

### LABELING - COMPLIANCE CHECKLIST

Many labeling software packages and suppliers claim compliance with 21CFR part11. It is worth noting that a piece of software of and by itself cannot be compliant. Any application must be supported by a properly conceived and performed validation project, following GAMP guidelines.

Also there are certain requirements that the software must achieve. The PRISYM [Medica](#) application was devised and created with due diligence and follows precisely the 21CFR part11 rule. PRISYM<sup>LS</sup> have created the following checklist of features that a software package should possess for compliance.

Apply it to any alternative you may be considering as an aid to gauging its suitability.

FDA REQUIREMENT	MEDICA	OTHER
<p><b><u>Accurate &amp; Complete Copies:</u></b> Does the package generate complete and accurate copies of every critical action performed on the system?</p>	✓	
<p><b><u>Protection of Records:</u></b> Are records protected to ensure accurate and speedy retrieval?</p>	✓	
<p><b><u>Limiting System Access:</u></b> Are records protected against unauthorised input, deletion or modification of data?</p>	✓	
<p>Does the software record any attempt at unauthorised access?</p>	✓	
<p><b><u>Secure Audit Trail:</u></b> Are records on the audit trail created by the system, independently of the users?</p>	✓	
<p>Is there an accurate date/time stamp of all entries that create or modify electronic records?</p>	✓	
<p>Does the system ensure that any changes to electronic records do not obscure previous data?</p>	✓	
<p><b><u>Operational System Checks:</u></b> Does the system enforce correct sequencing of steps and events as appropriate? (e.g. enforcing the approval process for label designs.)</p>	✓	

<p><b><u>Authority Checks:</u></b> Do checks exist to ensure that only authorised persons can use the system and provide electronic signatures for actions appropriate to their level of authority?</p>	✓	
<p><b><u>Signature / Record linking:</u></b> Are electronic signatures automatically linked to electronic records of actions?</p>	✓	
Does the signature / record linking ensure that signatures cannot be copied or transferred?	✓	
<p><b><u>Unique Signatures:</u></b> Does the system ensure that each electronic signature is unique, not allowing duplicates?</p>	✓	
<p><b><u>Two Distinct Components:</u></b> Does the system enforce a two part signature (User ID &amp; password)?</p>	✓	
Does the system prevent System Administrators from having access to user passwords?	✓	
Is there a mechanism for assisting users who have forgotten their password?	✓	
<p><b><u>Use of Components During Sessions:</u></b> Does initial sign on insist on use of both components?</p>	✓	
Does the system request password only for subsequent actions during a continuous session?	✓	
<p><b><u>Uniqueness of Combined Components:</u></b> Does the system ensure that no two users have the same id / password combination?</p>	✓	
Is each id / password combination directly attributable to a single individual, is the person's actual identity recorded against actions in the audit log?	✓	
Does a mechanism exist to ensure users do not simply reuse passwords (e.g. password history)	✓	

<p><b><u>Transaction Safeguards:</u></b> Does the system detect and signal any unsuccessful attempts at access?</p>	✓	
<p><b><u>Signature Manifestation:</u></b> Does the secure audit log (if it exists) show the printed name of the signer, the date/time of the signing and the meaning of the signature in a single record?</p>	✓	

For more information about Validation of Compliant Labeling Systems including our range of labeling and tracking products and services please contact +44 (0)118 936 4400 or email [info@prisymid.com](mailto:info@prisymid.com)