HACKETTSTOWN REGIONAL MEDICAL CENTER
ADMINISTRATIVE POLICY MANUAL

INFORMATION SYSTEMS SECURITY
CONFIDENTIALITY AND PASSWORD ASSIGNMENT

==========

Effective Date:	**03/00**	**Policy No:**	**IS-07**
Cross Referenced:	**AHC 6.1**	**Origin:**	**Information Systems**
Reviewed Date:	**11/03, 2/05, 1/08, 09/09, 6/12**	**Authority:**	**Chief Financial Officer**
Revised Date:	**05/05, 09/09**	**Page:**	**1 of 2**

PURPOSE:

HRMC adopts the AHC 6.1 Policy https://intranet.adventisthealthcare.com/policiesandprocedures/Corporate/Information%20Technology/AHC%206.1.pdf and all of its content except for the Procedures. The following are the Information Systems Security Confidentiality and Password Control procedures for Hackettstown Regional Medical Center.

REQUESTS FOR SYSTEM ACCESS FOR NEW/TRANSFERRED EMPLOYEES

Requests for system and remote access to systems that are managed by PHNS are made through the Information Technology Service Desk by completing the Computer System/Application Access Form, and forwarding to the IT Service Desk via E-mail. This form is also used to track Department Specific systems access (reference # 5 below). The User's Department Manager or Director must approve all requests.

PROCEDURE

1. The Computer System/Application Access Form must be completed by the Department Manager or Director and sent to Information Technology Service Desk via E-mail for the following:
   a. New employee hire.
   b. When the employee is terminated, under Disciplinary Suspension, or extended leave of absence.
   c. To change an employee's access functions (i.e. Change of status or Transfer).

2. Information Technology will issue a user ID and password, and/or terminate access accordingly.

3. Information Technology will notify the Department Manager or Director after the user ID and password has been created and/or deleted.

4. The Department Manager will file the original Computer System/Application Access Form in the employee's PDP file. If the user is a Contractor, Agent, or from an Agency, a separate folder must be kept with the PDP files, since this category of employees do not have a PDP file. This form will be updated as necessary for the entire length of service at HCH, and will follow the employee during any job transfers.

5. If the Department has a Department Specific System, it will be the responsibility of the respective Department Manager or Director to monitor their Department Specific Applications (i.e. Laboratory, Pharmacy, CT Scan, etc.) with regard to New Employee access. A Computer System/Application Access Form must be filled out and kept in the employee's PDP file, or in an automated file after the employee's systems access has been completed. This includes all (Employees, Contractors, Volunteers, Agents, or Agency Employees). This process is required to develop an audit trail for HIPAA Compliance.

NOTIFICATION OF RESIGNATION/TERMINATED EMPLOYEES

The Department Director/Manager will notify the Information Technology Service Desk via the Computer System/Application Access Form, for each employee that has resigned their employment with HRMC. In the event that an employee (including Contractors, Volunteers, Agents, or Agency Personnel) is involuntarily terminated by HRMC, Human Resources and Department Director/Manager will notify the Information Technology Help Desk regarding the termination, for immediate cancellation of all User IDs for that employee.

PROCEDURES

1. HRMC Human Resources will notify the IT Service Desk immediately following an ***involuntary*** termination of an employee. Information Technology will inactivate the individual's access to systems. Access to the computer system for ***involuntary*** terminations can be cancelled or disabled by request of Human Resources, Department Managers, Directors, or the Administrator on-Call, 24 hours a day, 7 days a week.

2. For all other terminations the Department Manager or Director will fill out the Computer System/Application Access Form, identifying that an employee has resigned or been terminated, and send the form via E-mail to the Service Desk. Upon receipt of the request, Information Technology will delete the employee's access to all HRMC computer systems that are controlled by PHNS. The Manager must file the form in the employee's PDP, or in a separate automated file for all Employees, Contractors, Volunteers, Agents, or Agency Employees, indicating that their access was terminated. This process is required to develop an audit trail for HIPAA Compliance.

3. It will be the responsibility of the Department Manager or Director to monitor their Department Specific Applications (i.e. Laboratory, Pharmacy, CT Scan, Etc) with regard to terminated employee's authorized access. After the employee's systems access has been deleted, the Employee's Computer System/Application Access Form should be filed in the respective PDP, or in a separate automated file indicating that the employee's access was deleted. This includes all (Employees, Contractors, Volunteers, Agents, or Agency Employees). This process is required to develop an audit trail for HIPAA Compliance.

4. At any given time, IT can take the following actions as a standard system administration practice:
   - Accounts that remain inactive for 6 months will be disabled.
   - E-mail mailboxes that have not been accessed for 6 months will be deleted after the Manager has been notified.