WHITE PAPER

IQVIA TECHNOLOGIES

IQVIA SmartSolve®'s Position Regarding 21 CFR Part 11 Requirements

KARI MILLER, Senior Director, Quality Solutions, IQVIA

Table of contents

Introduction

CFR Part 11 of Title 21 of the Code of Federal Regulations; Electronic Records; Electronic Signatures sets forth the requirements for the creation, modification, maintenance, archival, retrieval, and transmittal of electronic records, and also the use of electronic signatures when complying with the Federal Food, Drug and Cosmetic Act or any other Food and Drug Administration (FDA) regulation. These rulings became law in March 1997. Since that time, both industry and the FDA have been working to interpret the meaning and intent of Part 11, especially as technology is evolving.

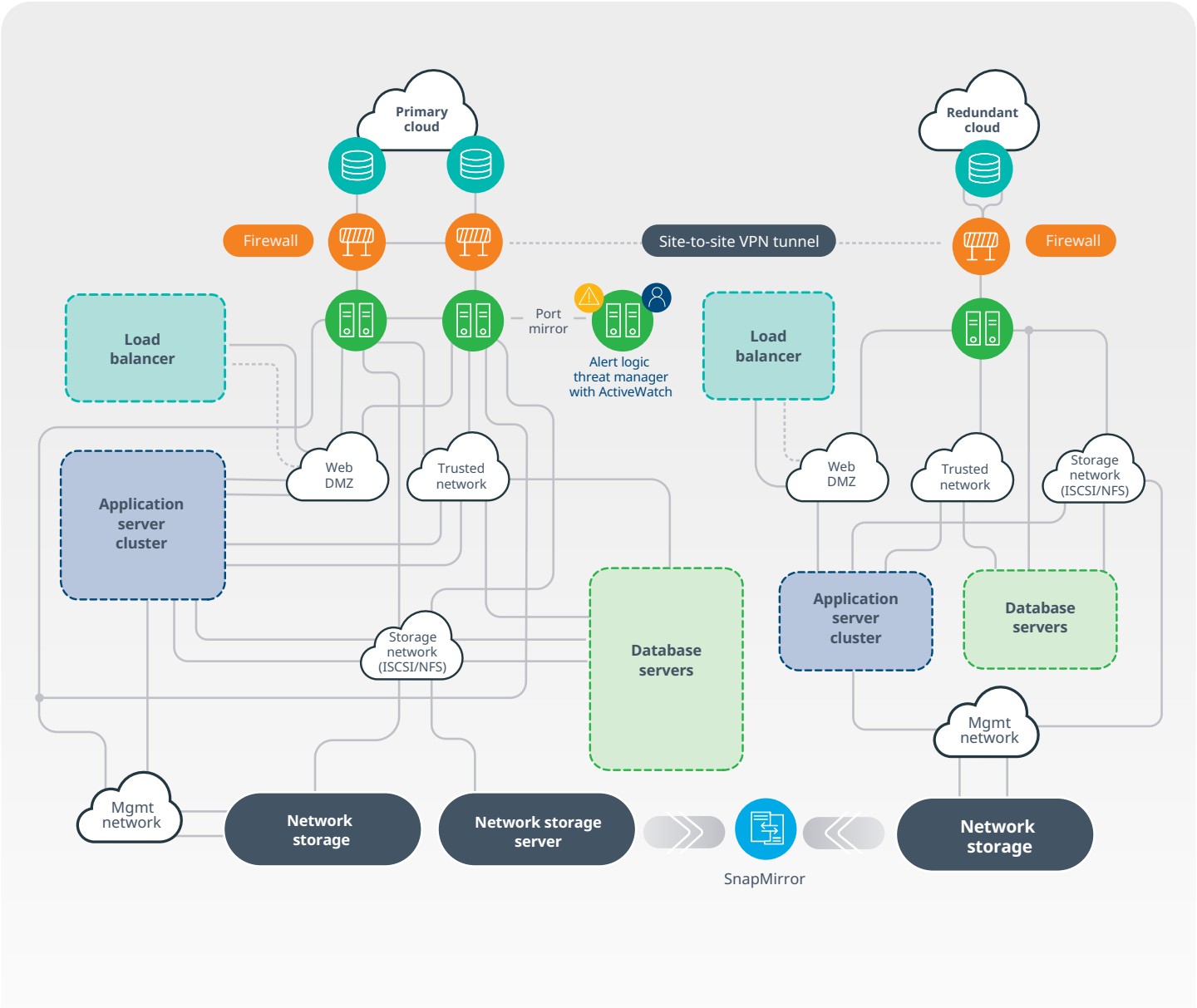
The FDA has created several documents with the assistance of industry representatives, to offer guidance in interpretation of the requirements. The IQVIA SmartSolve team is continuously monitoring the opinions of the FDA and furthering discussions with them as new technology and capabilities evolve, to ensure continued compliance support with the requirements.

