Appendix: Example of Responsibilities in a Quality Agreement

This appendix identifies and considers the responsibilities shared between the regulated company and the SaaS provider when establishing the quality agreement. The specific activities and acceptance criteria may differ from case to case and whether the regulated company or the SaaS provider is responsible for each activity.

Responsibilities		Regulated Company	SaaS Provider
1. Regulatory Authorization and Communications			
1.1	Maintain all registrations, licenses, and authorizations required by applicable laws and agencies to operate in support of pharmaceutical product life cycle activities.	X	
1.2	Manage communication to ensure information is available in a timely manner in response to requests or inquiries from regulatory authorities.	X	
1.3	Update key contacts as necessary.	X	X
2. Organization and Personnel			
2.1	Describe the general organization and reporting structure in organizational charts for management, technical operations, and the quality unit (or equivalent).	X	X
2.2	Identify regulations that are applicable (manufacturing, clinical, drug testing results, etc.) based on the intended use of the application and describe what actions need to be performed to adhere to regulatory requirements.	X	
2.3	Implement an SDLC per IT industry standards, supported by policies and procedures, and governance that is leveraged by the regulated company.		X
2.4	Have qualified personnel to perform the contracted services. These personnel will have the education, training, and experience to perform their assigned functions, which aligns with IT industry standards.		X
2.5	Maintain personnel training records, which align with IT industry standards. These training records should be made available for review during supplier assessments.		X
2.6	The quality unit, or equivalent, will ensure compliance with all federal regulations, GxPs, and other applicable laws on a continuous basis.	X	
3. Building and Facility			
3.1	Secure the facility with controlled building access to ensure only authorized personnel have access to the facilities.		X
3.2	Facility environment will be controlled and monitored to protect and support the equipment, servers, and activities required to support the services provided.		X

"Quality Agreements for SaaS Solutions Intended for GxP Use." *Pharmaceutical Engineering*® March-April 2022,

Responsibilities		Regulated Company	SaaS Provider
4. Equipment and Systems			
4.1	Use an industry-standard risk-based approach to understand and address the SDLC and verification and management of the systems and processes to support the SaaS.	X	X
4.2	Maintain the SDLC used to provide the services. These activities will be documented and available for review during audits.		X
4.3	Systems will be monitored for attempted/accomplished security breaches, and these will be managed and reported to applicable impacted parties.		X
4.4	System access will be limited to authorized staff using least-privileged principles.	X	X
5. Documentation Control (Preparation, Review, and Approval)			
5.1	There will be adequate procedures (SOPs) to describe all GxP functions performed, as required by the regulations.	X	
5.2	Current SOPs will be readily available to SaaS provider staff performing tasks. The document control system will manage versions, effective date, and control removal of obsolete documents. Procedures are each uniquely identified.		X
5.3	Documentation must be organized to ensure it is readily provided to the regulated company.		X
6. Deviations and Investigations			
6.1	Any departure from contracted (expected) agreements requiring an investigation, deviation justification, or tracking of a nonroutine event is captured in the SaaS provider's quality system. Types of exceptions include, but are not limited to, security breaches, data privacy breaches, and other IT service and application failures.		X
6.2	Investigations may include, but are not limited to, the determination of the root cause that led to corrective and preventative actions (CAPA).	X	X
6.3	Monitoring of incidents and problems for completion and effectiveness. This includes monitoring for and evaluation of trends regarding error types and frequency.	X	X
7. Change Control			
7.1	Operate in a state of control through management of changes to prevent unintended consequences to ensure the contractually agreed-upon quality expectations of the IT services and application management documentation.		X

Responsibilities		Regulated Company	SaaS Provider
7.2	Any changes specific to the user requirements or user specifications agreed to between the regulated company and the SaaS provider that may affect the service(s) by impacting quality, compliance, or interpretation of results will be communicated, reviewed, and agreed to by the regulated company in writing prior to implementation.	X	X
7.3	SaaS provider will provide the requested assistance in support of the regulated company's strategy to secure the appropriate support relative to the implementation and verification of the change.	X	X
8. Data Integrity and Handling			
8.1	Data will be maintained in such a way as to ensure security, confidentiality, and privacy at all times.		X
8.2	In the event of a data breach notification , each party will notify the other within a specified time frame.	X	X
8.3	Data will be stored (archived) in a manner that ensures the ability to recover them at all times.		X
8.4	All data associated with the SaaS application will be completely removable from all instances at the end of contract. Evidence of destruction from each instance (if applicable) shall be provided.		X
8.5	A business continuity/disaster recovery plan must be in place to cover all contingencies.	X	X
8.6	Audit logs will be configured as required in accordance with regulated company requirements and business processes supported by the application.	X	X
8.7	Review of audit trails for key critical business functions supporting predicate rule records must be enabled.	X	
9. Record Retention			
9.1	Determine record keeping requirements based on the intended use of the system and any applicable regulatory requirements and business needs.	X	
9.2	Retain all documentation, including paper records (as applicable) and electronic data files, in a secure and safe environment protected against damage, destruction, unintended changes, or disposal during the required time of storage. Records are to be stored in such a manner as to maintain their traceability, reliability, and integrity.	X	X
9.3	Retain documentation for an agreed-upon duration, after which the impacted party will be notified that the archival period has expired and request instruction for the transfer or destruction of documentation.	X	X

Responsibilities		Regulated Company	SaaS Provider
9.4	SaaS provider will have an agreed-upon period after receipt of the notification that the archival period has expired to communicate instructions for the transfer of the documentation to regulated company for ongoing retention.		X
10. Visits, Audits, and Inspections			
10.1	Provide expectations surrounding the right to perform audits for initial qualification of SaaS provider, at established intervals (e.g., biennial), and "for cause" to address specific issues, as warranted, at a mutually agreed-upon date/time.	X	X
10.2	Provide company contact list, organizational chart, regulatory inspection-related documents, index of SOPs, and policies.		X
10.3	Provide support to regulatory bodies during an inspection.	X	X
10.4	As applicable, the regulated company will contact their assigned SaaS provider key contact/quality assurance contact to discuss the audit policy, determine the date, and discuss the scope of the audit. The regulated company will send a finalized agenda prior to the audit date. At the conclusion of the audit, the regulated company will prepare a written report of the audit findings and submit them to the SaaS provider quality assurance contact within an agreed-upon timeframe.	X	
10.5	Where an audit identifies quality or nonconformance to an industry standard, the SaaS provider shall evaluate the findings and, if appropriate, implement suitable corrective and/or preventive measures within a mutually agreed-upon timeframe. The SaaS provider will provide a written response to the regulated company within an agreed-upon timeframe, setting forth the corrective actions to be taken, if any, and a timeline for implementation.		X
11. Subcontracting			
11.1	Changes to critical subservices performed by third parties that impact the regulated company should be identified, communicated, and agreed upon as part of a revision to the quality agreement, if impacted.	X	X
11.2	For any work subcontracted out, the SaaS provider is responsible for ensuring adherence to the requirements in this agreement by the subcontractor/subservice provider.		X