



**Andara Life Science, Inc.
Vendor Assessment:
STATKING Consulting, Inc.**



Table of Contents

Purpose.....3

Assessment Process3

Terms/Acronyms4

Checklist5

Summary Report.....18

Purpose

Vendors or suppliers affect the quality of manufacturing, laboratory, clinical or software performance. It is the manufacturer's responsibility to ensure that the manufacturing processes of their vendors and subcontractors meet the appropriate standards and regulations that govern them.

According to FDA 21 CFR Part 820 for Medical Devices, manufacturers must develop relationships with their vendors, conduct vendor audits, and document certification and analysis to ensure that the materials and components provided meet their quality expectations.

The process typically involves:

- Identification of evaluation criteria based on the client's requirements. Areas to be evaluated include those related to production, operations and management:
 - Hardware/Software
 - Equipment
 - Processes and Operations
 - Quality Assurance procedures in place
 - Existing Documentation
 - Security
 - Maintenance
 - Training
- Identification of critical and significant issues required for the assessment
- Implementation of an official assessment of vendors
- Evidence of vendor quality assessment and review processes (could be vendor's validation documentation or a vendor checklist and audit)
- Equipment or software installation qualification with a complete and accurate verification

Assessment Process

Andara will conduct this vendor assessment by:

- Collecting any existing information related to quality plan
- Obtaining information from vendor via questionnaire
- Analyzing quality documentation practices and requirements
- Obtaining references from the vendor
- Collecting signatures to ensure agreement by all parties
- Providing a report to summarize assessment findings and identify any corrective actions

Terms/Acronyms

| Term | Definition |
|------------------------------------|--|
| Standard Operating Procedure (SOP) | A formal, written document approved by management, which adequately explains a procedure to be followed. SOPs are not mere guidelines. Vendor should have documented evidence that employees/contractors have been trained on SOPs. Failure to follow SOPs should result in disciplinary action against the employee/contractor. |
| Clinical Data | Identifiable information from or about an individual consumer including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) |

Checklist

| Vendor Assessment Checklist | | |
|---|---|----------|
| General Information and Signoff | | |
| <p>Vendor Information:</p> <p>STATKING Consulting, Inc. 759 Wessel Drive, Suite 6 Fairfield, OH 45014 (513) 858-2989 (513) 858-3022 statking@statkingconsulting.com</p> <p>Reviewer Information:</p> <p>Safis Solutions, LLC 351 West 10th Street, Suite 319 Indianapolis, IN 46202-4122 (317) 274-0505 (317) 278-4102 www.safis-solutions.com</p> | <p>I (We) certify that the information contained in the attached survey form is accurate and complete as of the date indicated. The completed checklist was reviewed by an Officer of the company surveyed. All parties signing this checklist agree with the responses. All information obtained will be kept confidential.</p> <p>Any necessary corrective actions will be taken by all affected persons. A re-audit and summary report will be provided to all parties.</p> <p>A vendor assessment will be performed on a regular basis.</p> | |
| | | |
| Signature | Title | Location |
| | | |
| Signature | Title | Location |
| | | |
| Signature | Title | Location |
| | | |
| Services Provided | | |
| <p>Brief Description:</p> <p>STATKING, in business since 1989, will provide data-related services for clinical trials performed to obtain regulatory approval of the new OFS medical device. To comply with FDA guidelines, they are a GCP environment.</p> | | |
| Questionnaire | | |



Vendor Assessment Checklist

The following Questionnaire includes information gathered on existing SOPs, system documentation, data security procedures, requirements analysis, testing procedures, and references.

