SUBJECT: **ACES Account Management Policy** NUMBER: **III-40**

DATE: 1 February 2016

APPROVED BY:

Purpose

The purpose of this policy is to establish a standard for the creation, administration, use and removal of accounts that facilitate access to information through the Acute Care Enhanced Surveillance (ACES) system. An account consists of a user ID and a password which grants the user access to the ACES system.

Procedures

Account Creation

As the ACES service provider, KFL&A Public Health (henceforth abbreviated KFLAPH), shall make decisions regarding access to data within ACES.

- Each account requestor is required to fill out an ACES confidentiality agreement (see appended document) and submit the completed form to KFLAPH staff before access to ACES is considered. Potential users are also required to attend an ACES training session via webinar before their account information is released to them. Training sessions are set up by KFLAPH staff on an as-needed basis, can be attended remotely, and are scheduled for 90 minutes.

  Step 1: A potential user can email KFLAPH to request access. Emails must come from an official Local Public Health Agency (LPHA), an official Hospital, Public Health Ontario (PHO) or Ministry of Health and Long-Term Care (MOHLTC) email address.

  Step 2: KFLAPH emails the requestor an ACES confidentiality agreement.

  Step 3: The requestor completes the confidentiality agreement and returns it to KFLAPH via scanned copy. All fields are required to be filled out and include: date, requestors printed name, signature, email address, phone number, job title and agency of employment. The requestor also requires a sponsor/witness. For a hospital user account, this person can be the direct supervisor of the requestor but it can also be the hospital or hospital corporations signing authority from the original DSA received by KFLAPH. For a LPHA user account, the sponsor/witness can be the requestors' manager or it can be the LPHA's Medical Officer of Health (MOH) or Assistant Medical Officer of Health (AMOH).

  *NOTE: While KFLAPH does not have a defined list of authorizers, the onus is on the requestor to seek out the appropriate signatory. The language in the original Data Sharing Agreement (DSA) which KFLAPH entered into with

hospital(s) and the LPHA, as well as the requestor's confidentiality agreement expressly stipulates that the data in ACES, in some cases, can be considered personal health information and needs to be protected accordingly as defined in section 4 of the Personal Health Information Protection Act (PHIPA). Fraudulent use of the data in ACES or misrepresentations of one's self or one's signatory are expressly forbidden.

Step 4: Upon receipt of the confidentiality agreement, KFLAPH staff will approve the access and the ACES technical team will create a user account.

Step 5: Once the requestor has attended one of the aforementioned webinar ACES training sessions, they will be sent their account information and can begin using the system.

Password Management

Regardless of the situation, passwords are never to be shared or revealed to anyone besides the authorized user.

- Upon initial login, with the temporary password provided by KFLAPH staff, a user is prompted and required to change the password to something of their choosing.
- Passwords must be at least 8 characters in length and include an upper case letter, a lower case letter, a number and a unique character.
- The ACES system forces password changes on users quarterly (every 90 days). An account login attempt after this 90 day period will result in the user being directed to change their password before being able to continue into the ACES system.
- Users shall change their password immediately if they believe their password has been compromised.
- If a user has forgotten their ACES password, the ACES login page has a 'forget password' function which will allow the user to reset their password by using their registered e-mail address. A link will be sent automatically to the user with a link to create a new password.

Account deactivation

As the ACES service provider, KFLAPH reserves the right to revoke, disable or delete an account if it is determined that the account has been compromised, misused or is not being actively used. Accounts may be reinstated at the discretion of KFLAPH. A User is required to inform KFLAPH should they leave/change their current employed position under which access to ACES was originally granted.

- Regular audits of all ACES accounts will be done on a quarterly basis. During these audits, KFLAPH staff will review each active user account to ascertain if said user has logged into the system in the past 90 days. User accounts found to be inactive for 90 days will be deactivated immediately. No warning or notification will be sent in these cases.
- In some circumstances, at the discretion of KFLAPH, some accounts may be left active and reassessed at the next audit period.
- Users who have had their account deactivated can request reinstatement of their account, and in some cases these accounts may be reactivated. These instances will be logged at KFLAPH. Accounts that have been reactivated twice will not be reactivated a third time and will be permanently deleted. Exceptions and extenuating circumstances will be considered and may include maternity/paternity leave, leave of absences, sick leaves, extended vacations, and changes to the users employment role at their institution.