Trace Matrix

* BR 9.2: The system will create requestor user accounts by integrating into active directory
* BR 3.8: The system shall be able to route and track revisions to preventative maintenance plans.
* BR 7.2: The system shall provide standard reports, as well as the ability for a user to create and save searches.
* BR 4.50: The system shall provide authorized users a method to generate and review audit trail reports of work orders.
* BR 3.10: The system shall be able to calculate due dates for preventive maintenance.
* BR 10.1: The system shall provide the ability to interface with active directory
* BR 8.1: The system shall provide security to allow or disallow functionality on the system level, site level, and user level.
* BR 3.5: The system shall be able to store equipment numbers and corresponding detailed information
* UR-REG-36: The system must record the creation, change, and cancellation of access authorizations. (§11.300d, Annex 11 12.3, MHRA Data Section).
* UR-REG-35: The system must not allow users to amend or switch off the audit trail. (§11.10e, Annex 11 9, MHRA Audit Trail Section)
* UR-REG-34: The system audit trail must provide secure (not editable), date and time-stamped record of the action (obtained from a secure, reliable source, i.e. the server and not the client PC) and the identity of the operator any time an electronic record is created, modified, or deleted. (§11.10e, Annex 11 8.2, 9, 12.4, MHRA Audit Trail section; PDA Data Integrity Code of Conduct 3.3.1.3)
* UR-REG-33: The system must incorporate and maintain audit trails which record all relevant changes and deletions, with changes not obscuring previously recorded information, including changes executed by the system administrator.  The reason for the change or deletion must be documented.  The system must be able to generate printouts of the audit trail. (§11.10e, Annex 11 8.2, 9, MHRA Audit Trail section; EMA Q8, Q15, MHRA Raw Data Section)
* UR-REG-27: The system must demonstrate access levels granted to users and historical information regarding user access level and track any changes to system-specific accounts, privileges, and roles in the system. (§11.10d , Annex 11 12.1, MHRA Computerized System User Access section)
* UR-REG-25: The system must allow administrator to assign appropriate privileges to each user account. (§11.10d, Annex 11 12.1)
* UR-REG-24: The system must support individual user accounts/access, including unique logins for system administrators, to allow actions in the audit trail(s) to be attributed to a specific individual. (§11.10d, 2.1, MHRA Computerized System User Access section)

|  |  |
| --- | --- |
| URS ID # | Description |
| BR 9.2 | The system will create requestor user accounts by integrating into active directory |
| BR 3.8 | The system shall be able to route and track revisions to preventative maintenance plans. |
| BR 7.2 | The system shall provide standard reports, as well as the ability for a user to create and save searches. |
| BR 4.50 | The system shall provide authorized users a method to generate and review audit trail reports of work orders. |
| BR 3.10 | The system shall be able to calculate due dates for preventive maintenance. |
| BR 10.1 | The system shall provide the ability to interface with active directory |
| BR 8.1 | The system shall provide security to allow or disallow functionality on the system level, site level, and user level. |
| UR-REG-36 | The system must record the creation, change, and cancellation of access authorizations. (§11.300d, Annex 11 12.3, MHRA Data Section). |
| BR 3.5 | The system shall be able to store equipment numbers and corresponding detailed information |
| UR-REG-35 | The system must not allow users to amend or switch off the audit trail. (§11.10e, Annex 11 9, MHRA Audit Trail Section) |
| UR-REG-34 | The system audit trail must provide secure (not editable), date and time-stamped record of the action (obtained from a secure, reliable source, i.e. the server and not the client PC) and the identity of the operator any time an electronic record is created, modified, or deleted. (§11.10e, Annex 11 8.2, 9, 12.4, MHRA Audit Trail section; PDA Data Integrity Code of Conduct 3.3.1.3) |
| UR-REG-33 | The system must incorporate and maintain audit trails which record all relevant changes and deletions, with changes not obscuring previously recorded information, including changes executed by the system administrator.  The reason for the change or deletion must be documented.  The system must be able to generate printouts of the audit trail. (§11.10e, Annex 11 8.2, 9, MHRA Audit Trail section; EMA Q8, Q15, MHRA Raw Data Section) |
| UR-REG-27 | The system must demonstrate access levels granted to users and historical information regarding user access level and track any changes to system-specific accounts, privileges, and roles in the system. (§11.10d , Annex 11 12.1, MHRA Computerized System User Access section) |
| UR-REG-25 | The system must allow administrator to assign appropriate privileges to each user account. (§11.10d, Annex 11 12.1) |
| UR-REG-24 | The system must support individual user accounts/access, including unique logins for system administrators, to allow actions in the audit trail(s) to be attributed to a specific individual. (§11.10d, 2.1, MHRA Computerized System User Access section) |