Title: HIPAA PRIVACY COMPLIANCE: MONITORING FOR INAPPROPRIATE ACCESS OF MHS SYSTEMS THAT CONTAIN PHI

Scope:

All users of MultiCare Health System (MHS) electronic systems that contain protected health information (PHI).

Procedure Statement:

To establish the process at MHS for monitoring of inappropriate access of PHI.

It is MHS policy that patient information is only to be accessed when authorized, for a business purpose, and with a need to know.

Appropriate action will be taken to protect all PHI contained in MHS systems.

Procedure:

I. Detection of Inappropriate Access of MHS Systems that Contain PHI:

A. Each MHS system that contains PHI (should) contain a logging mechanism to record all user access within the system.

B. MHS uses a variety of tools and processes to detect potential inappropriate access of PHI.

C. All potential inappropriate access that is identified is questioned.

D. The user and date of the access are added to a master list for tracking.

II. Verification of Inappropriate Access:

A. It is the responsibility of the supervisor / ASP Contract Holder to determine if the access is appropriate or inappropriate.

B. The supervisor / ASP Contract Holder will report the results of their investigation to the MHS Privacy Office.

C. The Privacy Office will be notified through the use of the following voting buttons contained in the original e-mail request sent to the supervisor / ASP Contract Holder:

1. No Inappropriate Access
2. Inappropriate Access Confirmed

III. Action Taken In Response to Inappropriate Access:

A. MHS staff:

1. Human Resources is notified.
2. The user is sanctioned according to MHS policy and procedure.

B. Non-MHS staff:

1. Users are bound to the guidelines set forth in the MHS User Agreement and Confidentiality Statement.

IV. Tracking/Trending and Publishing of Results:

A. All potential inappropriate access is recorded and totaled.

B. Percentages of confirmed inappropriate access are tracked.

C. All statistics are reported quarterly as a record security issue to the Corporate Compliance Steering Committee.

D. All inappropriate use will be tracked and reported as required by law and MHS policy.

V. Definitions:

A. User – An individual who accesses a system for a particular action or function through the use of a unique identified user account.

B. ASP Contract Holder – Any non-MHS individual or entity that accesses MHS systems through the use of a unique identified user account

C. MHS Privacy Office – Responsible for ensuring compliance with all applicable state and federal patient privacy regulations at MultiCare Health System.

Point of Contact: MHS Privacy Office (253) 403-7475	
Affected Departments: Human Resources, IS Security, MHS Privacy Office	
Original Date:	3/10