Complaint Handling and Adverse Event Reporting Application – Software as a Service (SaaS)

Background: The manufacturer has decided to move from a paper-based process for complaint handling and adverse event reporting (e.g.: Medical Device Report (FDA), Techno vigilance (ANVISA), …) to a Software as a Service (SaaS) solution offered by a vendor. This solution is already used by other manufacturers as a "multi-tenant" approach. The application is configured to each tenant. The manufacturer is not interested in custom features at this time. The vendor issues quarterly software updates and bug fixes.

As a cloud-based application, the vendor performs regular code maintenance, functionality enhancements, patching, security updates, etc. The vendor uses third parties (sub-contractors to the vendor) to host the application and associated data. Vendor has determined that its sub-contractor has adequate security and encryption to protect the software and "tenant" data. Vendor issues software updates on a quarterly basis so "tenants" can perform regression testing (this could be automated) prior to quarterly software updates.

Manufacturer has the option to perform testing prior to quarterly updates from the vendor, or to accept the vendor's testing *in lieu* of manufacturer's own testing. Since there are other tenants using this cloud-based application, the manufacturer could factor in the broad use of the application and the other tenant's ability to identify software bugs or defects as part of "real life evidence" and instead take action only if bugs or defects are uncovered after the vendor's quarterly updates. Prior to engaging with the SaaS vendor, the manufacturer assessed the vendor's software development program (SDLC), quality management system (aligned with recognized standards for software development and providing software as a service), infrastructure support (availability and reliability of services), privacy, security, etc. The relationship with the vendor was documented in the form of a service level agreement, including components for quality, reliability, availability, privacy, security, etc.

The Manufacturer, as part of the risk management and assurance program, has evaluated the vendor's controls in the areas listed below (not exhaustive) and addressed them through a service level agreement and quality agreement:

- Infrastructure qualification and provisioning;
- Software validation;
- Change control and release management (infrastructure and software);
- Cybersecurity management;
- Access control;
- Backup and restore;
- Disaster recovery;
- Data center facilities maintenance and physical security;
- System administration, including patch management;
- Configuration management;
- Incident and problem management;
- Personnel training and qualification.

- Advanced notice of system maintenance down time.
- Advanced notice of changes and upgrades, as well as the ability to reject, or back-out changes, if GxP compliance is at risk.

Application's Intended Use: To collect information from customers/patients/users/healthcare providers regarding complaints and adverse events (via telephone to the call center, or self-reported via the Manufacturer's web site, and feeds via social media).

System Features: Standard off-the-shelf features will be used with configuration.

- The manufacturer will evaluate all reported events and determine when an investigation is required. The software will keep a record of such investigations and the decision when an investigation is not required, who made the decision not to investigate, the rationale, signature and date.
- Electronic signatures will be used to document the investigation's closure, decision for reporting the complaint as an adverse event to various health authorities, and the decision not to investigate certain complaints.
- The software can file electronic adverse event reports with multiple health authorities that have set up a system for receiving such reports electronically.
- The software will keep records of all complaints, investigations, customer communication logs, adverse event report and report log, etc.
- The software will produce an error handling report for all completed/successful electronic adverse events reported/filed with health authorities, as well as failed attempts.
- The software can analyze complaint data for track and trend purposes, and it can also download complaint and adverse event reporting to spreadsheets and statistical analysis software for analysis by the manufacturer.

Risk Assessment and Assurance Approach:

Due to the predicated records and signatures maintained in the software, the manufacturer determines that this software has a direct impact on quality system integrity, e.g.: loss of records, altering records after investigation is closed without audit trail, electronic signature not tied/linked to the record where it was applied.

The software can analyze complaint data for track and trend purposes, and it can also download complaint and adverse event reporting to spreadsheets and statistical analysis software for analysis by the manufacturer. The manufacturer considers this feature to directly impact the quality of products and patient safety if there is data loss, errors in track and trend of complaints to identify product issues, or if data is not accurately transferred to the statistical analysis software.

The manufacturer is also concerned about the accuracy of electronic adverse event reports to be filed with various health authorities, to ensure they are in the correct format, correct information being

reported, reporting to all health authorities that should receive the reports, error handling of these transactions, and confirmation of receipt by the health authorities. The manufacturer considers this to be of direct impact to the quality system and patient safety, as failure to report, or failure to report on time, might impact health authorities from determining if an imminent risk to the public exists.

