ICS 03.120.20
A 00

中华人民共和国国家标准

GB/T 22275.6—2008

良好实验室规范实施要求 第6部分：良好实验室规范原则在计算机化的系统中的应用

Requirements of conduct for Good Laboratory Practice(GLP)—Part 6:The application of the principles of GLP to computerised systems

2008-08-04 发布　　2009-04-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

前　言

GB/T 22275《良好实验室规范实施要求》分为7个部分：

——第1部分：质量保证与良好实验室规范；

——第2部分：良好实验室规范研究中项目负责人的任务和职责；

——第3部分：实验室供应商对良好实验室规范原则的符合情况；

——第4部分：良好实验室规范原则在现场研究中的应用；

——第5部分：良好实验室规范原则在短期研究中的应用；

——第6部分：良好实验室规范原则在计算机化的系统中的应用；

——第7部分：良好实验室规范原则在多场所研究的组织和管理中的应用。

本部分为GB/T 22275的第6部分。

本部分等同采用经济合作与发展组织(OECD)良好实验室规范(GLP)原则和符合性监督系列文件No. 10：《GLP原则在计算机化的系统的应用》[OCDE/GD(95)115]。

本部分进行了如下编辑性修改：

——删除了原文的前言和引言部分；

——删除了原文定义中的注1。

本部分的附录A为资料性附录。

本部分由全国危险化学品管理标准化技术委员会(SAC/TC 251)提出并归口。

本部分的起草单位：山东出入境检验检疫局、全国危险化学品管理标准化技术委员会。

本部分的主要起草人：车礼东、黄红花、王会永、于文莲、孙忠松。

良好实验室规范实施要求
第6部分：良好实验室规范原则在计算机化的系统中的应用

1 范围

GB/T 22275的本部分规定了GLP原则下计算机化的系统的应用与管理，包括各部门的责任、相关的培训、设备和仪器的要求、计算机化的系统的维护与灾难恢复、数据的记录与处理、计算机化的系统的安全、计算机化的系统的确认程序、关于其开发、确认、操作和维护的文档要求。

本部分适用于GLP原则下计算机化的系统的应用。

2 规范性引用文件

下列文件中的条款通过GB/T 22275的本部分的引用而成为本部分的条款。凡是注日期的引用文件，其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本部分，然而，鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本部分。

GB/T 19001 质量管理体系 要求

GB/T 22278 良好实验室规范原则

3 术语和定义

GB/T 22278中的术语和定义适用于本部分。

4 要求

4.1 范围

4.1.1 所有用于生成、测量和评价向管理机构提交的数据的计算机化的系统应以符合GLP原则的方式来开发、确认、运行和维护。

4.1.2 在计划中，研究的执行和报告可能会出于多种目的使用多个计算机化的系统。这些目的可能包括直接的或者间接的从自动化仪器采集数据，操作和控制自动化设备以及处理、报告和存储数据。对于这些不同的活动，计算机化的系统也有所不同，可以是一个可编程的分析仪器，也可以是一台连接至实验室信息管理系统的多功能个人计算机。在任何涉及计算机的范围，GLP原则都应被应用。

4.2 步骤

4.2.1 应用于以向管理机构提交为目的的研究执行中的计算机化的系统，应有适当的设计、足够的能力并适用于其预期目的。应有适当的操作程序来控制和维护这些系统，这些系统应以遵循GLP原则的方法来开发、确认和运行。

4.2.2 论证计算机化的系统是否适用于其预期目的是非常重要的，这称作计算机的确认。

4.2.3 确认程序将严格确保计算机化的系统达到它的设计要求。确认应采取正式的确认计划并在使用前进行。

5 GLP原则在计算机化的系统中的应用

下面提到的需要考虑的事项将对上文提到的GLP原则在计算机化的系统中的应用提供帮助。

5.1 责任

5.1.1 管理者

5.1.1.1 试验机构管理者对遵循 GLP 原则承担全部的责任。这些责任包括任命和有效地组织足够的具有适当资质和经验的人员，还包括确保仪器、设备以及数据处理程序符合适当的标准要求。

