# Confidentiality and Security Agreements

# SCOPE:

All facilities affiliated with the Company including, but not limited to, hospitals, ambulatory surgery centers, home health agencies, physician practices, and all corporate departments and divisions.

# PURPOSE:

To provide awareness of the importance of information security and confidentiality and to authorize and require agreements with workforce members, and external entities to protect Company information resources, including confidential patient information.

# POLICY:

A. **Information Confidentiality and Security Agreements with Individuals**

1. All Company employees and other individuals granted access to Company and/or patient protected health information (PHI) must sign and abide by the Confidentiality and Security Agreement (Agreement). The Agreement acknowledges specific responsibilities the individual has in relation to information security and the protection of sensitive information, including confidential patient information, from unauthorized disclosure.
2. Entities not owned and individuals not employed by the Company or an affiliate of the Company shall sign an Agreement if (i) the entity and individual provides services on premises owned or operated by the Company or an affiliate of the Company; (ii) the entity or individual has remote access to the Company's or its affiliates' information systems; or (iii) the entity or individual has access to Company's confidential information or PHI. All contracts for these services must contain enforcement provisions that are consistent with the Company's or its affiliates' disciplinary policies.
3. Any changes to the Agreement must be reviewed and approved in advance by Corporate Information Technology & Services (IT&S) and Legal Counsel.

B. **Business Contracts with Business Partners.** Relationships with an external entity involving access to Company information systems or the exchange, transmission, storage and maintenance or use of sensitive Company information require a formal contract including provisions to protect the confidentiality and security of Company information and/or systems in accordance with federal HIPAA Security Requirements.

C. **Sanctions.** Violations of this policy could lead to disciplinary measures up to and including termination of employment or business relationship. Suspected violations of this policy are to be handled in accordance with the *Information Security Policy, LPNT.IS.SEC.001*, *Protected Health Information Incident Response, HIPAA.GEN.007* and the Discipline section of the Code of Conduct. Violations may be reported in accordance with the *HIPAA Complaint Process & Disciplinary Actions Policy, HIPAA.GEN.003* located on the Compliance SharePoint site. In addition, violations may be reported to the Ethics Line at 1-877-508-LIFE.

D. **Policy Exceptions.** Exceptions to Information Security Policy are to be submitted to the Corporate IT&S Information Security Policy key contact for review and approval.

# PROCEDURE:

A. The Confidentiality & Security Agreement form will be posted and maintained by Corporate IT&S on the Company Intranet located under Security.

B. Each Company and Company affiliate employee and member of the workforce (e.g. volunteers, contract labor, etc.) must sign the Agreement at the time of employment. The completed Agreement will be maintained in the individual's personnel folder.

C. Each physician and allied health professional must sign the Agreement at the time he or she is appointed to a facility's medical staff. Completed Agreements will be maintained in the individual's credentials file.

D. Non-employed physician office staff must sign the Agreement at the time information system access is granted. Completed Agreements must be maintained in a central location by the Physician Support Coordinator or individual with a similar role in the business unit.

Representatives of vendors and other external entities must sign the Agreement at the time information access is granted. Completed Agreements must be maintained in the individual contract folder or system (*e.g.*, ShiftWise) by Facility personnel.

# REFERENCES:

**Government**

American Recovery and Reinvestment Act of 2009, Title XIII, Health Information Technology, Subtitle D: Privacy

Medical Records Confidentiality Act of 1995 (MRCA)

Health Insurance Portability and Accountability Act, Security Standards for the Protection of Electronic Protected Health Information, 45 CFR Parts 160, 162, and 164