WHITE PAPER

IQVIA SmartSolve®'s Position Regarding the Requirements of EU: Volume 4 GMP – Annex 11

KARI MILLER, Senior Director, Quality Solutions, IQVIA

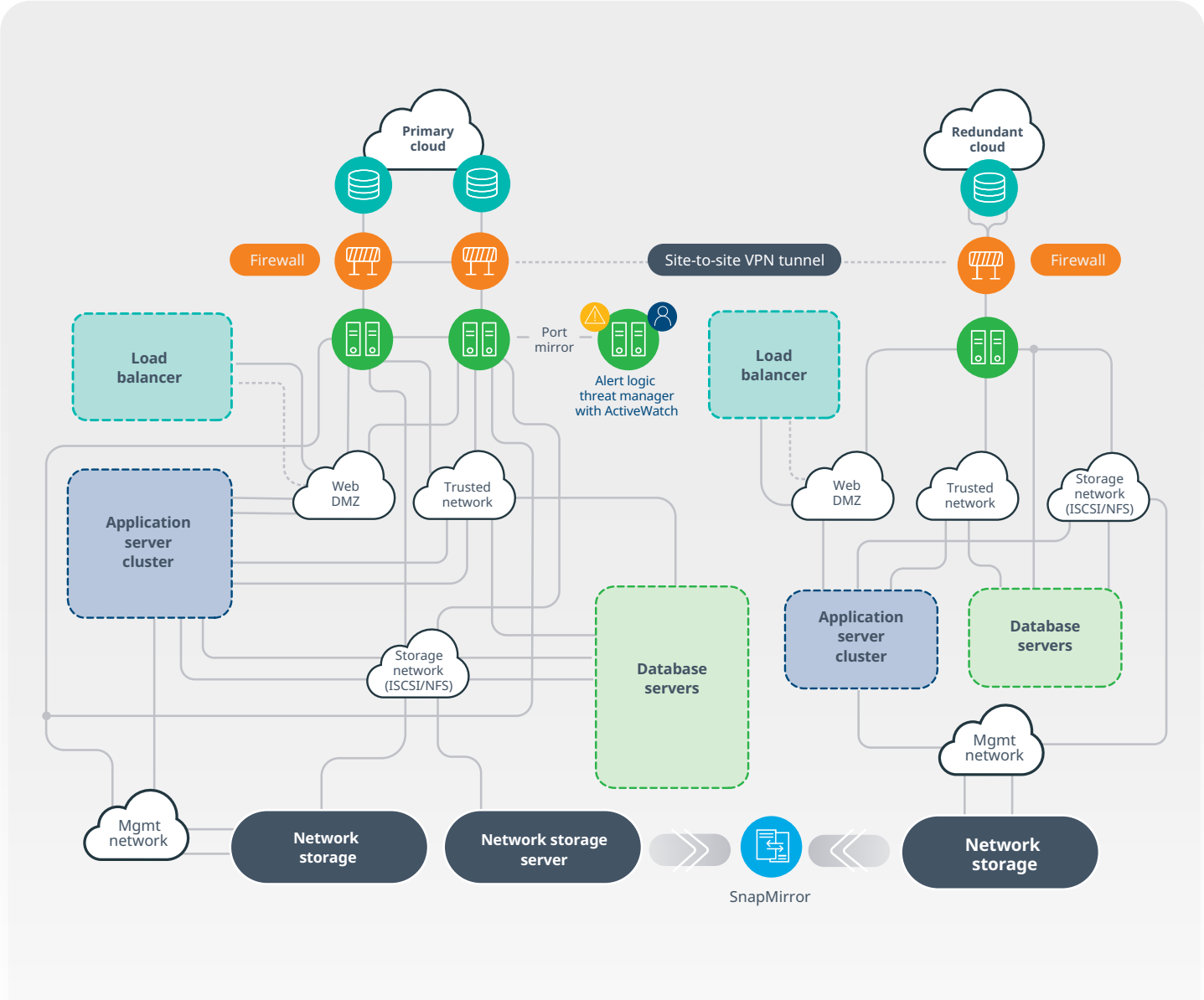
Table of contents

Introduction

Most regulatory bodies have laws, regulations and guidelines relating to electronic records and electronic signatures. They also typically define requirements for the creation, modification, maintenance, archival, retrieval, and transmittal of electronic records. The European Commission's EudraLex – Volume 4, Good Manufacturing Practice, Annex 11: Computerised Systems, which took effect on June 30, 2011 is the requirements document for the aforementioned in Europe.

