# PharmaMV™
# Advanced Process Control and Multi-Variate Monitoring Platform

## Support for the Food and Drug Administration 21 CFR Part 11 Regulation

# Table of Contents

# 1. Introduction

The PharmaMV platform is a suite of software tools for multi-variate analysis, modelling, data visualisation, process monitoring, control and optimisation. The platform is used to detect and eliminate faults, improve product quality and optimise batch and continuous pharmaceutical process units. The package combines multi-variate monitoring techniques to identify the root causes of abnormal process behaviour, with Model Predictive Control functionality to maintain or increase operational efficiency and product quality. This powerful combination of statistical models helps derive knowledge from historical data to improve future operation.

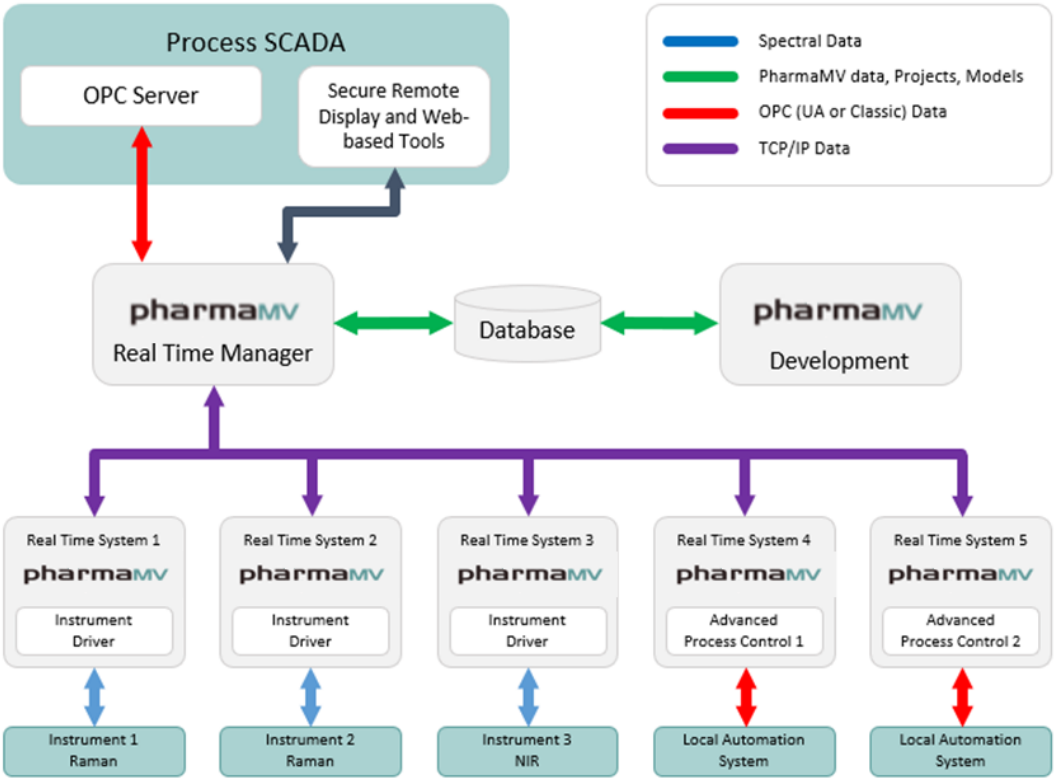
PharmaMV has been designed to meet the regulatory requirements of the Pharmaceutical industry. The Food and Drug Administration's (FDA) 21 CFR Part 11 guidance defines the requirements for computer-based systems in the pharmaceutical and food manufacturing industries. To achieve 21 CFR Part 11 compliance a system must support the required features for system access, electronic record controls and signatures. Furthermore, the system must be supplied with a full documentation set, validated against user requirements and controlled during routine manufacturing using standard operational procedures and training. Perceptive Engineering supports its clients in all aspects of the validation life cycle by providing qualification test scripts, support services and software tools to deliver compliant applications.

All aspects of Perceptive Engineering's operations are controlled by an ISO 9001:2015 Quality Management System (QMS). The QMS is rigorously applied to the development of the PharmaMV platform. The algorithms within the software are verified against industry standards on each release to ensure the accuracy and performance are maintained.