Applying critical thinking, the manufacturer tailors its assurance approach based on the following information:

Basic Assurance Assessment	• The vendor is an established player in the SaaS space • The vendor has passed a vendor audit. • The vendor documentation and testing are robust, and available for review.
Implementation Assessment	• The features implemented are standard and customization that could invalidate the vendor testing are absent. • A robust installation process is required to ensure the system is configured to meet manufacturer's needs.

The manufacturer determines the testing documentation from the software vendor is available and appropriate and can be leveraged in lieu of functional testing. A UAT (User Acceptance Testing) with unscripted testing or limited scripted testing at the business process level will be performed for the features identified above. The determination of unscripted vs. limited scripted is based on the manufacturer's risk management program (e.g.: FMEA, FTE, etc.) and the need to explicitly retain test evidence, etc.

What is the assurance approach for each of the features?

Feature, Operation or Function	**Intended Use**	**Risk**	**Assurance Approach**	**Record or Result**
The manufacturer will evaluate all reported events and determine when an investigation is required. The software will keep a record of such investigations and the decision	(1) To keep a record of all complaints. (2) To keep a record of decision to investigate (or not) a complaint. (3) To keep a record of complaint investigation.	Quality system integrity – decision to investigate (or not) is made outside of the software (i.e., detected by human component and manufacturer's SOPs)	Leverage vendor testing for these functions. Manufacturer performs User Acceptance Testing (UAT) with unscripted testing or limited scripted testing at the business process level.	Leverage vendor documentation and testing. Utilize electronic document management application (e.g.: PLM) to retain documents and approvals.

when an investigation is not required, who made the decision not to investigate, the rationale, signature and date			Since this is only impacting Quality System Integrity, might also consider Exploratory Testing	
Electronic signatures will be used to document the investigation's closure, decision for reporting the complaint as an adverse event to various health authorities, and the decision not to investigate certain complaints.	To apply electronic signatures to complaint and adverse event report records – compliant with 21 CFR 11	Quality system integrity – compliance risk	Leverage vendor testing for these functions. Manufacturer performs User Acceptance Testing (UAT) with unscripted testing or limited scripted testing at the business process level.	Leverage vendor documentation and testing. Utilize electronic document management application (e.g.: PLM) to retain documents and approvals.
The software can file electronic adverse event reports with multiple health authorities that have set up a system for receiving such reports electronically.	(1) Electronically submit mandatory adverse event reports to health authorities. (2) Report transaction handling errors. (3) Maintain electronic receipt of adverse event report being received and accepted by health authorities	Automated surveillance that can impact patient safety. There is human intervention by periodically reviewing report of transaction handling errors.	Leverage vendor testing for these functions. Manufacturer performs User Acceptance Testing (UAT) with unscripted testing or limited scripted testing	Leverage vendor documentation and testing. Utilize electronic document management application (e.g.: PLM) to retain documents and approvals.

The software will keep records of all complaints, investigations, customer communication logs, adverse event report and report log, etc	Maintain electronic record and audit trail compliant with 21 CFR 11	Quality systems integrity	Leverage vendor testing for these functions. Manufacturer performs User Acceptance Testing (UAT) with unscripted testing or limited scripted testing	Leverage vendor documentation and testing. Utilize electronic document management application (e.g.: PLM) to retain documents and approvals.
The software can analyze complaint data for track and trend purposes, and it can also download complaint and adverse event reporting to spreadsheets and statistical analysis software for analysis by the manufacturer.	(1) Generate reports of complaints, adverse events, investigation, root cause – using pre-defined parameters configured by the manufacturer	Functionality is intended to provide input and aid in human decision making process (application does not make the decision) about Product/patient/user safety complaint handling and adverse event data can be used to make determinations about field actions, corrections, removals, product design changes, product acceptability	Leverage vendor testing for this function. Manufacturer performs UAT with limited scripted testing or robust scripted testing	Leverage vendor documentation and testing. Utilize electronic document management application (e.g.: PLM) to retain documents and approvals.
	(2) Ability to transfer data to spreadsheets and statistical analysis software	Functionality is intended to extract data sets from application and transfer to data analytics applications for further analysis.	Leverage vendor testing for this function. Manufacturer performs UAT with limited scripted testing or exploratory testing.	Leverage vendor documentation and testing. Utilize electronic document management application (e.g.: PLM) to retain documents and approvals.