白皮书

Agilent
Trusted Answers

支持 21 CFR Part 11 和附录 11 的法规要求：用于 Cary 3500 的 Agilent Cary 紫外工作站软件

概述

US FDA 21 CFR Part 11（美国联邦法规第 21 章第 11 款）及其类似条款欧盟 Eudralex 第 4 章附录 11 中，介绍了受监管医药组织电子记录和电子签名的要求。21 CFR Part 11 于 1997 年公布，自 1999 年起施行。实施这些准则的目的是为确保所有合适的电子记录有因可循、清晰易懂、同步记录、原始、准确并且保存完整。

本白皮书为 Agilent Cary 紫外工作站与 OpenLab 软件（包括控制面板和内容管理应用程序）用户提供了有用的资源。Cary 紫外工作站软件用于 Cary 3500 紫外-可见分光光度计的仪器控制和数据分析。用户及其组织负责确保本软件包提供的功能使用得当，从而实现实验数据采集和处理的合规操作。除了软件提供的技术控制之外，用户组织还须建立程序控制（标准操作规程 (SOP)），以满足相关的非技术性要求。例如，还须建立内部审计计划等控制措施，确保系统操作人员遵循 SOP。

附录 1 详细介绍 Cary 紫外工作站软件如何支持用户及其组织，以达到 21 CFR Part 11 各章节以及欧盟附录 11 相关各章节的要求。该说明假定系统访问（包括仪器硬件和软件）由负责系统所含电子记录的工作人员控制。因此，系统按照 21 CFR Part 11.3(b)(4) 的定义设计为“封闭系统”。

21 CFR Part 11

21 CFR Part 11 涵盖受监管实验室运行的三个特定要素：

- 电子记录的安全性
- 工作归因
- 电子签名（如果使用）

安全性

安全性可以解释为“合适的人员具有访问合适信息的合适权限”。受监管组织必须既能验证系统用户的身份，又能仅允许经过培训并获得授权的个人访问系统（依据 11.10(d)、(i) 和 (g)；11.100(b)）。由于实验室工作人员所承担的责任根据其工作分配而有所不同，因而必须对数据访问权限加以区分和定义，使特定用户拥有特定数据集的特定访问权限类型，同时可能对其他数据集拥有不同的访问权限。

> “职责分离作为一项安全原则，以防止欺诈和错误为主要目标。通过在多个用户之间分散特定业务流程的任务和相关权限可实现这一目标。”
>
> Botha，Eloff，IBM 系统期刊[1]

工作归因

工作归因指记录执行工作的“人员、内容、时间、位置及原因”。自动化审计追踪可独立记录用户操作，从而将实验室工作人员与其执行的工作联系起来。通过审计追踪条目，工作人员和监管人员能够重建电子记录的完整历史。

- **人员：**明确指出负责创建、修改或删除记录的特定操作的人员
- **内容：**指所执行的操作，包括记录中所含的旧值和新值（如果适用）
- **时间：**明确声明操作发生的日期和时间
- **位置：**明确指出受影响的记录
- **原因：**解释变更受监管记录的原因。原因通常从预定义的原因列表中选择，以确保一致性并允许对条目进行搜索和排序

电子签名

虽然 21 CFR Part 11 不强制使用电子签名，但仍对使用电子签名时的要求进行了规定。在这种情况下，系统必须确保电子签名：

- 以不可撤回的方式链接到相应记录
- 显示签署人的全名、日期和时间，以及签名的意义或原因（例如出于审查、批准、职责或原创目的）
- 在每次显示或打印签署记录时出现

系统拓扑结构

安捷伦提供两种配置的 Cary 紫外工作站，其中数据存储在 OpenLab 中，您可以：

- 在连接到 Cary 3500 的 PC 上本地存储和管理数据
- 在 OpenLab 选项中集中存储和管理数据

请参阅“Cary UV Workstation With OpenLab Server or ECM 3.6 Software, System Topologies and Architectural Concepts”（配置 OpenLab 服务器或 ECM 3.6 软件的 Cary 紫外工作站：系统拓扑和架构概念），了解更多详细信息。

附录 1. 使用 Agilent Cary 紫外工作站满足 US FDA 21 CFR Part 11 和相关全球性法规中的要求

附录 1 表注

第一列

此表按照 US FDA 参考文件中的显示顺序介绍 21 CFR Part 11 要求[2]。欧盟附录 11[3] 等法规中的相关要求遵循 Part 11 中各节的规定。

第二列

出于完整性考虑，第二列列出 21 CFR Part 11 的所有要求及其他相关全局要求。“系统”指用于采集和处理数据的分析系统。

大多数要求通过技术控制（即软件功能）或程序控制（即 SOP）来满足。技术控制是由软件及软件供应商提供的控制，而程序控制则由用户组织负责。以粗体形式列出的 21 CFR Part 11 要求由技术控制解决。其他全局要求以常规字体形式列出。必须由过程控制解决的要求以蓝色列出。