## 1.1. Platform Components

The PharmaMV platform consists of three components. These support the development, operation and maintenance of **PharmaMV Projects.** The project is the primary electronic record in the PharmaMV platform. The projects provide a wrapper for the application components including models, application specific logic, dashboards, multi-variate controllers, optimisers and prediction engines as appropriate. A project can also be configured as a Process Analytical Technology (PAT) Method. Each component shares system-wide user access controls, an audit trail (the system messages database) and project management:

1. **PharmaMV Real-Time Manager (RT Manager).** The RT Manager provides version control and configuration reporting of projects and models through its inbuilt database. It allows seamless integration with production recipe/batch management systems. These features provide the ability to deploy PharmaMV applications in a distributed network.
2. **PharmaMV Development** provides a one-box toolset containing everything needed to get the most from process data. Designed and built by experts in process improvement, to tackle the challenges of increasing process capability, capacity and quality, it supports project and model development, traceable user actions and model records. Users of PharmaMV Development have controlled access to the **RT Manager** secure database allowing project development and model maintenance activities to be completed. Multiple Development systems can be connected to the same **RT Manager** secure system database.
3. **PharmaMV Real-Time** is a fully-featured system for executing Advanced Process Control (APC) and multi-variate monitoring strategies which have been designed in PharmaMV Development. It provides, all the latest APC technologies backed up with robust tools for Data Quality Monitoring, Process Monitoring and configurable Alarms and Events. Projects and associated models that have been configured in **PharmaMV Development** are executed in the Real-Time system. These projects are extracted as required from the **RT Manager's** secure database for execution in real-time.




Example Distributed PharmaMV System

# 2. 21 CFR Part 11 Requirements

The following sections describe the FDA's requirements for computer-based systems. Within each section of the regulation is a statement describing the tools provided in PharmaMV to support compliance.

## 2.1. PART 11—ELECTRONIC RECORDS; ELECTRONIC SIGNATURES

## SUBPART A – GENERAL PROVISIONS

### 11.1 Scope.

a) The regulations in this part set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.

b) This part applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations. This part also applies to electronic records submitted to the agency under requirements of the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in agency regulations. However, this part does not apply to paper records that are, or have been, transmitted by electronic means.

c) Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required by agency regulations, unless specifically excepted by regulation(s) effective on or after August 20, 1997.

d) Electronic records that meet the requirements of this part may be used in lieu of paper records, in accordance with § 11.2, unless paper records are specifically required.

e) Computer systems (including hardware and software), controls, and attendant documentation maintained under this part shall be readily available for, and subject to, FDA inspection.

### 11.2 Implementation.

a) Computer systems (including hardware and software), controls, and attendant documentation maintained under this part shall be readily available for, and subject to, FDA inspection.

The PharmaMV Platform is a computer system for the development and deployment of Advanced Process Control and monitoring applications for use in the pharmaceutical industry. The system stores electronic records which can include process and spectroscopic data, projects and associated models. All records are stored in a secure system database. Electronic records such as data, projects and models can be readily extracted for FDA inspection.

b) For records required to be maintained but not submitted to the agency, persons may use electronic records in lieu of paper records or

1) The requirements of this part are met; and

2) The document or parts of a document to be submitted have been identified in public docket No. 92S– 0251 as being the type of submission the agency accepts in electronic form. This docket will identify specifically what types of documents or parts of documents are acceptable for submission in electronic form without paper records and the agency receiving unit(s) (e.g., specific centre, office, division, branch) to which such submissions may be made. Documents to agency receiving unit(s) not specified in the public docket will not be considered as official if they are submitted in electronic form. Paper forms of such documents will be considered as official and must accompany any electronic

records. Persons are expected to consult with the intended agency receiving unit for details on how (e.g., method of transmission, media, file formats, and technical protocols) and whether to proceed with the electronic submission.

The PharmaMV platform provides pre-built project configuration and audit trail reports. Reports are available to provide a change history/audit trail and a complete description of all configured parameters. In addition, version comparison reports provide a summary of all changes in a project from one version to the next. Additional reports are also available for system events, messages and user comments.

**11.3 Definitions.**

a) The definitions and interpretations of terms contained in section 201 of the act apply to those terms when used in this part.

b) The following definitions of terms also apply to this part:

1) Act means the Federal Food, Drug, and Cosmetic Act (secs. 201–903 (21 U.S.C. 321–393)).

2) Agency means the Food and Drug Administration.

3) Biometrics mean a method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable.

4) 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.

5) Digital signature means an electronic signature based upon cryptographic methods of originator authentication that is 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.

6) 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.

7) 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.

8) Handwritten signature means the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.

9) 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.

10) Computer systems (including hardware and software), controls, and attendant documentation maintained under this part shall be readily available for, and subject to, FDA inspection.

## SUBPART A – GENERAL PROVISIONS

### 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:

The PharmaMV Platform is designed to be implemented as a closed system. The software provides the necessary tools to ensure authenticity, integrity and confidentiality of electronic records within a closed system with the appropriate user and system access controls.

a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.

