Western
Research

Electronic System Compliance Review – Western Research Ethics Manager (WREM)

Regulatory Compliance

Electronic Submission of Documents

WREM is a web-based electronic research management system driven by Infonetica's ERM software. Infonetica follows the Agile style development cycle, verification and validation. Validation is an integral part of their development. Once a user story is written, they begin developing the acceptance criteria and acceptance tests required to validate each user story. When a developer is given a user story to work on they can use the acceptance tests along with any other information (i.e. mock-ups) and the written requirements to ensure what they build is according to the specifications provided. When they finish development, they go through testing to ensure their work meets all requirements. After this the code is pushed to a test server where the Business Analyst performs their own validation using the acceptance tests before signing off on the piece of work.

Electronically signed regulatory documents are generated in compliance with 21 CFR Part 11: Electronic records and Electronic signatures. Signatories are required to log on WREM using a unique username and password in order to access the signature module. The username and password need to be re-entered at the time of signing. The signed date and time are logged in a secure electronic audit trail.

WREM allows for the electronic submission of applications and documents for research ethics review and oversight by one of Westerns Research Ethics Boards (REB).

All research ethics application materials, including all documents for review, must be submitted electronically via WREM. WREM has been developed in partnership with Infonetica Ltd. This continued relationship ensures that WREM will be continuously monitored and maintained to meet the needs of researchers and REBs across the province.

Documents for review include but are not limited to the following, as applicable, along with updates to these materials as available:

- Protocol(s)
- Investigator Brochures (IB), Product Monographs (PM) and/or Device Manuals
- Health Canada No Objection Letter/Notice of Authorization
- Proposed study budget
- DSMB/C charter
- Informed consent/assent forms and/or debriefing scripts
- recruitment materials
- Surveys, questionnaires and/or interview/focus group scripts
- Reportable event supporting documents
- Translated materials and certificates

Secure User Authentication

The Western WREM administrator must first approve users before they are provided access to the WREM system. All users are required to enter a username and password to access the system. The system uses strong passwords of 8 characters with at least one uppercase, one lowercase and one numerical value. User accounts are tied to levels of access according to user roles to ensure a controlled and secure environment. No duplicate emails are permitted, and users are not allowed to share the account information.

System Security

All data transferred between the user's device and WREM is encrypted using SSL. WREM is connected publicly to the internet, but all data transferred between the user's device and WREM is encrypted using SSL and must be accessed through a secure HTTPS connection which is only made after the user has successfully authenticated. No plain text transmission of passwords or other sensitive data is permitted. Other security measures implemented include the locking out of accounts after 5 unsuccessful login attempts, and access time-out for inactive users after 60 minutes of inactivity.

WREM uses a secure SQL database for data storage. The system is hosted on Western's own servers. System protection is provided through a combination of physical security at the data centre, network security via firewalls, and security measures within the application itself. Backend access, to either the database or the file system, is only available to authorized system administrators.

Access through apply.westernrem.uwo.ca requires that each user be manually assigned an appropriate role or have the application form manually shared with them. Roles provide a user with access and permissions for the entire study period; different roles have different levels of access (what a person can see) and permissions (what a person can do). Sharing provides access and permission on a single form; the person sharing the form manually selects the permissions for the recipient user.

Access to the review side of WREM is controlled by the Office of Human Research Ethics (OHRE) in coordination with the designated REB contact (e.g., Administrative Assistant, REB Manager or Director).

Database and log access for WREM is restricted to WREM System Administrators and Infonetica authorized staff. An audit log is generated by WREM to monitor application and document access.

Full data back-up and disaster recovery procedures are in place to ensure the safety, security and operation of the system. In addition, an independent security assessment company carries out the penetration test of the system on behalf of Infonetica to identify any potential vulnerabilities on the system that an attacker could exploit.

System Details

System validation is in place to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records?