Annex 11 was revised in January 2011 (effective date June 30, 2011) due to an increase in the usage and complexity of computerised systems for regulatory activities. It impacts manufacturers in the European Union/EEA (European Economic Area), and those manufacturers who export product to these jurisdictions. Annex 11 focuses on risk management throughout the entire lifecycle of the computerised GMP "process", encompassing personnel, suppliers and service providers, validation, data, accuracy checking, data storage, printouts, audit trails, change and configuration management, periodic evaluation, security, incident management, electronic signatures, batch release, business continuity and archiving. Annex 11's risk management approach is similar to ICH Q9 Quality Risk Management and the GAMP5 Guide – A Risk-Based Approach to Compliant GxP Computerised Systems. The EMA (European Medicines Agency) has provided supplemental responses to questions for additional clarification on their website. IQVIA SmartSolve is continuously monitoring the output of the European Commission and of the EMA, and feedback from customers operating in Europe to ensure that our solutions and tools are a vehicle for compliance with the requirements.

High-level overview of IQVIA SmartSolve's cloud offering



There are various regulations, guidance and standards that need to be considered when a life sciences company leverages the services of a cloud solution provider. This document identifies the requirements of EU GMP Volume 4 Annex 11 and how the IQVIA SmartSolve Cloud team and infrastructure support your compliance needs.

IQVIA SmartSolve's Position Regarding the Requirements of EU Volume 4 – GMP Annex 11: Computerised Systems

PRINCIPLE

ANNEX 11		IQVIA'S SMARTSOLVE SOLUTION
	This annex applies to all forms of computerised systems used as part of GMP regulated activities. A computerised system is a set of software and hardware components which together fulfill certain functionalities. The application should be validated; IT infrastructure should be qualified. Where a computerised system replaces a manual operation, there should be no resultant decrease in product quality, process control or quality assurance. There should be no increase in the overall risk of the process.	The customer is responsible for a program's suitability as used in the regulatory environment. IQVIA SmartSolve assists the customer with the validation process by providing documentation and records during the installation and through training services. A Validation Pack is also available that provides additional assistance to ensure reliability and consistent data including the Audit Trail. The Validation Packs are module specific and include IQ, OQ and PQ scripts.

GENERAL

ANNEX 11		IQVIA'S SMARTSOLVE SOLUTION
1.	**Risk Management** Risk management should be applied throughout the lifecycle of the computerised system taking into account patient safety, data integrity and product quality. As part of a risk management system, decisions on the extent of validation and data integrity controls should be based on a justified and documented risk assessment of the computerised system.	It is the responsibility of the customer to complete a risk assessment prior to iimplementation of the IQVIA SmartSolve application, to ensure an understanding of how the business needs will interact with the application, from the IT Department's Application/ database management procedures down to what is critical data, who can have access to it and what are the processes to ensure integrity of the data entry.
2.	**Personnel** There should be close cooperation between all relevant personnel such as Process Owner, System Owner, Qualified Persons and IT. All personnel should have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties.	It is the responsibility of the customer to develop policies regarding training of the regulations and that records be maintained. However, IQVIA's SmartSolve Training Management module, when used in conjunction with other modules, allows for additional access control to operations based on employee certifications. Training Management tracks all training activities, internal and external.

ANNEX 11		IQVIA'S SMARTSOLVE SOLUTION
3 3.1	**Suppliers and Service Providers** When third parties (e.g. suppliers, service providers) are used e.g. to provide, install, configure, integrate, validate, maintain (e.g. via remote access), modify or retain a computerised system or related service or for data processing, formal agreements must exist between the manufacturer and any third parties, and these agreements should include clear statements of the responsibilities of the third party. IT departments should be considered analogous.	IQVIA SmartSolve provides "Statements of Work" to the customer to ensure that the type of work and the expectations are clearly defined prior to engaging in its services. Additionally, Non-disclosure Agreements are available for execution by and with all customers.
3.2	The competence and reliability of a supplier are key factors when selecting a product or service provider. The need for an audit should be based on a risk assessment.	This is the responsibility of the customer. IQVIA SmartSolve welcomes its customers to conduct on-site audits at its facility and its third-party hosting facility.
3.3	Documentation supplied with commercial off-the-shelf products should be reviewed by regulated users to check that user requirements are fulfilled.	IQVIA SmartSolve provides multiple levels of documentation for its customers: • Release Notes • System Architecture Guide • Installation Manual • Data Definition File • Entity Relationship Diagrams • Full Online Help • Training Manuals (also available from the Training Group)
3.4	Quality system and audit information relating to suppliers or developers of software and implemented systems should be made available to inspectors on request.	IQVIA SmartSolve offers customers the Supplier Management module, which allows them to demonstrate to inspectors that they have a process for supplier evaluation, selection, and periodic review. Based on user setup, this evaluation process should include the results of the Quality System Audit and other audit information that is stored and retrievable not only for inspectors but for all those with the authority to review supplier performance, qualification, and selection criteria.

