OLIS-MORE FAQ — Security for Lab Automation, Mobile Orders, and Results Entry

What authorization is used to access OLIS-MORE?

- ONE® ID
- 2FA

OLIS-MORE users are authorized with a valid ONE®ID account and 2 Factor Authentication (2FA) that allows them to access the web form for placing orders and/or submitting results. 2FA—also referred to as the Challenge Phone Number—**provides a secondary means of identity verification through a separate and unconnected communication channel**. This, along with their ONE®ID login ID and password, will give users access to OLIS-MORE.

Note: If a user does not have a phone available when logging into ONE®ID, they will be presented with online Challenge questions before being provided with access.

Security Controls

If users are authorized for access under the authority of (UAO) multiple organizations, they must select the UAO under which they are completing the requisition (or swab). Access and searches are restricted to the site under which the UAO session is conducted.

Users must be aware of the sensitivity of information on their devices when using OLIS-MORE. They must diligently protect the information on these devices and perform secure logout procedures when they are not in use. All devices used for the purposes of accessing OLIS-MORE must be issued and managed or formally approved by the client's organization.

How secure is the online form with the direct interface to OLIS/using BYOD?

The communication between the browser and OLIS-MORE web server and the OLIS Repository is secured or encrypted through HTTPS with TLS v1.2 or higher.

Where is the data stored?

Submitted data is available in the Ontario Laboratories Information repository, which is stored in the Ontario Health Data Centre in Redis.

Is client data isolated in OLIS?

The data in OLIS-MORE is in a shared instance of Redis but access to the data at each HIC is restricted to the HIC itself.

Is Personal Health Information (PHI) data tokenized on the backend?

No. For more information on information security at Ontario Health, go to: ehealthontario.on.ca/en/security/guide

Logging and Monitoring Access and Incidences

All user access to the OLIS-MORE Application as well as the OLIS repository is logged and monitored via a Security Information and Event Management (SIEM) system by Ontario Health security staff.

Note: Ontario Health will only provide Application audit logs, which may include PHI, to the Ministry of Health.

How is the data accessed by internal users? And who has access?

Ontario Health internal access to the data in OLIS-MORE is restricted to troubleshooting and ticket resolution. The only users who have access to the OLIS-MORE backend are the Application Management and Support team.

Other Questions

Please reach out to the Ontario Health, Lab Automation Deployment Team (ac.labautomation@ontariohealth.ca) for additional information.

Please review the security safeguards implemented for protecting health information: ehealthontario.on.ca/en/security/safeguards

For any security and privacy related incident, please contact the Enterprise Service Desk at 1-866-250-1554 or OH-DS_servicedesk@ontariohealth.ca