第三列

一些要求既涉及技术控制又涉及程序控制。第三列列出了每个要求的职责。“S”指分析系统供应商。“U”指用户组织。以蓝色显示的行包含必须由用户组织专门解决的要求。蓝色也可以表示将由用户负责实施的技术控制。

第四列

在可用并合适的情况下，第四列提供相关的全局要求和注释。

第五列

第五列用“是”或“否”表示使用 Cary 紫外工作站中提供的技术控制能否满足要求。N/A 指不适用于该软件。

第六列

第六列说明如何使用 Cary 紫外工作站软件提供的技术控制满足法规要求。第六列还在适当的情况下为用户组织提供附加建议。

1. 验证

Part 11 及其他	要求	S，U	其他相关法规和注释	是/否	如果是，具体说明如何满足要求？如果否，对用户有什么建议？
Part 11 11.10(a)	1.1 是否对系统进行验证，以确保准确性、可靠性、一致的预期性能及识别无效或变更记录的能力?	S，U	所有法规均有要求。这是系统供应商和用户组织共担责任的典型示例。尽管用户组织对验证承担最终责任，但有些任务只能由软件供应商完成并且必须由其交付，例如开发期间的验证活动及相关文档。 第五章系统 第十三条在计算机化系统使用之前，应当对系统全面进行测试，并确认系统可以获得预期的结果。当计算机化系统替代某一人工系统时，可采用两个系统（人工和计算机化）平行运行的方式作为测试和验证内容的一部分。 第五章系统 第十三条在计算机化系统使用之前，应当对系统全面进行测试，并确认系统可以获得预期的结果。当计算机化系统替代某一人工系统时，可采用两个系统（人工和计算机化）平行运行的方式作为测试和验证内容的一部分。	是	安捷伦科技公司已对 Cary 紫外工作站的性能进行了广泛验证，并且软件附有软件质量声明。但该声明并不免除用户组织通过测试来评估准确度、可靠性和一致性能，以验证计算机化系统的预期用途的法规责任。用户组织仍需要根据监管预期验证其分析系统。 对于 Cary 紫外工作站，“受监管记录”是指: • 方法 • 批次结果文件 • 相关的审计追踪 • 电子签名 • 方法和结果报告 Cary 紫外工作站可以检测无效或更改的文件，用户将无法打开这些文件。
附录 11	1.2 基础设施是否合格?	U	附录 11. 原则 B 巴西 GMP 577	N/A	服务器和网络等基础设施的认证由用户组织负责。

2. 记录的准确副本以及安全保存和检索

Part 11 及其他	要求	S，U	其他相关法规和注释	是/否	如果是，具体说明如何满足要求？如果否，对用户有什么建议？
Part 11 11.10(b)	2.1 系统能否以便于阅读并且适合由 FDA 进行检验、审查和复制的电子形式生成准确完整的记录副本？	S	第五章系统 第十九条以电子数据为主数据时，应当满足以下要求： （一）为满足质量审计的目的，存储的电子数据应当能够打印成清晰易懂的文件。	是	记录可采取纸质打印形式或生成电子 PDF 文件。可随时使用 Cary 紫外工作站软件载入包含电子记录、数据、方法审计追踪、操作人员身份以及电子签名的结果文件，该文件可作为原始数据副本供 FDA 进行审核或检查。“已打印”报告可追溯至原始电子文件，并包括生成报告的日期和时间、生成报告和页码的用户和软件版本。
附录 11	2.2 能否将电子化存储的电子记录生成清晰的印刷版本？	S	附录 11.8.1 巴西 GMP 583	是	代表电子记录的打印输出可采取纸质打印形式或生成电子 PDF 文件。
巴西	2.3 是否有可确保适时对数据进行备份、检索和维护的控制措施？	S，U	巴西 585.2 第五章系统 第十九条以电子数据为主数据时，应当满足以下要求： （三）应当建立数据备份与恢复的操作规程，定期对数据备份，以保护存储的数据供将来调用。备份数据应当储存在另一个单独的、安全的地点，保存时间应当至少满足本规范中关于文件、记录保存时限的要求。	是	虽然备份数据和维护数据的过程由用户组织负责，但 Cary 紫外工作站也允许对所有相关文件进行备份。 有用于创建所有相关文件的适当定期备份的详细说明以及备份脚本。 请参阅 Cary 紫外工作站安装说明，了解更多详细信息。
Part 11 11.10(c)	2.4 系统是否对记录进行保护，使其能够在整个记录保存期内支持准确及时的检索？	S，U	中国 GMP 163	是	记录保留期取决于用户组织的流程和监管预期。然而，Cary 紫外工作站生成的所有原始数据、元数据以及结果数据均存储在安全的数据库中。 电子报告和导出的数据安全存储在 OpenLab 内容管理中。 其物理安全性（对工作站和服务器的物理访问控制）由用户组织负责。
附录 11	2.5 在归档期间是否对数据的可访问性、可读性和完整性进行了检查？	U	附录 11.17	N/A	用户组织负责确保在归档期间检查数据的可访问性、可读性和可靠性。
附录 11	2.6 如果对系统（例如计算机设备或程序）进行相关变更，能否确保并测试数据检索不受影响？	S，U	附录 11.17	是	系统的相关更改依照 ISO 9001 质量管理标准进行开发与测试。然而，用户组织负责确保实施和验证过程中数据的可读性。