PROJECT PHASE

ANNEX 11		IQVIA'S SMARTSOLVE SOLUTION
4 4.1	**Validation** The validation documentation and reports should cover the relevant steps of the lifecycle. Manufacturers should be able to justify their standards, protocols, acceptance criteria, procedures and records based on their risk assessment.	This is the responsibility of the customer. As a starting point, IQVIA SmartSolve provides a Validation Pack for each solution to satisfy the guidelines set out by GAMP5 and includes a collection of protocols and test matrices for functions accessible to a user within the IQVIA SmartSolve solutions. The following documents form part of the Validation Pack: • Functional Requirement Specifications • Validation Matrix (functions vs. test scripts, for development of the Test Plan) • Issues Tracking List • Test Scripts file with, among others, 1. Scope of the test case 2. Test case environment (customer responsibility) 3. Assumptions/Constraints associated with the test case • Test Case Data • Test Case Table (step-by-step instructions with expected/actual results) • Plan for Corrective Action and Re-Test • Attachments file (artifacts that are referred to in test scripts) These documents of course will need to be updated based on customer setup and configuration.
4.2	Validation documentation should include change control records (if applicable) and reports on any deviations observed during the validation process.	This is the responsibility of the customer. During the standard release cycle when updates/new releases are made available to the customer, the Release Notes document the changes that would be available as part of the Change Management documentation for upgrades.

ANNEX 11		IQVIA'S SMARTSOLVE SOLUTION
4.3	An up to date listing of all relevant systems and their GMP functionality (inventory) should be available. For critical systems, an up to date system description detailing the physical and logical arrangements, data flows and interfaces with other systems or processes, any hardware and software pre-requisites, and security measures should be available.	We will assist in the development of this for IQVIA SmartSolve customers at various stages of the implementation. Initially, prior to purchasing any equipment, an Architecture Landscape can be developed with the vision of how the solution needs to be deployed, which defines the hardware architecture required for IT to deploy. The IQVIA SmartSolve Implementation Services group can perform an "As-Is" business analysis with the business and then define if any changes will need to be made and document the business process flow through the application. The following is a typical enterprise implementation path that will capture the system inventory through the implementation phase. • System Deployment • Requirements Review • Solution Configuration • Integration Development and Configuration • Conference Room Pilot • User Acceptance Testing • Integration Testing • OQ and PQ Validation For smaller, out-of-the-box implementations, these steps are consolidated: • System Deployment • Solution Review • Solution Setup • User Acceptance Testing • OQ and PQ Validation
4.4	User Requirements Specifications should describe the required functions of the computerised system and be based on documented risk assessment and GMP impact. User requirements should be traceable throughout the lifecycle.	It is the responsibility of the customer to develop User Requirements and document how they interact with the software application process.

