Honeywell

Electronic Paperless Recorders

eZtrend QXe, Minitrend QX and Multitrend SX

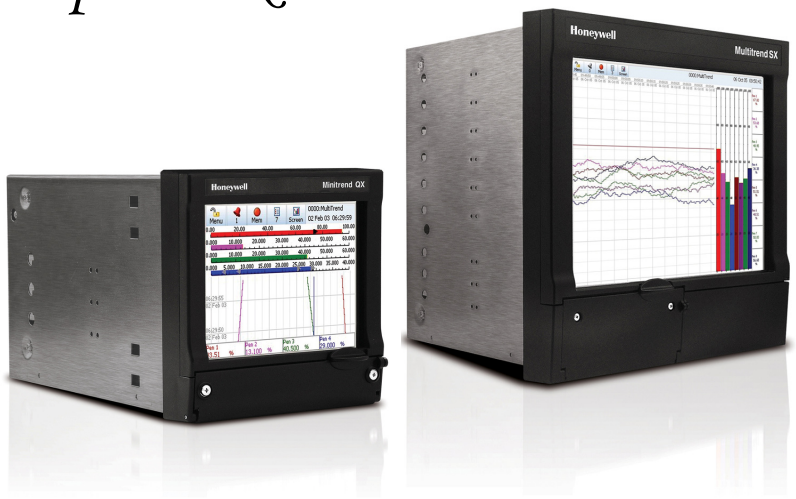
Meeting 21 CFR Part 11 Requirements

Honeywell Compliance Certificate

21 CFR Part 11

eZtrend QXe, Minitrend QX and Multitrend SX

Electronic Paperless Recorders



Honeywell Electronic Paperless Recorder

For Meeting 21 CFR Part 11 Requirements

Applicable on eZtrend QXe, Minitrend QX & Multitrend SX Models with the ESS option

(ESS= "Extended Security System")

21 CFR Part 11 Requirements Rev. April 1, 2004 Electronic records; Electronic signatures	Honeywell – eZtrend QXe, Minitrend QX and Multitrend SX	Additional Comments or Questions
Subpart B-Electronic Records *Subpart B, Section 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."* ➢	Creates write-once, read-only encrypted records which persons with access to the system cannot falsify by any normal means. All Software and playback utilities provide a means to examine the data, but not alter it.	Data can be exported to an application such as an Excel spreadsheet, and then manipulated as needed.
Subpart B, Section 11.10 (a). ➢ *"Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records."*	Honeywell Service offers Validation Services to help validate the system.	
Subpart B, section 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."* ➢ Per docket No. 92S-0251 the agency will accept the following electronic formats; PDF, SAS Transport, or ASCII, on the following media; CDROM or Magnetic Tape (DLT).	All data can be recorded to an external media; Compact Flash or USB Memory Key. Any graphics generated for PC or printout is generated from the numerically encrypted binary data. Therefore, either form of data is technically as accurate as the original. CRC error checking is embedded within the data records to assure the integrity of transmitted and copied records. Note: eZtrend QXe only supports USB	Data can also be converted to Excel spreadsheets for FDA inspection if the SW is not available to them.

21 CFR Part 11 Requirements Rev. April 1, 2004 Electronic records; Electronic signatures	Honeywell – eZtrend QXe, Minitrend QX and Multitrend SX	Additional Comments or Questions
Subpart B, section 11.10 (c). ➢ *"Protection of records to enable their accurate and ready retrieval throughout the records retention period."*	The above listed storage media can be filed for retention or the data could be copied to a CDROM for a longer lasting storage media. Disks can be labeled for asset number and period of time on media.	
Subpart B, section 11.10 (d). ➢ *"Limiting system access to authorized individuals."*	The recorders contain password protection with 50 possible 20 character usernames and 20 character passwords, which then provide 4 different levels of access to protect the various configuration areas within product configuration and display use. There is an Administrator function to manage passwords	The minimum number of characters for defining a "username" or "password" is 1. Can be set to require passwords with Alpha characters, numeric and/or symbols as part of the password.
Subpart B, section 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 for at least as long as that required for the subject electronic records and shall be available for agency review and copying."*	The recorder continuously generates a detailed audit trail that includes time/date stamps of operator access, operator actions, alarm status, system changes, disk insertion and removal, power outages and recovery, system diagnostics, setup changes, and other critical functions. The audit trail is an integral part of the electronic archive record and remains as long as the process records are retained. The audit trail is viewable on the same display as the process records. It keeps a record of all entries made into each level of the recorder, by user ID, with a time/date stamp and identification if access has been accepted or denied.	
Subpart B, section 11.10 (f). ➢ *"Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate."*	Not applicable to the recorder.	This does not apply, as operator functions are limited to screen changes and chart marks. There are no data entry sequences that would require such safeguards.

21 CFR Part 11 Requirements Rev. April 1, 2004 Electronic records; Electronic signatures	Honeywell – eZtrend QXe, Minitrend QX and Multitrend SX	Additional Comments or Questions
Subpart B, section 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."*	Recorder access is user ID/password protected and the actions taken can be traced to the username. Each Login profile can be allocated a level of authorized access (4 levels available) within various recorder functional areas. Each user is specifically assigned to the individual profiles. The recorder tracks all user entries and checksums are provided to prevent data from being changed without detection.	The 4 levels of user access are: Engineer (Master), which is the highest level, Supervisor, Technician, Operator. An Administrator function is available that sets up the restriction levels and can manage adding and deleting users.
Subpart B, section 11.10 (h). ➢ *"Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source data input or operational instruction."*	Does not apply directly to the recorder, but would need to be verified during validation.	
Subpart B, section 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."*	Does not apply directly to the recorder. Training would be through a SOP for paperless recorders.	
Subpart B, section 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."*	Does not apply directly to the recorder. User is responsible for adhering to the policies written.	

