PIONEER MEDICAL CENTER
P.O. Box 1228, Big Timber, MT
406-932-4603 Fax: 406-932-5468

POLICY and PROCEDURE		
Title	Information Security Management: Physical Safeguards	
Manuals	ADC – IM	HOS - IM
	ALF – IM	PH – IM
	CAH – IM	RHC - IM
Approved By	Date: 09/11/2015 By: Erik Wood Title CEO	

Highlights

Definitions

Server Security

Desktop System Security Requirements

Policy Statement

Pioneer Medical Center (PMC) is committed to conducting business in compliance with all applicable laws, regulations and PMC policies. PMC has adopted this policy to set forth the physical safeguards that will apply to ePHI and the media that stores ePHI.
The scope of this policy is to describe the physical safeguards applicable for each server, desktop computer system and wireless computer system used to access, transmit, receive and store ePHI to ensure that appropriate security is maintained and that access is restricted to authorized users. The intent of this policy is also to avoid unintentional and minimize incidental disclosure of protected health information.

Definitions

Electronic Protected Health Information (ePHI): Protected health information transmitted or maintained by electronic media.
Protected Health Information (PHI): Individually identifiable health information that is created or received by a Covered Entity, including PMC, (and some other health related entities) that relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.
Workforce Member: Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for PMC is under the direct control of PMC, whether or not they are paid by PMC.
Storage Device or Removable Media: hard drives, storage systems, removable disks, floppy drives, CD ROMs, PCMCIA cards, memory sticks, and all other forms of removable media and storage devices.

Procedure

A. Server Security Requirements

1. Information Services must ensure that all servers used to access, transmit, receive or store ePHI are appropriately secured in accordance with this Policy. Servers must be located in a physically secure environment.
2. The system administrator or root account must be password protected.
3. A user identification and password authentication mechanism must be implemented to control user access to the system.
4. A security patch and update procedure must be established and implemented to ensure that all relevant security patches and updates are promptly applied based on the severity of the vulnerability corrected.
5. Servers must be located on a secure network with firewall protection. If for any reason the server must be maintained on a network that is not secure, an intrusion detection system must be implemented on the server to detect changes in operating and file system integrity.
6. All unused or unnecessary services shall be disabled.

B. Desktop System Security Requirements

1. Information Services in conjunction with each department must ensure that each desktop system used to access, transmit, receive or store ePHI is appropriately secured in accordance with this Policy.
2. The system administrator or root account must be password protected.
3. A user identification and password authentication mechanism must be implemented to control user access to the system.

4. A security patch and update procedure must be established and implemented to ensure that all relevant security patches and updates are promptly applied based on the severity of the vulnerability corrected.
5. A virus detection system must be implemented including a procedure to ensure that the virus detection software is maintained and up to date.
6. All unused or unnecessary services must be disabled.
7. Desktop systems that are located in open, common, or otherwise insecure areas must also implement the following measures:
    a) An inactivity timer or automatic logoff mechanism must be implemented.
    b) The workstation screen or display must be situated in a manner that prohibits unauthorized viewing. The use of a screen guard or privacy screen is recommended.

Mobile Systems Security Policy

C. Mobile Systems Security Policy

1. Information Services in conjunction with each department must ensure that all mobile systems used by Workforce Members to access, transmit, receive or store ePHI are appropriately secured in accordance with this Policy.
2. The system administrator or root account must be password protected.
3. A user identification and password authentication mechanism must be implemented to control user access to the system. All mobile devices and laptops must use a boot password to ensure that the system is only accessible to authorized users.
4. A security patch and update procedure must be established and implemented to ensure that all relevant security patches and updates are promptly applied based on the severity of the vulnerability corrected.
5. A virus detection system must be implemented including a procedure to ensure that the virus detection software is maintained and up-to-date.
6. All unused or unnecessary services must be disabled.
7. Mobile stations that are located or used in open, common, or otherwise insecure areas must also implement the following measures:
    a) A theft deterrent device such as a laptop locking cable must be utilized when the device is unattended.
    b) An inactivity timer or automatic logoff mechanism must be implemented.
    c) Reasonable safeguards must be in place prohibit unauthorized entities from viewing confidential information such as logins, passwords, or PHI.
8. Personal Digital Assistants (PDAs) and other handheld mobile devices must not be used for long-term storage of ePHI. ePHI stored on hand held mobile devices must be purged as soon as it is no longer needed on that device.

Work Station Use

D. Work Station Use

1. To ensure that workstations and other computer systems that may be used to send, receive, store or access ePHI are only used in a secure and legitimate manner, workforce members who, and workstations and other computer systems that are used to, send, receive, store and access ePHI must comply with all HIPAA Safeguards.
2. Use of PMC's information systems and workstations by Workforce members is subject to audit/review and is not private in nature. To appropriately manage its information system assets and enforce appropriate security measures, PMC may log, review, or monitor any data (ePHI and non-ePHI) stored or transmitted on its information system assets.
3. PMC may remove or deactivate any workforce member's user privileges, including but not limited to, user access accounts and access to secured areas, when necessary to preserve the integrity, confidentiality and availability of its facilities, user services, and data.

Device & Media Controls

E. Device & Media Controls

1. Destruction of Storage Devices or Removable Media
    a) Prior to destroying or disposing of any storage device or removable media, (after being held in a secure area for 30 days) care must be taken to ensure that the device or media does not contain ePHI.
    b) If the device or media contains the only copy of ePHI that is required or needed, a retrievable copy of the ePHI must be made prior to disposal.
    c) If the device or media contains ePHI that is not required or needed, and is not a unique

copy, a data destruction tool must be used to destroy the data on the device or media prior to disposal. A typical reformat is not sufficient, as it does not overwrite the data.

2. Reuse of Storage Devices or Removable Media
    a) Prior to making storage devices and removable media available for reuse, (after being held in a secure area for 30 days) care must be taken to ensure that the device or media does not contain ePHI.
    b) If the device or media contains the only copy of ePHI that is required or needed, a retrievable copy of the ePHI must be made prior to reuse.
    c) If the device or media contains ePHI that is not required or needed, and is not a unique copy, a data destruction tool must be used to destroy the data on the device or media prior to reuse. A typical reformat is not sufficient, as it does not overwrite the data.
    d) If using removable media for the purpose of system backups and disaster recovery and the aforementioned removable media is stored and transported in a secured environment, the use of a data destruction tool between uses is not necessary.
3. Movement of Equipment Housing ePHI
    a) Information Services in conjunction with each PMC department shall develop a procedure to determine when an exact retrievable copy of ePHI is required prior to the movement of equipment storing such ePHI.
    b) When using storage devices and removable media to transport ePHI, each PMC department must develop a procedure to track and maintain records of the movement of such devices and the media and the parties responsible for the device and media during its movement.

Compliance

F. Compliance

1. Each workstation that is used to access, transmit, receive or store ePHI must comply with each of the aforementioned measures. If any of the aforementioned measures are not supported by the workstation operating system or system architecture, one of the following steps must be taken:
2. The server, desktop computer system, or wireless computer system must be upgraded to support all of the security measures.
3. An alternative security measure must be implemented and documented.
4. The workstation must not be used to send, receive or store ePHI.

REFERENCES
HIPAA 164.31 Physical Safeguards.

Regulatory Reference Sources	
OBRA Regulatory Reference Numbers	
Survey Tag Numbers (optional)	