Our Lady of Lourdes Health Care Services, Inc. and Affiliates including
Our Lady of Lourdes Medical Center
Lourdes Medical Center of Burlington County

Administrative and General Policy

POLICY NUMBER: AS0028PRI

NURSING CODE:

PAGE NUMBER: 1 of 7

TITLE: **HIPAA Security – Standards for Vendor Supplied or Supported Equipment**

ACCOUNTABILITY:

Chief Information Officer

OBJECTIVES:

RELATION TO MISSION:

Our Lady of Lourdes Health Care Services, Inc. a Catholic Health System – a member of Catholic Health East – dedicated to its Franciscan tradition of serving all, will demonstrate the value of **Integrity** by fostering an ethical and moral environment where the behavior of associates is positively impacted by adherence to the this policy.

RELATION TO OPERATION:

This policy provides guidance to all of Our Lady of Lourdes Health Care Services, Inc.'s and Affiliates' (OLLHCS, Inc.'s), trustees, officers, leadership associates, managers, supervisors, associates, medical staff, house staff, contractors, volunteers, students and others known as workforce members and assists us in carrying out our daily activities within appropriate ethical and legal standards regarding HIPAA federal law.

POLICY:

1.0 **Policy Purpose**

This document will define a set of security standards for vendor supplied modalities, workstations, servers, and applications. It establishes standards for systems that may not

be entirely under the control of OLLHCS in order to maintain the security and integrity of information stored on OLLLHS computer systems.

2.0 **Policy Scope**

These standards apply to all vendor supplied equipment attached to the OLLLHS LAN or WAN whether wired or wireless.

3.0 **Requirements**

3.1 Virus Protection

All network attached resources must be protected by OLLHCS approved antivirus software. OLLHCS standard antivirus should be used whenever possible so that installations can be monitored and managed centrally by OLLHCS Information Services. The following antivirus packages are approved and may be used if it is not possible to use the OLLHCS standard package:

Trend OfficeScan
Trend ServerProtect
Symantec Antivirus
McAfee VirusScan

Virus definitions must be updated regularly, and the antivirus software should be configured to update automatically at the most frequent time interval afforded by the product. If the software will not update automatically, the vendor must document the procedure that will be used to update the antivirus pattern file. An OLLHCS Network Coordinator and the IS Technical Director must approve the update procedure before any system can be attached to the OLLHCS network.

3.2 Operating System and Application Patch Management

All network attached resources must be kept current with security related patches and hotfixes for the operating system and all application software. Any vulnerability for which there is a known exploit that may result in local or remote

code execution or privilege escalation (including unauthorized data access) must be patched within 24 hours of the OS or application vendor's release of a patch. Vulnerabilities for which there is no known exploit must be patched within 96 hours of the vendor's release of a patch.

Vendors must notify OLLHCS through the Help Desk when they become aware of any vulnerability in the OS or application software on a device that they support at OLLHCS. The notification should include the date and time of discovery, a description of the vulnerability, the vendor's description of the severity, and the date and time that a patch is expected to be installed. OLLHCS may, at its sole discretion, disable the network connectivity to any vulnerable device. Any system unavailability due to security vulnerabilities, including any time that OLLHCS determines the device must be removed from the network, will be counted against any SLA or other service agreement between OLLHCS and the vendor.

3.3 Local Device Security

Any device that stores or allows access to ePHI or other confidential information must require unique individual user logins for local or remote device, application, and data access. The logins must meet the requirements defined in HIPAA security policies. For any account that is not unique to a single user and cannot be removed – for example, the Administrator or root accounts on Windows or Unix – there must exist an audit log that contains, at a minimum, the time and date of each successful or unsuccessful logon and logoff and, for any remote accesses, the IP address of the device that initiated the connection. Given the time and date of a logon or logoff and the source IP address (if available), the vendor must be able to identify the specific person who logged on to the system.

3.4 Application Surface Area

All applications must be installed with a minimal surface area – that is, any services that are not necessary for the operation of an application must be disabled, and those services that are enabled must be configured to support the minimal feature set necessary for the application to function. For example, if an

application requires Microsoft SQL Server and is running over TCP/IP, Named Pipes must be disabled. This is intended to reduce the amount of exposure that the server has to potential attack. Surface area will be evaluated during the pre-implementation audit, and vendors must be able to explain the purpose and potential exposure of any software running on any equipment that they manage.

3.5 Remote Access

Vendors may not install any software or device to provide remote access to any device connected to the OLLHCS network. This includes, but is not limited to, VPN clients, modems and remote control software. Vendors requiring remote access may request an OLLHCS VPN or dialup account through their OLLHCS Information Services contact.

