

KINGSTON, FRONTENAC AND LENNOX & ADDINGTON PUBLIC HEALTH

ACES SERVICE MANUAL

SUBJECT: ACES User Account Management Policy and Procedure

NUMBER: III-10

DATE: 25 June 2023

PAGE: 1 of 3

APPROVED BY: Hugh Guan

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 (KFLAPH), shall make decisions regarding access to data within ACES.

Each account requestor is required to fill out the online registration form, complete the ACES confidentiality agreement, and submit said agreement form to KFLAPH staff before access to ACES is considered.

- Step 1:** A potential user must first complete (and submit) the online registration form found at <https://aces.kflaphi.ca/#/> using the "Sign up" button. Prospective users must be employed at an official Local Public Health Agency (LPHA), an official Hospital, Public Health Ontario (PHO), the Ministry of Health (MOH), or an Ontario Health Region. Note: email addresses are not permitted to be used as usernames.
- Step 2:** The requestor must also complete the confidentiality agreement (found as a link above the submit button on the online registration form or in the Privacy and Security folder found at <https://www.kflaphi.ca/acute-care-enhanced-surveillance/>) and return it to KFLAPH with the required signatures 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 witness signature. Signatures must be handwritten or scanned images. For a hospital user account, this witness can be (1) the direct supervisor of the requestor or (2) the hospital or hospital corporation's signing authority. For an LPHA user account, the witness can be (1) the requestor's manager, or (2) the LPHA's Medical Officer of Health or the Associate Medical Officer of Health. For users at PHO, the MOH, or an Ontario Health Region, the witness must be the requestor's direct supervisor/manager.

*NOTE: While KFLAPH does not have a defined list of authorized witnesses, the onus is on the requestor to seek out the appropriate signatory. The language in the original Data Sharing Agreement (DSA) between KFLAPH, the hospital(s), and the LPHA 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). This guiding principle is reiterated in the confidentiality agreement. Inappropriate use of the data in ACES or misrepresentations of oneself or one's signatory are expressly forbidden.

- Step 3:** Upon receipt of the completed confidentiality agreement, KFLAPH staff will approve access and finalize the set-up of the user's account.

Step 4: The requestor will then be sent their account information with a temporary password and can begin using the system. The user will also be sent a link to our ACES training videos and ACES User Manual, which collectively provide an overview of the basic functionality of 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. User accounts that have been inactive for 85 days will be sent an automated email 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. In some instances, organizations will block these automated email reminders from our Team, and this is beyond our control. While this mechanism may work for the majority of users, it is still the user's responsibility to use ACES regularly enough to not have to rely on this feature.
- 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

15 June 2023