Clinical Research Support Office ("CRSO")

STANDARD OPERATING PROCEDURE

SOP NUMBER	**TITLE**
CTM-SOP-2002	CTMS Login Access
EFFECTIVE DATE	**WRITTEN BY**
8/15/2019	Jennifer Simpson
REVIEWED BY:	**REVIEW HISTORY:** 4/13/2020
JEN SIMPSON	

APPROVAL	
SIGNATURE	**DATE**

1. POLICY STATEMENT

   The Clinical Research Support Office (CRSO) has entered into an agreement with the University of Kentucky (UK) Identity Access Management (IAM) department and the UK Information Technology Services (UK ITS) to allow the CRSO Clinical Trials Management System (CTMS) team to provide and manage the login access to the employees of UK and select outside-institution individuals participating in the management of clinical research studies at UK.

2. PURPOSE

   To establish a standardized process for providing login access, define steps required, documents required, document retention period, and mandated role-based training to achieve login access to the CTMS.

3. SCOPE

   This policy is applicable to all end-users requesting CTMS login access.

4. RESPONSIBILITY

   The CRSO CTMS Information Technology (IT) Trainer, Markey Cancer Center Data Management Specialist/Trainer and CTMS Administrator will be responsible for providing and maintaining login access to the application.

   The CRSO CTMS Specialists have permission to create user contacts within the CTMS for purpose of protocol shell creation. This functionality does not allow login access.

5. PROCEDURE

Required Documents and Retention

1. The following documents must be filled out by all UK employees requesting login access.
    1.1. Online Forms
        1.1.1. Online Login Request form through Qualtrics https://uky.az1.qualtrics.com/jfe/form/SV_cAfhHoNTquxO6Vv
    1.2. Documents
        1.2.1. Proof of recent Health Insurance Portability and Accountability Act (HIPAA) training. This training may be completed through the UK Web Based Training in myUK Learning or through the Collaborative Institutional Training Initiative (CITI) training provided through UK.
            - Web based training (WBT) through the UK myUK Learning Portal must be performed annually. A printed certificate must show completion of the current year's WBT.
            - CITI training has an expiration of 3 years from the time of completion. A printed certificate of completion must be current, in good standing, and not expired.
        1.2.2. A signed UK ITS Confidentiality and Non-Disclosure Agreement document. This document will be available for signature when role-based training is performed in person or electronically (for digital signature or certification) for remote training.
        1.2.3. An electronic copy of the UK ITS Acceptable Use policy will be provided to each new CTMS login requestor.
        1.2.4. The HIPAA training document and UK ITS Confidentiality and Non-Disclosure Agreement document must be scanned and uploaded into the CTMS user contact record under the "Credentials" file.
        1.2.5. The hand-signed Non-Disclosure Agreement document will be retained within the CRSO office for a period of 3 years. At the end of the 3 years the physical document will be destroyed and only the electronic version will be retained within the end-users contact record within the CTMS.
2. The following documents must be filled out by all non-UK individuals identified as needing access to the CTMS
    2.1. Request Forms
        2.1.1. All external UK individuals requesting access must fill out the External UK CTMS Access Form. This is a CRSO created form that has been verified and accepted for use by the UK IAM department.
        2.1.2. This login request has an embedded HIPAA and non-disclosure statement that must be hand-signed. This statement has been verified

by the UK Chief Privacy Officer.

2.1.3. The login access must have the provided supervisor signoff page filled out and hand-signed.

2.2. Documents

2.2.1. Proof of recent HIPAA training.

2.2.2. An electronic copy of the UK ITS Acceptable Use policy will be provided to each new external to UK CTMS login requestor.

2.2.3. The HIPAA training document and External UK Login Access form with the signed HIPAA/Confidentiality and Non-Disclosure statement document must be scanned and uploaded into the CTMS contact record.

2.2.4. The Non-Disclosure Agreement document that is hand-signed will be retained within the CRSO office for a period of 3 years. At the end of the 3 years the physical document will be destroyed and only the electronic version will be retained within the end-users contact record within the CTMS.

Role-based Training Requirement

3. All new requests for CTMS access will be processed and granted access after role-based training is performed with a CTMS Trainer.
   3.1. A description of the end-users scope and/or job responsibilities must be outlined within the login access request form. Based on the defined scope, the CTMS Trainer will recommend the role-based training(s) that must be performed to obtain access.
   3.2. Depending upon the scope of the end-user, multiple role-based training modules may be required.
   3.3. Role-based training may be provided in person or remotely using a video conferencing tool of choice.
   3.4. All UK employees must enroll for their recommended role-based training using the myUK Learning Portal found at: https://myuk.uky.edu/irj/portal
      3.4.1. In the absence of posted classes, role-based training may be individually scheduled or as a group/department with the CTMS Trainer.
   3.5. External users (non-UK employees) will perform their role-based training that is manually scheduled with the CTMS Trainer.
   3.6. UK employees are encouraged to enroll into any of the training modules that interest them. They are not restricted to only those that pertain to their role. However, the role-based recommendations must be performed minimally to obtain access.
   3.7. Pre-existing users within the CTMS who have a change in their job functions or role will be required to perform the role-based training that pertains to their new role prior to having their permissions changed within the database.

Account Activation

4. After the login access form is completed, all required documents are signed/received, and role-based training has been performed the end-user will receive login access to the CTMS.
   4.1. The process of creating a new contact record within the CTMS requires an email verification step by the application.
   4.2. UK employees will use their Link Blue User ID (not the full email) and password to log into the CTMS.
   4.3. External to UK users will have contact UK ITS to request a University of Kentucky Link Blue ID and password.

Deactivation of Account

5. The CTMS is configured to automatically deactivate any accounts that have been inactive for ≥180 days that are application level user IDs.
   5.1. The CRSO will perform a monthly check and deactivate any accounts that are inactive for ≥ 180 days manually.
6. The CTMS is also configured to lock an account after 6 failed attempts to log in.

Reactivation of Account

7. Any employees at UK who have a deactivated account can contact the CRSO or Markey Cancer Center support office to have their account reactivated.
   7.1. If the deactivation occurred due to a failed password attempts; the reactivation can occur immediately after notification.
   7.2. If deactivation occurred due to a lack of activity for ≥180 days; a refresher training will be provided prior to reactivation.
   7.3. If deactivation occurred and during the course of that period there was any kind of change in job responsibilities; a full role-based training will be provided prior to reactivation.

6. ATTACHMENTS

- Copy of the CRSO Qualtrics UK CTMS Login Request Form (exported). Current as of the effective date of this SOP.
- Copy of the CRSO External UK CTMS Login Request Form. Current as of the effective date of this SOP.
- University of Kentucky/UK HealthCare User Confidentiality and Non-Disclosure Agreement.

6. REFERENCES

1. University of Kentucky/ UK HealthCare Enterprise Policies: https://ukhealthcare.mc.uky.edu/policies/enterprise/default.aspx
2. University of Kentucky / UK HealthCare Enterprise Policy and Procedure. Policy #A13-100 Acceptable Use Policy. Retrieved from: https://ukhealthcare.mc.uky.edu/policies/enterprise/_layouts/15/WopiFrame.aspx?sourcedoc=/policies/enterprise/Enterprise/A13-100%20Acceptable%20Use%20Policy.docx&action=default