

Data Management V3.XX 21 CFR Part 11 Compliance Grid

Sub-part\ Section\ Para-graph	Description	Data Management	
B		Electronic Records	
	11.10	Controls for closed systems	
	(a)	Validated?	Yes, it will also include indices that specifically trace tests to design specs, test categories and 21 CFR Part 11 sections.
	(b)	Accurate and complete copies?	Yes, ClinPlus Data Management stores its data in SAS data sets, an FDA standard.
	(c)	Protection of records	Password protected clinical data, encryption of the system password and good network security. Enhanced security can be achieved through SAS Share. Studies can have different passwords and randomly generated passwords. The system files can have different passwords than the clinical data. Different passwords can be used for read, write or alter access. Users can be warned when they try to clear passwords.
	(d)	Limiting system access to authorized personnel	Users have the option to limit access in three ways: 1) prompt for User Name and Password, 2) Prompt for password and get userid from network login and 3) no password required, get userid from network login. This last option is there in case you are using a Citrix Server. In addition, security can be set like network security, where a user is made a member of a group and that group gives access to certain tasks.
	(e)	Computer-generated, time-stamped audit trails	Yes, all system and data operations are audited, i.e. the audit trail starts at first key data entry.
	(f)	Operational system checks to enforce permitted sequencing of steps and events	Yes, i.e. second key is only after first key.
	(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 or group.
	(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.
	11.50	Signature manifestations	
	(a)	Name, date, time and meaning	Yes, Name means the Real Name.
	(b)	Controls for (a)	Yes
	11.70	Signature/record binding	The Administrator's password must be controlled procedurally or you might be able to edit data behind the scenes. Using version 3.2X EDC capabilities, the Investigator signature is linked to the data through the COVER program. This means that in order to tell if the data has been modified after

Applies to all Data Management v3.XX versions.

S:\office docs\21CFRPart11ComplianceDMV3.XX_v1.04.doc

Data Management V3.XX 21 CFR Part 11 Compliance Grid

Sub-part\ Section\ Para-graph		Description	Data Management
			the Investigator has been signed, a special COVER program has to be run. Still the electronic signature cannot be excised, copied or transferred without administrator privileges, detailed knowledge of how the system works and advanced SAS programming knowledge.
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	Depends on 11.10 (d). If option 3 is chosen, you cannot be compliant, unless you are running it under a Citrix Server or something similar.
		(b) Biometrics	None of our products precludes or requires the use of biometrics.
	11.300	Controls for identification codes/passwords	
		(a) Userid uniqueness	No duplicate userids allowed. Our clients ensure that their users do not share userids.
		(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		Not applicable	

Applies to all Data Management v3.XX versions.

S:\office docs\21CFRPart11ComplianceDMV3.XX_v1.04.doc