ANNEX 11		IQVIA'S SMARTSOLVE SOLUTION
4.5	The regulated user should take all reasonable steps, to ensure that the system has been developed in accordance with an appropriate quality management system. The supplier should be assessed appropriately.	This is the responsibility of the customer. IQVIA SmartSolve welcomes its customers to conduct on-site audits at its facility and its third-party hosting facility. IQVIA SmartSolve has a well-documented Software Development Lifecycle (SDLC) process, starting from the requirements definition, creation of the design documentation, development of programming specifications, development of unit test plans, integration of test plans, and management of the entire development lifecycle for feedback collection and introduction of improvements back into the system. The tools used to support this process provide complete traceability of requirements mapped to design use cases — traceable all the way to test cases and results. All software and user documentation are maintained in a source code management system. A change management system is used for managing, tracking and approving all change requests, bugs and new feature requests. Additionally, IQVIA SmartSolve is certified to ISO 9001. A Quality Assurance Specialist is responsible for annual internal audits and reviews each project's activities and work products to ensure they conform to IQVIA SmartSolve's process standards. The Quality Control group is responsible for ensuring the software products are tested to meet customer and system requirements specifications.
4.6	For the validation of bespoke or customised computerised systems there should be a process in place that ensures the formal assessment and reporting of quality and performance measures for all the lifecycle stages of the system.	This is the responsibility of the customer. IQVIA SmartSolve welcomes its customers to conduct on-site audits at its facility and third-party hosting facility.
4.7	Evidence of appropriate test methods and test scenarios should be demonstrated. Particularly, system (process) parameter limits, data limits and error handling should be considered. Automated testing tools and test environments should have documented assessments for their adequacy.	IQVIA SmartSolve utilises several tools to manage and track all supporting documents and processes for the SDLC. These tools provide complete traceability of requirements mapped to design use cases — traceable all the way to test cases and results. This is carried out for all IQVIA SmartSolve releases and applies to both cloud and on-premise deployments.
	If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process.	IQVIA SmartSolve provides services for Data Migration from existing systems to the new application. There are validation steps through this process to ensure that all the data are moved and that they are moved to the correct new location.

OPERATIONAL PHASE

ANNEX 11		IQVIA'S SMARTSOLVE SOLUTION
5	**Data**	IQVIA SmartSolve integration leverages the same security that the IQVIA SmartSolve application utilises to ensure that the appropriate security must be present before any automatic updates can occur. IQVIA SmartSolve's web services are built upon SOAP and REST protocols — to ensure security and data integrity while transferring information.
6	**Accuracy Checks** For critical data entered manually, there should be an additional check on the accuracy of the data. This check may be done by a second operator or by validated electronic means. The criticality and the potential consequences of erroneous or incorrectly entered data to a system should be covered by risk management.	Modules are structured such that actions can only be performed in the appropriate sequence. Required steps, such as approval routing, cannot be skipped. The customer is responsible for determining what the "critical data" are for each business process that interacts with IQVIA SmartSolve. The solution will allow the customer to deploy multiple aspects of "control" for critical data: • Enforce what is "required" information • Enforce that information entered must be "validated" to ensure that corrupt data are not entered • Set up who can add or modify data
7 7.1	**Data Storage** Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period.	IQVIA SmartSolve provides minimum system requirements to ensure proper functioning of the software. All data are encrypted at rest and in motion, however, it is the responsibility of the customer to develop and implement appropriate back-up protocols. All modules have multiple levels of security. The first level limits access to the module itself in conjunction with network access through user names and domain passwords. The other levels of security limit access to menu options for functions and reports within the system. Users can only execute transactions to which they are authorised. Access to individual documents as well as individual reports in all modules is controlled by security within the module. IQVIA SmartSolve supports both Single Sign-On (SSO) and Federated SSO, as it is Okta certified. Based upon the risk assessment of the customer, a procedure and frequency should be developed to ensure that the data being captured by the users of the system are accurate and that the system can support accessibility to those who are defined as users and exporting of readable data.

ANNEX 11		IQVIA'S SMARTSOLVE SOLUTION
7.2	Regular back-ups of all relevant data should be done. Integrity and accuracy of back-up data and the ability to restore the data should be checked during validation and monitored periodically.	IQVIA SmartSolve provides minimum system requirements to ensure proper functioning of the software. It is the responsibility of the customer to develop and implement appropriate back-up protocols and security measures to ensure records are protected. This is the responsibility of the IT department within the customer organisation, based upon the risk assessment determined after the analysis of what business processes are included in the IQVIA SmartSolve application.
8 8.1	**Printouts** It should be possible to obtain clear printed copies of electronically stored data.	All modules contain reports that can be printed or viewed. Existing reports can be edited, and additional reports can be created in Smart Insight, and/or Quality Intelligence and added to the system for use by the end user. All previewed reports may be exported to an electronic format for dissemination. All audit-trailed information can be easily viewed as well.
8.2	For records supporting batch release it should be possible to generate printouts indicating if any of the data has been changed since the original entry.	All changes to data made within the application are stamped with the name of the originator and the time and date of the change. Each field-level change creates an individual entry in the Audit Trail; therefore, the previously recorded change information is retained. The data can be maintained indefinitely and can be tracked via the Audit Trail module. Data can be easily viewed or printed.
9	**Audit Trails** Consideration should be given, based on a risk assessment, to building into the system the creation of a record of all GMP-relevant changes and deletions (a system generated "audit trail"). For change or deletion of GMP-relevant data the reason should be documented. Audit trails need to be available and convertible to a generally intelligible form and regularly reviewed.	All changes to data made within each module are stamped with the name of the originator and the time and date of the change. Each field-level change creates an individual entry in the Audit Trail; therefore, the previously recorded change information is retained. The data can be maintained indefinitely and can be tracked via the Audit Trail module. Data can be easily viewed or printed.
10	**Change and Configuration Management** Any changes to a computerised system including system configurations should only be made in a controlled manner in accordance with a defined procedure.	It is the responsibility of the customer to provide a change management process. IQVIA SmartSolve provides tools and services to help customers move "configurations" from one environment where they can work through the development to the next environment for their validation or production. A formalised change request and change management process is in place for our IQVIA SmartSolve cloud customers that complies with these requirements.

