Title: TECHNOLOGY: NON-MHS ACCESS, CONNECTIONS, AND ELECTRONIC DATA SERVICES

Scope:

This policy is applicable to all non-MHS entities that are requesting access to, connecting to, receive electronic data from, provide electronic data to, or are providing electronic data services for MHS.

Policy Statement:

The purpose of this policy is to define the requirements for:

- Access or connection to MHS systems by entities not employed by MHS.
- Receiving electronic data from, providing electronic data to, or receiving electronic data services from Non-MHS entities.

Special Instructions:

1. Any suspicious activity or suspected violations of policies or regulations should be reported using one of the following methods:
   a. MultiCare manager, director, or administrator
   b. Human Resources: 253-403-1260
   c. Corporate Compliance - 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:
      1.) 253-459-8300
      2.) 253-697-2100
      3.) 866-864-6121
      4.) compliance@multicare.org
      5.) compliance@goodsamhealth.org
   d. HIPAA Hotline 253-403-7475 or hipaaprivacy@multicare.org
   e. Legal Services - Provides legal advice and training; consultations regarding unusual occurrences and case management of litigation; answers insurance questions.
      1.) 253-403-1107
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 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 this policy by MHS employees will be handled in accordance with MHS's Progressive Guidance policy. Violations of this policy by non-MHS entities may result in the cancelation of current or future contracts.

Table of Contents:

Procedure:

I. Contract Requirements:

A. Prior to conducting business with non-MHS entities, a contract must be reviewed by Information Services and Legal to ensure adequate protections are provided for MHS and MHS data.

B. The contract must be on file in the contract management system (currently TractManager) before any access or connectivity approvals can occur.

C. Contracts that permit access to personal health information (PHI), as defined by HIPAA, must include a Business Associates Agreement (BAA). BAA agreements are available through the HIPAA Privacy Specialist or Risk and Legal office.

D. Contractual Clauses:

1. For contracts where the entity accesses MHS information there must be a contractual clause requiring the entity to have a policy or policies that address:

   a. Access controls – including, but not limited to, unique user ids, password requirements, and logging.

   b. Data confidentiality.

   c. Metrics and reporting.

   d. Audits and investigations.

2. For contracts where the entity stores or handles MHS information there must be a contractual clause requiring the entity to have a policy of policies that address:

   a. The requirements listed above for accessing MHS information.

   b. Data protection – including, but not limited to, encryption, firewalls, routers, and intrusion detection.

3. In addition to the contractual clauses requiring policies, there must be contractual clauses allowing MHS, or its designated representative, to conduct on site or remote reviews or audits of the steps taken to protect MHS information.

II. Individual User Confidentiality/Privacy Statements:

A. All individual user access to MHS systems containing sensitive information requires an individually signed User Confidentiality/Privacy Statement.

B. Access through an entities system to MHS systems where an individual login is not required (i.e. permanent VPN connections) does not require an individually signed statement since the contractual clauses cover confidentiality and privacy.

III. Audits of Non-MHS Entity Compliance:

A. As noted in the Contracts section of this policy, MHS, or its designated representative may conduct on site or remote reviews or audits of the steps taken to protect MHS information.

B. Reviews or audits may be in the form of reviewing external auditor reports, reviewing external penetration testing results, reviewing the policies and procedures, conducting an audit, conducting interviews, walkthroughs, questionnaires or tours.

C. The findings, evidence, and other information gathered and retained during these reviews or audits will be only that necessary to prove to MHS reviewers or auditors that MHS has taken appropriate steps to ensure that affiliated entities are utilizing best practices for protecting MHS information.

IV. Effective Date:

1. The requirements of this policy are effective as of the date of posting and are not retroactive to any pre-existing contracts or agreements.
2. Upon renewal of existing contracts or agreements, this policy is in full effect regardless of the existence of a pre-existing relationship with the non-MHS entity.

V. Definitions:

Audit – An examination of the controls and processes for an information system.

Control – Specific actions or activities associated with IT systems to ensure that business objectives are met. Controls can be automated or manual, reports, documents, or processes that are periodically validated by management to be accurate and periodically tested to ensure they meet the requirements.

Evidence – Anything that is used in the determination of the facts of a suspected activity or event.

Findings – A determination or interpretation of what the evidence means. Findings are normally classified as positive (there is sufficient evidence to prove a suspected action or event), negative (there is not sufficient evidence to prove a suspected action or event), or inconclusive (there may or may not be enough evidence to prove a suspected action

	or event). **Investigation** – An examination of the technical evidence to determine the factuality of a suspected activity or event. **Logging** – the recording of events in an information system. These events can be changes to data, log in/out, viewing data, etc… **Sensitive Information** – Information about patients, employees, financials, or other sensitive business information. **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.
	References: Public Law 104-191 – Health Insurance Portability and Accountability Act of 1996 (HIPAA) RCW 70.02 – Uniform Health Information Act RCW 70.129.050 – Privacy and Confidentiality of Personal and Medical Records Title 45 CFR Part 164 (Security and Privacy) Subpart C (Security Standards for the Protection of Electronic Protected Health Information)
	Point of Contact: Information Security Services – 459-7482

Approval By: MHS Policy and Procedure PILOT	***Date of Approval:***
Original Date: Revision Dates: Reviewed with no Changes Dates:	

Distribution: MHS Intranet

This Policy Replaces:

MHS: HIPAA Compliance: Application, Data and Network Systems Access for Non MHS Entities