BULLHOOK
Community Health Center

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

Systems and Communications Protections Policy 5023

Purpose:

The purpose of this policy is to define administrative, physical and technical controls that are in place to control who is allowed to have physical access to Bullhook Community Health Center facilities or rooms that house BCHC's information and communication systems. These include protections at non-BCHC data centers and network rooms that house BCHC equipment.

Scope:

This systems and communications protections policy applies to all facilities or rooms belonging to or being leased by BCHC, and within which BCHC information systems or communications system components are located. Specifically, the scope of this policy includes:

- Data centers or other facilities or rooms housing BCHC's information systems and communications technology infrastructure.
- Data rooms or other facilities within shared purpose facilities for which one of the purposes is the housing of BCHC systems infrastructure.
- Switch and wiring closets or other facilities for which the primary purpose is not the housing of IT infrastructure

Policy:

Access to rooms containing BCHC information systems and communication systems are limited to authorized BCHC workforce members, only. Access authorization will be through the use of authorization credentials (Proximity badges or keys) that have been issued by BCHC Management Team to the workforce member.

Access to Facilities Housing Systems and Communications

Access to BCHC facilities will be controlled at defined access points through the use of locked doors and workforce member issued proximity cards with specific security access. All authorized personnel are required to authenticate themselves at these access points before physical access to facilities, information systems or information system display mechanisms is allowed. The delivery and removal of information systems will also be controlled at these access points. No equipment will be allowed to enter or leave the facility without prior authorization and all deliveries and removals will be logged.

Approved Access List

An approved list of authorized personnel will be established and maintained for the off-site data centers, and switch rooms such that newly authorized personnel are immediately appended to the list and those personnel who have lost authorization are immediately removed from the list. This list shall be reviewed and, where necessary, updated. This review will take place on a quarterly basis, by Management Team.

In the event that visitors need access to the off-site data centers or network switch facilities or rooms that house BCHC information systems and communication systems, or they need access to the information systems themselves, those visitors must have prior authorization by BCHC Management Team, they must be positively

identified, and they must have their authorization verified by a member of the Executive Team before physical access to those off-site facilities is granted. Once access has been granted to those off-site facilities, visitors must be escorted by a BCHC workforce member, and their activities must be monitored at all times with the exception of a maintenance vendor performing maintenance on the servers. Those vendors will have a signed Business Associate Agreement on file at BCHC.

Data Center Access and Sign-In

Access to BCHC servers and/or the health center data center is strictly controlled. Individuals gaining access to the data center will be required to sign in on a sign-in sheet. Sign-in sheets will be maintained for at least six months, should review of those sheets be needed.

References:

1. HIPAA Security Rule

Chief Executive Officer Date 8-21-15

Chair, Board of Directors Date 8-10-15

Date Approved	6/24/2015 QI Committee	
Date revised		
Date first adopted	7/13/2015	