使用安捷伦 ChemStation Plus 确保分析数据符合 FDA21CFR 第 11 部分的要求

Technical Note

介绍

1997 年 8 月 20 日，美国食品药品管理局（FDA）颁布了一项新的法规，使得制药公司可以以电子签名方式批准结果，并能将书面追踪文件转成电子记录。这项法规被称做联邦法规21条，第11部分（被称做21CFR第 11 部分），它适用于受 FDA 管辖的所有企业。

这项法规对制药企业处理数据产生的影响比预期的影响要大得多。*“企业想要有一个有关电子签名的法规，但他们得到的却是一项有关电子记录的法规”*（Martin Browning, FDA 前任检查员，在华盛顿特区一次验证研讨会上的报告）。

21CFR 第 11 部分有关电子记录的要求对于制药企业来说并不陌生，因为它只是对以前一些法规的内容进行了总结。

但是，21CFR 第 11 部分将重点放在了检查措施的实施上，来保护电子记录并使之更安全。虽然 21CFR 第 11 部分对于制药企业的行为和分析仪器供货商的要求不确定，而且会变化，但它确实值得在实验室实施，因为它能帮助企业解决制药研究中一个最重要的问题 — 如何将新产品更快速地推向市场。

有关实施电子数据管理最主要的好处是能潜在地增加企业的劳动生产率。企业可以减少用纸输出的数据量，加快数据检查和批准的过程，并从基于计算机化系统控制的自动化技术中获益，例如在制造或药物溶出度实验中。

在这项法规中，有关计算机化系统的一些基本要求引起了审计人员的注意。法规涵盖了验证的基本要求：有限制的存取数据、确保数据完整性和可追溯性。

当然要确保所有的工作符合 FDA 法规的要求必须靠企业的努力，但同时大部分的法规也会影响分析系统和它们的供货商。

这篇文章讲述了色谱数据处理系统如何帮助企业符合 FDA 法规的要求。安捷伦 ChemStation Plus 数据库模块可以保证如果使用单机 Microsoft® Access 数据库或基于服务器的 Oracle® 数据库，都可以满足数据安全性、数据完整性和审计追踪的需要。

Agilent Technologies

21CFR 第 11 部分的要求

为了满足 FDA 法规和指南有关电子记录和计算机化系统的要求，理解数据安全处理的概念是非常重要的。图 1 做了最好的说明：

- 数据安全性 — 通过采取物理限制登录系统的办法和防止未授权的登录来保护数据

- 数据完整性 — 保护原始数据和元数据，避免受到非法修改，将原始数据与元数据联系在一起，使得可以随时生成原始结果，例如在审计的时候和将新结果的拷贝文件化。

- 审计可追溯性 — 用文件记录谁什么时间对结果做了什么，以及监控用户向原始数据中添加再分析结果。

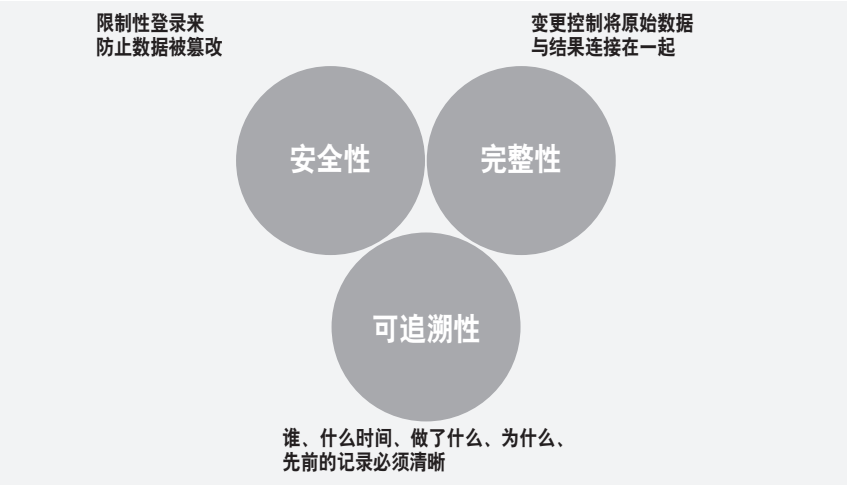


图 1
数据完整性的三角型

计算机化系统中数据安全性的总体内容 - 开放系统与封闭系统的比较

在讨论色谱数据系统安全性的细节之前，需要对计算机化系统中数据安全性的整体内容进行考虑。

我们都知道通过一个公共网络来传递数据很容易被外部未授权的人截获，例如“黑客”。他们或者是出于个人的娱乐，或者是出于恶意，可以非法登录获取数据。如果使用带有用户 ID 和密码的电子鉴别技术来批准保密或重要的数据，用户必须确保他们的签名与数据间有着不可分割的关联，并且没有人能够拷贝这个签名或取得这个密码。在公开系统中，这需要额外的加密技术，例如，一个结合了数据加密的公钥/私钥。相反，如果要使非授权人不能登录一个计算机化系统，用户就必须要确保他们的签名是私有的，并且不能被未授权人获得。

FDA 同样会区分这两种系统，并把它们定义为*开放*和*封闭*系统。因此如果要想符合附加的要求，必须通过开放系统查看公共网络系统，通过封闭系统查看*受保护*的网络。

安捷伦 ChemStation Plus 是为封闭系统设计的，因此在符合 21CFR 第 11 部分的情况下，只能用于封闭系统。

在 FDA 看来，*“封闭系统是一种环境，它的登录受到那些对电子记录内容负责的人的控制”(11.3.5)*。判定一个系统是封闭系统的标准是：在确认是否是封闭系统的时候，不是在一个时间点内进行检查，而是要进行一个持续的过程，并要对系统的控制文件化。开放系统与之相反，*“那些对电子记录内容负责的人不控制系统的登录”*。

总而言之，开放系统需要额外的加密技术来确保所有数据在网络上传输的安全。

封闭系统的登录控制会是什么样子呢?

保护公司网络数据的基本部分是用于intranet和其它网络的防火墙,以及网络本身物理上的登录控制，这可以确保未授权人不能进入系统。

但还是要进行额外的实时检查、文件记录和控制步骤来确保系统是按封闭系统来处理。这些要求已在表2中列出：

1. **验证**
2. **控制系统的登录**
3. **审计追踪**
4. **检查权限和系统**
5. **准确完整的拷贝**
6. **保护系统和记录**
7. **足够的培训**

图2
一个封闭系统的要求

这七条的详细说明如下：

- 对创建和维护电子记录的系统进行验证，来确保系统南通性能的安全、可靠和连续，以及有能力识别非法和篡改过的记录。
- 只有授权的人才可以登录系统
- 使用安全的、计算机生成的、带时间标记的审计追踪（先前的信息一定要清晰）
- 检查操作系统（加强步骤和事件批准的先后顺序）
- 进行权限检查来确保只有被授权的人才可以登录计算机系统、签署一个记录、使用操作系统和计算机系统的输入输出设备、修改记录以及执行操作。
- 有能力创建准确和完整的记录拷贝 — 系统必须可以创建准确和完整的电子记录拷贝，拷贝应同时以人可读的和电子格式存在，以便 FDA 检查员监控和检查。
- 记录的保护，例如使用 Windows NT® 的 NTFS 或数据库的保护措施，来确保在记录保留时间内，记录的准确性和随时可恢复性。
- 对开发、维护和使用电子记录系统的操作人员进行足够的教育和培训。

