PharmOut

Part 11 Supplier Assessment Checklist

1. Controls for Closed Systems

21 CFR Part 11 Requirement 11.10 (a) - “Validation of systems to ensure accuracy, reliability, consistent intended performance and the ability to discern invalid or altered records.”

Expectation - The system is validatable in accordance to GAMP 5 or equivalent standard.

Supplier Question	**Response**
Can you supply documents in accordance to the Software Development Life Cycle (SDLC) set out in GAMP 5? That is, supply evidence that the system accords to the User Requirement Specification (URS) supplied and that this is traceable to system design requirements and functional specifications.	
Are you willing to undergo a supplier audit either personally by PharmOut staff or their delegate; or by postal audit questionnaire?	
Does the system have an audit trail and is this audit trail accessible for reporting purposes?	
Can you supply information regarding any system upgrades, fixes, or services packs so that all changes to the system are fully understood?	
Are you willing to perform system changes in accordance to our change control procedure?	
Can you provide PharmOut with test scripts for unit, integration, system, Installation Qualification, Operational Qualification, or regression testing?	

21 CFR Part 11 Requirement 11.10 (b) - “The ability to generate accurate and complete copies of records in both human readable and electronic form for inspection, review and copying by the agency.”

Expectation - Accurate and complete copies of electronic records in human readable form are accessible.

Supplier Question	Response
Is the data accessible in human readable form in both hard and electronic copy?	
Is the related metadata accessible in human readable form in both hard and electronic copy? Eg. audit trails, configuration information, methods, and user information.	

21 CFR Part 11 Requirement 11.10 (c) - “Protection of records to enable their accurate and ready retrieval throughout the records retention period.”

Expectation - Data can be backed up and retrieved readily. The system will be able to read and print data created in previous versions of the system for the length of the data’s retention period.

Supplier Question	Response
Are you able to provide, or aid in the development of, backup and restore procedures for both the data and its associated metadata?	
Are you able to provide assurance that the data and its associated metadata will be maintained over the retention period regardless of upgrades to the software or operating system?	

21 CFR Part 11 Requirement 11.10 (d) - “Limiting system access to authorised individuals”.

Expectation - The system limits user access according to pre-configured rules that can be maintained.

Supplier Question	Response
Is access to the system limited to authorised individuals?	
Are there multiple user access levels available?	

Supplier Question	Response
Is the system protected from unauthorised access by a user ID / password system?	
Is there an auto disabling of the account after "n" unauthorised attempts?	
Is there a security mechanism that logs and notifies management of unauthorised use of user accounts?	
Are users accounts protected from deletion and can only be made inactive if no longer required?	
Can password rules be enforced via the system? Eg. password length, expiry, type of characters used, etc.	

21 CFR Part 11 Requirement 11.10 (e) - "Use of secure, computer generated, time stamped audit trails to independently record the date and time of operator entries and actions that create, modify or delete electronic records. Record changes shall not obscure previously recorded information."

Expectation - The system has an audit trail that records and maintains the required information.

Supplier Question	Response
Is there a computer generated audit trail?	
If so, is the computer generated audit trail always on, that is, can it be turned off by system administrators or operators?	
Does the audit trail function independently of operators?	
Does the audit trail record the date, local time, and operator name and provide an indication of all operator entries, for example, creation, deletion, and modification?	
Does the audit trail functionality allow users the opportunity to enter a reason for operator action?	

Supplier Question	Response
Does the system electronically retain original entries when the entries have since been amended or deleted?	
Does the system security protect the audit trail from accidental or intentional modification, moving or deletion of electronic records?	
Are you able to provide assurance that the audit trail will be maintained over the retention period of its associated data regardless of upgrades to the software or operating system?	
Can the audit trail be accessed in human readable form in both hard and electronic copy?	

21 CFR Part 11 Requirement 11.10 (f) - "Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate."

Expectation - The system should allow operations to be set in a pre-defined order if necessary.

Supplier Question	Response
If required, does the system enforce permitted sequencing of steps and events?	
Is the sequencing mechanism automatic and independent of the user?	

21 CFR Part 11 Requirement 11.10 (g) - "Use of authority checks to ensure that only authorised individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand."

Expectation - The system limits user access according to pre-configured rules that can be maintained.

Supplier Question	Response

Supplier Question	Response
Does the system ensure that only authorised users can use the system, electronically sign a record, alter records, or perform other operations?	

21 CFR Part 11 Requirement 11.10 (h) - "Use of device (eg: terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction."

Expectation - If required the system will ensure the use of certain devices as sources of data and/or commands

Supplier Question	Response
If required, does the system enforce requirements that only certain devices can be used as the source of data and/or commands?	

21 CFR Part 11 Requirement 11.10 (I) - "Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training and experience to perform the assigned tasks."