2. 记录的准确副本以及安全保存和检索（接上页）

Part 11 及其他	要求	S，U	其他相关法规和注释	是/否	如果是，具体说明如何满足要求？如果否，对用户有什么建议？
附录 11	2.7 数据是否同时使用物理和电子方法保证安全以防损坏?	S，U	附录 11.7.1 巴西 GMP 584 第五章系统 第十条系统应当安装在适当的位置，以防止外来因素干扰。 第五章系统 第十九条以电子数据为主数据时，应当满足以下要求： （二）必须采用物理或者电子方法保证数据的安全，以防止故意或意外的损害。日常运行维护和系统发生变更（如计算机设备或其程序）时，应当检查所存储数据的可访问性及数据完整性。	是	系统生成的所有原始数据、元数据以及结果数据均存储在受保护的位置。其物理安全性由用户组织负责。
临床指南	2.8 是否已实施有允许重新构建电子源/原始文档以便 FDA 审查（临床）研究和实验室测试结果的控制措施?	S	临床计算机指南 F2 FDA 问答	是	所有原始数据、结果、日志及相关的审计追踪均保留在安全存储中，允许根据需要重新构建实验室测试结果。
临床指南	2.9 提供给 FDA 的信息能否充分描述和说明源/原始数据的获取和管理方法，以及使用电子记录采集数据的方法?	U	临床计算机指南 F2 FDA 问答	N/A	由用户组织负责描述源/原始数据的获取和管理方法，以及使用电子记录采集数据的方法。
附录 11	2.10 系统是否允许对所有相关数据进行定期备份?	S	附录 11.7.1 中国 GMP 163 巴西 GMP 585 Part 211，68 b	是	虽然备份数据由用户组织负责，但此系统也允许对所有相关文件进行备份。
附录 11	2.11 是否定期检查、验证并监测备份数据完整性、准确性以及恢复能力?	U	附录 11.7.2 中国 GMP 163 巴西 GMP 585 Part 211，68 b	N/A	由用户组织负责确保备份数据的完整性和准确性，并定期检查、验证和监测恢复的数据。
临床计算机指南	2.12 规程和控制措施是否准备就绪，以避免通过不进入保护系统软件的外部软件应用程序变更、浏览、查询或报告数据?	S，U	临床计算机指南 E	是	应用程序生成的电子记录以受保护的格式存储，其他软件应用程序无法访问。如果该记录通过其他应用程序进行了更改，那么在尝试读取记录时系统将检测到相应更改。
临床计算机指南	2.13 是否已实施控制措施来阻止、检测并规避计算机病毒、蠕虫或其他潜在的有害软件代码对研究数据和软件的影响?	S，U	临床计算机指南 F	是	安捷伦已将 Cary 紫外工作站和 OpenLab 软件与行业标准防病毒应用程序一起进行了测试。然而，实施防病毒软件由用户组织负责。

3. 授权访问系统、功能和数据

Part 11 及其他	要求	S，U	其他相关法规和注释	是/否	如果是，具体说明如何满足要求？如果否，对用户有什么建议？
Part 11 11.10(d)	3.1 系统访问是否仅限于经过授权的人员？	S，U	中国 GMP 183 163 巴西 GMP 579 ICH Q7.5.43	是	系统的访问受限，只有经系统管理员明确授权的用户才能访问系统。每位用户均通过唯一的 ID 和密码组合进行识别。访问系统时要求输入 ID 和密码。
	3.2 每个用户是否通过（例如）自己的用户 ID 和密码等明确识别？	S，U	若干封警告信	是	用户组织负责授予适当的系统权限。每位用户均通过唯一的 ID 和密码组合进行识别。访问系统时要求输入 ID 和密码。
临床	3.3 是否有控制措施用于维护累计记录，使其在任意时间点都能指出获得授权的人员姓名、头衔及其访问权限的描述？	S，U	临床计算机指南 4	是	OpenLab 控制面板记录用户的详细信息，例如全名、描述/头衔和访问权限。访问权限在 OpenLab 控制面板中设置，任何变更都将记录到活动日志中。还可以针对项目、角色和权限、系统和用户以及群组角色分配生成报告。这些报告适用于需要执行定期安全性审查的组织。用户或用户组角色和权限可供 Cary 紫外工作站应用程序中的登录用户使用。