这些检查将确保：

- 建立书面的规章制度，来保证每个人对与自己电子签名有关的行为负责，这可以防止记录和签名被篡改。
- 对系统文件进行适当的控制（系统操作和维护文件的分发控制、获取控制和使用控制）
- 建立修订和变更控制规程来维护审计追踪，审计追踪应按时间顺序记录系统文件的制订和修改

正确的数据安全文件记录同样会影响制药企业本身。应该为物理登录和数据获取建立控制规程。大部分公司已经满足封闭系统的要求，并根据这些要求对封闭系统进行了实时检查。

以下专门对FDA规范中的封闭系统进行了分析，并解释了安捷伦 ChemStation Plus 色谱数据系统如何解决封闭系统的7个*基本*问题,以及最终如何通过电子签名来确认。

安捷伦 ChemStation Plus 根据 FDA 的要求实施数据的安全性、完整性和审计追踪

系统认证

系统认证通常包括安装、操作和持续的性能认证。安捷伦科技提供了全套的认证服务，例如内置自动化过程的软件，或是安捷伦提供的附加服务，来确认系统所有的关键功能都已被检查。安捷伦 ChemStation Plus的认证工作可以通过不同的模块来设定。对于单机版的仪器控制和数据获取，安捷伦 ChemStation Plus包括了内置的例行检查规程，使用户定期检查系统。对于文件记录和这些认证的安全操作，将由安捷伦认证工程师进行。

安捷伦ChemStation Plus的网络扩展功能能够被单独认证或作为一个独立系统安装。但客户和服务器软件要单独认证，认证必须由经过安捷伦资格确认的工程师来进行，他还要确保（在成功地进行完所有验证后）完成一套完整的认证文件留给用户，这样用户使用的才是一个*认证过的系统*。

通过这些认证过程，可以确保用户是按给定的技术参数来操作仪器，并按供货商的设计来执行所有操作。

限制系统登录和密码策略

密码保护是通过一个用户管理界面进行，它允许只有正确输入用户名和密码的用户才能登录安捷伦 ChemStation Plus，并执行敏感的操作。用户管理中有一个额外的功能，它可以为每一个用户创建不同的登录级别。安捷伦 ChemStation Plus提供四种预定义的级别：用户、操作者、经理和管理员。除了这几种之外，还提供用户自定义的登录级别，在这个登录级别下，用户权限的定义是完全公开的 — 每一个用户都可以具有自己单独的权限。

法规在章节11.200和11.300部分规定了必须要遵守的几种标准，来确保密码和用户ID的唯一，并与手写签名有相等的效力...(1)：*电子签名必须至少由两个独立部分组成，例如一个识别代码和一个密码...(3)，这可以确保如果有第二个人想使用这个签名，必须要与至少两个或更多的人合作才能完成...11.300(b)要对ID代码和密码进行定期检查、修改和召回，...（d）...对系统保密单元的任何未授权使用都要进行检测和报告。*

章节11.50对手写签名进行了规定：*签名必须包含...（1）签字人名字的打印形式，(2）日期和时间（3）签名*。安捷伦ChemStation Plus在用户的设置中要求两个相互独立的名字：用户登录名和用户显示名，用户显示名将出现在每一份为这个用户创建的文件上。请见图3a。签名由一个强制备注字段提供，这个字段必须在所有数据变化生效前填写。所有的行为以及相应的日期和时间都将记录在与之相关的审计追踪中。

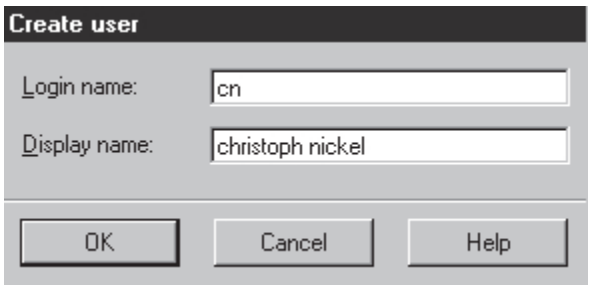


图3a
第一次进入安捷伦ChemStation Plus时的登录界面

限制性系统登录的一个最重要的要求是只有用户自己知道他们的密码，管理员只能管理用户和他们的 ID，而不知道密码。因此在软件中实施分两步。第一步，数据库管理员创建用户，并给予合适的权限。然后当用户第一次登录到应用程序中时，会显示一个登录屏幕，要求输入密码，见图 3b。



图 3b
指定个人密码的提示

在点击OK后，一个更改用户密码的对话框会自动弹出来，见图 3c。

这两步确保只有用户自己知道密码。如果密码丢了或忘了，数据库管理员会清除这个密码，然后用户重复第一次登录时的过程。

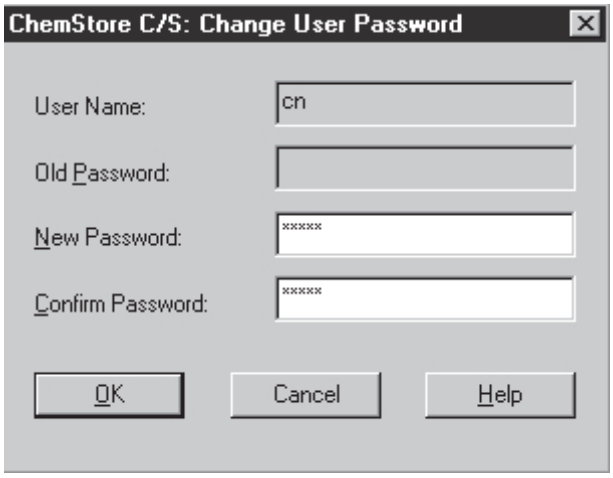


图 3c
第一次登录安捷伦 ChemStation Plus 时个人密码的设定

为了定期检查和修改密码，应用程序包含一个*密码管理*的功能，来实现公司的密码策略，例如最小密码长度，失效期，密码唯一性和帐号锁定。请见图 3d。

最后，所有试图登录到系统的活动，包括不成功的登录都会记录到数据库日志中，随之记录的还有时间标记、用户 ID、登录原因、以及在这个例子中进行不成功登录的PC主机名。这个数据日志是应用程序的一部分，所有的内容不需要用户干预，而是计算机生成的，请见图 3e。