The PharmaMV platform employs encryption, file protection and monitoring mechanisms to detect invalid or altered records. Once a project electronic record is set to a released state and deployed in the PharmaMV Real-Time system, it cannot be altered or modified, as user interface access is removed. The project directory is protected through user access controls. In addition, all files associated with the released project are continuously monitored to ensure they have not been subject to external modification by an authorised user.

Perceptive Engineering Ltd can provide consultancy services, supporting documentation and test scripts to support the client with system validation. This support covers the entire project life cycle including Installation, Operational and Performance Qualification Scripts. Standard templates are also available for functional and detailed design specification.

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.

The PharmaMV Platform provides pre-configured project configuration, version history, version comparison and audit trail reports. Reports are provided in PDF format and can be generated for inspection by the agency at any time.

c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.

All records associated with the PharmaMV system are stored in a secure database. Access to this database is restricted to authorised personnel. Original records contained within the database are protected from modification and deletion. The database can be archived or backed up through standard operating procedures by authorised personnel.

d) Limiting system access to authorized individuals.

Access to the PharmaMV system is limited to authorised individuals by the user management system. Configurable user groups assigned to pre-defined privileges are provided to control access to records and system functions. The user management system supports Microsoft Active Directory integration, allowing central control of user groups and privileges.

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 as long as it is required for the subject electronic records and shall be available for agency review and copying.

All operator entries, alarms, events and record changes are recorded and stored in the system messages database. Each entry is stored with an associated date/time stamp and meta-data including the project name, username, type, severity and associated details text. Previous information is stored along with the new value entered by the operator so that previous information is not obscured. The system message audit trail is retained for the lifetime of the system and may be archived as necessary. All entries in the database can be extracted from the database at any time for agency review. The audit trail can be exported as a PDF report, or CSV format at any time.

f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.

All operator changes and entries to the system are limited to actions defined by the administrator and privilege management system. PharmaMV also automatically checks any critical parameters such as Advanced Process Control constraints and setpoints against pre-defined limits. Invalid entries are automatically rejected and logged in the system messages database. Sequencing of operator actions is provided through administrator configurable and pre-defined workflows.

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.

All system users are subject to authorization checks. Users are required to enter a unique username/password combination to access the system. User privileges are controlled by Active Directory groups than can be assigned privileges from read-only/view to full administrator access. PharmaMV provides centrally-managed user security through internal and Active Directory features:

1. Active Directory functions:
    a. Encryption of user passwords.
    b. Configurable password complexity requirements.
    c. Configurable password ageing.
    d. Limits applied to password recycling.
2. Configurable User Inactivity timeout.

Changes to projects and methods must be electronically signed before being committed to the database.

Released methods require an additional level of authorization before being committed to the database.

h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.

PharmaMV supports data collection and import from multiple data input sources including process, operator entries, online analysers, offline quality/lab systems and spectroscopic analysers. It is critical to the deployment of robust Advanced Process Control and Monitoring applications that all data sources are checked for validity. PharmaMV provides sophisticated configurable device, communications, logical and statistical checks for each data source to determine the validity of all inputs in real-time. The system provides "Data Quality Monitors" (DQM) which allow multiple checks to determine data quality (Good, Bad and Suspect). The validity checks configured in the DQM can be applied to historical data and in real-time allowing seamless transfer of data quality checks to online applications. The results of the data quality checks propagate through all aspects of the system with full traceability through the database.

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.

Perceptive Engineering provides a range of training services that are designed to meet the requirements of each system user. Training workshops are provided to introduce PharmaMV's capabilities on a variety of topics, including Digital Twins, Advanced Process Control and our unique PATNAV methodology (introduction to the application and use of PAT tools for process optimisation). Building upon the workshops, one- to three-day PharmaMV training courses are available to facilitate deeper understanding of the software platform. These training courses comprise of classroom sessions and interactive case studies and can be customised for the needs of expert system users such as system owners, chemometricians and APC engineers. For operational staff hands-on system training can also be provided as well as system specific user guide documentation.

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.

The establishment of written policies that hold individuals accountable and responsible for their actions is the responsibility of the client. Perceptive Engineering Ltd can provide consultancy services for the development of workflows and documentation as necessary to support this requirement.

k) Use of appropriate controls over systems documentation including:

1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.

Each release of PharmaMV is supplied with a full set of documentation in electronic form, specific to that version of the software. This documentation is supplied to the client as part of the installation.

Perceptive Engineering can also provide full documentation sets for delivered systems, in line with regulatory and user requirements. The control and distribution of such documents within the client's organisation is the sole responsibility of the client.

2) Revision and change control procedures to maintain an audit trail that documents time sequenced development and modification of systems documentation.

