



PIONEER MEDICAL CENTER

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

POLICY and PROCEDURE		
Title	Automatic Logoff	
Manuals	ADC - IM	LTC - IM
	ALF - IM	RHC - IM
	CAH - IM	PH - IM
	HOS - IM	
Approved By	Date: <u>05/07/2013</u> By: <u>Erik Wood</u> Title <u>CEO</u>	

Highlights

Policy Statement

Pioneer Medical Center is committed to conducting business in compliance with all applicable laws, regulations and PMC policies. To ensure that access to all servers and workstations that access, transmit, receive, or store ePHI is appropriately controlled; the following procedures must be followed.

Servers, workstations, or other computer systems containing ePHI repositories that have been classified as high risk (See PMC Security Management Policy) must employ inactivity timers or automatic logoff mechanisms. The aforementioned systems must terminate a user session after a maximum of, but not limited to, 120 minutes of inactivity except for physician or other key devices, which will terminate after a maximum of 240 minutes.

Definitions

Definitions

- Electronic Protected Health Information (ePHI) – Is 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.

Automatic Logoff

Procedure

1. Servers, workstations, or other computer systems located in open, common, or otherwise insecure areas that access, transmit, receive, or store ePHI must employ inactivity timers or automatic logoff mechanisms. (I.E. Password protected screen saver that blacks out screen activity.) The aforementioned systems must terminate a user session after a maximum of, but not limited to, 15 minutes of inactivity.
2. Applications and databases using ePHI, such Electronic Medical Records (EMR) must employ inactivity timers or automatic session logoff mechanisms. The aforementioned application sessions must automatically terminate after a maximum of, but not limited to, 120 minutes of inactivity except for physician or other key devices, which will terminate after a maximum of 240 minutes.
3. Servers, workstations, or other computer systems that access, transmit, receive, or store ePHI, and are located in locked or secure environments need not implement inactivity timers or automatic logoff mechanisms.
4. If a system requires the use of an inactivity timer or automatic logoff mechanism as detailed in the aforementioned procedures, but does not support an inactivity timer or automatic logoff mechanism, one of the following procedures must be implemented:
 - a. The system must be upgraded or moved to support the minimum HIPAA Security Automatic Logoff procedures.
 - b. The system must be moved into a secure environment.



PIONEER MEDICAL CENTER

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

- c. All ePHI must be removed and relocated to a system that supports the minimum HIPAA Security Automatic Logoff procedures.
- 5. When leaving a server, workstation, or other computer system unattended, workforce members must lock or activate the systems Automatic Logoff Mechanism (e.g. CNTL, ALT, DELETE and Lock Computer) or logout of all applications and database systems containing ePHI.
- 6. This policy includes, but is not limited to, the aforementioned procedures. This policy and its procedures must be reviewed and evaluated on a periodic basis to ensure that they maintain their technical viability and effectiveness. (See HIPAA Security Evaluation of Compliance Procedures Policy)

REFERENCES

HIPAA 164.312 Technical Safeguards

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