ANNEX 11		IQVIA'S SMARTSOLVE SOLUTION
11	**Periodic Evaluation** Computerised systems should be periodically evaluated to confirm that they remain in a valid state and are compliant with GMP. Such evaluations should include, where appropriate, the current range of functionality, deviation records, incidents, problems, upgrade history, performance, reliability, security and validation status reports.	IQVIA SmartSolve provides a Validation Pack for each module and for every upgrade/patch that is provided. The user can leverage and utilise these scripts to validate the IQ, OQ and PQ for each upgrade made available through IQVIA SmartSolve's release process. These scripts can then be reused at a periodic timeframe, contingent upon the frequency determined by the customer's risk management analysis. It is the responsibility of the customer to develop policies regarding controlled access to system manuals and system-related documentation. Documentation provided by IQVIA SmartSolve Software is revision controlled.
12 12.1	**Security** Physical and/or logical controls should be in place to restrict access to a computerised system to authorised persons. Suitable methods of preventing unauthorised entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas.	IQVIA SmartSolve provides minimum system requirements to ensure proper functioning of the software. It is the responsibility of the customer to develop and implement appropriate back-up protocols and security measures to ensure records are protected. All modules have multiple levels of security. The first level limits access to the module itself in conjunction with network access through user names and domain passwords. The other levels of security limit access to menu options for functions and reports within the system. User rights that are assigned on an as-needed basis accomplish this. Users can only execute transactions to which they are authorised. Access to individual documents as well as individual reports in all modules is controlled by security within the module. IQVIA SmartSolve supports both Single Sign-On (SSO) and Federated SSO, as it is Okta certified. IQVIA SmartSolve offers the option to use LDAPS in addition to the Windows domain. The system has a user ID and password authentication protocol that will not allow the entry of duplicate active records.
12.2	The extent of security controls depends on the criticality of the computerised system.	The IQVIA SmartSolve application offers the ability to provide granular controls down to a specific field level based upon the criticality of the information entered and the determination of who can make any and what type of changes.
12.3	Creation, change, and cancellation of access authorisations should be recorded.	The system is tightly integrated with the network security of the Windows domain; all of the security policies identified within the Windows domain are automatically inherited by the system. IQVIA SmartSolve supports both Single Sign-On (SSO) and Federated SSO, as it is Okta certified. Additionally, the solution has the ability to track, using the Audit Trail, all changes made to an individual user's account within the application.