5.1.1.2 管理者有责任确保计算机化的系统适用于其预期目的。应建立计算机相关规定和操作程序，以确保计算机化的系统以遵循 GLP 原则的方式来开发、确认、运行和维护。管理者还应确保这些规定和操作程序被理解和执行，并确保这些要求被有效监督。

5.1.1.3 管理者还应指派人员专门负责计算机化的系统的开发、确认、运行和维护。该负责人应具有相应的资质和经验，接受过适当的培训，以便能够遵循 GLP 原则来履行他们的职责。

5.1.2 项目负责人

5.1.2.1 项目负责人应在 GLP 原则下负责整个研究的全面实施。因为许多研究可以利用计算机化的系统，项目负责人应充分了解其负责的研究领域中涉及到的任何计算机化的系统。

5.1.2.2 项目负责人在电子数据记录方面的责任与在纸质数据记录方面的责任相同，因此只有经过确认的系统才可应用于符合 GLP 原则的研究中。

5.1.3 人员

所有使用计算机化的系统的人员有责任遵循 GLP 原则来操作这些系统。负责计算机化的系统的开发、确认、运行和维护的人员有责任按照 GLP 原则和公认的技术标准来开展这些工作。

5.1.4 质量保证

5.1.4.1 计算机化的系统的质量保证的职责应由管理者明确并且在书面的规定和程序中予以说明。质量保证计划应包括保证计算机化的系统的确认、运行和维护的所有阶段能够满足现有标准的程序和实践。还应包括关于已购入系统的介绍以及计算机化的系统内部开发过程的程序和实践。

5.1.4.2 质量保证人员应负责监督计算机化的系统遵循 GLP 的情况，并应接受必要的专业培训。他们应对这些系统十分熟悉以便作出客观的评价。某些情况下指定专业的审核人员可能是必要的。

5.1.4.3 质量保证人员应对计算机化的系统内存储的数据拥有直接的只读权限以便进行审查。

5.2 培训

5.2.1 GLP 原则要求试验机构拥有具有适当资质和经验的人员，有书面的培训计划，包括在岗培训，如果适当的话，还包括参加外部培训课程。所有的培训记录应被保留。

5.2.2 上述规定也同样适用于与计算机化的系统有关的所有人员。

5.3 设备和仪器

应有足够的设备和仪器以便遵循 GLP 原则正确地实施研究。对于计算机化的系统来说还有许多特殊注意事项。

5.3.1 设备

5.3.1.1 应考虑计算机硬件、外围设备、通讯设备以及电子存储介质的物理位置。极端的温湿度、灰尘、电磁干扰以及靠近高压线都应予以避免，除非设备是经特殊设计专门用于这些环境下的。

5.3.1.2 还应考虑计算机设备的电力供应，在适当的情况下应给那些突然中断就会对试验结果造成影响的设备提供后备电源或者不间断电源。

5.3.1.3 应有适当的设备来确保电子数据存储介质的安全。

5.3.2 仪器

5.3.2.1 硬件和软件

5.3.2.1.1 计算机化的系统的定义是将一组硬件和软件设计和组合在一起，执行一个或一组特定的功能。

5.3.2.1.2 硬件是计算机化的系统的物理组成部分，它包括计算机单元本身及其外围设备。

5.3.2.1.3 软件是一个或一组用来控制计算机化的系统运行的程序。

5.3.2.1.4 因此所有适用于仪器的GLP原则同样适用于硬件和软件。

5.3.2.2 通讯

5.3.2.2.1 有关计算机化的系统的通讯大致上可以分为两种：计算机之间的通讯和计算机与外围设备间的通讯。

5.3.2.2.2 所有的通讯连接都是造成误差的潜在因素，可能会导致数据的丢失或损坏。适当的安全及系统完整性的控制应在整个计算机化的系统的开发、确认、运行和维护过程中充分的执行。

5.4 维护和灾难恢复

所有的计算机化的系统都应以某种方法来安装和维护以确保其准确、连续的运行。

5.4.1 维护

应有包含日常预防维护和故障检修的书面程序。这些程序应清楚地注明相关人员的任务和责任。当维护活动对硬件和(或)软件作出必要改变时，可能需要对整个系统再一次进行确认。在系统的日常操作过程中，应保存任何检测到的问题或冲突，以及采取的纠正措施的记录。