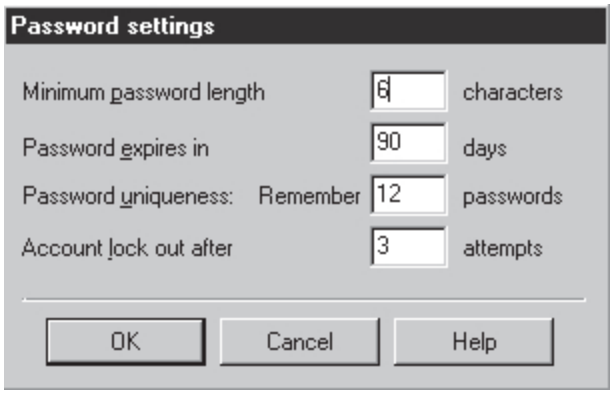
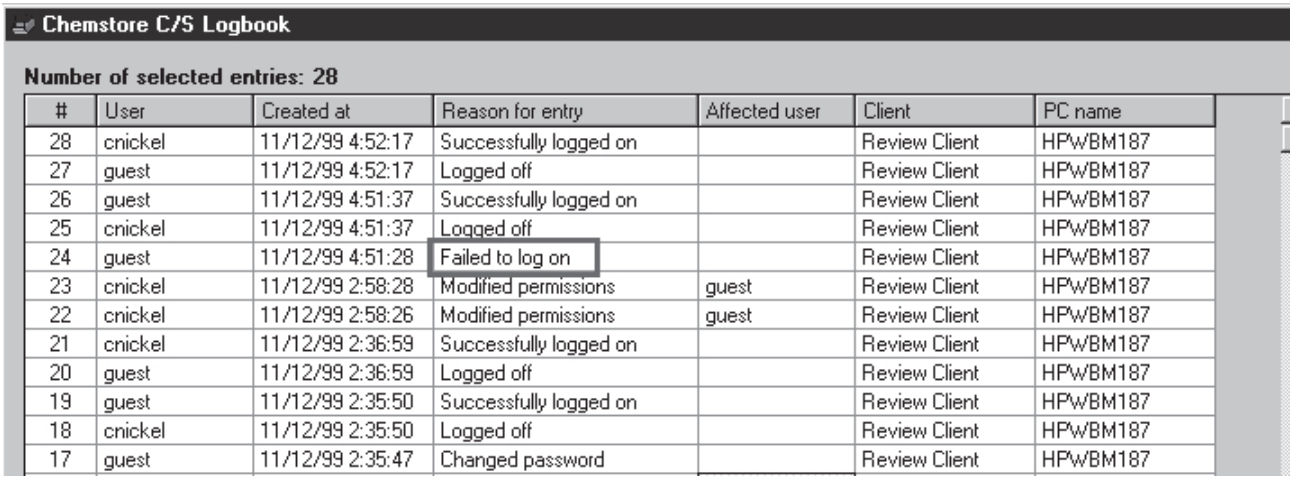


图 3d
在安捷伦 ChemStation Plus 中密码策略的设定



Chemstore C/S Logbook

Number of selected entries: 28

#	User	Created at	Reason for entry	Affected user	Client	PC name
28	cnickel	11/12/99 4:52:17	Successfully logged on		Review Client	HPWBM187
27	guest	11/12/99 4:52:17	Logged off		Review Client	HPWBM187
26	guest	11/12/99 4:51:37	Successfully logged on		Review Client	HPWBM187
25	cnickel	11/12/99 4:51:37	Logged off		Review Client	HPWBM187
24	guest	11/12/99 4:51:28	Failed to log on		Review Client	HPWBM187
23	cnickel	11/12/99 2:58:28	Modified permissions	guest	Review Client	HPWBM187
22	cnickel	11/12/99 2:58:26	Modified permissions	guest	Review Client	HPWBM187
21	cnickel	11/12/99 2:36:59	Successfully logged on		Review Client	HPWBM187
20	guest	11/12/99 2:36:59	Logged off		Review Client	HPWBM187
19	guest	11/12/99 2:35:50	Successfully logged on		Review Client	HPWBM187
18	cnickel	11/12/99 2:35:50	Logged off		Review Client	HPWBM187
17	guest	11/12/99 2:35:47	Changed password		Review Client	HPWBM187

图 3e
未授权的系统登录记录

这篇文章的审计追踪部分详细说明了数据库日志文件。

除了密码设定外，应用程序本身保留了先前使用过的用户名和密码的组合，以避免重复使用，甚至可以在电子记录保留期间保存这个记录。

但是限制性系统登录也与应用程序本身绑在了一起：所有敏感的活动，象改变运行批准状态、删除数据、管理用户和维护服务器数据库，都是作为用户权限加以控制。建议设置一个数据库管理员来负责维护服务器和进行用户管理。这将用户复查工作与管理工作分开了。密码本身用一个四步过程加密，来防止有人通过网络做手脚。

系统检查

这一部分主要讲述身份确认和操作系统的检查。登录系统时的身份确认或者可以通过系统管理员来实时进行，这样确保了未授权人不能登录系统，或者可以作为操作系统定期认证的一部分。

操作系统的检查可以确保在序列过程中，预定义的序列不会被改变或修改。这些检查大部分用在GMP的环境中。在这些环境中，生产系统受到控制，同时自动分析序列也受到控制。但是从分析角度讲，序列分析的执行比较容易保证，因为在数据分析过程中，至少会有一个数据获取的过程。这很容易在安捷伦ChemStation的run-time checkist中自动设置并记录，见图4。

电子记录的保护

确保数据安全的最重要的一个方面就是电子记录的保护。应用于本地存储数据和中央存储数据的安全工具是不一样的。本地数据的安全是通过NTFS许可机制加以实现的，它可以防止除系统管理员之外的所有用户获取数据。安捷伦ChemStation Plus的中央数据是保存在Oracle服务器数据库中，它结合了数据库功能的两个要素来保护电子记录：以二进制格式保存数据和数据库恢复工具。

第一个要素防止了从应用程序之外对数据的非法获取，例如可以避免使用浏览器程序对数据进行删除、修改或覆盖。也就是说，数据库以二进制方式保存数据，并通过24位散乱数值摘要算法的加密得到保护。

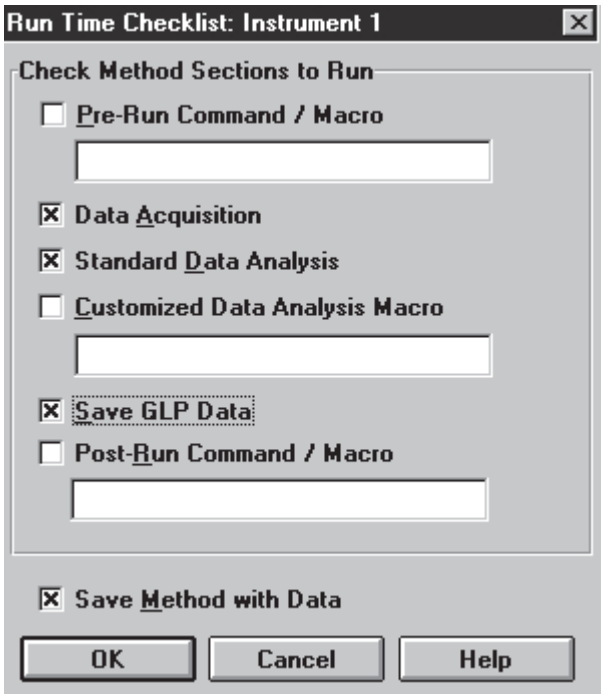


图 4
只有获得许可的序列步骤运行清单

这个数据库的数据只能通过 DBMS 来访问。用户不能通过浏览器类型的工具来获取数据。这将防止所有系统用户对色谱数据和结果进行非法操作。

第二个要素，Oracle 数据库恢复工具仅仅对基于服务器的 Oracle 数据库有效。可以通过这些工具对数据进行备份，以及在系统崩溃时启用恢复机制，使用户避免数据的偶然丢失。这些工具通过测量上一次数据恢复时间与系统崩溃时间的差别，来提供不同级别的恢复功能。时间差别越小，安全水平就越高。最高的安全级别可以恢复崩溃前最后一分钟的数据。实施这种级别的恢复会影响服务器的硬件设置，并需要有一个具有 Oracle 数据库管理经验的管理员。因此建议在安装和实施安捷伦 ChemStation Plus 服务器之前精心设计备份和恢复策略。对于硬件布局和安全设置，请参考相关 Oracle 文件，并查看安捷伦 ChemStation Plus 的说明书。

