Investigator Site File Assessment Form/F

About the ISF Assessment…

This Form/F allows a site to assess the GCP compliance of their Electronic Investigator Site File (eISF) system. Sponsors and sites will use the assessments to discuss any risks and appropriate solutions.

Investigator Site

Please complete this form if your Investigator Site File System is or will be used to hold essential records for Clinical Trials.

Date of ISF Assessment Completion

Day | Month | Year

Your Institution

Address line 1

line 2

City

State / Region

Postal Code

Country

Official Institution Name

Official Site Name (*within institution*)

Centre Number *(Optional)*

	User Contact Details	Backup User Contact Details
First name		
Last Name		
Phone Number (*optional*)		
E-mail Address		
Role		

System Details

System Name: Alfresco Community (MidtX)

Developer/Vendor Company Name: HYLAND Alfresco Community

Version Number: 7.2.0

Release Date: Day - Month - Year 2022

Is your system hosted (web-based) or on-site (local)? On-site. Alfresco share v. 14.96, Alfresco community 7.2.0

eInvestigator Site File Criteria

Please provide an answer for each question in order for the assessment to be considered complete.
Note: Multiple roles within your organization may be needed to complete this form, such as study coordinator and site IT, or other roles.

Assessment Question	*Investigator Site Response*	*Comment -- If response is "No", additional information and/or plans to correct deficiencies are required. (Max = 120 char)*

Audit Trail

1. Does the system have a readable, readily available, and indelible audit trail to include recording date/time/originator?

- (●) *Yes*
- ( ) *No **

Note. *Site must ensure that audit trail (audit log) functionality has been installed and is working correctly. If an appropriate audit trail is not available, additional process controls, such as a signed and dated print out will have to be introduced to maintain the information.*

2. Does the audit trail include the reason for any record change or deletion if this is required by regulation in your region?

- ( ) *Yes*
- (●) *No**
- ( ) *N/A*

There is no way to register the reason for a change

3. Does the system audit trail include record viewing and downloading?

- (●) *Yes*
- ( ) *No*

Only file based logging, must be requested two businessdays in advance.

Note. *If an appropriate audit trail is not available, additional process controls, such as a signed and dated print out, will have to be introduced to maintain the information.*

4. Are there processes and/or system controls in place that prevent the modification of the audit trail, turning off the audit trail, or changing system date/time?

- (●) *Yes*
- ( ) *No*

This can only this be done by a administrator.

Note. *This may be handled via the site operating system and associated procedures or via a hosting vendor. The site should ensure the method employed is working.*

5.^ Does the system and/or process adequately provide for identifying the local time?

- (●) *Yes*
- ( ) *No*
- ( ) *N/A*

We use a local timeserver, all log timestramps are in UTC.

Note. Where the system use may span time zones or the system may be located in a different time zone than where the study is being conducted, the time zone of the investigative office should be used in the audit trail, or there must be a clearly documented consistent way to derive the local time from the timestamp on the audit trail.

Access Control

6. Does the system have the ability to create, maintain, apply and revoke the roles, access permissions and capabilities of each user that accesses the system, such that users have access only to those system functions and data that are appropriate to their role?

- (●) *Yes*
- ( ) *No **

Roles are assigned indivially and the users handled by the company IDM.

Note. *Sites must ensure that accounts are configured so that users have access to only those features that they should have access to (often referred to as roles). Also, there should be an administrator to grant accounts to users upon justification of their need for an account. A process should be in place to ensure that access is removed when an employee no longer has justification for using the system (such as getting assigned to a different area or leaving the organization). If you are using a hosted system, be sure that the vendor will provide the user administration and that you understand and employ the process for obtaining and removing accounts.*

7. Is there a process to periodically produce and review a list of all users, including past users, their access level/rights and the start and end date of these access rights?

- (●) *Yes*
- ( ) *No*

The user list must be reviewed at least twice per year.