As industry needs develop and technological capabilities emerge, IQVIA SmartSolve evolves its solution to support its customers' quality and compliance requirements. Cloud solutions allow customers to focus more on enhancing quality and compliance processes and less on the technology that manages them. IQVIA SmartSolve's cloud solution provides secure, enterprise-class managed hosting services through enterprise-grade facilities, network and staff.

IQVIA SmartSolve's cloud offering provides premier industry required security and reliability to support a life science company. IQVIA SmartSolve's cloud operation provides:

- Experience with managing quality and compliance solutions in the cloud since 2007.
- SOC 2 Type 2 certification.
- Compliance with the HIPAA HITECH Security Rule.
- Resources trained in handling Protected Health Information (PHI) and following Standard Operating Procedures (SOPs) that protect confidential data.
- Validation services for installation and operational qualifications (IQ and OQ) to FDA and GAMP5 guidelines.
- Advanced network security and full redundancy for the protection, disaster recovery, and maintenance of its customers' intellectual property.
- Encryption of data at rest and in flight.
- Hosting in dedicated, hardened facilities that are SOC 2 certified, PCI DSS compliant, and Type 1 AT 101 (HIPAA) compliant.

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 21 CFR Part 11 and how the IQVIA SmartSolve cloud team and infrastructure support your compliance needs.

Definitions per 21 CFR Part 11

- **Electronic record** means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.
- **Digital signature** means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.
- **Electronic signature** means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.
- **Closed System** means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.
- **Open System** means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.

IQVIA SmartSolve's on-premise and cloud support of customer requirements to 21 CFR Part 11

IQVIA SmartSolve's cloud solution utilizes the same solution as for IQVIA's On-Premise customers; therefore, the On-Premise response is applicable for the cloud operation, with additional information noted under IQVIA SmartSolve's cloud operation that is unique to cloud.

SUBPART B — ELECTRONIC RECORDS

§11.10 Controls for Closed Systems

Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:

21 CFR PART 11		IQVIA'S SMARTSOLVE SOLUTION
Section		
§11.10 (a)	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	**IQVIA's SmartSolve Solution:** The end user is responsible for a program's suitability as used in the regulatory environment. IQVIA's SmartSolve solution is developed using a consistent Software Development Lifecycle (SDLC) methodology for new product development, enhancement and maintenance of existing solutions. It defines a consistent process from requirements gathering, software development, quality control, change management, configuration management, validation verification, quality assurance practices and release management. The IQVIA SmartSolve Management solutions offer a hierarchical view of the audit trail, providing a record activity log that captures specific field-level changes through the audit trail. **IQVIA's SmartSolve Solution On Premise:** IQVIA's SmartSolve Services Team can provide IQ documentation on a customer's qualified system during installation. IQVIA SmartSolve provides a Validation Pack to accelerate customers through the OQ process, and can assist in training customers to quickly create PQ documentation for their implementation. IQVIA SmartSolve's Validation Pack includes the Audit Trail functionality. **IQVIA's SmartSolve Cloud Operation:** Installation and Operational Qualification (IOQ) consists of Hardware and Software Qualification. IQVIA's SmartSolve Application Deployment Guide is used to define the infrastructure for the cloud environment. A Validation protocol is conducted for an IQ and OQ; the information is documented, signed and approved by IQVIA SmartSolve Executive Management and the Quality Assurance department, and stored in a controlled environment. **Method of Execution:** IQVIA SmartSolve's QA Validation team executes the Validation Pack OQ scripts on the standard application which is installed in a validated environment. When the OQ is completed it is signed off by IQVIA's SmartSolve Quality Assurance Department Head. The standard version-controlled solution is then available to SmartSolve cloud customers in a secured environment. Customers are responsible for final PQ based on their configurations. All modifications to the customer environment are initiated through customer-initiated change control.

