

Coding v3.XX 21 CFR Part 11 Compliance Grid

Sub-part\ Section\ Para-graph	Description	Coding
B	Electronic Records	
11.10	Controls for closed systems	
(a)	Validated?	Yes
(b)	Accurate and complete copies?	Yes, Coding stores its data in Oracle tables, SQL Server tables or SAS data sets.
(c)	Protection of records	Yes, the user has no access to the records other than to code them. They cannot modify fields other than those that are mapped. There is no manual access to the data through the system.
(d)	Limiting system access to authorized personnel	Yes, personnel need to be setup as a user in the system.
(e)	Computer-generated, time-stamped audit trails	Yes. Reason for change is always implicit.
(f)	Operational system checks to enforce permitted sequencing of steps and events	NA
(g)	Authority checks	Yes, same as 11.10 (d)
(h)	Device (e.g., terminal) checks	NA. This is best handled by the network operating system. We think that device checks are good for high-risk activities such as control of a server. However, we do not believe that there are any functions of this system that need to have security greater than the security provided by creating a trusted user.
(i)	Training	DZS Personnel have been instructed regarding this regulation. Clients are responsible for training their own personnel as to the seriousness and gravity of using and abusing their userids and passwords.
(j)	SOPs	Same as (i)
(k)	System documentation	Client's responsibility, DZS provides product user guides.
11.30	Controls for open systems	Not open, unless the Client's network is an open system.
11.50	Signature manifestations	There is no signing process within the system. Electronic records do end up being linked to the user that coded them.
(a)	Name, date, time and meaning	NA
(b)	Controls for (a)	NA
11.70	Signature/record binding	NA

Coding v3.XX 21 CFR Part 11 Compliance Grid

Sub-part\ Section\ Para-graph	Description	Coding
C	Electronic Signatures	
11.100	General Requirements	
(a)	Unique to one individual	No duplicate userids allowed. Our clients ensure that their users do not share userids.
(b)	Identity of the individual	Client's responsibility
(c)	Certify to the agency	Client's responsibility
11.200	Identification mechanisms and controls	
(a)	Two distinct identification components	Yes.
(b)	Biometrics	None of our products preclude or require the use of biometrics.
11.300	Controls for identification codes/passwords	
(a)	Userid uniqueness	Client's responsibility for their network. Our clients ensure that their users do not share userids. An account must be defined in the coding tool even if they are using LDAP integration for passwords. The system does not allow duplicate userid's.
(b)	Periodically checked, recalled, or revised	Yes, passwords can be aged with minimum or maximum ages. The System Administrator can force Users to change their password at their next login. The System Administrator can disable a user's account.
(c)	Deauthorize lost, stolen, missing, or potentially compromised userids	The System Administrator can disable a user's account.
(d)	Prevent unauthorized use of passwords and/or identification codes	Yes, system can be locked after a user defined number of failed logins. Locked accounts stay locked for a defined number of minutes or indefinitely. Client is responsible for making sure that user's do not share userids and/or passwords.
(e)	Initial and periodic testing of devices	NA