HEALTH TECHNOLOGY

DTO Doctors Technology Office
A GPSC initiative

ROLE-BASED ACCESS TO ELECTRONIC SYSTEMS GUIDE

Summary

This guide helps private practice clinics to implement an access management framework that will protect confidentiality and personal information using a role-based access concept. Staff access to clinical systems and devices are provisioned by defined roles which can be mapped similarly within workstation user accounts and most EMRs.

Why Clinics Need Role-Based Access

Using role-based access, privacy is designed directly into the clinic infrastructure. By limiting the access of each staff role to only the software or systems they need to do their jobs, the burden of managing that access is reduced and unnecessary security gaps are closed.

Creating default staff roles based upon required access improves the efficiency of provisioning and deprovisioning new or departing staff. Standard role access and accounts can be distributed or disabled as needed while only needing to maintain access rules for each role instead of each user.

When designing software architecture at the clinic, IT staff can use the role matrix to understand the permissions for various account types needed for network, workstations and business applications.

Guiding Principles

1. Access to all information systems is strictly controlled and provided on a “need-to-know basis” to reduce unnecessary risk. Only authorized users are allowed access to:
    a. Clinic wired and wireless network systems
    b. Clinic device operating systems
    c. Clinic EMR
    d. Clinic software applications
    e. External systems providing patient information such as CareConnect
2. Access to all Clinic’s information systems (including remote access) must be strictly controlled according to individual roles and responsibilities documented by the *Access Rights Per Role* form.
3. Administrative accounts are not to be used for every day operations and must be available only to individuals who perform system maintenance tasks.

4. Contracts, agreements, or statements of work defining third-party access to Clinic's information must be reviewed and approved by the Privacy Officer and Security Lead prior to signing.

5. Access to Clinic's information must be monitored through audit logs that track what systems were accessed with a timestamp and user identification.

6. Audit logs must be maintained for sufficient time to provide evidence in the event of security breaches or incidents.

Role-Based Access Tools

The checklist and forms provided in this guide provide a resource to assist in defining role-based access and policy. The forms provided contain common example roles and permissions and clinics can update the form content as needed to match individual needs.

Access Rights Management Checklist

Review the Access Rights Management Checklist to help identify the fundamental aspects of the clinic access rights management policy.

Access Rights Per Role Matrix Form

Use this form to identify and document all roles and corresponding permissions at the clinic (eg. Physician, MOA, Office Manager, Security Lead, Billing Support, etc.). Consider level of responsibilities and identify what is common and what is unique. Unique responsibilities might require a separate role so it can be easily distributed amongst users. Roles may be shared as needed. For example, Billing Support as a separate role might be granted to some office staff as well as to all or selected physicians.

User Access Maintenance Form

Use this form to track which access roles are assigned each staff member or other person working within the clinic.

Related Materials

Physician Office IT Security Guide	User-friendly guide focusing on key safeguards for private practices to ensure their compliance with regulatory requirements. Concise (35 pages) reference for technical terminology and concept.
Doctors of BC Privacy Toolkit	Comprehensive resources for physicians to assist in complying with the Personal Information Protection Act (PIPA).

DISCLAIMER

This document provides general guides and approaches only. We strongly recommend that you retain a knowledgeable and qualified IT professional to regularly assess and maintain your clinic's technology.

For more information, guidance, or support contact:

Doctors Technology Office
604 638-5841
DTOinfo@doctorsofbc.ca
www.doctorsofbc.ca/doctors-technology-office

Access Rights Management Checklist

Use this checklist to help identify and define key components for the clinic's access rights policy and support the ongoing management of the *Access Rights Per Role Matrix* and *User Access Maintenance* forms.

- ☐ Access rights to information and information systems are implemented by the Security Lead according to *Access Rights per Role* form.
- ☐ Set-up for new users is requested by _____ and implemented by _____.
- ☐ User accounts and related access rights are updated upon:
  a. start of employment
  b. change in employment status, including promotion or role change
  c. employment termination
- ☐ Individual access rights are documented by _____ using the *User Access Maintenance* form. It is reviewed every _____ months.
- ☐ Staff, contractors, and third-parties can access only the information that is required to fulfill relevant responsibilities and tasks (need-to-know basis).
- ☐ Staff, contractors, and third-parties are provided with the lowest level of user rights applicable to their role (role-based access).
- ☐ Access to all systems, networks, and information is approved by the Privacy Officer. See *Access Rights per Role Matrix* form.
- ☐ Access *Rights per Role Matrix* is regularly reviewed every _____ months.
- ☐ Audit of individual access is performed every _____, documented by the audit log and retained for _____ years.
- ☐ Appropriate access rights are assigned to individuals based on their role and responsibilities. See *User Access Maintenance* form.
- ☐ Individuals who are granted system administrative rights should not use this log in for daily tasks.
- ☐ Defined roles and associated access rights are adhered to when creating user accounts in the clinic network, workstations, or EMR.

ACCESS RIGHTS PER ROLE MATRIX FORM

Page #: Last Updated:

	Privacy Officer	Security Lead	GP	Office Manager	MOA	Billing Support	Transcriptionist	Intern	IT Support
EMR									
Network									
Wireless									
Remote Access									
PharmaNet									
Teleplan/Billing									
Server/System Admin									
CareConnect									

USER ACCESS MAINTENANCE FORM

Page #: Last Updated:

Name	Role(s) Granted (Based on Access Rights per Role Matrix)	

Reviewed and Confirmed by: _____ *Print Name* _____ *Signature* _____ *Date*