21 CFR PART 11		IQVIA'S SMARTSOLVE SOLUTION
§11.10 (b)	The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.	**IQVIA's SmartSolve Solution:** Contains reports that can be printed, viewed and exported to electronic form. Existing reports can be modified with appropriate security, and new reports added to the system to view, print and export the information into an electronic file. Pre-defined saved searches and ad hoc search queries allow information to be queried, viewed and exported into an electronic file. In addition, there are configurable web services that can be used to export data to human readable formats. **IQVIA's SmartSolve Cloud Operation:** Leverages the capabilities of the IQVIA SmartSolve solution installed.
§11.10 (c)	Protection of records to enable their accurate and ready retrieval throughout the record's retention period.	**IQVIA's SmartSolve Solution:** Provides for multiple levels of security within the application, to ensure that only those individuals assigned appropriate security can access and view specific types of records/data. The Audit Trail information can be moved, exported and saved in a unique location for archiving and retrieval as required through the record retention period. **Customer Procedural Control:** Is required to develop and implement appropriate back-up protocols and security measures to ensure records are protected. **IQVIA's SmartSolve Cloud Operation:** Provides protection for records/data on servers in a data center via multiple layers of physical security; from 24/7 full security and surveillance monitoring to the use of controls, such as, biometrics, locks and traps throughout the facility. Data is secured electronically by controlled network access. IQVIA's SmartSolve cloud operation conducts scheduled snapshots of data and securely transmits those snapshots to a disaster recovery site where data can be accessed in the event of a declared disaster of the primary site. These snapshots are routinely restored and checked for accuracy. All customer data is kept intact unless requested through change control by the customer, to truncate or archive.

21 CFR PART 11		IQVIA'S SMARTSOLVE SOLUTION
§11.10 (d)	Limiting system access to authorized individuals.	**IQVIA's SmartSolve Solution:** Limits system access to authorized individuals through a trusted authentication provider; this ensures that the user's ID and authentication method, such as, password/smart card/ biometric, are "authenticated" for individual user access based upon company policy. The IQVIA SmartSolve solution requires each user ID to be unique. Once the user is authenticated, the IQVIA SmartSolve solution checks the roles and security uniquely assigned to the user ID to ensure they are authorized to be in the solution and to have access to records and activities they need to perform. The IQVIA SmartSolve solution has multiple levels of security, based on the principle of least privilege. The system offers a timeout capability after a configurable period of time, so that an unauthorized user cannot have access to idle records. **IQVIA's SmartSolve Cloud Operation:** Access Control Policy has been established in accordance with NIST Special Publication 800-53, which includes separation of duty, policy, and procedures. This protocol limits information system access to authorized users or devices (including other information systems), and to the types of transactions and functions that authorized users are permitted to exercise. **Account Management and Access Enforcement:** IQVIA's SmartSolve cloud operation ensures proper user identification and authentication management, such as, verification prior to access, limits for repeated attempts, and revoke for terminated users, etc.