Quality System Plan

| Quality System Documentation | Y | N | Notes |
|-------------------------------|---|---|-------|
| SOP: Validation Planning | | | |
| SOP: ER/ES | | | |
| SOP: Risk Management | | | |
| SOP: Vendor Management | | | |
| SOP: System Requirements | | | |
| SOP: Design | | | |
| SOP: Testing | | | |
| SOP: Traceability | | | |
| SOP: Change Control | | | |
| SOP: Implementation Plan | | | |
| SOP: Operational Support | | | |
| SOP: Training | | | |
| SOP: Change Management Plan | | | |
| SOP: Backup and Restore | | | |
| SOP: Record Retention | | | |
| SOP: Periodic Review | | | |
| SOP: Security Plan | | | |
| SOP: Security Administration | | | |
| SOP: System Retirement | | | |
| SOP: Business Continuity Plan | | | |
| SOP: Disaster Recovery Plan | | | |
| SOP: Master Document List | | | |
| SOP: Documentation Standards | | | |
| SOP: Vendor Assessment | | | |
| SOP: Risk Assessment | | | |

Quality System Activities

| Good Documentation Practices | Y | N | Notes |
|------------------------------|---|---|-------|
|------------------------------|---|---|-------|



| Vendor Assessment Checklist | | | |
|---|----------|----------|--------------|
| Each document is uniquely identified | | | |
| Unique titles summarize document purpose | | | |
| Signatures and printed names of approvers | | | |
| Revision history includes <ul style="list-style-type: none"> <input type="checkbox"/> Version number <input type="checkbox"/> Reason for revision <input type="checkbox"/> Name of reviser | | | |
| Approval date and time are documented | | | |
| Approval signature meanings documented | | | |
| ER/ES Management | Y | N | Notes |
| ER management <ul style="list-style-type: none"> <input type="checkbox"/> Records are in human readable form <input type="checkbox"/> Record retention process in place <input type="checkbox"/> Records are secure <input type="checkbox"/> Audit trail is provided and retrievable | | | |
| ES management <ul style="list-style-type: none"> <input type="checkbox"/> Unique user ID/password <input type="checkbox"/> Printed name of signer <input type="checkbox"/> Date and time stamp of signature <input type="checkbox"/> Security in place to prevent unauthorized use of ID/password | | | |
| Requirements Analysis | Y | N | Notes |
| Requirements are documented | | | |
| Functional requirements are included | | | |
| Security requirements are included | | | |
| ER/ES requirements are included | | | |
| Traceable to Design | | | |
| Traceable to Testing | | | |
| Traceability matrix exists | | | |
| Design Analysis | Y | N | Notes |
| Detailed Design Specifications included | | | |
| Programming Standards included | | | |
| Source Code Review procedures in place | | | |
| Testing Procedures | Y | N | Notes |
| Test Plan | | | |
| Test Cases/Scripts exist and are traceable to | | | |



| Vendor Assessment Checklist | | | |
|--|----------|----------|--------------|
| requirements and design | | | |
| Installation Qualification | | | |
| Functional testing | | | |
| Unit testing | | | |
| Integration testing | | | |
| Parallel testing | | | |
| System testing | | | |
| Acceptance testing | | | |
| Data conversion testing | | | |
| Regression testing | | | |
| Test Summary Report | | | |
| Training | Y | N | Notes |
| Resumes indicate knowledgeable personnel capable of performing operations correctly | | | |
| Training Records exist | | | |
| Change Management | Y | N | Notes |
| Method for handling changes is in place | | | |
| Change Control Review Board exists | | | |
| Training | Y | N | Notes |
| Training Records exist | | | |
| Periodic Review | Y | N | Notes |
| Schedule for periodic reviews exists | | | |
| Backup and Restore | Y | N | Notes |
| Backup files are stored in a separate and secure location | | | |
| Business Continuity | Y | N | Notes |
| Impact analysis (identifies and quantifies any potential loss of critical business assets) | | | |
| Risk assessment exists | | | |
| A crisis plan (process for continuity) | | | |
| Disaster Recovery | Y | N | Notes |
| DRP maintained in a separate and secure location | | | |
| Ordered list of the activities required for | | | |