8. Is there a policy/procedure/training that each account is assigned to one dedicated user and that instructs users not to share their account or to leave their account open for others to use?

- (●) *Yes*
- ( ) *No*

The users are controlled by company IDM.
The company security guidelines forbids that users share credentials etc.

9.^ Is there a system and/or process to ensure the investigator has oversight of and continuous access to eISF records for the full retention period?

- (●) *Yes*
- ( ) *No **

When the auditor has a Regional-id assigned by the IDM, he/she can be granted a rolebased access to site in question.

Assessment Question	Investigator Site Response	Comment -- If response is "No", additional information and/or plans to correct deficiencies are required. (Max = 120 char)

10. ^ Can the monitor, auditor and inspector, within reasonable timeframe, obtain direct access to eISF records in order to perform their regulatory duties?

(●) Yes ( ) No

Monitor, auditor or inspector can have a Regional-id assigned by the IDM, the can be granted a rolebased access .

Note. The investigator (or appropriate delegate) should be available to browse the records on demand in case of audit, inspection or for monitoring purpose. It is recommended this requirement be part of the contract between the sponsor and the investigator (or the study center).

11. ^ Is there a documented site procedure in place to ensure study staff are not unintentionally unblinded in studies where this is a requirement?

( ) Yes ( ) No ( ) N/A

Local procedure

Note. If your site does now or may in the future handle blinded studies, this question must be answered. For example, information on pharmacy distribution should not be available for study staff to see.

12. Is there a limited number of unsuccessful log-in attempts permitted by the system?

( ) Yes (●) No *

MidtX has basic authentication only. Unsuccessful login attempts are handled through RM Citrix, which require MFA

Note. An example of an unsuccessful log-in attempt is a forgotten password. This may be handled via the site operating system and associated procedures or via the EHR system. Site must ensure that this feature is installed and turned on.

13. Does the system keep a log of unauthorised access attempts and is there a process in place to periodically review the log of unauthorised access attempts?

(●) Yes ( ) No

Yes, but there is no periodic review of the log.

Note. An example of an unauthorised access attempt is a hacking attempt. This may be handled via the site operating system and associated procedures or via the EHR system. Site must ensure that this feature is installed and turned on.

14. Does the system require secure access via (Check all that apply)

Access requires login through the Regions Citrix or local domain pc.

- [x] Required password change (indicate interval in the comment block)
- [ ] Fingerprint
- [ ] Face recognition
- [ ] Device (e.g. smart phone code)
- [x] Single Sign-on
- [ ] Same Sign-on
- [x] Other Two factor authorization

Note. Site must ensure that this feature is installed and turned on. If access is provided via a password, site is responsible for establishing reasonable intervals. If managing password updates via a process, the site must provide and enforce a documented site process requiring password change.

15. Is there a process that in case of security incident that exposes privacy data, the sponsor and relevant data protection supervisory authority are notified?

(●) Yes ( ) No

16. Is there an automatic log-off or other access lock (e.g., password protected screen saver) after a period of inactivity?

(●) Yes ( ) No *

Screen saver on the pc expires after 10 minutes
MidtX disconnects unused sessions after 2 hours.

Note. Site must ensure that this automatic feature is installed and turned on. If using password protected screen-saver function from your laptop or desktop system to satisfy this requirement, users should not have the ability to turn off the password-protected screen saver functionality.

Data Backup, Retention and Recovery

17. Are there sufficient system and/or process controls for backup and recovery procedures, that includes documentation that can be produced for inspection by a monitor, auditor or inspector?

(●) Yes ( ) No *

Note. This may be handled via the site operating system and associated procedures or via the eISF system.

18. Are there process or system controls in place to ensure that the eISF documents and associated metadata (including audit trail), continue to be available, are human-readable and understandable, and are retained in an archive for the legal period?

(●) Yes ( ) No *

Audittrail and logfiles are kept in a database, and can be extracted on request.
Documents are kept in a file system.