Yes. Logs are maintained on user log in, downloads, various actions on the study (e.g., when users were given access and by whom, application of signatures, correspondence to and from the REB of Record, etc.). Essential components of the application have been tested for accuracy, reliability, and functionality using specific test cases. Test cases validate functions on a screen work correctly; added records function as intended; input data is accurate when viewed; user access is limited to role, etc. Test cases are authored by OHRE staff members. The test cases are run by OHRE staff members, users from Western and its affiliates (e.g., Lawson)/REB (via User Acceptance Testing).

Accurate and complete copies of records are available in both readable and electronic form?

Yes. Records are up-to-date, accurate, and complete to the extent that data has been entered into WREM. Applications can be viewed electronically or printed by users with the appropriate access.

Records are protected to enable their accurate and ready retrieval throughout the records retention period?
Yes. The individual records along with the audit trail data needed to reproduce the entire record history are stored for the entirety of the retention period.
System access is limited to authorized individuals?
Yes. All users are required to enter a username and password (8 or more characters with at least one uppercase, one lowercase and one numerical value) to access WREM. In order to gain access to a study (or a form within a study), the individual must be given access by the project owner or a user who already has access. Users can only give access/permissions that are the same or lesser than their current access (i.e., a user cannot give a greater level of access then they have).
Checks are done to ensure that only authorized individuals use the system?
Yes. Users must have an active account to access WREM. Audit logs track user access to the system. The 'collaborators' tab of the application displays any user with access/permission on a particular form. The OHRE receives automatic notification of any individual attempting to log into the 'wrong' side of the system (e.g., someone with applicant access attempting to log in to the REB portal) and for any individual without an account who attempt to access the REB side. Logs are maintained on user access, including successful and unsuccessful log-in/log-out attempts. Infonetica Ltd. also conducts independent threat risk assessments.
Secure, computer-generated, time-stamped audit trails are available to independently record the date and time of operator entries and actions that create, modify, or delete electronic records, maintained?
Yes. Reports and audit logs will provide this information.
Record changes do not obscure original entries?
Yes. All versions of an application form and any attached document submitted to the REB are maintained and accessible.
Operation system checks are done to ensure that the permitted sequencing of steps and events are accurate and that the data is valid?
WREM has workflow routing with a standardized sequence of steps that must be followed. The smart form features within WREM ensure that data is entered for all questions identified as mandatory. The Principal Investigator is responsible for ensuring the accuracy of information provided to the REB of Record.
Persons who develop, maintain, or use electronic record systems have the proper education, training, experience to perform their tasks (training logs)?
Training is provided to OHRE staff and on an ongoing basis as required. The OHRE provides regular web-based training sessions open to all members of the research community. User manuals are available to research teams and the Western Research Ethics Boards.
Policies are in place to hold individuals accountable for actions initiated under their electronic signatures in order to deter record and signature falsification?
WREM uses an electronic signature tied to individual user accounts. Each user has a unique user ID and password with the policy that user account information must not be shared. WREM displays any signature that is requested (if applicable) and applied, including by whom, when and the status of the current signature. Any applied signature is automatically invalidated if the form is unlocked at any point after signature is applied. This information is displayed to any user with access to the applicable form.

As described in the Terms and Conditions and Privacy Policy, users may only use WREM for lawful purposes related directly to the use of the WREM. Individuals may not use, and shall take all reasonable steps to ensure that no other person uses, WREM in a way that does not comply with the terms of any laws or that is in any way unlawful. Users are responsible for keeping their password and user details confidential. Should the OHRE identify or otherwise become aware of concerns around the falsification of an electronic signature, the user’s account would be suspended and the designated institutional representative(s) at the participating site would be notified.
SOPs/instruction manuals are in place to ensure there is appropriate control over the distribution, access, and use of the system?
Yes. Links to this information are available on the Western human research ethics website (https://www.uwo.ca/research/ethics/human/WesternREM.html) and documentation of Infonetica’s security and testing policies is available upon request. User access control is also described above.