3.6 Power

Servers, workstations or other devices that provide a function that is critical for patient care, has significant vulnerability and high replacement costs or significantly impacts patient accounting functions must be connected to an emergency power circuit and an uninterruptible power supply (UPS) with sufficient capacity to power the attached equipment for a minimum of 15 minutes. Equipment that provide a non-critical patient care or patient accounting function must be connected to an emergency power circuit, but does not require a UPS. All other equipment may be connected to a normal power circuit.

3.7 Auditing

OLLHCS Information Services may, at any time, audit the security of any computer system located in an OLLHCS facility or connected to an OLLHCS network. This audit may include local or remote vulnerability scans, OS or application configuration inspection, attempted exploitation of known vulnerabilities, or any other method deemed appropriate by OLLHCS IS. The vendor must provide local administrator, root, or equivalent access to any workstation or server for the purpose of conducting these audits.

TITLE: **HIPAA Security – Standards for Vendor Supplied or Supported Equipment**

Before any device or application is installed, OLLHCS IS will conduct an audit with the vendor to ensure that the installation complies with the standards in this document and with industry best practices. The vendor must obtain IS signoff prior to implementation. After signoff, the vendor must obtain approval for all application or hardware changes through OLLHCS IS change management processes.

3.8 Change Control

All changes to production systems must be scheduled and approved through the OLLHCS IS change management process. Depending on the nature and extent of the change, a new security audit may be required prior to implementation. Vendors should work with their contact in IS to submit a request at least two weeks prior to the scheduled change. Emergency change requests, such as those intended to address problems with system availability, security, or data integrity, may be submitted at any time for immediate consideration.

4.0 Responsibilities

4.1 OLLHCS Leadership

OLLHCS leadership shall ensure their staff adheres to the requirements outlined in this policy and all subordinate procedures related to Security Standards for Vendor Supplied or Supported Equipment. Leadership staff must also follow all requirements in this policy and related procedures and immediately report any known breach of corporate security policy to the Director of Compliance and Privacy Officer.

4.2 OLLHCS Workforce

All members of the OLLHCS workforce shall comply with this policy and all referenced policies to ensure privacy of sensitive OLLHCS information assets. Members of the OLLHCS workforce shall report any known breach of this policy and/or its subordinate procedures to a member of their leadership or to the

Director of Compliance and Privacy Officer, either in person or via the Corporate Compliance Hotline.

4.3 Business Associate

Business associates are expected to abide by federal law(s) and the terms agreed upon in the Business Associate Agreement. All business associates of OLLHCS shall comply with this policy and all referenced policies to ensure the security of sensitive OLLHCS information assets. Any known breach of this policy and/or its subordinate procedures shall be immediately reported to an OLLHCS representative responsible for the business associate, or to the Director of Compliance and Privacy Officer, either in person or via the Corporate Compliance Hotline.

4.4 OLLHCS HIPAA Security Officer

The OLLHCS HIPAA Security Officer shall maintain and update all polices related to Security Standards for Vendor Supported Equipment to ensure that they are comprehensive and consistent with local, state, and federal law. The OLLHCS HIPAA Security Officer reserves the right to review any Internet/Intranet activities and usage. The OLLHCS HIPAA Security Officer shall be made aware of any breach of corporate security policy and advise the associates leader and appropriate Vice President as to the severity of the breach.

5.0 Accountability

Our Lady of Lourdes Health Care Services, Inc. and Affiliates including
Our Lady of Lourdes Medical Center
Lourdes Medical Center of Burlington County

Administrative and General Policy

POLICY NUMBER: AS0028PRI

NURSING CODE:

PAGE NUMBER: 7 of 7

TITLE: **HIPAA Security – Standards for Vendor Supplied or Supported Equipment**

Associates and users of OLLHCS information assets who are found to be in violation of any part of this policy are subject to disciplinary action up to and including termination of employment or contract and legal action. Retaliatory action shall not be taken against individuals who identify and/or report violations of security policy. For detailed sanction information, see AS009PRI – Training on HIPAA Policies and Procedures – section Corrective Action Guidelines, AS0013PRI – Mitigation of Use and Disclosure Violations and AS0100PER – Discipline and Termination of Employment.

APPROVED BY:

Alexander J. Hatala, President and Chief Executive Officer

ORIGINAL & REVISION DATE(s): 04/17/06; 04/30/09

NEW EFFECTIVE DATE: 04/30/12

REQUIRES REAUTHORIZATION IN: 04/30/15