21 CFR Part 11
Pyris Enhanced Security

Electronic Records – System Design

CFR Ref.	Question	Pyris Enhanced Security
11.10(a)	Does the supplier have a QMS?	ISO 9001
11.10(a)	Is it possible to see on the system whether or not records have been altered?	Pyris Enhanced Security appends a checksum to all records. Attempting to open a file that has been altered outside the system will generate an error message and an entry in the audit trail. For valid but altered records version number will be applied.
11.10(a)	Can the system identify invalid records?	Pyris Enhanced Security appends a checksum to all records Attempting to open a file that has been altered outside the system will generate an error message and an entry in the audit trail
11.10(b)	Is the system capable of producing accurate and complete copies of records in **electronic form** for inspection, review and copying by the FDA?	All files can be read using the Pyris Application Software. In addition the data can be exported as ASCII text which can be viewed using an ASCII editor.
11.10(b)	Is the system capable of producing accurate and complete copies of records in **paper form** for inspection, review and copying by the FDA?	All files can be printed using the Pyris application software
11.10(c)	Are the records readily retrievable throughout their retention period	Records are always retrievable using the version of Pyris Application Software used to create them or newer versions. In addition the data can be exported as ASCII text which can be viewed using an ASCII editor.
11.10(d)	Is system access limited to authorised individuals?	Pyris Software and the computer that it runs on meet the requirements of a closed-system. Pyris Enhanced Security uses a secure login process with the ability to define user groups with different permissions that reflect the workflow of the laboratory To ensure only authorised individuals can use the system: • No two individuals can have the same combination of user name and password • Reuse of password is not allowed • Old accounts can be disabled and cannot be reassigned • Passwords must be periodically checked, recalled or revised (password ageing) • Account lockout after an administrator-specified number of failed logins In addition, the administrator is able to limit access to individual instruments to specified users.
11.10(e)	Is there a secure, computer generated, time stamped audit trail that records the date and time of operator entries and actions that create, modify, or delete electronic records?	The Audit Trails created by the system records every significant action performed by the operator which affect the analytical results or electronic records written to a file. Each Audit Trail includes date, time, operator name, action performed, and other parameters , which may be needed to describe what was done.
11.10(e)	Upon making a change to an electronic record, is	The original file will be left intact and a new version created.

CFR Ref.	Question	Pyris Enhanced Security
	previously recorded information still available (i.e. not obscured by the change)?	The old version of any file is copied to an Archive directory. The version number are incremented to indicate that a changed version was created. .
11.10(e)	Are there utilities/tools available to ensure that an electronic record's audit trail captured using one version of software will be readable in the next version of the software?	Records with their Audit Trail are always retrievable using the version of Pyris Application Software used to create them or newer versions. In addition the data can be exported as ASCII text which can be viewed using an ASCII editor
11.10(e)	Is the audit trail available for review and copying by the FDA?	The audit trail is defined to be an electronic record. Records are always retrievable using the version of Pyris Application Software used to create them or newer versions. In addition the data can be exported as ASCII text which can be viewed using an ASCII editor.
11.10(f)	If the sequence of system steps or events is important, is this enforced by the system (e.g. as would be the case in a process control system)?	Some features of Pyris already provide this, such as Player, Calibration wizard, calculation user interfaces. Others require SOP's
11.10(g)	Does the system ensure that only authorised individuals can use the system, electronically sign records, access the operation or computer system input or output device, alter a record, or perform other operations?	Pyris Software and the computer that it runs on meet the requirements of a closed-system. Pyris Enhanced Security uses a secure login process with the ability to define user groups with different permissions that reflect the workflow of the laboratory To ensure only authorised individuals can use the system: • No two individuals can have the same combination of user name and password • Reuse of password is not allowed • Old accounts can be disabled and cannot be reassigned • Passwords must be periodically checked, recalled or revised (password ageing) • Account lockout after an administrator-specified number of failed logins In addition, the administrator is able to limit access to individual instruments to specified users.
11.10(k)	Is the distribution of, access to, and use of systems documentation controlled?	Electronic documents furnished with the Pyris Software System are present on the CD which cannot be changed by the user. The CD has a part number which identifies the version of the documents present on the CD.
11.10(h)	If it is a requirement of the system that input data or instructions can only come from certain input devices (e.g. terminals) does the system check the validity of the source of any data or instructions received? (Note: This applies where data or instructions can come from more than one device, and therefore the system must verify the integrity of its source, such as a network of weigh scales, or remote, radio controlled terminals).	Manual input of serial number is enforced. A SOP is required to assure update if instrument gets exchanged.

Electronic Signatures – System Design

CFR Ref.	Question	Pyris Enhanced Security
11.50	Do signed electronic records contain the following related information? - The printed name of the signer (NB. the user id alone is not acceptable) - The date and time of signing - The meaning of the signing (such as approval, review, responsibility)	Yes
11.50	Is the above information shown on all screen based and printed copies of the electronic record?	Yes
11.70	Are signatures linked to their respective electronic records to ensure that they cannot be cut, copied, or otherwise transferred by ordinary means for the purpose of falsification?	Yes
11.200 (a)(1)	Are non-biometric signatures made up of at least two components, such as an identification code and password, or an id card and password?	Yes
11.200 (a)(1)(i)	When several non-biometric signings are made during a continuous session, is the password executed at each signing? (Note: both components must be executed at the first signing of a session)	Yes
11.200 (a)(1)(ii)	If signings are not done in a continuous session, are both components of the non-biometric electronic signature executed with each signing?	Yes,
11.300 (b)	Do passwords periodically expire and need to be revised?	Yes, User defined expiration date
11.300 (b)	Is the system configured to detect attempts at unauthorised access?	Yes User defined number of attempts

Electronic Signatures – Operational Controls and Procedures

CFR Ref.	Question	Pyris Enhanced Security
11.100(a)	Are user id codes (and therefore electronic signatures) unique to an individual?	Yes
11.200 (a)(3)	Would an attempt to falsify a non-biometric electronic signature require the collaboration of at least two individuals?	Yes
11.300(a)	Are controls in place to maintain the uniqueness of each combined identification code and password, such that no individual can have the same combination of identification code and password?	Yes
11.300(b)	Are procedures in place to ensure that passwords are periodically revised? (e.g., does the system automatically force password ageing?)	Yes
11.300(b)	Is there a procedure for removing or dis abling system access if a person leaves or is transferred? (e.g., can access be removed while retaining access history?)	Yes
11.300(d)	Is there a procedure for detecting attempts at unauthorised use and for informing security? (e.g., is the system capable of detecting and reporting to the system security unit any attempts at unauthorised use of passwords and/or identification codes?) Urgent and immediate.	Unauthorised attempts at access logged in login history file. The users SOP describe a procedure for regular review of the history file.
11.300(d)	Is there a procedure for reporting repeated or serious attempts at unauthorised use to management?	N/A