VISN 1 MEMORANDUM OF UNDERSTANDING
Between
Clinical Engineering Consolidated Program
And
Office of Information and Technology Field Operations, VISN 1
September, 2007

1. Introduction

This Memorandum of Understanding (MOU) represents the agreement between Clinical Engineering Consolidated Program (CECP) and Office of Information and Technology Field Operations (IT) for the provision of services provided by each group concerning computerized equipment. This MOU is intended to provide a framework for establishing a cooperative and productive working relationship between CECP and IT.

2. Statement of Purpose

Due to the proliferation of networked medical devices there needs to be clear guidelines and delineation of services provided by CECP and IT. The Clinical Engineering Consolidated Program will provide biomedical engineering services and system management services for items that are medical systems. IT will provide services for the hospital local area network and systems defined as information technology. Systems and devices will be implemented within national and regional standards and within the framework of accepted security policy and practices. This agreement will also define the terms and conditions under which CECP and IT will interact with each other. It is anticipated that this arrangement will result in more efficient operations and improved utilization of resources.

3. Definitions

Medical systems are defined as equipment used for diagnostic, therapeutic, or clinical monitoring purposes used in the delivery of patient care. These include systems that incorporate computers but are dedicated to the delivery of care or special purpose systems like Digital D-ray, Ultra Sound, CT, MRI modalitities, Picture Archiving and Communications Systems (PACS), Bar Code Medicine Administration systems, drug dispensing machines, blood analyzers, lab equipment, dialysis, digital cameras and editing equipment, ICU monitoring systems, and Cardiac Catheterization Lab digital archiving systems, among others.

IT systems are defined as systems necessary to operate and support routine daily information processing including the medical center information systems, clinical/administrative (VistA) and financial (IFCAP/FMS) and the hospital network. This equipment includes desktop computers, laptop computers, printers, servers, etc., and communications equipment to include routers, switches, hubs, data cabling, etc.

Access is defined in terms of entry to physical spaces as well as protected logical systems such as servers, computers or other devices.

Permission is defined as the approval by supervisor or authorizing authority. Permission is required for access to physical or logical systems.

Change Management is defined as the planning and tracking of changes of system operation and implementation to help assess impact on other systems.

4. Agreement on Tasks, Permissions and Competencies

The essential level of trust will be established by consideration of three elements:

- Need to perform type of task
- Level of permission required to complete task
- Level of education, training and experience commensurate with competency to perform the task.

It is the joint responsibility of the facility ISO, facility CIO and facility Chief of Clinical Engineering (CCE) to assure that all three elements are present prior to granting of access. Lists of persons granted physical access to secure locations and persons granted logical system access to devices will be kept by the facility CIO on the facility SharePoint site. This agreement sets forth four major task areas. Need to perform any one of these task areas, once attested to by the facility ISO, facility CIO and facility CCE is sufficient for granting of access. Annual review of access will be conducted by the facility ISO.

1) System Administration of Application (logical access to systems) or System Clinical User Operations
    i) Maintaining user access lists
    ii) Changing a parameter or configuration
2) System Management of Operating System and Application (logical access to systems)
    i) Changing a parameter or configuration
    ii) Ongoing System Service Support
        (a) Maintenance & Repair
        (b) Backup
        (c) Data security
3) Physical Access to Computer rooms
    i) Installations
    ii) Moves/adds/changes
    iii) Decommissioning of equipment
4) Physical Access to Network closets
    i) Installations
    ii) Moves/adds/changes
    iii) Decommissioning of equipment

5. Documentation of Baseline Configurations & Change Management

Lists of systems and devices will be kept on the Digital Health Architecture SharePoint site and a subcommittee will be charged with assigning principal responsibility or subcontractor role for each device or system (see IRM-CES Excel spreadsheet). Baseline configuration documents for every system will be kept in document libraries on facility SharePoint sites. Documentation of all changes to configuration will be archived in chronological order in the same location. Standard templates for documents will be developed and shared among all facilities in the VISN.

6. Transitional plans

In cases where primary responsibility or ownership of a system is transferred from one service line to the other, an orderly transfer of knowledge from current system owners to future system owners will take place. Transition plans must include all baseline configuration documents and change documents since system inception.

7. Joint Management of Systems & Backups

Where appropriate and mutually agreed upon, joint management of systems will be planned. For example, racking of servers in standardized fashion, UPS & cable management, backup systems and file storage systems will be shared except where prohibited by vendor requirement or prohibited by the protected status of a system. Baseline configuration, changes to configuration and outlines of shared responsibility will be created as minimum criteria for such systems and stored on the facility SharePoint site. If a system server is located in the IRM computer room, IT will perform tape switching on CE systems, if mutually agreed upon. The process for backup of critical data will be developed for medical devices containing patient information. Storage of backup tapes for medical and IT systems will follow accepted VISN backup policies and procedures.

8. Security Clearance and Background Checks

CE employees who need access to the computer room and network closets will meet the same requirements IT staff have for this level of access. This could include background security checks and training.

9. Disputes Under this Agreement

Any dispute in the interpretation of this agreement will be presented to the VISN CIO and VISN Chief of Clinical Engineering only after, and if, local negotiations have reached an impasse. Final arbitration may be obtained from the Network Director.

10. Terms of Agreement and Renewal

The undersigned hereby agree to the terms and conditions of this MOU.

11. Approvals

David Goodman, Ph.D., Acting Deputy VISN 1 CIO for IRM Affairs	Henry Stankiewicz, VISN 1 Clinical Engineer
Donna Cabral, Acting Deputy VISN 1 CIO for VISN Affairs	Jeannette Chirico-Post, M.D. VISN 1 Network Director