

## 21 CFR Part 11 Memory Jogger

28-Feb-03

Subpart A-General Provisions	Subpart B-Electronic Records	Subpart C-Electronic Signatures
<p><b>11.1 Scope***</b></p> <ul style="list-style-type: none"> <li>a. – criteria for reliability</li> <li>b. – created under records requirements</li> <li>c. - electronic signatures meet requirements</li> <li>d. – electronic records meet requirements</li> <li>e. – computer systems</li> </ul> <p><b>11.2 Implementation</b></p> <ul style="list-style-type: none"> <li>a. – maintained records</li> <li>b. – submitted records</li> </ul> <p><b>11.3 Definitions</b></p>	<p><b>11.10 Controls for closed systems</b></p> <ul style="list-style-type: none"> <li>a. – validation***</li> <li>b. – copies of records***</li> <li>c. – protection and retention of records***</li> <li>d. – limited access</li> <li>e. – computerized audit trails***</li> <li>f. – operational system checks</li> <li>g. – authority checks</li> <li>h. – device checks</li> <li>i. – trained users</li> <li>j. – written policies to hold signature users accountable</li> <li>k. – controls over system documentation</li> </ul> <p><b>11.30 Controls for open systems</b></p> <p>Confidentiality and additional measures for data integrity</p> <p><b>11.50 Signature manifestations</b></p> <ul style="list-style-type: none"> <li>a. – name, date/time, meaning</li> <li>b. – human readable</li> </ul> <p><b>11.70 Signature/record linking</b></p> <p>Controls to avoid falsification, copying, and assure link integrity</p>	<p><b>11.100 General requirements</b></p> <ul style="list-style-type: none"> <li>a. - uniqueness</li> <li>b. – verification of individual’s identity</li> <li>c. – certification to FDA</li> </ul> <p><b>11.200 Electronic signature components and controls</b></p> <ul style="list-style-type: none"> <li>a. – non-biometric           <ul style="list-style-type: none"> <li>1. – two components               <ul style="list-style-type: none"> <li>i – one reentered for each signing in a session</li> <li>ii – both reentered for first signing of each session</li> </ul> </li> <li>2. Use by genuine owner only</li> <li>3. Collaboration by two or more</li> </ul> </li> <li>b. – biometric</li> </ul> <p><b>11.300 Controls for Identification Codes and Passwords</b></p> <ul style="list-style-type: none"> <li>a. – maintaining uniqueness of ID/password combination</li> <li>b. – periodic checks/revision</li> <li>c. – loss management</li> <li>d. – transaction safeguards</li> <li>e. – token testing</li> </ul>

The items highlighted and asterisked are those directly affected by FDA’s Federal Register Notice and Draft Part 11 Scope and Application Guidance issued Feb 2003 when all prior guidance and the compliance policy guide were withdrawn. FDA indicated it will exercise enforcement discretion on these items significantly reducing the burden on industry of this rule while it reexamines it as part of a modernization effort. Detailed explanations are available in a separate training aide to subscribers of SoftwareCPR.com.