数据版本化

通过将完整数据安全地、版本化地保存在一个地方，来维护数据的完整性。FDA 法规要求将数据拷贝到其它媒介时要完整准确，并同时要以电子方式和人可读的方式进行。什么是拷贝完整？完整的分析数据被定义为所有的色谱信号、光谱数据、积分结果、定量结果、仪器运行参数和用于获得最终结果的数据分析方法细节。它还包括日志以及在最终结果创建过程中的设置和活动。

日常工作经常要求分析结果有多个拷贝，所有的再分析数据都必须以版本形式与原始数据和结果保存在一起。安捷伦 ChemStation Plus 以计算机操作系统使用的本地时区时间作为进针时间，并将它与唯一的进针 ID 相结合，定义为*初始*运行版本。根据这个定义，所有与初始运行有关的再处理拷贝和再分析版本都

被连接在一起，这就提供了一个带所有中间步骤和结果的最终结果的完整历史。这个版本是用户独立的，计算机生成的，并被记录在了审计追踪中。另外，FDA 法规要求记录人员的变更操作和再处理过程的时间标记。文件化的过程将在审计追踪内容中进行详细讨论。

安捷伦 ChemStation Plus 不允许从一个样品的完整版本清单中删除单个版本，这就确保了完整的历史并保留了原始进针的审计追踪。为了删除数据，用户必须具有归档或删除数据的权限，然后只能删除一次运行的所有版本，请见图 5a。没有办法删除一些中间版本，例如去掉*不好的结果*。

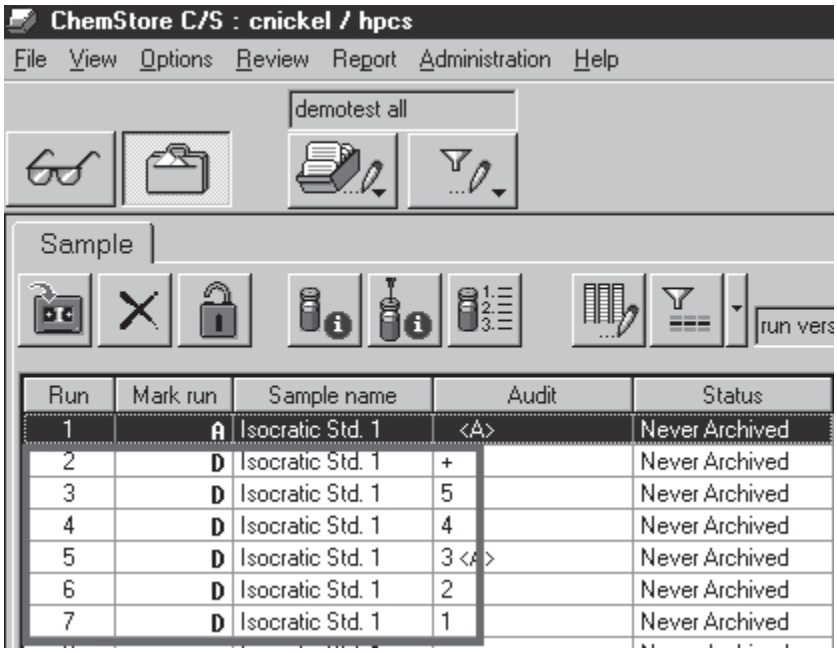


图 5a
包括删除保护的自动数据版本

安捷伦 ChemStation Plus 的自动数据版本包含了一次进针的所有相关数据：原始数据、方法和序列。

安捷伦 ChemStation Plus 允许在原始数据成功转移到数据库后，在本地删除原始数据。这个删除过程受到 ChemStore C/S 假脱机应用程序的控制，这就避免了如果网络出现问题而丢失数据的可能性。这个假脱机程序负责向服务器转移数据的过程，并确保所有数据都很完整，并储存在数据库表中。对向服务器数据库完整转移数据的过程检查是强制性的，这可以使删除原始数据过程只在本地驱动器上进行。整个数据传输过程被记录在 ChemStation 的日志和 ChemStation Plus 审计追踪中。安捷伦 ChemStation 的日志将显示传输过程的初始化，安捷伦 ChemStation Plus 的审计追踪将记录整个传输过程，包括时间标记。

通过这个数据传输过程，用户可以将所有数据存储在一个地方，并防止丢失任何数据，并记录每一个传输步骤。管理员将决定他们是否可以保存所有数据到数据库中，并配置研究过程，见图 5b。

符合21CFR第11部分的创建过程需要保存所有相关数据到安捷伦 ChemStation Plus 的数据库中，见图 5b。因此这将确保在一个中心长期保存所有结果，以及相关的元数据和用于创建结果的计算。

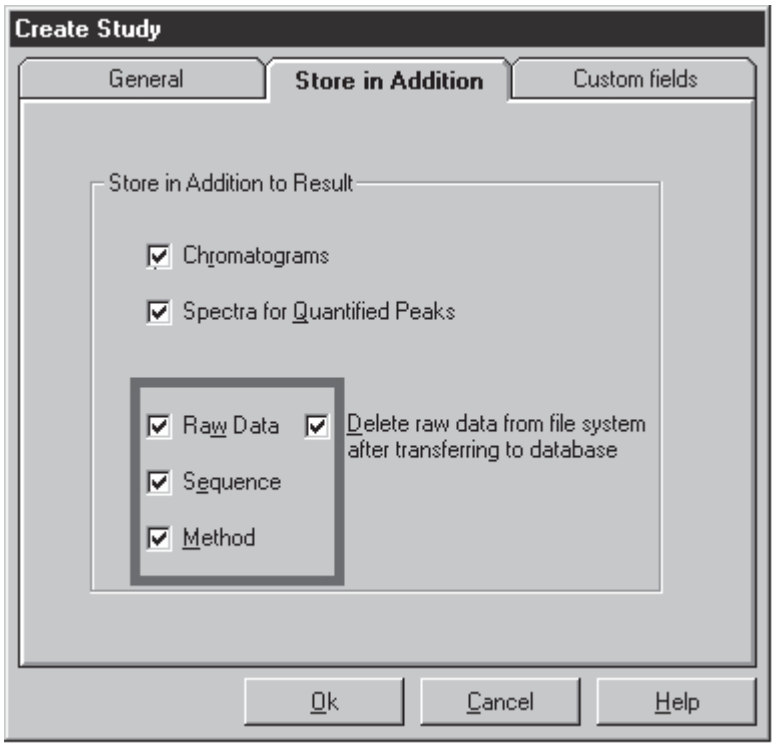


图 5b
数据完整性的设置

正确和完整的拷贝

完整和准确拷贝数据的第一步是将数据从本地应用程序转移到网络服务器的数据库中。这个转移过程的准确性是通过对原始和转移后的结果进行散乱数值校验计算来得到保证的。转移后的结果是以色谱语言形式保存的原始数据和元数据的完整拷贝。色谱元数据是积分和校正参数或是建立的序列分析校正。当将原始序列和方法与原始数据保持在一起的时候，完整的元数据就已经保存了。转移过程的建立请见图5b。

