DEPARTMENT: Information Protection	**POLICY DESCRIPTION:** Information Security – Monitoring of User Accounts and User Activity
PAGE: 1 of 2	**REPLACES POLICY DATED:** 2/25/98, 8/1/99, 4/14/03 (IS.AA.014), 4/21/05, 1/15/10, 11/1/2012, 12/1/14
EFFECTIVE DATE: April 1, 2016	**REFERENCE NUMBER:** IP.SEC.021 (formerly IS.SEC.021)
APPROVED BY: Ethics and Compliance Policy Committee	

SCOPE: All Company-affiliated facilities including, but not limited to, hospitals, ambulatory surgery centers, imaging and oncology centers, physician practices, shared services centers and corporate departments, Groups, Divisions and Markets.

PURPOSE: To provide facility leadership with requirements to monitor workforce member's information system user accounts and associated electronic user activity in order to detect potentially inappropriate or unauthorized access to sensitive or restricted information in support of the Company's Information Systems Account Management (ISAM) Program.

POLICY:

1. Each Company-affiliated facility is responsible for a user account monitoring program that prevents and detects irregularities in user activity during the normal course of business.

2. Facilities must support the ISAM Program by documenting risk-based decisions about periodic reviews of user accounts. See Information Protection Access Control Standards for User Access Management (AC.UAM.01-04) for specific requirements and standardized documentation tools.

PROCEDURE:

Monitoring of Information System User Accounts and Activity

1. Designated reviewer(s) must complete required periodic user account and/or user activity reviews in accordance with application-specific ISAM documents for information systems that store, process, or transmit sensitive or restricted information.

2. All monitoring reports must be maintained in compliance with Federal requirements, State requirements, and in accordance with the Records Management Policy, EC.014.

3. Unless mandated by state requirements, monitoring reports for clinical systems must not be combined with a patient's clinical record.

DEFINITIONS:

Designated Reviewer: Individual who is assigned to a role responsible for making a determination about the appropriateness of a user account or user activity based upon having knowledge of a user's role(s) and/or current responsibilities. Examples of roles that may be designated by a Business Owner to

DEPARTMENT: Information Protection	**POLICY DESCRIPTION:** Information Security – Monitoring of User Accounts and User Activity
PAGE: 2 of 2	**REPLACES POLICY DATED:** 2/25/98, 8/1/99, 4/14/03 (IS.AA.014), 4/21/05, 1/15/10, 11/1/2012, 12/1/14
EFFECTIVE DATE: April 1, 2016	**REFERENCE NUMBER:** IP.SEC.021 (formerly IS.SEC.021)
APPROVED BY: Ethics and Compliance Policy Committee	

perform periodic reviews may include Managers, Department Directors, Sponsors of non-employees, etc.

Information Systems Account Management (ISAM) Program: The ISAM Program is maintained by the Information Protection & Security Department for the purpose of providing Business Owners, ITG Product Owners, and other key stakeholders with standardized processes and tools needed to establish and maintain reasonable safeguards related to the approval, creation, modification, removal, monitoring, and overall management of user accounts. ISAM Program resources are stored on Atlas Connect.

Sponsor of a non-employee: A Sponsor has direct knowledge about a non-employee's role, responsibilities, status, licensure, certification, etc. and is responsible for making a determination about initial access, as well as performing periodic access reviews if required.

REFERENCES:

1. Appropriate Use of Communication Resources and Systems Policy, EC.026
2. Records Management Policy, EC.014
3. Information Security Policy, Electronic Communications, IP.SEC.002
4. Information Security Standard: Electronic Data Classification, AM.IC.01
5. Information Security Standard: Monitoring System Use, COM.M.03
6. Information Security Standard: Information Systems Account Management Procedures, AC.UAM.01
7. Information Security Standard: User Access Authorization, AC.UAM.02
8. Information Security Standard: Periodic User Account Review, AC.UAM.04
9. Information Security Standard: Termination Notification, WS.TCE.01
10. Information Systems Account Management (ISAM) Program Atlas page
11. Information Systems Account Management (ISAM) Document Template
12. Information Systems Account Management (ISAM) Manual
13. Information Security Guidance: Managing Access for Parallon Workforce Management Solutions Nurses