21 CFR Part 11 Requirements Rev. April 1, 2004 Electronic records; Electronic signatures	Honeywell – eZtrend QXe Minitrend and Multitrend Plus	Additional Comments or Questions
Subpart B, section 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.*	Does not apply directly to the recorder. These specifics would need to be included or addressed in the SOP. Changes made to the Setup of the recorder are logged in the Audit trail with time/date stamp and user ID. "Status - Maintenance" menu in the recorder provides information on the date & time, to a 100th of a second, of the last time the set up was actually changed. This can be used to validate whether a recorder configuration was changed since the last time this was inspected.	
Subpart B, section 11.30. Controls for open systems. ➢ *"Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls 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."*	Systems at most Pharmaceutical companies would most likely be closed systems unless they are linked to the network or located in an area that cannot ensure limited access. It is more prudent to assume an Open System environment. The recorder creates write-once, read-only encrypted records, which persons with access to the system cannot falsify by any normal means. All Software and playback utilities provide a means to examine the data, but not alter it.	

21 CFR Part 11 Requirements Rev. April 1, 2004 Electronic records; Electronic signatures	Honeywell – eZtrend QXe, Minitrend QX and Multitrend SX	Additional Comments or Questions
Subpart B, section 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."* *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)."*	Users must login and enter their password before taking any action. If the user makes an entry, performs a system change, or executes a pre-configured message, he must include his password to execute the change. His secret password serves as the electronic signature. The audit trail function will be appended to include the user's login name to indicate the identity of the user.	First timer users are forced to use the default password and immediately change their password on login before taking any action.
Subpart B, section 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 records created by the recorder are not as complex as other computer records that this section is intended to address. Each record created is protected by encryption and linked to the user's ID (signature) with time stamping. The data archive also is linked to the recorder's configuration for added security and understanding of the recorded data.	
Subpart C-Electronic Signatures *Subpart C, section 11.100 (a).General requirements* ➢ *"Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else."*	The recorder provides the ability to assign 50 unique user ID names. Each user has to secretly enter and maintain his password. The assignment of unique user ID names to individuals needs to be managed by the SOP.	The user with Administrator level access can delete a specific user ID or delete "all" users to a default. The Administrator does not have access to stored user passwords; these are stored at the recorder and are not visible.

21 CFR Part 11 Requirements Rev. April 1, 2004 Electronic records; Electronic signatures	Honeywell – eZtrend QXe, Minitrend QX and Multitrend SX	Additional Comments or Questions
Subpart C, section 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."*	Does not apply directly to the recorder. This requirement needs to be managed by the user according to their SOP.	
Subpart C, section 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."*	Does not apply directly to the recorder. This requirement needs to be managed by the user according to their SOP.	
Subpart C, section 11.100 (1). ➢ *"The certification shall be submitted in paper form with a traditional handwritten signature, to the Office of Regional Operations (HFC-100)."*	Does not apply directly to the recorder. This requirement needs to be managed by the user according to their SOP.	
Subpart C, section 11.100 (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."*	Does not apply directly to the recorder. This requirement needs to be managed by the user according to their SOP.	

21 CFR Part 11 Requirements Rev. April 1, 2004 Electronic records; Electronic signatures	Honeywell – eZtrend QXe, Minitrend QX and Multitrend SX	Additional Comments or Questions
Subpart C, section 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."* *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 use 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."*	The recorder software will require the user to enter his user ID and password to gain access to the recorder's functions. This will serve as his electronic signature. Only single signings or messaging taken within a user session is allowed – this is tracked with time/date stamp and user ID, then the user is logged out. A user session can be terminated with an automatic recorder time-out function, which returns the recorder to normal safe state (process screen display) if a logged in user does not perform any action within a specified time (1 to 10 minutes). A user will be required to re-enter both login (user ID) and password.	First timer users are forced to use the default password and immediately change their password on login before taking any action.
Subpart C, section 11.200. continued *2) "Be used only with 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.* *b) "Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners."*	Each user is assigned a unique user ID and only the user ID can define his associated password within the recorder. Acceptance of the use of an individual's unique user ID/password by anyone other than the genuine owner needs to be addressed in the SOP.	

21 CFR Part 11 Requirements Rev. April 1, 2004 Electronic records; Electronic signatures	Honeywell – eZtrend QXe, Minitrend QX and Multitrend SX	Additional Comments or Questions
Subpart C, section 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:"* *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."* *b) "Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging)."* *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."* *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 the unauthorized use to the system security unit, and, as appropriate, to organizational management."* *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."*	Written procedures would need to include the specific controls for maintaining, issuing, testing, and tracking of the assigned identification codes and passwords. Passwords will expire on a configurable interval of 1 to 365 days. A new password will then be required, having provided the old one, before accessing any other functions. If a user fails to successfully login after 1 to 10 attempts as set by the administrator, the recorder will disable the login-password combination and log the occurrence on the audit trail. The administrator having Engineer (master) level access will have to obtain a password from the manufacturer that allows access enabling all users to be deleted and re-create all new user ID's and have the user create new passwords. The Administrator can delete the user ID if the user has forgotten their password and re-create a new user ID entry and not be locked out the log-in function. The user would then be treated as a new first time user, be required to use the default password and immediately create a new password before proceeding with any other action.	