21 CFR PART 11		IQVIA'S SMARTSOLVE SOLUTION
§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. Such audit trail documentation shall be retained for a period of at least as long as that required for the subject electronic records and shall be available for agency review and copying.	**IQVIA's SmartSolve Audit Trail:** Captures the operator creating, modifying or deleting electronic records within the system. The audit trail captures changes to data across all solutions, along with the ID of the operator and the date/time stamp (UTC) when the activity occurred. Field-level changes are captured along with their previous values, thereby retaining previously recorded information. IQVIA's SmartSolve Management solutions offer a hierarchical view of the audit trail, providing a record activity log that captures specific field-level changes through the audit trail. The Audit Trail information can be moved/exported and saved in a unique location for archiving and retrieval through the record retention period. Audit Trail information can be easily viewed and output in HTML or PDF format. **IQVIA's SmartSolve Cloud Operation:** Leverages the capabilities of the IQVIA SmartSolve solution installed. Additionally, it creates, protects, and retains information system audit records. This type of audit record enables the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity. In addition, it ensures that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions. IQVIA's SmartSolve cloud operation utilizes authoritative Network Time Protocol (NTP) sources for its time-synchronization, to synchronize all critical system clocks and times. All the customer data is kept intact unless requested through change control by the customer, to truncate or archive.
§11.10 (f)	Use of operational system checks to enforce permitted sequencing of steps and events as appropriate.	**IQVIA's SmartSolve Solution:** Has a standard workflow with configurable policies, such as approval routings, that can be defined by the administrator, to ensure that the user's path is sequenced appropriately. To support data integrity, proper codification and sequencing, initial setup data can be required for field-level validation as information is entered. **IQVIA's SmartSolve Cloud Operation:** Leverages the capabilities of the IQVIA SmartSolve solution installed.

21 CFR PART 11		IQVIA'S SMARTSOLVE SOLUTION
§11.10 (g)	Use of authority checks to ensure that only authorized 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.	**IQVIA's SmartSolve Solution:** Limits system access to authorized individuals through a trusted authentication provider; this ensures the user's ID and authentication method, such as password/smart card/biometric, are "authenticated" for individual user access based upon company policy. The IQVIA SmartSolve solution requires each user ID to be unique. Once the user is authenticated, the IQVIA SmartSolve solution checks the roles and security uniquely assigned to the user ID to ensure the individual is authorized to be in the solution and to have access to records and activities they need to perform. IQVIA's SmartSolve solution has multiple levels of security, based on the principle of least privilege. The electronic signature is controlled with the same multi-level mechanism by authenticating the user who is signing off on the record, and also by verifying the user is authorized to sign the record. **IQVIA's SmartSolve Cloud Operation:** Leverages the capabilities of the IQVIA SmartSolve solution installed and follows IQVIA's SmartSolve Cloud Access Control Policy, which has been established in accordance with NIST Special Publication 800-53. IQVIA's SmartSolve cloud operation limits information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems), and to the types of transactions and functions that authorized users are permitted to exercise.
§11.10 (h)	Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	**IQVIA's SmartSolve Solution:** Limits system access to authorized individuals through a trusted authentication provider; this ensures that the user's ID and authentication method, such as password/smart card/biometric, are "authenticated" for individual user access based upon company policy. The IQVIA SmartSolve solution requires each user ID to be unique. Once the user is authenticated the IQVIA SmartSolve solution checks the roles and security uniquely assigned to the user ID to ensure the individual is authorized to be in the solution and to have access to records and activities they need to perform. IQVIA's SmartSolve solution has multiple levels of security, based on the principle of least privilege. **IQVIA's SmartSolve Cloud Operation:** Correlates information from monitoring tools employed throughout the network to achieve organization-wide situational awareness. Additionally, there is testing on the transmission of information (data) to other systems. There is an established Network Trust relationship between IQVIA and the customer. All communication is encrypted for transmission between systems for security.