安捷伦提供了几种接口，可以使数据拷贝到外部应用程序或纸上。

结果数据的电子拷贝可以以报告文件的形式得到，例如以电子表格形式 .XLS，或通用文件格式 .XML、.CSV、和 .HTML。结果拷贝的自动创建是安捷伦 ChemStation 序列的一部分。安捷伦 Chemstation 的 manager 具有管理员权限，能够在数据自动采集和转移（*运行序列*）过程结束时，通过*打印到文件*命令，输出数据到预先定义的位置，见图5c。

可以将屏幕内容出现的交互式数据输出到剪贴板或 Microsoft Excel 中。自动输出到文件的数据是受到校验和保护的，这可以确保原始数据和输出拷贝的一致性（...*完整准确的电子记录拷贝*...），见图 5c。

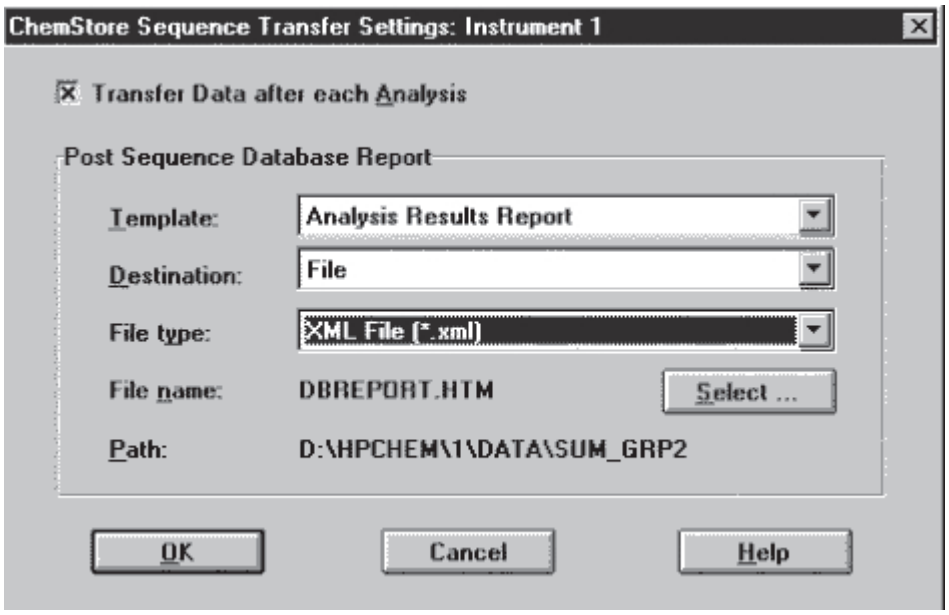


图 5c
输出到文件的自动报告

但是在建立数据拷贝的时候，用证据证明结果被完整准确的复制，不仅对于审计员来说很重要，而且对用户也同样重要。怎样才能在很长一段时间，例如超过十年，在不牺牲数据完整性的情况下，维护电子记录呢？安捷伦 ChemStation Plus随产品提供了一个例行归档程序，可以进行符合法规的长期数据的保存。归档工具是基于查询进行工作。它可以根据一个简单的数据库查询，让用户选择一个自定义的运行号，然后建立一个归档单元来进行归档。每一个归档单元都具有一个唯一的ID号。所有的归档单元都被保留，以便日后将所有的运行再解档到它们在数据库中的原始位置。所有与运行相关的信息，特别是审计追踪，都与运行数据保存在一起。如果特定的运行或时间记不清了，不用解档就可以对归档单元进行搜索。

为了节约服务器的空间，可以将归档任务与实际数据库的删除运行结合起来。如果运行过程已被归档，但还在数据库中，那所有这些已归档的运行过程将被锁定，这可以确保在带有拷贝版本的归档单元的数据库中，*非活动*运行过程的准确性。除了可以进行简单浏览外，所有获取这些非活动运行过程的请求都将被禁止。

归档和删除属于用户的一种权限，可以对它们进行配置，并通过对这些活动进行电子签名，用密码再确认方式来进行保护。图 5b 显示了一个创建归档单元的例子。

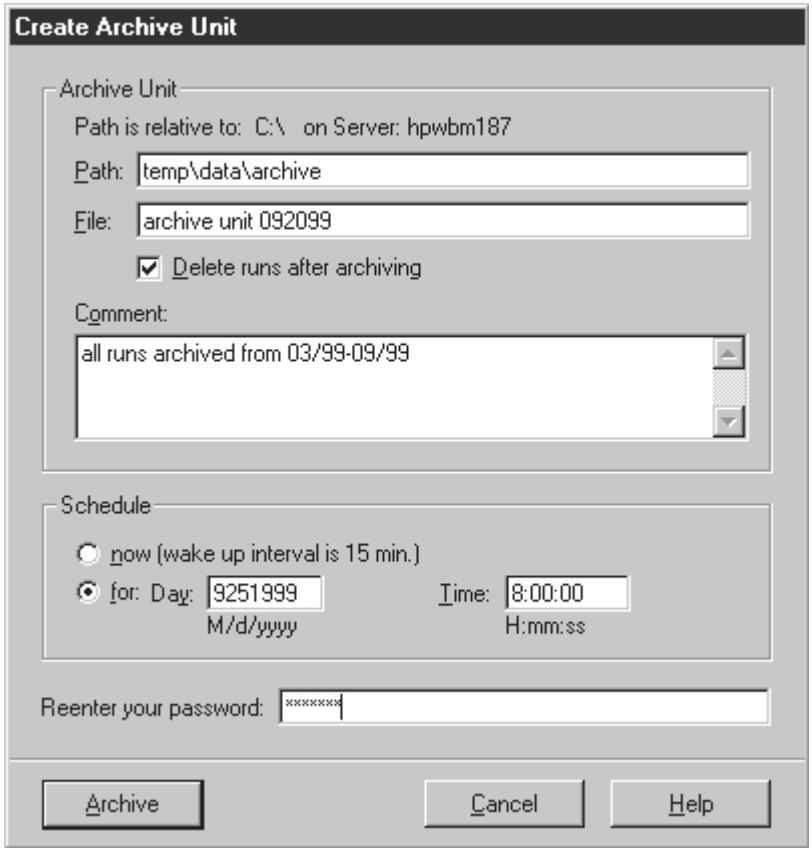


图 5d
运行过程的归档 / 删除设置

审计追踪

对所有电子记录要求的核心是审计追踪，因为这是唯一的、用户独立的、用于确保电子记录安全的工具，这是法规所规定的（*...11.10（e）...一个计算机生成的、带时间标记的审计追踪，用来独立记录操作者输入内容以及进行创建、修改、或删除电子记录的活动和日期时间*）。

