What to look for in an IRT (Interactive Response Technology) audit trail review

User Access and Authentication

1. **Complete and Accurate Logs**: Ensure that all user access logs are comprehensive and accurate. For example, verify that logs show when users logged in and out, and that there are no missing entries.
2. **Timely Account Requests**: Check that user accounts are requested and approved in a timely manner. For instance, new clinical team members should have their accounts set up before they start working.
3. **Proper Use of Accounts**: Confirm that accounts are used correctly, such as ensuring that users are not sharing accounts.
4. **Solid Authentication Processes**: Verify that user authentication methods (e.g., passwords, two-factor authentication) meet regulatory standards.
5. **Frequent Account Updates**: Regularly update account lists and deactivate accounts that are no longer in use, such as those of former clinical team members.

Data Entry and Modifications

1. **Review Logs for Entries and Changes**: Examine logs to ensure all data entries and modifications are recorded.

2. **Timestamp and User Linkage**: Ensure each data entry and modification is timestamped and linked to a specific user.
3. **Justification and Documentation**: Verify that any changes to data are justified and properly documented. For example, if a data entry is corrected, there should be e.g. a Note to File explaining why the change was necessary.

System Configuration Changes

1. **Log Checks for Configuration Changes**: Review logs for any changes to system settings.
2. **Authorization and Documentation:** Ensure that configuration changes are authorized and documented. For instance, a change in system settings should have an approval from a senior team member.
3. **System Integrity and Data Security:** Verify that changes do not compromise system integrity or data security. For example, a change in data storage settings should not make the data vulnerable to unauthorized access.

Audit Trail Integrity

1. **Secure and Tamper-Proof Audit Trail:** Ensure the audit trail is secure and cannot be tampered with.
2. **Complete Audit Trail:** Verify that the audit trail is complete and includes all necessary information.
3. **Check for Gaps and Inconsistencies:** Look for any gaps or inconsistencies in the audit trail. For example, there should be no missing entries or unexplained anomalies.

Compliance with Regulatory Requirements

1. **Regulatory Compliance**: Ensure the audit trail review process complies with relevant regulations, such as FDA 21 CFR Part 11, ICH and EMA guidelines for computerized systems.
2. **Document Review Process and Findings**: Document the review process and any findings in a way that meets regulatory standards. For example, keep detailed records of the review process and any issues identified.

Incident Investigation and Resolution

1. **Investigate Anomalies**: Investigate any anomalies or suspicious activities found during the review.
2. **Document Investigation and Actions**: Document the investigation process and any actions taken to resolve issues. For instance, if an unauthorized access attempt is detected, document the steps taken to address it.
3. **Implement CAPA**: Implement corrective and preventive actions (CAPA) as needed to prevent future issues.

Best Practices for Conducting an IRT Audit Trail Review

1. **Regular Reviews**: Conduct audit trail reviews regularly, such as quarterly or biannually, depending on the complexity of the study counting from the IRT Go-Live.
2. **Training**: Ensure everyone involved in the review process is properly trained and understands the importance of audit trail reviews.
3. **Thorough documentation**: Keep thorough documentation of the review process, findings, and any corrective actions taken.
4. **Continuous Improvement**: Use findings from audit trail reviews to continuously improve system processes and security measures.