| Vendor Assessment Checklist | | | |
|--|--|--------------------------------------|--|
| recovery | | | |
| Backup and recovery procedure for computer system components and data (or referenced if a separate document) | | | |
| List of key contacts | | | |
| Verification Plan (all system components are in place, the data was restored, and the system is ready for production use) | | | |
| Process includes an analysis of potential lost or corrupted data and the actions to be taken to resolve any issues | | | |
| System hardware inventory exists | | | |
| System software/application inventory exists | | | |
| DRP is tested | | | |
| Data Security/Integrity | | | |
| Questions | | Notes | |
| <p>Check all of the following Standard Operating Procedures (SOPs) that you have in place and in writing as it relates to clinical data:</p> <p>_____ (1) Internal access SOPs to restrict access to clinical data to those who need access to do their jobs.</p> <p>_____ (2) SOPs to restrict use of the clinical data of client to only those uses allowed by Client and the data subjects.</p> <p>_____ (3) SOPs to restrict collection of clinical data from individuals under the age of 18 unless a mechanism for gaining parental consent has been established.</p> <p>_____ (4) SOPs to collect clinical data only as directed by clients in an appropriate Work Order or agreement.</p> <p>_____ (5) SOPs that limit clinical data in all reports to anonymized clinical data only, unless the distribution of the report within Vendor is limited to those individuals who have been authorized with access to clinical data.</p> | | <p>List specific SOP names here.</p> | |



Vendor Assessment Checklist

- ____ (6) SOPs to protect clinical data from external threats (e.g., firewall monitoring and intrusion detection SOPs) and to otherwise securely store the clinical data using industry best practices
- ____ (7) Secure transfer SOPs to transfer clinical data from vendor to client or any third party utilizing only a VPN, encryption technology, physical point to point connection, or other secure manner of data transport
- ____ (8) If Vendor utilizes subcontractors to handle or manage clinical data, SOPs to verify that the subcontractor protects clinical data in a manner at least equivalent to the manner in which Vendor protects clinical data
- ____ (9) SOPs to train all personnel of Vendor, subcontractors, and temporary workers that have access to clinical data, or will otherwise be responsible for complying with the provisions of any client Agreement, on Consumer Data Protection Policies and SOPs
- ____ (10) We do not currently have written SOPs or Policies on these topics

Do you provide clinical data-related SOP training to all employees and temporary workers and their management who (check all that apply):

- ____ (1) use the data
- ____ (2) are engaged in the collection of clinical data
- ____ (3) are involved in storing and/or securing the data (including IT Security, DBAs, and physical security)
- ____ (4) are involved in the transfer of the data

Indicate here if this information is covered in SOP (list SOPs).



| Vendor Assessment Checklist | |
|---|---|
| <p>If you utilize subcontractors and/or temporary workers for any clinical data functions, check all that apply:</p> <p><input type="checkbox"/> (1) We do not use subcontractors or temp workers for any clinical data functions</p> <p><input type="checkbox"/> (2) Collection of clinical data</p> <p><input type="checkbox"/> Call center</p> <p><input type="checkbox"/> Web Hosting</p> <p><input type="checkbox"/> White mail processing</p> <p><input type="checkbox"/> Data entry/data compilation</p> <p><input type="checkbox"/> Other</p> <p><input type="checkbox"/> (3) Storage of clinical data</p> <p><input type="checkbox"/> On-line Data hosting</p> <p><input type="checkbox"/> Off-line Data hosting</p> <p><input type="checkbox"/> Off-site backup storage</p> <p><input type="checkbox"/> Other hosting</p> <p><input type="checkbox"/> (4) Use of clinical data</p> <p><input type="checkbox"/> Fulfillment activities</p> <p><input type="checkbox"/> Opt-out processing</p> <p><input type="checkbox"/> (5) Transfer of clinical data</p> <p><input type="checkbox"/> (6) Access control administration related to clinical data</p> <p><input type="checkbox"/> (7) Securing clinical data</p> <p><input type="checkbox"/> Intrusion detection vendor</p> <p><input type="checkbox"/> Firewall monitoring</p> | <p>Indicate here if this information is covered in SOP (list SOPs).</p> |
| <p>How do you keep the clinical data from being used for purposes other than those designated by Andara? Check all that apply:</p> <p><input type="checkbox"/> (1) Password-based security access restrictions are used</p> <p><input type="checkbox"/> (2) Detailed SOPs and policies prohibiting use of clinical data other than as specified in the agreement with clients</p> <p><input type="checkbox"/> (3) Training of the SOPs and policies and the obligations of the agreement with client is provided with each new project</p> | <p>Indicate here if this information is covered in SOP (list SOPs).</p> |