21 CFR PART 11		IQVIA'S SMARTSOLVE SOLUTION
§11.10 (i)	Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.	**Customer Procedural Control:** It is the responsibility of the customer to develop policies regarding training of the regulations and the maintenance of records. IQVIA's SmartSolve Training Management solution, when used in conjunction with other solutions, provides additional access control to activities based on employee certifications as well as tracking all training activities. **IQVIA's SmartSolve Cloud Operation:** Limits access to information systems and sensitive data to only those individuals whose role requires such access. Additionally, individuals are provided with security awareness and training sessions to ensure employees are aware of and executing the policies and procedures required for a secure operation.
§11.10 (j)	The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.	**Customer Procedural Control:** It is the responsibility of the customer to develop policies and procedures governing accountability and responsibility for electronic signatures. **IQVIA's SmartSolve Solution:** Guards against falsification of records by capturing activities of the operator in the audit trail. The IQVIA SmartSolve Management solutions offer a hierarchical view of the audit trail, providing a record activity log that captures specific field-level changes through the audit trail. **IQVIA's SmartSolve Cloud Operation:** Implements Information Security Program Management controls to provide a foundation for the organization's Information Security program. The security authorization process for information systems requires the implementation of a risk management framework and the employment of associated security standards and guidelines. IQVIA's SmartSolve cloud operation creates, protects, and retains information in System Audit Records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and ensures that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

21 CFR PART 11		IQVIA'S SMARTSOLVE SOLUTION
§11.10 (k) (1)	Use of appropriate controls over systems documentation including: adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.	**Customer Procedural Control:** It is the responsibility of the customer to develop policies regarding controlled access to system manuals and system-related documentation. IQVIA's SmartSolve Document Management solution provides control over the access to these types of documents for distribution, viewing and version control. **IQVIA's SmartSolve Cloud Operation:** Periodically assesses the security controls in customers' information systems to determine if the controls are effective in their application. Documentation is maintained in a revision-controlled repository managed by IQVIA's SmartSolve QA Department.
§11.10 (k) (2)	Use of appropriate controls over systems documentation including: revision and change control procedures to maintain an audit trail that documents time sequenced development and modification of systems documentation.	**Customer Procedural Control:** It is the responsibility of the customer to develop policies regarding controlled access to system manuals and system-related documentation throughout the lifecycle of the system. Documentation provided by IQVIA is revision controlled. **IQVIA's SmartSolve Cloud Operation:** Establishes and maintains baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective System Development Life Cycles (SDLCs); and establishes and enforces security configuration settings for information technology products employed in customer information systems. IQVIA SmartSolve uses a formal process to document changes to applications, operating systems, and IQVIA's SmartSolve cloud network environment. All change control documentation reflects a record of change including the date and time of change, the reason for change, the name of the person making the change, and the person or persons who authorized the change. All IQVIA's SmartSolve cloud resources undergo formal change control procedures to ensure that only authorized changes are committed to production. Change control procedures include risk assessments, planning and testing of changes, approval process, fallback procedures, audit trails, etc.

SUBPART B — ELECTRONIC RECORDS

§11.30 Controls for Open Systems

21 CFR PART 11		IQVIA'S SMARTSOLVE SOLUTION
Section		
§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. Such procedures and controls shall include those identified in §11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	**IQVIA's SmartSolve Cloud Operation:** Brings together the IQVIA SmartSolve solution on the required hardware/infrastructure per IQVIA's SmartSolve Architecture Deployment Guide, the necessary procedures and cross-functional team to support your requirements to 21 CFR Part 11. IQVIA's SmartSolve cloud solution access is controlled by the customer's administrators. IQVIA's SmartSolve cloud operation supports "Closed System Control" as defined above in §11.10 (a)–(k)(2). In addition, IQVIA's SmartSolve cloud solution supports document encryption through the following: 1. During transmission, data is encrypted via https using Secure Sockets Layer (SSL) protocol with "128 bit encryption." 2. IQVIA encrypts data at rest via SAN (Storage Array Network) drive-level encryption technology. Closed System means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system. Open System means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.

SUBPART B — ELECTRONIC RECORDS

§11.50 Signature Manifestations

21 CFR PART 11		IQVIA'S SMARTSOLVE SOLUTION
Section		
§11.50 (a) (1-3)	Signed electronic records shall contain information associated with the signing that clearly indicates all the following: 1. The printed name of the signer; 2. The date and time when the signature was executed; and, 3. The meaning (such as review, approval, responsibility, or authorship) associated with the signature.	Electronic records are stamped with the name, date and time when the user's signature is applied. The meaning of each signature is automatically indicated with the signed record. The signature manifestation is available for viewing in the electronic record, audit trail and reports and is stored in the database, linked to the electronic record. **IQVIA's SmartSolve Cloud Operation:** Leverages the capabilities of the IQVIA SmartSolve solution installed.

