Title: TECHNOLOGY: ACTIONS FOR POLICY VIOLATIONS BY NON-MHS ENTITIES

Scope:

This policy is applicable to all non-MultiCare Health System (MHS) entities that have access to, connect to, receive electronic data from, provide electronic data to, or provide electronic data services to MHS.

Policy Statement:

This policy describes the actions that will be taken upon detection of a policy violation by non-MHS entities. Policy violations include information security and privacy violations addressed by HIPAA, HITECH, PCI-DSS, SOX, Federal and State laws, contractual, and any other published MHS policies.

For the purpose of this procedure, access is defined as individuals with assigned username and password access to MHS systems, organizations or businesses that connect to, receive electronic data from, provide electronic data to, or provide electronic data services to MHS.

Actions will be taken based on a decision from a committee formed to include the relevant MHS departments. The committee may include, but is not limited to: Information Services, Compliance, Human Resources, and Legal.

Special Instructions:

1. Any suspicious activity or suspected violations of policies or regulations should be reported using one of the following methods:
   a. MHS manager, director, or administrator
   b. MHS Corporate Compliance – MHS Corporate Compliance is responsible for ensuring adherence to laws, rules and regulations, including Medicare and other Federal payor programs. Internal Audit is responsible for auditing and improving financial and operations processes:
      i. 253-459-8300
      ii. 253-697-2100
      iii. 866-864-6121
      iv. compliance@multicare.org
      v. compliance@goodsamhealth.org
   c. MHS HIPAA Hotline 253-403-7475 or hipaaprivacy@multicare.org
   d. MHS Legal Services - Provides consultations regarding unusual occurrences and case management of litigation.

i. 253-403-1107

e. MHS Information Security Services

i. 253-459-7482

2. For the purpose of monitoring and reporting, personal use of MHS Information Systems or components connected to MHS Information Systems will be monitored and reported as MHS business use. Use of MHS electronic resources may be monitored, recorded, and reported by the company and may be disclosed to any party (internal or external) as deemed appropriate.

3. Violations of policies by MHS entities will be handled in accordance with MHS's HR: Progressive Guidance policy. Violations of policies by non-MHS entities will be handled in accordance with the following policy.

Table of Contents:

Procedure:

I. Violations That Will Cause Immediate Removal of Access:

A. Policy violations that involve a suspected reportable breach of information will be cause for immediate removal of access.

B. Two or more individuals from the same organization that are suspected of causing a reportable breach may be cause for immediate removal of access for the entire organization.

C. Any organization or business without individual user access that is suspected of causing a reportable breach may be cause for immediate removal of access for the entire organization or business.

D. MHS will make the final determination on removal of access.

II. Violation That Will Cause Progressive Action by MHS:

A. If at any time in the progressive action process a breach is suspected, action will be taken in accordance with the previous section.

B. Discovery of suspected policy violations without justification from the non-MHS entity:

1. The first detection will result in a notification to the non-MHS entity's appropriate contact.

a. A response or justification from the non-MHS entity that the violation was investigated and corrected must be sent in writing to the MHS reporting authority within one (1) month of the

notification.

2. A second detection of the same type of violation as noted on the notification or a detection of another type of violation without an appropriate response to a previous violation will result in a warning that further violations without an appropriate response or justification will be cause for removal of access.
3. A third detection of the same type of violation as noted on any previous notification or detection of another type of violation without any appropriate response to the previous notifications will result in removal of access.
4. Any subsequent detections of the same type of violation as noted on any previous notification or detection of another type of violation without any appropriate response to the previous notifications may result in removal of access for the entire organization or business.

III. Re-Instatement of Access:

A. Access may be reinstated following the receipt of an appropriate response or justification and review by the committee that originally authorized the removal of access.

IV. Definitions:

Access - individuals with assigned username and password access to MHS systems, organizations or businesses that connect to, receive electronic data from, provide electronic data to, or provide electronic data services to MHS.

Systems - includes, but not limited to, computer equipment, telephones, software, operating systems, storage media, networks, electronic mail (email/e-mail), world wide web browsing, file transfers, telecommunications, messaging, and mobile devices.

Point of Contact: Information Security Services

Approval By:	***Date of Approval:***
MMC Approvals:	
MHS Policy and Procedure Committee	***7/10***
PILOT	***7/10***
MGSH Approvals:	
Clinical Operations	***8/10***
Policy Council	***8/10***
QIC	***8/10***
MEC	***8/10***
PAC	***8/10***
Original Date:	*7/10*
Revision Dates:	*none*
Reviewed with no Changes Dates:	*none*

Distribution: MHS Intranet