Vendor Assessment Checklist

| | |
|--|---|
| <p>____ (4) All employees sign a confidentiality and proprietary information non-disclosure agreement that prohibits such actions</p> <p>____ (5) All contractors and temporary workers sign a confidentiality and proprietary information non-disclosure agreement that prohibits such actions</p> | |
| <p>Please check all of the following methods you use to store/maintain hardcopies of clinical data that you may receive from Andara or any partner or vendor on Andara's behalf:</p> <p>____ (1) Stored in a 24 hour limited access office accessible only by authorized codes or passkeys by people assigned to work with clinical data and trained on the SOPs and policies;</p> <p>____ (2) Stored in an office that is locked after work hours and not secure during office hours</p> <p>____ (3) Stored in locked file cabinets within a department and the file cabinets are secured with access only by a few individuals with keys</p> <p>____ (4) Stored in a 24 hour secure, passcode/passkey access building, but is not otherwise secured from individuals who gain access to the building</p> <p>____ (5) We destroy all hardcopies by shredding or other secure means once we've entered the information in the system</p> | <p>Indicate here if this information is covered in SOP (list SOPs).</p> |
| <p>How will you transfer clinical data to Andara? Indicate all that apply:</p> <p>____ (1) Virtual Private Network (VPN)</p> <p>____ (2) SSL encrypted website with password controlled access</p> | <p>Indicate here if this information is covered in SOP (list SOPs).</p> |



Vendor Assessment Checklist

| | |
|--|---|
| <p>____ (3) Encrypted clinical data sent FTP</p> <p>____ (4) Encrypted clinical data sent email</p> <p>____ (5) FTP unencrypted</p> <p>____ (6) email unencrypted</p> <p>____ (7) CD burned and mailed via overnight carrier or regular mail</p> <p>____ (8) Physical point to point connection used</p> | |
| <p>Do you conduct background checks for employees and contractors with access to clinical data?</p> | <p>Indicate here if this information is covered in SOP (list SOPs).</p> |
| <p>When employees and/or contractors work with clinical data, where do they temporarily store the information?</p> <p>____ (1) Floppy Disc</p> <p>____ (2) Lap Top hard drive</p> <p>____ (3) Desk Top hard drive</p> <p>____ (4) Log/prep bins for data entry</p> <p>____ (5) No local storage is allowed</p> | <p>Indicate here if this information is covered in SOP (list SOPs).</p> |
| <p>What procedure is in place to ensure that the information on the temporary storage device is erased or destroyed?</p> <p>____ (1) SOP to erase or destroy temporary storage prior to every log-off, system sleep or system shut-down</p> <p>____ (2) Temporary storage devices cannot be removed from secure facilities</p> <p>____ (3) SOP to erase or destroy temporary storage on a periodic basis.</p> <p>____ (4) No temporary storage used (#5 is</p> | <p>Indicate here if this information is covered in SOP (list SOPs).</p> |



| Vendor Assessment Checklist | |
|---|---|
| checked in preceding question) ____ (5) Currently no SOPs | |
| System Security | |
| Questions | Notes |
| <p>What firewall technology do you use: _____</p> <p>What intrusion detection technology do you use: _____</p> <p>When was your written information technology firewall and security SOP last updated: ____ (1) within last 6 months ____ (2) within last year ____ (3) within last two years ____ (4) not within last two years ____ (5) We do not have a written SOP for this, we just have systems in place</p> | <p>Indicate here if this information is covered in SOP (list SOPs).</p> |
| <p>Indicate all that apply:</p> <p>____ (1) all of the clinical data we store and maintain or otherwise have on our systems are located behind a firewall</p> <p>____ (2) we utilize an Incident Response Team, have an SOP for its operations, and the appropriate individuals are trained on it</p> <p>____ (3) virus detection software is installed and updated in accordance with industry best practice</p> | <p>Indicate here if this information is covered in SOP (list SOPs).</p> |
| <p>Indicate procedures you have in place to monitor & detect server vulnerability, check all that apply:</p> <p>A written vulnerability assessment is completed: ____ (1) no less than every six months ____ (2) at least once a year ____ (3) at least once every two years ____ (4) when serious intrusion attempts are detected ____ (5) never performed</p> <p>Written vulnerability findings are addressed:</p> | <p>Indicate here if this information is covered in SOP (list SOPs).</p> |