安捷伦ChemStation Plus的审计追踪做了什么？它为每一次进针创建了它自己的审计追踪表，在这张表上，用进针时间和唯一的进针ID来定义进针。首先，审计追踪总是将这一次进针的所有再处理结果的版本列出来。第二步，在这张表上列出了所有与样品有关的数据，并使它们与原始的进针紧密不可分割。审计追踪被定义为*自动的用户独立的记录所有系统本身所产生数据的相关变化。这个记录应包括谁什么时候改变了什么。*

什么是追踪?在安捷伦ChemStation Plus中，*与信息相关的运行被定义为*

- 数据库中新的输入条目
- 从悬而未决转变为批准或拒绝的状态变化
- 用户填写字段的内容变化
- 数据重新回到应用程序中，进行一次或更多次的再分析
- 所有的再分析/再处理过程 — 新版本的每一个结果
- 运行状态变化的强制备注
- 每一个运行版本所有归档 / 解档 / 再打开活动

什么时候执行变化？用当地时间（计算并记录与GMT的不同）表示的修改时间和处理时间可以说明变化发生的时间。处理时间记录了数据从应用程序转到数据库的时间，修改时间记录了执行活动时产生审计追踪的时间。

另外，这两个时间标记显示了数据修改和传输的时间差别，这个差别说明了每一个运行版本活动的情况。

是谁做的？*谁做的修改*这一列用用户显示名（与用户ID紧密不可分割，见图3a）来记录谁修改数据。修改数据后，会再次输入密码来进行确认。

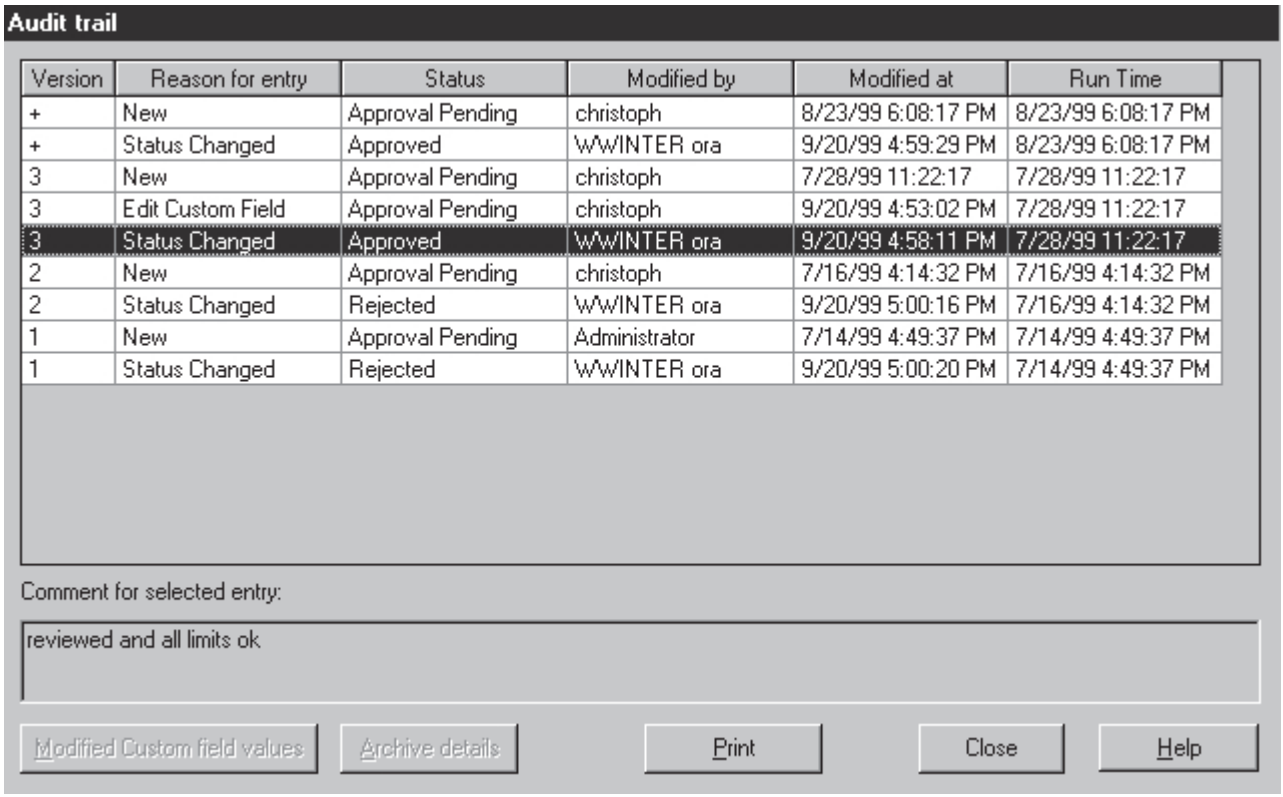


图 6a
安捷伦 ChemStation Plus 的审计追踪表

审计追踪的所有信息都必须以可打印的状态存在（11.10（e）*检查人员应该能够检查和拷贝审计追踪文件*...）。应该能从表中直接打印审计追踪，或可以在完整的报告中为一套运行过程进行单独配置。

有一些问题，特别是管理员级别的应用问题，是与运行相关的审计追踪不能回答的。数据库中高级别的修改活动，例如登录与注销、改变用户的权限、清除用户密码、将旧的或单机版的数据库转移到客户 / 服务器数据库中，都将被追踪并被记录到*数据库的审计追踪*或 ChemStore C/S日志中。这个日志允许按字段对数据进行分类和检查。

以下的字段将在数据库日志中显示，请见图 6c。

- 进样编码
- 创建记录的用户名字（用户显示名）
- 创建记录的时间
- 记录的原因（登录 / 注销、应用程序加锁 / 解锁、用户管理 / 权限和密码的变更、用户填写字段的内容变化、数据库的转移、运行批准和拒绝和归档操作）
- 受影响的用户（涉及到权限变化的）
- 使用的范例（仪器部分或浏览客户端）
- PC 主机名称