Changes made to project documentation, once released and approved by Perceptive Engineering Ltd and the client, are subject to formal change control procedures as defined by the client's quality requirements and Perceptive Engineering's Change Control procedure. Any proposed change shall be requested by completing a Change Request Form. Each Change Request is assigned a unique reference number and recorded in time sequenced audit trail on the document revision table and in Perceptive Engineering's Change Request list.

**11.30 Controls for open systems.**

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.

An open system is a computer system that is not controlled by the same people responsible for its contents [1]. The PharmaMV platform is specifically designed to operate as a closed system. Should the client wish to implement an open system additional controls must be put in place to ensure the Authenticity, Integrity, Confidentiality and Irrefutability of the electronic records within.

**11.50 Signature manifestations.**

a) Signed electronic records shall contain information associated with the signing that clearly indicates all of 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.

The PharmaMV platform requires electronic signing of projects when they are checked into the database. Each signature includes the full username and login name of the signer, the date/time stamp associated with signature execution and meta data including comments, notes and associated change request documentation identification numbers.

b) The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).

The PharmaMV platform includes the items identified in paragraphs (a)(1), (a)(2), and (a)(3) to the human readable form available with each record. The human readable forms include version history reports, configuration reports and version difference reports. Each report can be viewed on screen and is available in PDF format.

**11.70 Signature/record linking.**

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.

The electronic signature associated with a record is linked to the project in the database. It cannot be overwritten by any ordinary means. The audit trail for each project is stored in the database and each electronic signature associated with the record cannot be overwritten or transferred.

## SUBPART C—ELECTRONIC SIGNATURES

**11.100 General requirements.**

a) 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.

Unique Electronic signatures are linked to each authorised user. Integration with the client's Active Directory server and group policies within, ensure that signatures are unique and cannot be transferred to falsify records.

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.

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 and equivalent to traditional handwritten signatures.

    1) The certification shall be signed with a traditional handwritten signature and submitted in paper form to the Office of Regional Operations (HFC–100), 5600 Fishers Lane, Rockville, MD 20857.

    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.

It is the client organisation's responsibility to conform with this guidance. Specifically, the client must notify the FDA of its intention and state that it will consider electronic signatures to be as legally binding as ink signatures.

**11.200 Electronic signature components and controls.**

a) Electronic signatures that are not based upon biometrics shall:

1) Employ at least two distinct identification components such as an identification code and password.

All authorised users of the PharmaMV system are assigned an electronic signature which consists of two identification components: a user ID and a password. These components are controlled by the customer's Active Directory administrator.

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.

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.

Correct entry of both electronic signature components is required to access the system during any continuous period of access. Incorrect entry of either component will deny access to the PharmaMV system. An inactivity timer is applied to each system user. If the user does not interact with the system for a period that exceeds the timeout value, they will be logged out and will be required to re-enter both components of their electronic signature.

2) Be used only by their genuine owners; and

3) 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.

It is the client's responsibility to ensure that electronic signatures are only used by the assigned individual. By providing Active Directory integration, PharmaMV supports extensive security features for electronic signatures through Active Directory integration as listed in section 11.10 (g).

Under routine system use electronic signatures would only be used by their genuine owners. In exceptional circumstances where no workaround is available, authorised system users may require access to the electronic signature of another individual. This would require collaboration of two individuals; an administrator to generate a random password and a supervisor to set the new password to gain access to the electronic signature.

b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.

Biometric systems may be integrated into the PharmaMV system via Active Directory. It is the responsibility of the client and the supplier of such systems to ensure that they can only be used by the assigned individuals.

**11.300 Controls for identification codes/passwords.**

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

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.

All authorised users of the PharmaMV system are assigned an electronic signature that consists of a unique username and password. Username uniqueness is enforced at a system wide level.

b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).

Automated polices for Password complexity, recycling and ageing are set at system wide level. Configuration of these policies is managed by the administrator of the active directory server.

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.

The active directory system administrator can modify a user's privilege levels or reset their associated password at any-time. Users can change their active directory password should they believe their security credentials have been compromised.

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.

All activities relating to user access are logged in the system messages database. The database entries include all successful and unsuccessful attempts to access the system including user login, logout and failed log in attempts. Attempted access by unauthorised users is immediately logged. Each failed entry attempt is stored in the system messages database with the date/timestamp, entered username and the reason for the failed log in.

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.

Authentication devices such as tokens or cards are the responsibility of the device manufacturer and the client for use with active directory. These devices should be tested to ensure they function properly as per FDA guidelines.

# 3. References


| | | |
|---|---|---|
| [1] | the-ultimate-guide-to-21-cfr-part-11.pdf | The Ultimate Guide to 21 CFR Part 11. A Straight-forward Line by Line Translation into Plain English.<br>https://www.perficient.com/-/media/files/guide-pdf-links/the-ultimate-guide-to-21-cfr-part-11.pdf |