ANNEX 11		IQVIA'S SMARTSOLVE SOLUTION
12.4	Management systems for data and for documents should be designed to record the identity of operators entering, changing, confirming or deleting data including date and time.	All changes to data made within each module are stamped with the name of the originator and the time and date of the change. Each field-level change creates an individual entry in the Audit Trail; therefore, the previously recorded change information is retained. The data can be maintained indefinitely and can be tracked via the Audit Trail module. Data can be easily viewed or printed where appropriate.
13	**Incident Management** All incidents, not only system failures and data errors, should be reported and assessed. The root cause of a critical incident should be identified and should form the basis of corrective and preventive actions.	IQVIA SmartSolve provides various monitoring utilities to assist in the monitoring and detection of any errors through the use of various logs and event viewers.
14	**Electronic Signature** Electronic records may be signed electronically. Electronic signatures are expected to: a. have the same impact as hand-written signatures within the boundaries of the company, b. be permanently linked to their respective record, c. include the time and date that they were applied.	Each electronic record is stamped with the name of the individual carrying out a signed activity, and the time and date that the signature was applied to the electronic record. The meaning of each signature is automatically indicated with the signed record. The electronic signature data is maintained and secured in the same manner as electronic records. All modules contain reports that can be printed or viewed. The system is secure; there are no means to remove or copy signatures from/to documents by ordinary means. All changes to data made within each module are stamped with the name of the originator and the time and date of the change. Each field-level change creates an individual entry in the Audit Trail; therefore, the previously recorded change information is retained. The data can be maintained indefinitely and can be tracked via the Audit Trail module.
15	**Batch Release** When a computerised system is used for recording certification and batch release, the system should allow only Qualified Persons to certify the release of the batches and it should clearly identify and record the person releasing or certifying the batches. This should be performed using an electronic signature.	The IQVIA SmartSolve application has the ability to create unique security that can be assigned to a specific person who is a "Qualified Person" either defined through remote certification and documentation or through the Training Management module. The solution has a configurable electronic signature.
16	**Business Continuity** For the availability of computerised systems supporting critical processes, provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (e.g. a manual or alternative system). The time required to bring the alternative arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequately documented and tested.	Hardware (content switch) and software (driver) based Network Load Balancing (NLB) options provide both scalability and increased availability (high availability) environments for global enterprise deployments of the IQVIA SmartSolve application. NLB options are supported through both hardware and software configurations. These options allow customers to scale out by adding additional web servers to support increased demand. This also provides failover capability in the event that a failure occurs in one of the web servers.

ANNEX 11		IQVIA'S SMARTSOLVE SOLUTION
17	**Archiving** Data may be archived. This data should be checked for accessibility, readability and integrity. If relevant changes are to be made to the system (e.g. computer equipment or programs), then the ability to retrieve the data should be ensured and tested.	IQVIA SmartSolve provides minimum system requirements to ensure proper functioning of the software. It is the responsibility of the customer to develop and implement appropriate back-up protocols and security measures to ensure records are protected. • Audit Trail Archiving is available for record retention • The database is partitioned to easily allow for the utilisation of database tools utilising SQL's Enterprise Edition or Oracle tools to archive records

References

1. EudraLex, the Rules Governing Medicinal Products in the European Union, Volume 4, Good Manufacturing Practice, Medicinal Products for Human and Veterinary Use, Annex 11: Computerised Systems. Revision 1 https://ec.europa.eu/health/system/files/2016-11/annex11_01-2011_en_0.pdf

The scope of today's life science companies is becoming increasingly global, both in the demand for, and the sale of, life-enhancing products. These organisations must be able to support manufacturing and distribution throughout the world while addressing the potential operational risks, as well as overcoming the quality, safety and revenue pressures inherent in the industry.

The world's leading enterprise compliance and quality management companies, like IQVIA, are lowering those risks and strengthening the profitability of our customers, through enterprise-wide, automated solutions. Manufacturers then are able to dedicate their resources to designing higher quality products that will directly benefit patients' quality of life.

IQVIA is committed to helping organisations produce the highest quality products, and we believe that quality management should have a positive impact on your bottom line. We've pioneered quality management software solutions for more than 20 years. We brought industry best practices to the life sciences sector, and we've partnered with the world's leading companies to enhance their quality processes, positively impact their financial performance, and achieve regulatory success.

For more information, visit us at **www.iqvia.com**

About the author

KARI MILLER
Senior Director,
Quality Solutions,
IQVIA

As QMS Regulatory and Product Management Leader for IQVIA, Kari Miller is responsible for driving the strategic product roadmap, and delivery of industry best practices and regulatory compliance solutions for quality management. Kari has more than 25 years of experience delivering software solutions for life sciences. She brings that knowledge to her current team as they focus specifically on translating market and industry requirements into industry-leading enterprise quality management solutions that meet the needs of the heavily regulated life sciences QMS market. Kari earned a Bachelor of Science in Business Administration and a Bachelor of Science in Psychology from Marian College of Fond du Lac, Wisconsin.

IQVIA TECHNOLOGIES

CONTACT US
2400 Ellis Road | Durham | NC 27703 | United States
iqvia.com/contactus