21 CFR PART 11		IQVIA'S SMARTSOLVE SOLUTION
§11.50 (b)	The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section 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 (such as electronic display or printout).	The electronic signature is maintained and secured in the same manner as the electronic records. If additional signatures are required, they are appended to the record for full signature history. The signature manifestation is available for viewing in human readable format in the electronic record, in the audit trail and in reports. The information, once viewed, is available for export into many different types of electronic formats. **IQVIA's SmartSolve Cloud Operation:** Leverages the capabilities of the IQVIA SmartSolve solution installed.

SUBPART B — ELECTRONIC RECORDS

§11.70 Signature/Record Linking

21 CFR PART 11		IQVIA'S SMARTSOLVE SOLUTION
Section		
§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.	Every signature is automatically linked to its corresponding record when the signature occurs. There is no capability to remove or copy signatures from/to records by ordinary means. The audit trail keeps a complete history of when signatures occur and when there are changes. **IQVIA's SmartSolve Cloud Operation:** Leverages the capabilities of the IQVIA SmartSolve solution installed.

SUBPART C — ELECTRONIC SIGNATURES

§11.100 General Requirements

21 CFR PART 11		IQVIA'S SMARTSOLVE SOLUTION
Section		
§11.100 (a)	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	**IQVIA's SmartSolve Solution:** Requires each user ID to be unique; therefore, the electronic signature and the signature manifestation will be unique to that user. **IQVIA's SmartSolve Cloud Operation:** Leverages the capabilities of the IQVIA SmartSolve solution installed.
§11.100 (b)	Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.	**Customer Procedural Control:** It is the responsibility of the customer to establish policies and procedures to verify the identity of the individuals using the system. **IQVIA's SmartSolve Cloud Operation:** Leverages the capabilities of the IQVIA SmartSolve solution installed.

21 CFR PART 11		IQVIA'S SMARTSOLVE SOLUTION
§11.100 (c)	Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.	**Customer Procedural Control:** Each customer is required to notify the FDA in writing of their intention to use electronic signatures. It is the responsibility of the customer to perform this notification per FDA recommendations. **IQVIA's SmartSolve Cloud Operation:** Leverages the capabilities of the IQVIA SmartSolve solution installed.
§11.100 (c) (1)	The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fisher Land Rockville, MD 20857.	
§11.100 (c) (2)	Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.	

SUBPART C — ELECTRONIC SIGNATURES

§11.200 Electronic Signature Components and Controls

21 CFR PART 11		IQVIA'S SMARTSOLVE SOLUTION
Section		
§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.	**IQVIA's SmartSolve Solution:** Requires a combination of a user ID and password for identification. The solution does not include "remember me" capabilities to ensure proper identification. **IQVIA's SmartSolve Cloud Operation:** Leverages the capabilities of the IQVIA SmartSolve solution installed.
§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.	The initial login requires the entry of both the user ID and password. Subsequent signings require the entry of both electronic components that are authenticated for every signature. **IQVIA's SmartSolve Solution:** Offers a configuration that allows each signature location to capture the user ID and password, individually or in combination, with authentication occurring for every instance of a signature. **IQVIA's SmartSolve Cloud Operation:** Leverages the capabilities of the IQVIA SmartSolve solution installed.