Note. Sites are responsible for knowing the legal retention period for clinical research source records and for ensuring that methods employed to meet this requirement are working.

19. ^ Is there a documented process for continuing operations if the system is not accessible?

( ) Yes (●) No

This is handled by local procedures.

Note. There should be a documented site process/plan describing how to handle an emergency or unexpected shutdown. Site should have access to these documents. The site should confirm and request immediate remediation if there is nothing already in place and/or if the process has not been tested.

Assessment Question	Investigator Site Response	Comment -- If response is "No", additional information and/or plans to correct deficiencies are required. (Max = 120 char)

20. Is there a documented and tested process for recovery from a disaster and/or an unexpected system unavailability?

○ Yes
◉ No

Note. *The group responsible for backups, recovery plans for the system software/hardware (whether it is your IT department or a vendor) should have a documented site process describing how recovery from an emergency or unexpected shutdown will be handled and proof that this process was tested. Site should have access to these documents.The site should confirm and request immediate remediation if there is nothing already in place and/or if the process has not been tested.*

System Development & Maintenance

21. ^ Are there documented records showing that those maintaining or using the system are qualified (have the necessary training and experience to be able to perform their assigned tasks)?

◉ Yes
○ No

The technicians have several years of experience on the technical platform. PI is responsible for site staff.

22. Does the site utilise a process to demonstrate that the development, hosting, deployment and maintenance (e.g. system changes) of the computerised system is sufficiently validated and documented?

◉ Yes
○ No *

System changes are controlled through a documented ITIL framework.

23. Are there processes to address computerised system incidents through to their resolution?

◉ Yes
○ No

ITIL is partly implemented

24. Is there a process to periodically review and affirm the continued suitability of the computerised system taking into account the potential cumulative risks and impacts of changes to the system, requirements, version releases, and computing environment of the system?

◉ Yes
○ No

Partly

25 . Are there sufficient information security practices to manage, preclude, and report security issues?

◉ Yes
○ No

Note. *This may be handled via the site operating system and associated procedures. The site should ensure the method employed is working and documented. Site should check with their IT support that cyber security measures are in place and updated regularly.*

26. If electronic records are received from other systems (internal or external), are there appropriate technical or procedural controls to assure confidentiality and integrity of records received from these systems?

◉ Yes
○ No
○ N/A

there are no integrations to other systems, except IDM (AD and BSK)
All data is transferred manually by the users

27. ^ If this computerised system is provided by a Service Provider, are there formal agreements in place to clearly define 1) responsibilities of each party (Site and Service Provider and Service Provider's GxP-related subcontractors) and 2) oversight of the Service Provider?

○ Yes
○ No
◉ N/A

System is hosted on-prem

Note. *The department responsible can achieve this by an appendix to the contract, an SLA (Service Level Agreement), or in a "statement of work" that can be downloaded from the vendor website.*

28. If electronic signatures are used in this system to fulfill clinical research requirements, are all of the following true: 1) it is permanently linked to its respective record, 2) it includes the name of the signer, 3) it includes the time and date of e-signature execution, 4) the meaning associated with the e-signature is indicated (e.g., creation, confirmation, approval), 5) system can recognise if a record has been altered and make the signature invalid

○ Yes
○ No *
◉ N/A

ADDITIONAL INFORMATION

Additional Comments from Site

MidtX has been risk & secuty evaluated, August 2024, by Central Denmark Region (in danish, for internal use only).

I have assessed this completed document and I accept the risks and mitigations identified in this document as per ICH E6 R3 2.12.10 and 3.16.1 vi and vii.

Principal Investigator signature and date

Based on clinical research regulations and guidances, it is strongly recommended to mitigate this item, dependent on the nature of the study, prior to using eSource from this system.

^ indicates a process question that must be answered if the site is using a previously completed eISF assessment or Form/F from another part of their organisation.

Instructions and License Agreement pertaining to this Assessment can be found in the eSRA Handbook which can be downloaded from https://eclinicalforum.org/site-sys-assts.

