# CLINIC INFORMATION

## CONTACT INFORMATION:

|  |  |
| --- | --- |
| Name: |  |
| Address: |  |
| Phone: |  |
| Email: |  |

## EMERGENCY CONTACTS:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Title |  | Name |  | Contact Information |
| Privacy Officer\* |  |  |  |  |
| Security Lead\*\* |  |  |  |  |
| EMR Technical Support |  |  |  |  |
| Local ITSupport Line |  |  |  |  |
| Alarm Company |  |  |  |  |
| Office of the Information Privacy Commissioner  |  | Enquiry BC |  | Vancouver: (604) 660-2421BC: (800) 663-7867info@oipc.bc.ca |
| Doctors Technology Office |  | Support Desk |  | (604) 638-5841 DTOtechsupport@doctorsofbc.ca |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

\* Privacy Officer – one physician responsible for structuring and managing the privacy program.

\*\* Security Lead – an individual with IT and network management experience responsible for developing and maintaining technology standards and procedures.

# PASSWORD MANAGMENT POLICY

The purpose of this policy is to implement secure practices regarding individual password management.

This policy applies to all individuals provided with access to Clinic EMR and computer systems.

1. All Clinic information systems must require sufficient and strong authentication methods such as password, token, certificate etc..
2. Passwords must be:
	1. unique (not used in any other situations)
	2. complex enough to meet the Password Management Checklist requirements
	3. kept strictly confidential and not shared between individual users.
3. Passwords are never shared between individual users to allow for accurate audit of access to Clinic information systems.
4. Users should be aware of their responsibilities for the protection of their passwords to ensure unauthorized access is not allowed.
5. Users who are provided with an account to any information system at the Clinic must follow this policy and associated Password Management Checklist.

PASSWORD MANAGEMENT CHECKLIST

|  |  |
| --- | --- |
| Passwords expire every \_\_\_\_ months and users must then change it.  | **☐** |
| Generic passwords (such as ‘locum’) are not to be used. | **☐** |
| Passwords are not written down and if digitally stored, the file is protected (encrypted) with a strong master password. | **☐** |
| Users are initially provided with a secure temporary password to access any information system. | **☐** |
| Users are instructed to change the temporary password provided upon the first login. | **☐** |
| Users are aware of their responsibilities for maintaining the confidentiality of their passwords: |  |
| Users are aware that passwords cannot be shared. | **☐** |
| Users are aware that their passwords must be unique. The same or similar passwords must not be used on different accounts. | **☐** |
| Users are informed that passwords should not include dictionary words or common terms such as a name or clinic address. | **☐** |
| Users are following the require complexity of the password which at the minimum must include a minimum of 8 characters which are a combination of uppercase characters, lowercase characters, numerals, and symbols (! $ # %). | **☐** |

# INFORMATION ACCESS POLICY

The purpose of this *Information Access Policy* is to provide safeguards protecting confidentiality and personal information in compliance with the Personal Information Protection Act (PIPA) and other applicable legislation. This policy is not intended for public distribution.

This *Information Access Policy* applies to:

* All Clinic’s personnel (full-time or part-time).
* All contractors and third parties that perform work on behalf of the Clinic.
1. Access to all information systems is strictly controlled and provided on a “need-to-know basis”. Only authorized users will be allowed access to:
	1. Clinic wired and wireless network systems
	2. Clinic operating systems
	3. Clinic EMR
	4. Clinic software applications
	5. 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.
	1. Audit logs must be maintained for sufficient time to provide evidence in the event of security breaches or incidents.
	2. Exceptions to this policy must be approved by the Privacy Officer and documented to assist during investigations or security risk assessment, as applicable.

Requirements for Access Rights Control

|  |  |
| --- | --- |
| Clinic maintains a list of current information systems and software applications. The list includes product name and version and is updated every \_\_\_\_\_\_\_\_\_\_\_\_ months or when any change occurs. See the *Electronic Device Inventory List*.  | **☐** |
| 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 *Access Rights Administration* form.  | **☐** |
| Individuals who are granted system administrative rights should not use this log in for daily tasks.  | **☐** |
| Each individual who granted access to Clinic’s information system(s) is responsible for using a unique login and strong password. See *Password Management Policy*. | **☐** |

|  |
| --- |
| **Step 1:** List all information systems at the Clinic. Examples include: EMR, Network, Wireless, Remote, Server, Operational System, CareConnect, MSP, etc.  |
| **Step 2:** List all roles at the Clinic, for example 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. For example, Billing Support as a separate role might be granted to some office staff as well as to all or selected physicians. |
| **Step 3:** For all roles, associate the level of access to each information system necessary: Administrator, Regular User, View-only. |
| **Step 4:** Create a matrix of roles at the Clinic and access level for systems. See *Access Rights per Role* form example. |
| **Step 5:** Create a form to manage individual access at the Clinic. See the *User* *Access* *Maintenance* form example. |

ElectroniC Device Inventory List

Page #: Last Updated:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Computer Name/ Computer type**(e.g., Clinic001/Laptop or Samsung02/Phone) | **OS/Version**(e.g., Windows 10) | Computer Location or Owner | **Serial #****Asset Tag #** | **Attached hardware**(e.g., LaserJet Pro MFP) | **Additional Applications installed** | **Notes (**Approximate purchase date, sufficient resources left, etc.+) |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

ACCESS RIGHTS PER ROLE matrix

Page #: Last Updated:

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Role at the Clinic**  | **EMR** | **Network(Y/N)** | **Wireless(Y/N)** | **Remote (Y/N)** | **Care-Connect** | **Pharma-Net** | **Server / System Admin** | **Teleplan/ Billing System** | **Other Information Systems or Software Required** |
| EMR |  |  |  |  |  |  |  |  |  |
| Security Lead |  |  |  |  |  |  |  |  |  |
| GP |  |  |  |  |  |  |  |  |  |
| Office Manager |  |  |  |  |  |  |  |  |  |
| MOA |  |  |  |  |  |  |  |  |  |
| Billing Support |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |

Access Rights Administration

|  |  |
| --- | --- |
| 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 the Clinic’s office administration who notifies the Security Lead. | **☐** |
| User accounts and related access rights are updated upon:1. start of employment
2. change in employment status, including promotion or role change
3. employment termination
 | **☐** |
| Individual access rights are documented by the Security Lead using the *Ongoing Maintenance of User Accounts* form. | **☐** |
| The *Ongoing Maintenance of User Accounts* form is **reviewed** by the Office Manager and Security Lead, then **approved** by the Privacy Officer on a periodic basis every \_\_\_\_\_\_\_\_\_\_\_ months.  | **☐** |
| During each review, the *Ongoing Maintenance of User Accounts* form is completed, dated, signed, and then stored to ensure that the Clinic’s Policyis followed.  | **☐** |

User Access Maintenance form

Page #: Last Updated:

| **Name** | **Role(s) Granted (Based on Access Rights per Role Matrix)** | **Correct Yes/No** |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Reviewed and Confirmed by: |  |  |  |  |  |
|  | *Print Name* |  | *Signature* |  | *Date* |