4. 电子审计追踪

Part 11 及其他	要求	S，U	其他相关法规和注释	是/否	如果是，具体说明如何满足要求？如果否，对用户有什么建议？
Part 11 11.10(e)	4.1 是否有由计算机生成的带有时间戳的安全审计追踪，以独立记录操作人员登录及其创建、修改或删除电子记录行为的日期和时间？	S	中国 GMP 163 第五章系统 第十六条计算机化系统应当记录输入或确认关键数据人员的身份。只有经授权人员，方可修改已输入的数据。每次修改一个已输入的关键数据均应当经过批准，并应当记录更改数据的理由。应当根据风险评估的结果，考虑在计算机化系统中建立一个数据审计追踪系统，用于记录数据的输入和修改。	是	所有用户活动都记录在由计算机生成的带时间戳的安全审计追踪内。审计追踪针对所有方法和结果创建。
FDA GLP	4.2 审计追踪是否记录做出变更的人员、变更内容、变更时间及原因？	S	FDA 21 CFF 58.130 e 临床计算机指南 2 临床源数据 3	是	审计追踪包括变更的操作人员、变更日期、变更时间、变更前后的值以及执行变更的原因。
附录 11	4.3 系统能否生成打印结果以说明自原始录入后电子记录是否发生了变更？	S	附录 11，8.2	是	当对 Cary 紫外工作站数据进行更改时，将在审计追踪中生成一个条目，记录原始文件已更改、以及更改的时间和日期以及执行更改的操作人员。可查看审计追踪、以电子形式进行审查，并能进行打印。 审计追踪报告可生成为 PDF 文件，并安全存储在 OpenLab 内容管理中。

4. 电子审计追踪（接上页）

Part 11 及其他	要求	S，U	其他相关法规和注释	是/否	如果是，具体说明如何满足要求？如果否，对用户有什么建议？
FDA GMP	4.4 审计追踪是否包括对应用于测试的已建立方法的任何更改？ 4.5 这些记录中是否包括修改原因？	S	Part 211.194 8b	是	方法具备完整的审计追踪，其中包括任意方法修改的原因。
	4.6 审计追踪功能是否配置为始终开启并且无法由系统用户关闭？	S，U	警告信	是	审计追踪由计算机生成，该功能始终处于开启状态。审计追踪自动与相关的应用程序数据文件共同保存。
附录 11	4.7 审计追踪能否以一般可理解的形式用于定期审查？	S	附录 11，9	是	审计追踪的设计形式应能方便读取和理解。 系统允许特定用户在任意时间通过应用程序查看器查看审计追踪。 系统设计应能使权限用户以电子方式审查审计追踪条目，审查过的条目将与电子记录一并永久保存。
	4.8 审计追踪内容能否配置为仅记录相关活动，以对审计追踪信息进行现实而有意义的审查？	S	附录 11 以及与审计追踪审查相关的许多警告信对此有隐含要求。	是	审计追踪内容用户无法配置和编辑。审计追踪可以按用户或条目类别进行筛选。还可以搜索审计追踪的每个条目的审查。在 OpenLab 控制面板内，可以在显示内容之前对审计追踪内容进行筛选，以满足用户审查信息时的偏好。
Part 11 11.10(e)	4.9 变更记录时，先前记录的信息是否保持不变？	S		是	先前记录的条目永远不会被覆盖或更改。即使记录被更改，它们也会永久地记录在审计追踪中。 先前记录的信息以唯一文件名保存，该文件名与该电子记录相关联。
Part 11 11.10(e)	4.10 审计追踪文档是否至少保留与主体电子记录要求同样长的时间？	S，U		是	审计追踪自动与相关的电子记录共同保存，无法从中分离。
Part 11 11.10(e)	4.11 审计追踪是否可供 FDA 审查和复制？	S		是	审计追踪可供审查和打印。
附录 11	4.12 能否将电子化存储的电子记录（例如电子审计追踪）生成清晰的印刷版本？	S	附录 11，8.1	是	审计追踪可供审查和打印。