Expectation - All users of the system will be trained.

Supplier Question	Response
Can you supply training and/or training manuals to ensure users are trained to the level expected to ensure proper use of the system?	
Can you supply training directed at various levels of access to the system? I.e., general users, key users, administrators, and technical support as appropriate?	

21 CFR Part 11 Requirement 11.10 (k) - "Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit trail that documents time sequenced development and moderation of systems documentation."

Expectation - Changes to system documentation should be controlled and ideally captured in an electronic audit trail.

Supplier Question	Response

Supplier Question	Response
Is there an audit trail that captures changes made to on line documentation?	
Does this audit trail comply with the requirements in 11.10 (e)	

2. Controls for Open Systems

21 CFR Part 11 Requirement 11.30 - "Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt."

Expectation - If there's no ability to control user access via a User ID and password system, the system must encrypt the data.

Supplier Question	Response
Is data able to be encrypted?	
Are digital signatures used?	

3. Signature Manifestations

21 CFR Part 11 Requirement 11.50 (a) - "Signed records shall contain information associated with the signing that clearly indicates the printed name of the signer, the date and time of signature execution, and meaning associated with the signature:"

11.50 (b) - "The items identified above (11.50 (a)) shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record."

Expectation - When an electronic signature is used information regarding the operator and the reason for signing must be displayed.

Supplier Question	Response

Supplier Question	Response
Do signed electronic records contain the following related information? The printed name of the signer. The date and time of signing. The meaning of the signing (such as approval, review, and responsibility).	
Is the above information shown on displayed and printed copies of the electronic record?	

4. Signature/record linking

21 CFR Part 11 Requirement 11.70 - “Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.”

Expectation - The system must not allow the link between the electronic signature and electronic record to be removed in any way.

Supplier Question	Response
Are signatures linked to their respective electronic records to ensure that they cannot be cut, copied, or otherwise transferred?	

5. Electronic Signatures – General Requirements

21 CFR Part 11 Requirement 11.100(a) - “Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.”

Expectation - The system must enforce uniqueness of User IDs and passwords

Supplier Question	Response
Does the system ensure that each User ID is unique and cannot be duplicated?	
Does the system ensure that User IDs and passwords cannot be reused or reassigned to another user?	

21 CFR Part 11 Requirement 11.200 (a) (1) - "Electronic signatures that are not based upon biometrics shall: Employ at least two distinct identification components such as an identification code and password."

Expectation - The system uses two components to execute an electronic signature.

Supplier Question	**Response**
Does the system use at least two distinct components when executing an electronic signature?	
What are these two components?	

21 CFR Part 11 Requirement 11.200 (a) (1) (i) - When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components. Subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual."

11.200 (a) (1) (ii) - "When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components."

Expectation - The system should enforce the entering of both components of the electronic signature at the first signing and the password for each subsequent signing is a continuous session. Both components of an electronic signature must be executed if subsequent signing occurs in a non continuous session.

Supplier Question	**Response**
Are both components of the electronic signature executed at the first signing of a session?	
When several signings are made during a continuous session, is the password executed at each signing?	
If signings are not done in a continuous session, are both components of the electronic signature executed with each signing?	

21 CFR Part 11 Requirement 11.200 (a) (3) - "Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals."

Expectation - The system is designed such that only the user can know both components of an electronic signature.

Supplier Question	Response
When a user is added to the system, does the system enforce a password change at first logon?	
When viewing a user's system account details, is the password component not viewable on screen?	

21 CFR Part 11 Requirement 11.200 (b) - "Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners."

Expectation - The system enforces uniqueness of biometric signatures.

Supplier Question	Response
Are the biometric identifiers based on measurements of unique individual physical features?	
What is the biometric identifier used in this system?	

21 CFR Part 11 Requirement 11.300 (b) - "Ensuring that identification code and password issuances are periodically checked, recalled, or revised (eg. to cover such events as password aging)."

Expectation - The system should enforce changing of password at predefined periods. Removal of obsolete Users ID and passwords should not remove the record of their historical use.

Supplier Question	Response
Does the system force passwords to be periodically changed?	
If a user account is rendered inactive, is the history of that user account maintained?	

21 CFR Part 11 Requirement 11.300 (d) - "Use of transaction safeguards to prevent unauthorised use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorised use to the system security unit, and, as appropriate, to organisational management."

Expectation - The system has the technical means to deactivate accounts after an incorrect combination of User ID and password has been repeatedly entered. The system can notify administrators of attempted unauthorised use.

Supplier Question	Response
Does the system provide a mechanism for detecting attempts of unauthorised use and for informing the administrator or any other designated persons when such attempts occur?	
Does the system deactivate a user account after ‘n’ unauthorised attempts to log in?	
Does the system allow administrators to reactivate accounts if required?	

DOCUMENT END