另外，日志还为所有的表格提供预定义的过滤器，可以在检查和审计中只显示感兴趣的数据。

根据数据库日志和当前授权用户和他们相应的权限清单，能在记录保留时间内检查应用程序的安全状态。

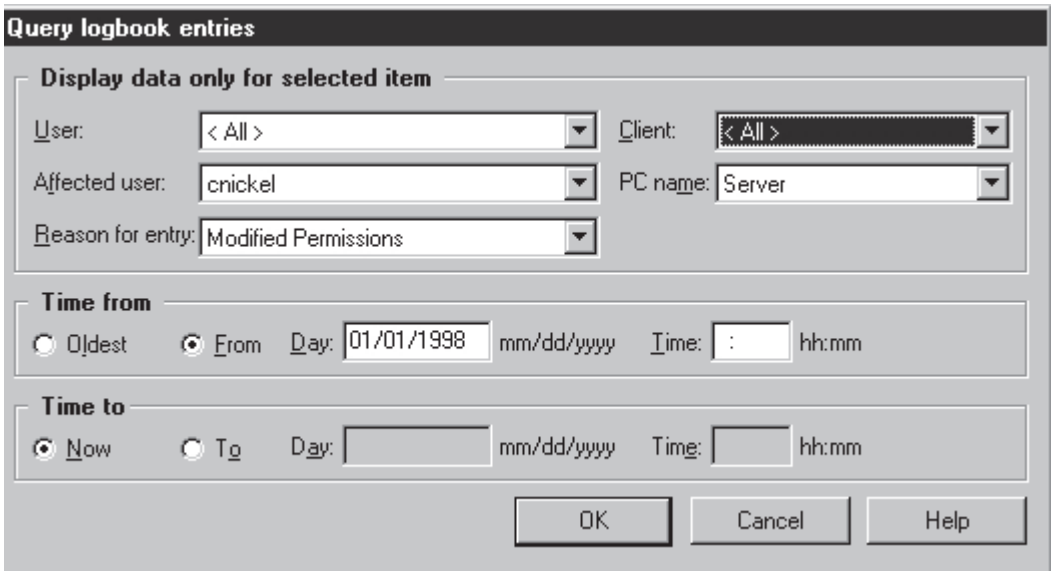
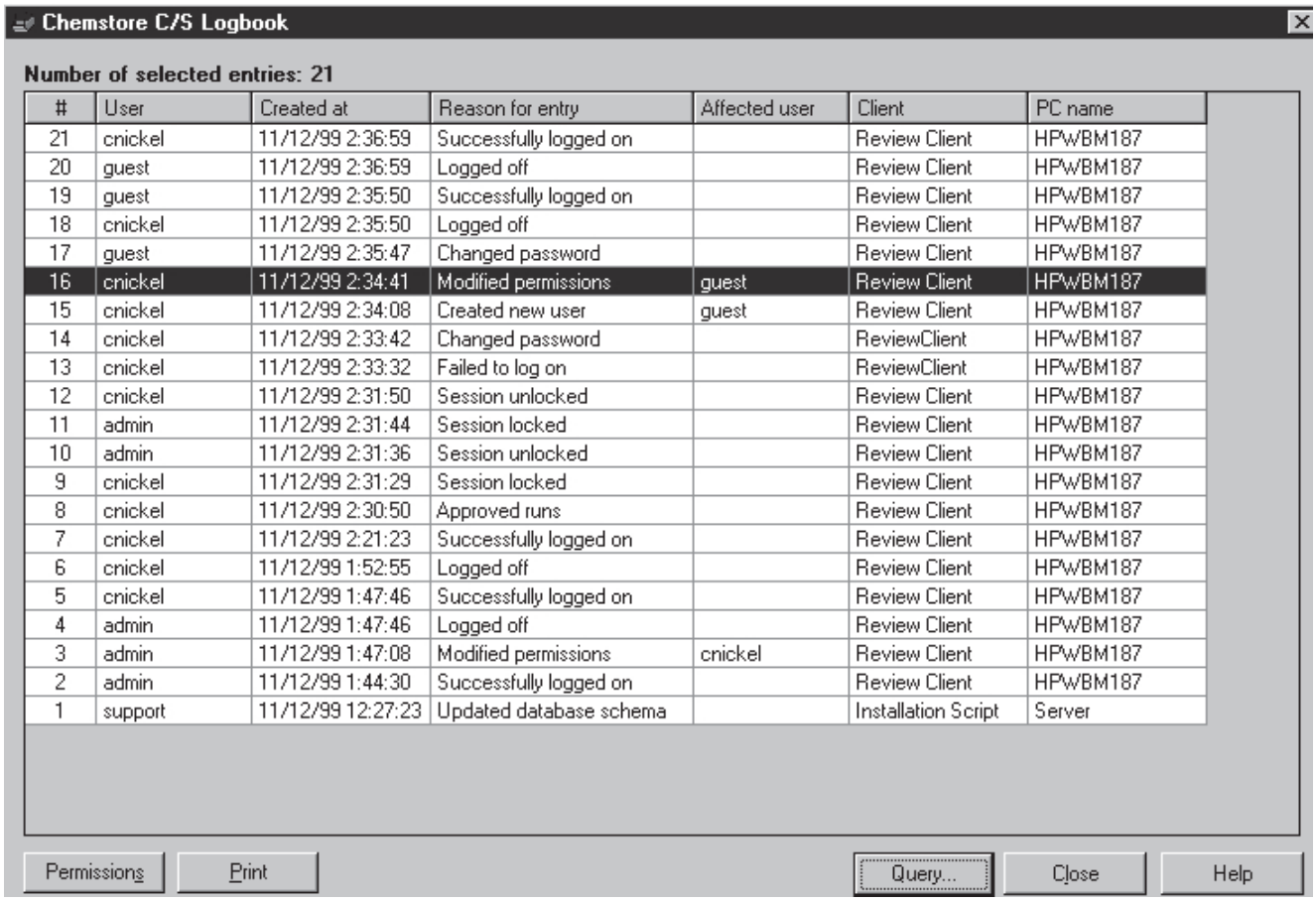


图 6b
数据库日志查询



#	User	Created at	Reason for entry	Affected user	Client	PC name
21	cnickel	11/12/99 2:36:59	Successfully logged on		Review Client	HPWBM187
20	guest	11/12/99 2:36:59	Logged off		Review Client	HPWBM187
19	guest	11/12/99 2:35:50	Successfully logged on		Review Client	HPWBM187
18	cnickel	11/12/99 2:35:50	Logged off		Review Client	HPWBM187
17	guest	11/12/99 2:35:47	Changed password		Review Client	HPWBM187
16	cnickel	11/12/99 2:34:41	Modified permissions	guest	Review Client	HPWBM187
15	cnickel	11/12/99 2:34:08	Created new user	guest	Review Client	HPWBM187
14	cnickel	11/12/99 2:33:42	Changed password		ReviewClient	HPWBM187
13	cnickel	11/12/99 2:33:32	Failed to log on		ReviewClient	HPWBM187
12	cnickel	11/12/99 2:31:50	Session unlocked		Review Client	HPWBM187
11	admin	11/12/99 2:31:44	Session locked		Review Client	HPWBM187
10	admin	11/12/99 2:31:36	Session unlocked		Review Client	HPWBM187
9	cnickel	11/12/99 2:31:29	Session locked		Review Client	HPWBM187
8	cnickel	11/12/99 2:30:50	Approved runs		Review Client	HPWBM187
7	cnickel	11/12/99 2:21:23	Successfully logged on		Review Client	HPWBM187
6	cnickel	11/12/99 1:52:55	Logged off		Review Client	HPWBM187
5	cnickel	11/12/99 1:47:46	Successfully logged on		Review Client	HPWBM187
4	admin	11/12/99 1:47:46	Logged off		Review Client	HPWBM187
3	admin	11/12/99 1:47:08	Modified permissions	cnickel	Review Client	HPWBM187
2	admin	11/12/99 1:44:30	Successfully logged on		Review Client	HPWBM187
1	support	11/12/99 12:27:23	Updated database schema		Installation Script	Server