21 CFR PART 11		IQVIA'S SMARTSOLVE SOLUTION
§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.	The initial login requires the entry of both the user ID and password. Subsequent signings require the entry of both electronic components that are authenticated for every signature. **IQVIA's SmartSolve Solution:** Offers a configuration that allows each signature location to capture the user ID and password, individually or in combination, with authentication occurring for every instance of a signature. **IQVIA's SmartSolve Cloud Operation:** Leverages the capabilities of the IQVIA SmartSolve solution installed.
§11.200 (a) (2)	Electronic signatures that are not based upon biometrics shall be used only by their genuine owners.	**Customer Procedural Control:** It is beyond the scope of the system to ensure that users do not provide others with access to their user ID and password. **IQVIA's SmartSolve Cloud Operation:** Leverages the capabilities of the IQVIA SmartSolve solution installed.
§11.200 (a) (3)	Electronic signatures that are not based upon biometrics shall 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.	**Customer Procedural Control:** It is beyond the scope of the system to ensure that users do not provide others with access to their user ID and password. **IQVIA's SmartSolve Cloud Operation:** Leverages the capabilities of the IQVIA SmartSolve solution installed.
§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.	**IQVIA's SmartSolve Solution:** Does not provide signatures based on biometrics in our solutions. Should users add biometric capabilities, it will be the customer's responsibility to validate the third-party solution. **IQVIA's SmartSolve Cloud Operation:** Leverages the capabilities of the IQVIA SmartSolve solution installed. Utilization of biometrics is a validation for the authentication provider.

SUBPART C — ELECTRONIC SIGNATURES

§11.300 Controls for Identification Codes/Passwords

Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:

21 CFR PART 11		IQVIA'S SMARTSOLVE SOLUTION
Section		
§11.300 (a)	Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.	**IQVIA's SmartSolve Solution:** Requires unique user identification codes. **Customer Procedural Control:** It is beyond the scope of the system to ensure that users do not provide others with access to their user ID and password. **IQVIA's SmartSolve Cloud Operation:** Leverages the capabilities of the IQVIA SmartSolve solution installed.

21 CFR PART 11		IQVIA'S SMARTSOLVE SOLUTION
§11.300 (b)	Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	**IQVIA's SmartSolve Solution:** Does not store the password, it leverages the authentication from a provider; therefore, it is dependent on the provider of the security policies for frequency of changes for the passwords. **IQVIA's SmartSolve Cloud Operation:** Leverages the capabilities of the IQVIA SmartSolve solution installed.
§11.300 (c)	Following loss management procedures to electronically de-authorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable rigorous controls.	**Customer Procedural Control:** Is required for the authentication provider as IQVIA's SmartSolve solution does not have devices that bear or generate identification code or password information. The local administrator needs to manage the loss. **IQVIA's SmartSolve Cloud Operation:** Leverages the capabilities of the IQVIA SmartSolve solution installed.
§11.300 (d)	Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.	**IQVIA's SmartSolve Solution:** Is tightly integrated with the security of the authentication provider; all of the security policies are identified within the authentication provider. **IQVIA's SmartSolve Cloud Operation:** Access Control Policy has been established in accordance with NIST Special Publication 800-53. Deploy extrusion and intrusion detection (IDS/IPS). IQVIA's SmartSolve cloud operation limits information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems), and to the types of transactions and functions that authorized users are permitted to exercise. **Account Management and Access Enforcement:** IQVIA's SmartSolve cloud operation ensures proper user identification and authentication management such as, verification prior to access, limits for repeated attempts and revoke for terminated users, etc.
§11.300 (e)	Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.	**Customer Procedural Control:** This is not applicable for IQVIA's SmartSolve solution as there are no devices that bear or generate identification code or password information. **IQVIA's SmartSolve Cloud Operation:** Leverages the capabilities of the IQVIA SmartSolve solution installed. Customer Procedural Control would be required for the initial and periodic testing.

References

1. Guidance for Industry, 21 CFR Part 11; Electronic Records; Electronic Signatures
2. National Institute of Standards and Technology (NIST) Special Publication 800-53 “Security and Privacy Controls for Information Systems and Organizations”
3. PIC/S PI 011-3 Good Practices for Computerised Systems in Regulated GxP Environments (2007)
4. FDA: Computerized Systems used in Clinical Investigations, 2007

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 organizations 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 organizations 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.

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

IQVIA TECHNOLOGIES