5. 操作和设备校验

Part 11 及其他	要求	S，U	其他相关法规和注释	是/否	如果是，具体说明如何满足要求？如果否，对用户有什么建议？
Part 11 11.10(f)	5.1 是否存在可执行允许步骤和事件序列（如有必要）的操作系统校验？	S		是	在需要事件序列时，通过系统校验强制执行。 如果 QA/QC 中仅使用已批准的方法，即可通过限制用户访问所保存的已批准方法或通过电子签署文件并防止进一步修改来实现。 在 Cary 紫外工作站中，针对电子记录的强制执行事件序列体现在软件确保在允许数据采集和分析前所需设置和设备可用，或确保在关闭该应用程序前保存了文件。
Part 11 11.10(g)	5.2 是否进行授权检查以确保仅有经授权的个人可使用系统、签署电子记录、访问操作或计算机系统输入或输出设备、更改记录或执行当前操作？	S	Part 211，68 b	是	对应用程序和记录的访问根据所分配的权限进行控制与限制，权限可由权限或管理员用户进行配置。
	5.3 系统是否设计为可记录输入、变更、确认或删除数据（包括日期和时间）的操作人员身份？	S	附录 11，12.4	是	审计追踪和活动日志中记录了在系统中执行操作的操作人员身份。
Part 11 11.10(h)	5.4 系统是否允许设备校验在适当情况下确定数据输入源或操作指令的有效性？	S	对于此要求存在两种同样有效的解释。系统应设计为： 在向“源”传送指令或从“源”传送数据之前，确认计算机与数据输入“源”（即仪器）之间通讯正常。 系统创建的受监管记录必须明确指明数据“源”（即生成数据的仪器或组件）。	是	1. 系统设计可始终确保仪器与计算机工作站之间的有效连接 2. 系统识别仪器型号和序列号，并在审计追踪中将它们记录为数据源 注：计算机工作站将在上述支持的拓扑结构部分中定义
Part 11 11.10(i)	5.5 是否有记录证明开发、维护或使用电子记录/电子签名系统的人员具备执行相应任务的受教水平、培训技能和经验？	U	中国 GMP 18 巴西 571	N/A	由用户组织负责维护记录，证明开发、维护或使用电子记录和电子签名系统的人员具备执行相应任务所需的教育、培训和经验。 相关的安捷伦员工已经接受过数据可靠性相关方面的培训。
	5.7 员工是否在此规程方面进行过培训？	U	Part 11 11.10(j) 隐含要求	N/A	由用户组织负责对其工作人员进行培训。

5. 操作和设备校验（接上页）

Part 11 及其他	要求	S，U	其他相关法规和注释	是/否	如果是，具体说明如何满足要求？如果否，对用户有什么建议？
Part 11 11.10(k)	5.8 对于系统文档是否有适当的控制措施，包括： (1) 对系统操作和维护文档的分配、访问和使用是否有充分控制？ (2) 修订和变更控制规程，以对记录时序开发和系统文档修改的审计追踪进行维护？	U	中国 GMP 161 第五章系统 第十一条应当有详细阐述系统的文件（必要时，要有图纸），并须及时更新。此文件应当详细描述系统的工作原理、目的、安全措施和适用范围、计算机运行方式的主要特征，以及如何与其他系统和程序相接。	N/A	由用户组织负责建立系统文档。
Part 11 11.10(i)	5.9 是否存在修订和变更控制规程，以对记录时序开发和系统文档修改的审计追踪进行维护？	S，U	第五章系统 第十七条计算机化系统的变更应当根据预定的操作规程进行，操作规程应当包括评估、验证、审核、批准和实施变更等规定。计算机化系统的变更，应经过该部分计算机化系统相关责任人员的同意，变更情况应有记录。主要变更应当经过验证。	是	安捷伦为 Cary 紫外工作站以及 OpenLab 解决方案维护开发和测试文档。根据要求，此文档可供用户进行审查。 用户组织负责在原位置维护其系统以及相关变更文档。

6. 数据可靠性、日期和时间准确性

Part 11 及其他	要求	S，U	其他相关法规和注释	是/否	如果是，具体说明如何满足要求？如果否，对用户有什么建议？
附录 11	6.1 与其他系统进行数据电子化交换的计算机系统是否包括用于数据正确性、安全输入以及处理的适当内部校验？	S	附录 11.5	N/A	系统中未实施此类功能。
附录 11	6.2 是否对数据准确性进行额外校验？ （此校验可以由其他操作人员完成，或采用经验证的电子方式。）	S，U	附录 11-6 巴西 GMP 580 ICHQ7-5.45 第五章系统 第十五条当人工输入关键数据时（例如在称重过程中输入物料的重量和批号），应当复核输入记录以确保其准确性。这个复核可以由另外一个操作人员完成，或采用经验证的电子方式。必要时，系统应当设置复核功能，确保数据输入的准确性和数据处理过程的正确性。	N/A	系统中未实施此类功能。
临床计算机指南	6.3 是否建立了控制措施以确保系统日期和时间的正确性？	S，U	临床计算机指南 D.3	是	安捷伦建议对系统进行配置以参考时间服务器来确保系统日期和时间的准确性。此配置在操作系统中进行并受其控制。

6. 数据可靠性、日期和时间准确性（接上页）

Part 11 及其他	要求	S，U	其他相关法规和注释	是/否	如果是，具体说明如何满足要求？如果否，对用户有什么建议？
临床计算机指南	6.4 日期和时间能否仅可由授权人员更改，并在检测到系统日期或时间差异时通知此人？	S，U	临床计算机指南 D.3	是	Cary 紫外工作站使用操作系统与本地 Windows 时间同步。 用户组织负责： – 限制对 Windows 时间设置的访问，只对授权人员开放 – 维护程序控制，设置和维护 Windows 时间的准确性
临床计算机指南 I	6.5 是否为跨不同时区的系统采用清晰表明所用时区参考的时间戳？	S，U	临床计算机指南 D.3	是	时间戳始终显示为 UTC 格式。

7. 开放式系统的控制（仅适用于开放式系统）

Part 11 及其他	要求	S，U	其他相关法规和注释	是/否	如果是，具体说明如何满足要求？如果否，对用户有什么建议？
Part 11 11.30	7.1 是否对规程和控制措施进行设计，以确保电子记录从创建时刻到接收时刻的真实性、可靠性以及适当情况下的保密性？	S，U		N/A	根据 21 CFR Part 11.3(b)(9) 的规定，不应将系统部署为“开放式”系统。
Part 11 11.30	7.2 是否存在文档加密和使用适当数字签名标准等其他方式，以确保必要情况下记录的真实性、可靠性和保密性？	S		N/A	根据 21 CFR Part 11.3(b)(9) 的规定，不应将系统部署为“开放式”系统。

8. 电子签名 — 签名表现形式以及签名/记录链接

Part 11 及其他	要求	S，U	其他相关法规和注释	是/否	如果是，具体说明如何满足要求？如果否，对用户有什么建议？
附录 11	8.1 使用电子签名时，该签名在公司范围内是否与手写签名具有同等效力？签名是否永久链接至相应记录？ 其中是否包括适用的时间和日期？	S，U	附录 11.14 ICH Q7.6.18 第五章系统 第二十三条电子数据可以采用电子签名的方式，电子签名应当遵循相应法律法规的要求。	是	用户组织必须确立电子签名的法律效力。 签名将永久链接至相应记录，该记录可包括最终报告。已签署的电子记录显示签署人的姓名、执行签名的日期和时间以及签名的意义。
Part 11 11.50 (a)	8.2 已签署的电子记录是否包含明确说明下列内容的签署相关信息： (1) 签署人的姓名 (2) 执行签名的日期和时间 (3) 与签名相关的含义（如审查、批准、责任或作者身份）	S		是	应用程序生成一份报告，其中标明： 1) 签署人的全名和签名级别 2) 执行签名的日期和时间 3) 强制输入的备注以表明签名的原因。
Part 11 11.50(b)	8.3 本节 (a)(1)、(a)(2) 和 (a)(3) 条中确定的项目是否受到与电子记录相同的控制？是否包括在任何便于阅读形式的电子记录（例如电子显示或打印输出）中？	S		是	所有电子签名组件均可显示和打印。
Part 11 11.70	8.4 电子签名和手写签名是否链接到相应的电子记录，以确保签名无法以常规手段删除、复制或转移从而伪造电子记录？	S		是	电子签名嵌入结果和方法文件中，无法从一份记录或文件转移至另一份记录或文件。
Part 11 前言	8.5 如果在固定的较短时间内未执行输入或操作，是否有用户特定的自动非活动断开连接方法可以“注销”用户？	S	Part 11 前言 第 124 节	是	自动会话锁定允许用户组织设置一段时间，超过这段时间之后用户将自动注销。

9. 电子签名一般要求以及签名组件与控制措施

Part 11 及其他	要求	S，U	其他相关法规和注释	是/否	如果是，具体说明如何满足要求？如果否，对用户有什么建议？
Part 11 11.100(a)	9.1 每个电子签名是否专属于一个用户且无法再次使用或重新分配给其他用户？	S，U		是	系统不允许重复的用户 ID。每个用户都有唯一的登录名和唯一的签名，不能为其他用户所用。系统中的用户名需要具备唯一性，且不能重新分配给其他用户。 如果用户组织使用公司的 Windows 登录来验证用户，任何两位用户不得拥有相同的用户 ID 和密码组合。用户组织负责管理用户名和密码策略。
Part 11 11.100(b)	9.2 组织在建立、分配、认证或批准个人的电子签名或该电子签名的任何元素之前，是否会验证个人的身份？	U		N/A	由用户组织负责在建立、分配、认证或批准个人的电子签名或该电子签名的任何元素之前验证工作人员的身份。
Part 11 11.100(c)	9.3 使用电子签名的个人在使用时或使用前是否已向机构证实系统中 1997 年 8 月 20 日及之后使用的电子签名与传统的手写签名具有同等法律约束力？ 9.4 使用电子签名的个人是否根据机构要求提供其他认证或证明表明特定电子签名与签署人的手写签名具有同等法律约束力？	U		N/A	由用户组织负责认证使用电子签名的工作人员符合这些要求。
Part 11 11.200(a) (1)	9.5 不基于生物识别的电子签名是否采用至少两种不同的身份识别组件，例如身份识别代码和密码？	S，U		是	进行电子签名要求同时提供身份识别码（用户标识）和密码。
Part 11 11.200(a) (1) (i)	9.6 当个人在一个连续的受控系统访问期间执行一系列签署操作时，第一次执行的签署是否使用了所有电子签名组件？	S		是	所有电子签名都要求同时提供身份识别码（用户标识）和密码。

9. 电子签名一般要求以及签名组件与控制措施（接上页）

Part 11 及其他	要求	S，U	其他相关法规和注释	是/否	如果是，具体说明如何满足要求？如果否，对用户有什么建议？
Part 11 11.200(a) (1) (ii)	9.8 当个人在一个连续的受控系统访问期间执行一次或多次签署操作时，每次执行的签署是否使用了所有电子签名组件？	S		是	当个人在一个受控访问期间在应用程序中签署一系列文件中的第一份文件时，必须要求用户输入三个签名组件，即用户 ID、密码和签名的意义。
Part 11 11.200(a) (2)	9.9 是否有合适的控制措施确保不基于生物识别的电子签名仅可由其真正所有者使用？	S		是	可对 OpenLab 解决方案和 Windows 进行配置，使管理员可向新账户或忘记密码的用户分配初始密码，但需要用户在其首次登录时更改该密码。这样，仅有相应个人掌握用户 ID/密码组合。无论 OpenLab 解决方案使用公司的 Windows NT 登录来验证用户还是由 OpenLab 管理用户，任何两位用户不得拥有相同的用户 ID/密码组合。用户有责任不与其他实验室成员共享用户名和密码。
Part 11 11.200(a) (3)	9.10 管理和执行电子签名的方式能否确保除真正所有者之外，任何人尝试使用个人电子签名时都要求两个或两个以上用户的合作？	S，U		是	OpenLab 解决方案中，必须使用该用户的用户名和密码才启用其电子签名。应用程序用户的密码通过加密的方式保存在数据库中，在软件的所有位置中均以星号形式显示。 可对 OpenLab 解决方案进行配置，使管理员可向新账户或忘记密码的用户分配初始密码，但需要用户在其首次登录时更改该密码。这样，仅有相应个人掌握用户 ID/密码组合。所有者之外任何希望使用电子签名的用户都需要用户和系统管理员的自愿合作。
Part 11 11.200(b)	9.11 基于生物识别的电子签名设计是否旨在确保签名不为真正所有者之外的任何人使用？	S		N/A	此系统不提供生物识别签名。

10.身份识别码和密码的控制措施

Part 11 及其他	要求	S，U	其他相关法规和注释	是/否	如果是，具体说明如何满足要求？如果否，对用户有什么建议？
Part 11 11.300 (a)	10.1 是否有合适的控制措施可维持每个身份识别码和密码组合的唯一性，从而不会出现两个用户拥有相同身份识别码和密码组合的情况？	S，U		是	Cary 紫外工作站身份验证可以与 Windows 用户管理（包括对域级别用户的使用）相关联。如果使用 Windows 用户和组管理，管理员可以适当地配置 Windows 密码策略设置。 无论 OpenLab 解决方案使用公司的 Windows 域登录来验证用户还是由 OpenLab 解决方案管理用户，任何两位用户不得拥有相同的用户 ID/密码组合。
Part 11 11.300(b)	10.2 是否有合适的控制措施确保对发布的身份识别码和密码进行定期检查、找回或修改（例如，将此类事件归类为密码过期）？	S，U		是	Cary 紫外工作站身份验证可以使用 Windows 域认证，如此密码更新间隔被配置为 Windows 密码策略设置的一部分。管理员可定义一个时间段，密码可在这一时间段内自动定期修改。这可以防止用户使用重复密码。 可对 OpenLab 解决方案中管理的用户进行配置，以便自动定期地修改密码。

10. 身份识别码和密码的控制措施（接上页）

Part 11 及其他	要求	S，U	其他相关法规和注释	是/否	如果是，具体说明如何满足要求？如果否，对用户有什么建议？
Part 11 11.300(c)	10.3 对于承载或生成身份识别码或密码信息的令牌、卡片及其他设备丢失、被盗、缺失或其他有潜在损害的情况，是否有规程可通过电子方式取消其授权，并通过适当、严格的控制措施发布临时或永久的替代项?	U	第五章系统 第十四条数据的输入或修改只能由经许可的人员进行。杜绝未经许可的人员输入数据的手段有：使用钥匙、密码卡、个人密码和限制对计算机终端的访问。应当就输入和修改数据制订一个授权、取消、授权变更，以及改变个人密码的规程。必要时，应当考虑系统能记录未经许可的人员试图访问系统的行为。对于系统自身缺陷，无法实现人员控制的，必须具有书面程序，相关记录本及相关物理隔离手段，保证只有经许可的人员方能进行操作。	N/A	由用户组织负责建立这些规程。
Part 11 11.300(d)	10.4 是否有合适的交互安全防护可避免未经授权使用密码和/或身份识别码，可检测并将未经授权使用尝试立即直接报告给系统安全部门和组织管理部门（适当情况下）？	U	第五章系统 第十四条数据的输入或修改只能由经许可的人员进行。杜绝未经许可的人员输入数据的手段有：使用钥匙、密码卡、个人密码和限制对计算机终端的访问。应当就输入和修改数据制订一个授权、取消、授权变更，以及改变个人密码的规程。必要时，应当考虑系统能记录未经许可的人员试图访问系统的行为。对于系统自身缺陷，无法实现人员控制的，必须具有书面程序，相关记录本及相关物理隔离手段，保证只有经许可的人员方能进行操作。	N/A	由用户组织负责建立这些交互安全防护。
Part 11 11.300(e)	10.5 是否有控制措施可以对设备（例如承载或生成身份识别码或密码信息的令牌或卡片）进行初始和定期测试以确保其正常运行且没有未经授权的变更?	U		N/A	由用户组织负责建立对设备进行初始和定期测试的控制措施，以确保其正常运行且没有未经授权的变更。

11. 系统开发和支持

Part 11 及其他	要求	S，U	其他相关法规和注释	是/否	如果是，具体说明如何满足要求？如果否，对用户有什么建议？
附录 11	11.1 软件或系统是否依照相应的质量管理体系进行开发?	S，U	附录 11 4.5 巴西 GMP 577 GAMP 这是系统供应商和用户组织的共同责任。用户应要求供应商提供记录，证明软件开发在质量管理体系 (QMS) 框架内进行。 第二章原则 企业应当能够提供与供应商质量体系和审计信息相关的文件。	是	安捷伦软件根据符合 ISO 9001 的安捷伦科技生命周期进行开发和测试。生命周期检查点的交付成果经过管理系统的审查和批准。该产品符合其功能和性能规范，并在发货时满足放行标准。

11. 系统开发和支持（接上页）

Part 11 及其他	要求	S，U	其他相关法规和注释	是/否	如果是，具体说明如何满足要求？如果否，对用户有什么建议？
巴西	11.2 软件供应商转包软件和维护服务时是否签订正式协议，协议中是否包括承包方的责任？	S，U	巴西 GMP 589 这是系统供应商和用户组织的共同责任。供应商必须与转包商签订协议，而用户必须验证协议的正当性。 第二章原则 第四条企业应当注重计算机化系统供应商的管理，制定相应的操作规程。供应商提供产品或服务时（如安装、配置、集成、验证、维护、数据处理等），企业应当与供应商签订正式协议，明确双方责任。	是	安捷伦要求所有供应商签订正式协议，并遵守 ISO 9001 供应商质量管理政策。
ICH Q10	11.3 对于外包（开发和支持）活动，合同委托方和合同承接方之间是否签订了书面协议？	S，U	ICHQ10，2.7 c	N/A	安捷伦要求与所有供应商签订正式协议（详情参阅 LSCA 质量手册第 7.4 节）。
ICH Q10	11.4 缔约方（承包方）的质量相关活动是否定义了责任和沟通流程？	S，U	ICHQ10，2.7 c	N/A	安捷伦要求与所有供应商签订正式协议（详情参阅 LSCA 质量手册第 7.4 节）。
Part 11 11.10(i)	11.5 软件开发和支持人员是否经过培训？	S，U	这是系统供应商和用户组织的共同责任。供应商必须确保其工作人员经过培训，用户应通过审计等方式保证软件开发工程师经过培训且该培训记录具有存档。 第三章人员 第五条计算机化系统的“生命周期”中所涉及的各种活动，如验证、维护、管理等，需要各相关的职能部门人员之间的紧密合作。在职责中涉及使用和管理计算机化系统的人员，应当接受相应的使用和管理培训。确保有适当的专业人员，对计算机化系统的设计、验证、安装和运行等方面进行培训和指导。	是	安捷伦要求与所有供应商签订正式协议（详情参阅 LSCA 质量手册第 7.4 节）。

参考文献

1. R. A. Botha, J. H. P Eloff. “Separation of duties for access control enforcement in workflow environments” IBM Systems Journal – End-to-end security 40(3), 666-682 (2001)
2. U.S. Food and Drug Administration. CFR - Code of Federal Regulations Title 21. Title 21—Food and Drugs, Chapter I—Food and Drug Administration Department of Health and Human Services, Subchapter A—General. Part 11 Electronic Records; Electronics Signatures [在线] https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=11（2015 年 11 月 4 日查阅）
3. European Commission Health and Consumers Directorate-General. Public Health and Risk Assessment. Pharmaceuticals. EudraLex. The Rules Governing Medicinal Products in the European Union.Volume 4. Good Manufacturing Practice.Medicinal Products for Human and Vetrinary Use. Annex 11. Computerised Systems. [在线] http://ec.europa.eu/health/files/eudralex/vol-4/annex11_01-2011_en.pdf（2015 年 11 月 4 日查阅）

更多信息

有关我们的产品与服务的详细信息，请访问我们的网站 www.agilent.com。

www.agilent.com

安捷伦对本资料可能存在的错误或由于提供、展示或使用本资料所造成的间接损失不承担任何责任。

DE44426.2696412037

本资料中的信息、说明和指标如有变更，恕不另行通知。

© 安捷伦科技（中国）有限公司，2021

2021 年 9 月 1 日，中国出版
5994-1318ZHCN

查找当地的安捷伦客户中心：
www.agilent.com/chem/contactus-cn

免费专线：
800-820-3278，400-820-3278（手机用户）

联系我们：
LSCA-China_800@agilent.com

在线询价：
www.agilent.com/chem/erfq-cn

Agilent
Trusted Answers