图 6c
数据库日志

在审计状态，一个用户能用证据说明数据的实时安全状态，以及当有管理员权限的用户登录系统时，系统短暂的不安全性。

举个例子，一个用户登录到系统，并执行了一些敏感操作，例如归档或删除数据。在检查状态，负责的操作者能够证实，除了这个时间线（timeline）以外，通过显示如下内容，全部的应用程序是安全的。

- 当前权限的清单
- 在数据库日志中，对数据检查时期内的用户权限的所有改变情况进行查询

只有图 6c 中带有修改权限原因的行被选中后，许可按扭才会被激活。当按下后，一个模板会弹出来，它将显示会影响用户的旧权限和新权限，请见图 6d。

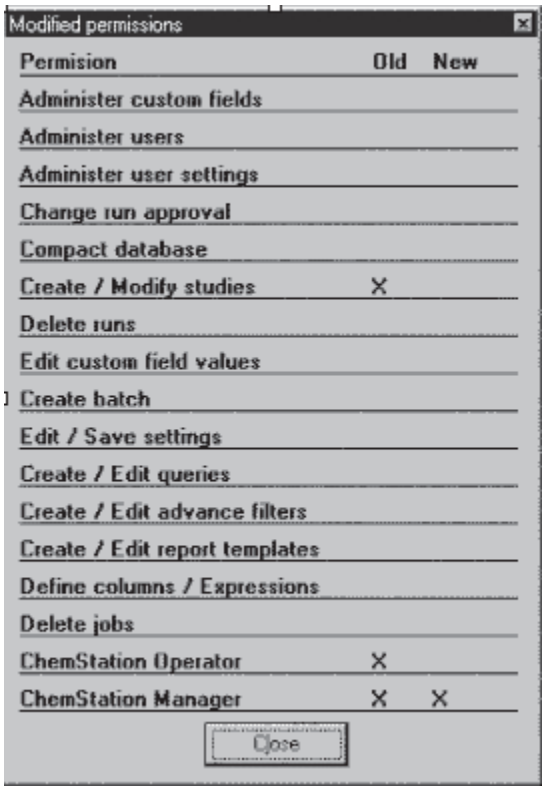


图 6d
数据库日志中用户权限的变更

电子签名

*封闭*和*开放*系统中的电子签名过程是不一样的。开放系统通常公开提供数据，并且不限制登录，因此通常情况下不适用于法规环境下的公司。大部分规范的制药公司物理控制登录，并通过防火墙来保护网络。如果它们具备先前讨论的必要条件，那就可以看作是*封闭*系统。例如一个封闭系统的例子“*如果记录是保存在公司的网络中，并对网络的登录进行控制，即使是通过公共的电话线或 T1 线路也不例外，那这个系统就是封闭系统*”（Paul Motise, FDA）。

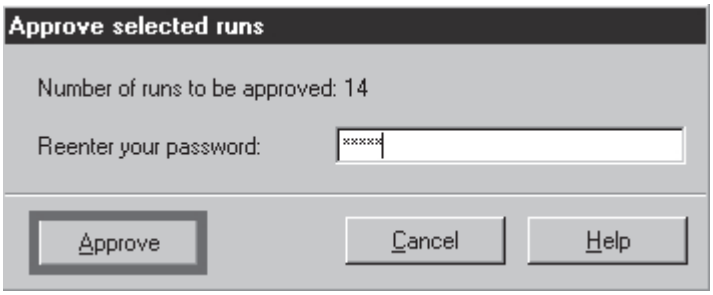


图 7
电子签名的提示屏幕

对于电子签名，FDA 的要求是非常明确的：“*每一个人的电子签名必须是唯一的，且不能重复使用，或再分派给其他人*”（11.100）

[...]电子签名必须至少包括两个部分（11.200），例如一个用户 ID 和一个密码。（在封闭系统中）[1]

电子签名的定义可以确保：一个执行电子记录的电子签名必须与相关的电子记录相关联，来确保签名不能修改、拷贝，否则有可能通过一般方式传送伪造的电子记录（11.70）[1]。

有关对密码安全性要求的详细讨论，已经在先前的数据安全、限制性系统登录和密码策略章节中讨论过了。如以上所说，在封闭系统中，一个电子签名应至少包括两部分来使一个用户身份唯一，用户 ID 和密码。

在安捷伦ChemStation Plus中，结果的批准和拒绝受到保护并被文件化。首先系统管理员会为每一个用户进行权限设置。然后出现批准和拒绝的签名提示来进行身份和密码确认，再加上强制备注后退出，见图 7。

所有其它敏感操作（象改变与运行相关的数值，例如批号等等）和归档、删除运行过程，与以上描述的过程是一样的。

1. 验证	1. 所有软件模块的 IQ 和 OQ/PV
2. 控制系统登录	2. 数据库的用户管理和密码保护
3. 审计追踪	3. 数据库中计算机生成的记录
4. 检查（权限和系统）	4. 用户配置文件和系统 SN ID
5. 准确和完整的拷贝	5. 归档 / 解档和文件输出
6. 保护（系统和记录）	6. 通过在数据库中保存完整的数据来保护带有用户权限和密码的所有数据
7. 足够的培训	7. 使用供货商提供的课程和研讨会

图 8
安捷伦 ChemStation Plus 对封闭系统要求的支持

总结

有关电子数据和电子签名的指南将对实验室用户、管理者以及分析仪器供货商的日常工作产生巨大影响。即使现在有关电子签名的法规是基于实用的基础，但是实验室电子数据的处理将会变得越来越专有和与众不同。

指南十分复杂，如果想要在实验室正确地实施需要实验室用户、管理者和仪器供货商的共同努力。对于化学分析数据，公司必须确保他们的实验室 — 全体部门当然更好 — 满足*封闭系统*的要求。

这篇技术文章阐述了安捷伦 ChemStation Plus如何帮助用户确认一个封闭系统。所有的项目已在图2中列了出来。除了第7条，对用户进行足够的培训，请见图8。如果应用程序供货商与将安捷伦 ChemStation Plus 作为色谱数据处理系统的用户共同努力，这些要求是可以实现的。

参考文献

1. “Elctronic Records, Electronic Signatures 21 CFR Part 11,” Department of Health and Human Services, Food and Drug Administration Docket No. 92N-0251RIN 0910-AA29

2. “Implementing Electronic records and signatures with the Agilent ChemStation Family,” Technical Note, publication number 5966-2315E

3. Agilent ChemStation Plus specifications, publication number 5968-5596E

Microsoft and Windows NT are U.S. registered trademarks of Microsoft Corp.

Oralcle is a U.S. registered trademark of Oracle Corp.



安捷伦对本文中存在的错误，以及因使用本材料造成的任何损失和后果不承担法律责任。

本文中的信息、说明及规格如有更改恕不另行通告。

©安捷伦科技公司，2003

中国印刷
2004年04月13日
5968-7930CHCN

Agilent Technologies