures
Deficiencies:
Corrective Action to Be Taken:
Date Corrective Action Completed:

Standard: Evaluation
Requirement: Compliance with the Security Rule is and this Manual is periodically evaluated
Deficiencies:
Corrective Action to Be Taken:
Date Corrective Action Completed:

Standard: Business Associates
Requirement: Business associates must guarantee in writing the security of PHI
Deficiencies:
Corrective Action to Be Taken:
Date Corrective Action Completed:

Standard: Facility Access Controls
Requirement: Polices and Procedures must control access to PHI and facility itself
Deficiencies:
Corrective Action to Be Taken:
Date Corrective Action Completed:

Standard: Workstation Use
Requirement: Policies and Procedures must detail authorized and unauthorized uses of workstation
Deficiencies:
Corrective Action to Be Taken:
Date Corrective Action Completed:

Standard: Workstation Security
Requirement: Policies and Procedures must ensure that only authorized
employees have access to workstations
Deficiencies:
Corrective Action to Be Taken:
Date Corrective Action Completed:

Standard: Device and Media Controls
Requirement: All hardware, software and media storage are erased before being disposed.
Deficiencies:
Corrective Action to Be Taken:
Date Corrective Action Completed:

Standard: Access Control
Requirement: Passwords are used to access PHI
Deficiencies:
Corrective Action to Be Taken:
Date Corrective Action Completed:

Standard: Access Control
Requirement: Emergency and off-hour access is limited but available when absolutely necessary, with appropriate safeguards
Deficiencies:
Corrective Action to Be Taken:
Date Corrective Action Completed:

Standard: Audit Controls
Requirement: Actual systems are inspected periodically to ensure integrity of PHI
Deficiencies:
Corrective Action to Be Taken:
Date Corrective Action Completed:

Standard: Integrity
Requirement: Policies and Procedures ensure that electronic PHI cannot be inappropriately altered or destroyed.
Deficiencies:
Corrective Action to Be Taken:
Date Corrective Action Completed:

Standard: Person or Entity Authentication
Requirement: Identity of those who access electronic PHI must be authenticated
Deficiencies:
Corrective Action to Be Taken:
Date Corrective Action Completed:

Standard: Transmission Security
Requirement: Transmissions are periodically inspected to ensure only authorized receipts
Deficiencies:
Corrective Action to Be Taken:
Date Corrective Action Completed: