Pharmagraph - enVigil-FMS - 21 CFR Part 11

Pharmagraph was formed specifically to deploy monitoring systems in the pharmaceutical industry and accommodate its unique demands such as quality, reliability, security of data and to ensure compliance with regulatory guidelines. The parent company, Acquisition Systems Limited has been supplying systems to the pharmaceutical industry since 1992 and formed Pharmagraph in 2001 to focus on pharmaceutical and life science applications.

The Pharmagraph head office is based in Finchampstead, Berkshire, UK, with a Northern office in Cheshire UK, as well as Stirling, Scotland and Lisburn, Northern Ireland. Pharmagraph deploy systems worldwide through a network of representatives serving Europe, Asia, United States, China and India.

Pharmagraph publish the enVigil software family and design/manufacture a range of hardware products to suit environmental monitoring applications for the Pharmaceutical and Life Science industries.

enVigil-FMS has been running since 2004. This has evolved from our legacy 'Lookout' software over 25 years ago. enVigil-FMS is a constantly evolving product that will be supported for many years to come. It has been deployed World-wide and is supported by over 25 distributors around the World.

The following *enVigil-FMS* mechanisms enable compliance with 21 CFR part 11 and EU-GMP Annex 11 regulatory expectations and is also detailed in the 21 CFR Part 11 Compliance Matrix

- *enVigil-FMS* is a 'closed' system. enVigil-FMS systems are deployed on either a Windows private network or an organisation's Windows domain and therefore inside the control of the organisation that owns the data. Windows account credentials (domain users or private network users) are used to control access to the enVigil FMS software.
- *enVigil-FMS* is a 'hybrid' system. It offers electronic records but does not offer electronic signatures as standard (this is optional); hand written signatures may be applied to reports produced from the secure electronic records.
- *enVigil-FMS* does not offer or support modification of its data log, alarm log or audit log files, neither does it offer insertion or deletion of records.
- Log files are written in a proprietary binary format with integrity check codes.
- All log files are written in a date-hierarchical file structure enabling log data, alarm data and audit trail data pertaining to a date (or range of dates) to be readily collated for inspection.
- An audit trail is automatically maintained for the database, showing time and date stamped records of any parameter changes, the original and new values of the parameter and who performed the change.
- The audit trail captures loading and saving of the database and starting and stopping of system processes.
- The *enVigil-FMS* system does not allow operators to access the workstation desktop or operating system files. System menus, 'Alt-Tab' and 'Ctrl-Alt-Del' are disabled during normal operation.
- All users are required to have unique user names with passwords.
- Users are required to log in to operate the system.
- The system automatically logs users out after ten minutes inactivity.
- User log-in activity (including failed login attempts) is recorded to the audit trail.

Pharmagraph software development and test protocol documentation is available for inspection at Pharmagraph, 39 Ivanhoe Road, Hogwood Industrial Estate, Finchampstead, Berkshire, RG40 4QQ UK.

John Wallingford	**Ross Wallingford**
Operations Director	**Software Manager**
For Pharmagraph – Acquisition Systems Ltd.	**For Pharmagraph – Acquisition Systems Ltd.**

The details of how the enVigil software addresses the requirements of 21 CFR Part 11 are detailed in the table below:

Section	Requirement	How
11.10 (a)	Validation of systems to ensure accuracy, reliability, consistent intended performance and the ability to discern invalid or altered records	enVigil is a modular software system falling under the 'Configurable Off The Shelf' category. enVigil software remains standard across all projects. The *configuration* is specific to each project. Primary records are written to disk with integrity check codes. Any attempted modification of an existing record will be detected and indicated on any reports being viewed or printed.
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.	Data is in a proprietary format and cannot be viewed externally but printed reports are available for external viewing throughout the retention period.
11.10 (c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Log files are written in a proprietary binary format with integrity check codes. All log files are written in a date-hierarchical file structure enabling log data, alarm data and audit trail data pertaining to a date (or range of dates) to be readily collated for inspection. enVigil provides automatic backup of recorded data using an auto archive process. Primary records are retained until manually deleted.
11.10 (d)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	All log files are written in a date-hierarchical file structure enabling log data, alarm data and audit trail data pertaining to a date (or range of dates) to be readily collated for inspection.
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 at least as long as that required for the subject electronic records and shall be available for agency review and copying.	An audit trail is automatically maintained for configuration parameters, showing time and date stamped records of any parameter changes, the original and new values of the parameter and who performed the change. The audit trail captures loading and saving of the database and starting and stopping of system processes. User log-in activity (including failed login attempts) is recorded to the audit trail.

Section	Requirement	How
11.10 (f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	No user-level sequencing of steps or events is involved. Creation of logging ‘events’ including periodic, alarm and audit data is entirely automatic.
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.	All users are required to have unique user names with passwords. Users are required to log in to operate the system.
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.	Location of sensor inputs to the system is fixed by physical addresses within the measurement system.
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.	Initial training of operators and managers/administrators is carried out as part of project handover. Subsequent training and SOPs are the responsibility of the customer.
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.	This is the responsibility of the end customer/client. Handover training and customer SOP should outline the impact of any signature given in enVigil FMS.
11.10 (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. (2)Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	This is achieved through procedure. Initial training of operators and managers and/or administrators is carried out as part of project handover. Subsequent SOP authoring and distribution are the responsibility of the customer.

Section	Requirement	How
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.	The enVigil backend that is responsible for creating electronic records and managing system logins (enVigil Server and enVigil Security services) have been developed as Windows Services. Supported operating systems (Windows 7 onwards) employ 'Session Hardening' to further ensure authenticity, integrity, and the confidentiality of electronic records. All electronic data records and signatures have integrity checks and can be viewed only by enVigil FMS client viewers. enVigil stores all data on the Windows OS File system that, if required, can be stored on encrypted devices.
11.50 (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 signature is applied by operators of the system by supplying the Windows User ID and Password (Domain or Local account). The User ID is recorded against the signature record, the printed name of the signer is not given but the User ID is. The full name is traceable as it is stored internally against the Windows Account used to apply the signature. Each signature is stored with a date and time of execution. enVigil can be set up with up to six roles (e.g. Approver, Reviewer etc) that each signature can be applied as.
11.50 (b)	(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).	Associated printouts of batch records will display any electronic signatures where applied. Batches can be easily recalled to review any applied signatures.

Section	Requirement	How
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.	Each electronic signature in enVigil has a unique integrity code that is generated based on the entire contents of the report that is being signed together with all aspects of the signature transaction (e.g. user, date/time, role..). If any part of the data is changed the integrity check code will fail and the signature will be marked as invalid.
11.100 (a)	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	enVigil FMS enforces unique usernames, its user system is entirely based on Windows User accounts (domain or local). Electronic signatures are applied using the Windows User credentials and once signed cannot be over-signed or modified. Each signature contains the user ID as part of its integrity code.
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.	Since enVigil uses Windows User accounts and all signatures are applied using Windows account credentials this is the responsibility of the end customer/client. Often the creation of user accounts is used for site wide systems (e.g. domain user accounts) and therefore the identity of the individual is verified before such an account is created.
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.	Initial training of operators and managers/administrators is carried out as part of project handover and should explicitly cover the use of the signature to be the legally binding equivalent of traditional handwritten signatures. This is also advised to be included in any SOP or training records and is deemed to be the responsibility of the end customer.

Section	Requirement	How
11.200 (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. (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. (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.	(1) enVigil uses a Username and Password combination when applying signatures (i) Signatures are applied in the Batch Review program, that when first run requires both username and password to apply a signature. Further signatures require only the password to be entered as the last username is remembered by the system (ii) When the Batch Review program is closed (e.g. signature session ended) the last username is cleared, therefore the next time Batch Review is run both username and password is again required (2) Only genuine owners can apply signatures due to authentication requirements. (3) No sharing of electronic signatures is permitted in enVigil FMS
11.200 (b)	*Electronic signatures based upon biometrics …*	(Not applicable)
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.…	enVigil FMS does not allow any duplicate Usernames so that the combination of username and password is always unique.
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).	enVigil FMS can enforce password change after a configurable amount of time and other password hardening features available in the Windows Operating system upon which its security system is based

Section	Requirement	How
11.300 (c)	Following loss management procedures to electronically deauthorize 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.	(Not Applicable)
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.	enVigil uses Windows authentication and such events can be monitored in the Windows Security Audit.
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	(Not Applicable)