

## HALTON HEALTHCARE SERVICES

---

# Access to Technology Policy

---

<b>Developed By:</b>	Information Systems	<b>File Number:</b>	
<b>Approved By:</b>	Draft	<b>Review Frequency:</b>	Q 1 years
<b>Original Approval Date:</b>	October 2004	<b>Review/Revision Date:</b>	October 2005

---

### 1.0 Policy

Halton Healthcare Services provides information and communication technology to its staff, physicians, volunteers and affiliates for the purpose of performing their job functions. HHS and all users of these systems share a responsibility to ensure the information they contain is protected from unauthorized access, loss, corruption, theft or destruction. Access to many of the information and communications systems in use at HHS requires individual authentication parameters (user codes, passwords) which define the users access privileges and ensure unauthorized parties cannot access the systems. This policy sets out the conditions under which users are granted access, and defines the procedure that is used to accomplish this.

### 2.0 Procedure

#### 2.1 User Codes and Passwords

Individual authentication parameters belong exclusively to the user to whom they are assigned and should never be shared with others. All users assigned individual authentication parameters are responsible for taking the necessary precautions to ensure they are not revealed. Many of HHS' information systems track user activity based on authentication parameters, and users are responsible for all activity that occurs under their unique parameters. Users who suspect that their authentication parameters may be known by others must immediately arrange to have them changed (refer to section 2.2 of this Policy). It is a breach of HHS Policy (refer to Appropriate Use of Technology Policy) to reveal your authentication parameters, as well as to knowingly use the parameters of another user or to knowingly impersonate another user in any way.

#### 2.2 Obtaining a User Code and Password

Information Systems is responsible for the administration of authentication parameters on all HHS information and communication technology. In some cases, Information Systems delegates this responsibility to individuals in other departments who are designated as System Administrators for niche systems. Section 2.4 of this policy lists the departments responsible for assigning user access to various systems, however users may contact the Information Systems Help Desk (X7777) to determine a course of action when they require access to technology. User Codes are designed to identify both the user and the functions within an application that can be accessed. Information Systems can only grant access to employees or contractors under the direction of their supervisor, to volunteers under the direction of the Manager of Volunteers, to medical staff under direction of the Chief of Staff, and to "Agents" of HHS (as defined in the Personal Health Information Protection Act) under the direction of the Privacy Officer. Information Systems (or delegated system administrators in the case of niche systems) is responsible for ensuring that all access is properly authorized, and that all required policies have been reviewed (and signed/filed if necessary) prior to granting access.

All users of information and communication technology at HHS must read and sign the Confidentiality Policy prior to obtaining access. They must also review and be familiar with this policy and the Appropriate Use of Technology policy. Other policies (EMR Access Policy, Remote Access Policy) may require review and the user's signature depending on the type of access to be provided.

### 2.3 Selecting and Protecting Your Password

Selecting a safe password, and ensuring it is not revealed is a very important component of HHS' overall security framework. Passwords are never displayed when entered, but users should ensure when they authenticate that their keystrokes can not be observed by others. Passwords should be selected in order to prevent the need to record them in writing, but should not be easily guessed by others (i.e. you or a significant other's birthdate, nicknames etc.). All passwords should be a minimum of 5 characters and should be changed at least twice annually. A combination of alphabetic and numeric characters is recommended. Names and dictionary words should not be used. A recommended approach is to start with something that is known to you, but would be difficult to determine by others (the street you grew up on) and add a digit or special character (substitute "\$" for an "s").

### 2.4 System Administration

Access to all information and communication systems is done by system administrators, who create user accounts and assign required functions. Typically when accounts are created, users are asked to select a password and then are automatically required to change their password at prescribed intervals based on system parameters (every 6 months). In some cases a temporary password is assigned, and the user is required to change the password on their first login. Below is a list of systems which require authentication and the department responsible for user administration. Management staff (Directors, Managers, Coordinators, Supervisors) in these departments should be contacted to arrange access.

System \_\_\_\_\_ Department

#### *Core Systems*

Network/Domain Authentication	Information Systems
Meditech (all modules)	Information Systems

#### *Niche Systems*

Access Control/Photo I.D.	Parking & Security
Budman	Finance
Computation	Food Services
PICIS O.R. Management	Information Systems
Diabetic Education Database	Diabetic Education
Dictaphone	Clinical Information Services/Diagnostic Imaging
Doctors Database	Medical Staff Office
EDI	Materials Management
Expeditor Patient Tracking	Information Systems
GCAMS	CardioResiratory
GRASP	MDH ER
HealthScreen	Information Systems
Infomed	Information Systems
Interqual	Decision Support
IRS	Administration
MARS Holter System	CardioResiratory
Med2020	Clinical Information Services
Med-e-care CCRS	Information Systems
MediHR	Human Resources
Meridian Mail	Information Systems
WoSyst	Environmental Services
MUSE Marquette	CardioResiratory
Parklane	Occupational Health
Amano Parking	Parking & Security

System \_\_\_\_\_ Department

*Niche Systems, (continued)*

PCM Elcombe	Connect Care
Prism	Connect Care
PTAC	Information Systems
Quadramed	Information Systems
Raiser's Edge (OTM)	Foundation OTMH
Raiser's Edge (MDH)	Foundation MDH
Raiser's Edge (GH)	Foundation GH
Royal Bank Deposits	Finance
Silverware	Food Services
VMAX	CardioResiratory
Volunteer Works	Volunteer Services
Workstream	Human Resouces
Paradigm	Laboratory
PACS (Radiology)	Diagnostic Imaging
PACS (Cardiology)	Cardiorespiratory
Omicell	Pharmacy
Medworxx	Information Systems
Clinsaver	Decision Support
MMM Instrument Tracking	Operating Room

Reviewed By/Consultation With: Health Informatics Steering Committee, Senior Management Committee

Signed By: \_\_\_\_\_  
Title: VP, Finance and Information Systems

(Archived Copy Only)

I, \_\_\_\_\_, have read and understood the above policy, and agree to  
**(name, please print)**  
abide by the conditions of this policy. I am aware that if I act against this policy, my actions could be  
cause for discipline, up to and including termination or loss of privileges.

\_\_\_\_\_  
Name and Title Date