| Vendor Assessment Checklist | |
|---|---|
| <p> <input type="checkbox"/> (1) in next release or implementation of the application <input type="checkbox"/> (2) next release or within 60 days, whichever is sooner <input type="checkbox"/> (3) Prior to next vulnerability assessment <input type="checkbox"/> (4) As operating system versions are updated and patches are applied </p> | |
| <p>Indicate procedures you have in place to monitor and detect unauthorized INTERNAL access attempts to clinical data:</p> <p>Internal unauthorized access attempts are:</p> <p> <input type="checkbox"/> (1) monitored and detected at the database level <input type="checkbox"/> (2) monitored and detected at the server level <input type="checkbox"/> (3) monitored and detected through use of internal firewalls <input type="checkbox"/> (4) detected when breaches are discovered </p> | <p>Indicate here if this information is covered in SOP (list SOPs).</p> |
| <p>When was the last time the company audited its security programs regarding the physical security and loss prevention of clinical data, e.g. theft of servers, removable media, or client computers?</p> <p> <input type="checkbox"/> (1) Within last six months <input type="checkbox"/> (2) Between 6 months and two years ago <input type="checkbox"/> (3) More than two years ago <input type="checkbox"/> (4) Program has never been audited </p> | <p>Indicate here if this information is covered in SOP (list SOPs).</p> |
| <p>Please indicate which of the following applies to your business continuity plans (BCPs):</p> <p> <input type="checkbox"/> (1) Physical building BCP for flood, fire, other natural disaster <input type="checkbox"/> (2) Off-site hot site recovery for all systems </p> | <p>Indicate here if this information is covered in SOP (list SOPs).</p> |



| Vendor Assessment Checklist | |
|---|---|
| <p>____ (3) Off-site cold site recovery for all systems</p> <p>____ (4) Contingency sites for recovery operations meet the same security requirements as the primary site</p> <p>____ (5) BCP plans are reviewed and tested at least annually</p> | |
| <p>Indicate the procedures in place to backup your critical systems:</p> <p>____ (1) weekly full volume backups</p> <p>____ (2) daily incremental backups</p> <p>____ (3) all backups removed off-site daily</p> <p>____ (4) all backups removed off-site weekly</p> <p>____ (5) backups not performed</p> <p>____ (6) Other: _____</p> | <p>Indicate here if this information is covered in SOP (list SOPs).</p> |
| Physical Building Security | |
| Questions | Notes |
| <p>Describe the physical security restrictions at all of your company locations maintaining or handling clinical data. Check all of the following that apply:</p> <p>____ (1) secure buildings with individualized passcodes/card access</p> <p>____ (1a) secured in this manner only after normal work hours</p> <p>____ (1b) secured in this manner 24 hours a day</p> <p>____ (2) secure computer facilities with individualized passcodes/card access</p> <p>____ (2a) Also restricted to only those specifically authorized and trained to work with clinical data</p> | <p>Indicate here if this information is covered in SOP (list SOPs).</p> |

**Vendor Assessment Checklist**

- ____ (2b) secured in this manner only after normal work hours
- ____ (2c) secured in this manner 24 hours a day
- ____ (3) secure records storage facilities with individualized passcodes/card access
- ____ (3a) Also restricted to only those specifically authorized and trained to work with clinical data
- ____ (3b) secured in this manner only after normal work hours
- ____ (3c) secured in this manner 24 hours a day

References

Please provide three references.

- 1.
- 2.
- 3.



Summary Report

| Vendor Assessment Summary Report |
|----------------------------------|
| |
| Assessment Summary |
| |
| Corrective Actions Required |
| |