

KINGSTON, FRONTENAC AND LENNOX & ADDINGTON PUBLIC HEALTH

KNOWLEDGE MANAGEMENT SERVICE MANUAL

SUBJECT: ACES Account Management Policy and Procedure

NUMBER: III-40

DATE: 11 Jan 2019

PAGE: 1 of 3

APPROVED BY: Paul Belanger

Purpose:

The purpose of this policy and procedure 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 the online registration form and complete the ACES confidentiality agreement and submit said agreement form to KFLAPH staff before access to ACES is considered. Potential users will also be directed to the three ACES training videos that have been created to give users a run-through of the basic functionality of the system.

Step 1: A potential user must first complete (and submit) the online registration form found at <https://aces.kflaphi.ca/#/>. Prospective users must be employed at an official Local Public Health Agency (LPHA), an official Hospital, Public Health Ontario (PHO), the Ministry of Health and Long-Term Care (MOHLTC), or a Local Health Integration Network (LHIN).

Step 2: The requestor completes the confidentiality agreement (which is found as a link at the top of the online registration form) and returns it to KFLAPH via scanned copy. All fields are required to be filled out and include: date, requestor's printed name, signature, email address (must be an official work 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 corporation's signing authority from the original DSA received by KFLAPH. For a LPHA user account, the sponsor/witness can be the requestor's manager, or it can be the LPHA's Medical Officer of Health (MOH) or Associate Medical Officer of Health (AMOH). For users at PHO, the MOHLTC or a LHIN, the sponsor/witness must be the requestor's direct supervisor/manager.

*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). Inappropriate use of the data in ACES or misrepresentations of oneself or one's signatory are expressly forbidden.

Step 4: Upon receipt of the confidentiality agreement, KFLAPH staff will approve access and the ACES technical team will finalize the set-up of the user's account.

Step 5: The requestor will then 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 special character (e.g., #, \$, &, *).
- The ACES system will force 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.

- Automated audits of all ACES accounts will be done on a moving 90-day period. During these audits, our system will check each user account to ascertain if said user has logged into the system in the past 85 days. If the user account has been inactive for 85 days an automatic email will be delivered to the user reminding them that they have 5 days to log in to the system. If the user has still not logged into the system after 90 days, the account will be deactivated immediately. No further warning or notification will be sent in these cases.

KINGSTON, FRONTENAC AND LENNOX & ADDINGTON PUBLIC HEALTH

KNOWLEDGE MANAGEMENT SERVICE MANUAL

NUMBER: III-40

SUBJECT: ACES Account Management Policy and Procedure

PAGE: 3 of 3

- 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. Users with accounts that have been reactivated numerous times may have their access revoked at the discretion of KFLAPH. Exceptions and extenuating circumstances will be considered and may include maternity/paternity leave, leave of absences, sick leaves, extended vacations, and changes to the user's employment role at their institution.

ORIGINAL DATE:

1 February 2016

REVISIONS:

11 January 2019