EDGE CLINICAL RESEARCH MANAGEMENT SYSTEM

MONITORING PROCEDURES

AI Employee Conduct- EDGE Access

AI employees may, by virtue of their role as the EDGE Coordinator, EDGE Developer or ACRC Project Management Staff, have assigned to them Lead Administrative Roles in the EDGE Clinical Research Management System. Additionally they may have administrative privileges for areas designated for the use of other organizations, only for the purposes of site set-up and system customization. Each AI employee is responsible to ensure that they are not accessing any organizational area past the time that the super-user has been authorized to manage the organizational site. At this time, administrative access will be revoked from AI employees. When using EDGE, AI employees should follow the privacy considerations outlined in the EDGE training presentation and privacy quiz.

AI Employee Conduct- Technical Support

AI Employee Super-Users may request technical support from AI employees and should provide express written permission (email). Using online screen-sharing, the Super-User should be able to demonstrate the technical request without providing access to the organizational site to the AI employee. For all technical requests that require direct access into project records where administrative privileges will have to be granted, these technical requests should be routed to the EDGE-UK development team and AI will only be notified once the request has been resolved.

Monitoring and Audit Responsibilities

*Of note, after initial configuration and set-up of an organization in EDGE, AI and ACRC do not have access to authorized user lists, access controls or training records of employees outside of their own organization. AI monitoring of the activities of other organizations in EDGE is only possible through the participation and compliance of each organization's EDGE Lead Local Administrators and Super-Users. The confidentiality and data sharing agreement signed between participating organizations outlines the expected responsibilities and conduct related to sharing this information.

- The site administrator at each sub-licensee will keep up-to-date details of all their organization's users. It is the responsibility of the sub-licensee and the site administrator to ensure that each end user successfully completes the EDGE privacy training and complies with applicable policies, procedures and legal requirements. Updating access controls is managed by the site administrator.
- A list of all authenticated users is maintained in EDGE. As per the executed sub-license agreement, the partner site retains the responsibility for managing its list of authorized users and ensuring that only such users access EDGE.

Authorized User List

AI Internal

All EDGE accounts for AI employees will be activated when appropriate by the EDGE Developer. Monthly monitoring of the number, status, and privileges assigned to EDGE accounts for AI employees will be performed the ACRC Manager. In the event of any irregularities, the ACRC Manager will request suspension of the relevant EDGE account by the EDGE Developer.

AI External

As part of due diligence, the EDGE Developer will request bi-annually from all Super-Users, or Lead Local Admin, a list of all authorized users from their respective organizations.

Any irregularities such as non-registered email domains (not @ahs.ca or @ualberta.ca), generic email accounts (pharmacy@ahs.ca), will be flagged for follow-up.

Any irregularities in access controls (ie. granting admin access to many individuals) will be flagged for follow-up.

As part of due diligence, the EDGE Developer will request quarterly reports from all Super-Users, or Lead Local Admin, verifying that all authorized active EDGE users have signed the End User Agreement/IMA and completed the privacy quiz. If needed, this record will be reconciled against the internal record of course completion collected at AI upon completion of the privacy quiz.

It is the responsibility of the EDGE Developer to send a request to the submitting Super-User or Lead Local Admin to investigate the irregularity and provide a response.
The EDGE Developer will recommend suspending the accounts of all individuals identified as not having completed the Privacy Quiz and/or signing the End User Agreement/IMA until such time as they have both been completed. Account suspension or termination will be at the discretion of the Lead Local Admin or Super-User or, if required such as when a conflict of interest is identified, the organizational signatory identified on the relevant Sub-license agreement.

Any irregularities requiring potential breach investigation should be investigated in reference to the EDGE-Alberta Privacy Breach Management Policy.