5.4.2 灾难恢复

5.4.2.1 程序应对在计算机化的系统部分或全部发生故障时所采取的方法进行适当的描述。方法可包括计划的硬件冗余备份、转印到纸质系统等。所有的意外保障计划应以书面形式充分记录和确认，并且应能够确保连续数据的完整性，以及不会在任何方面对研究造成危害。符合GLP原则的研究执行人员应了解这些意外保障计划。

5.4.2.2 计算机化的系统的恢复程序将视系统的危险程度而定，但是要点是应保存所有软件的备份。如果恢复程序应对硬件或者软件做出更改，那么可能需要对系统进行重新确认。

5.5 数据

5.5.1 GLP原则对原始数据的定义是所有的原始的实验室记录和文件，包括直接由设备界面录入到计算机的数据，是研究中原始的观察和活动结果，也是重建和评估研究报告所必需的数据。

5.5.2 遵循GLP原则运行的计算机化的系统可以通过多种方式和原始数据联系在一起，例如，电子存储介质、计算机或设备打印输出和微缩胶片拷贝。对于每个计算机化的系统，都应对原始数据进行界定。

5.5.3 当计算机化的系统应用于进行原始数据的电子化采集、处理、报告或者存储时，系统的设计应能够保留全部的审核索引以显示数据的所有改变并且没有掩盖原有的数据。它应能够通过使用标有时间及日期的(电子化的)签名将所有的数据改变与更改人关联起来。应给出数据更改的理由。

5.5.4 当使用电子化的手段来保存原始数据时，有必要考虑该类型数据长期保存和计算机化的系统预期寿命的要求。硬件和软件的改变应能够保证原始数据的连续使用和保存，避免完整性被破坏的风险。

5.5.5 校准原始数据有效性或准许某一过程或研究重建所必需的支持信息，例如维护和校准记录，应在档案中保存。

5.5.6 计算机化的系统的操作程序中还应描述当系统崩溃时替代的数据采集程序。在这种情况下任何由人工记录并随后输入至计算机中的原始数据应被清晰地注明，并且应作为原始记录进行保存。人工备份程序应使得任何数据丢失的风险降至最低并且确保这些替代的记录保存下来。

5.5.7 当系统由于被淘汰需要将电子原始数据从一个系统转移到另一个系统时，这一过程应被充分记录，并且它的完整性应经过校验。当这种转移无法进行时，原始数据应先被转移到另一个介质中，并且在破坏任何原有电子数据之前要先经过精确复制的校验。

5.6 安全

书面的安全程序应能够保护硬件、软件和数据免于损坏或者未经授权的修改或丢失。本部分中所述的安全包括避免计算机化的系统及其数据被未经授权的使用或更改。还应避免潜在的由于病毒或者其他间谍程序引起的数据损坏。在系统短期或者长期崩溃的情况下也应采取安全措施以确保数据的完整性。

5.6.1 物理安全

物理安全措施应能够限制计算机、通讯设备、外围设备和电子存储介质仅由经过授权的人使用。对于不是特定计算机场所内的设备(例如个人计算机或者终端),至少应采用标准的试验机构访问控制。无论如何,当这种设备是远程设置的时(例如可移动设备以及调制解调器连接),需要采用额外的措施。

5.6.2 逻辑安全

对于每个计算机化的系统或者软件,应有逻辑安全措施来避免对计算机、软件或数据的非授权使用。应确保只使用认可的版本和已验证的软件。逻辑安全可以包括使用密码来确认唯一的用户身份。任何来自外部资源的数据或软件的传入应被控制。这些控制可以由计算机操作系统、特殊的安全程序、应用程序内置的功能或者上述所有形式来提供。

5.6.3 数据完整性

鉴于维护数据的完整性是GLP原则的主要目标,那么所有与计算机化的系统相关的人员都应意识到上述安全措施的必要性。管理者应确保相关人员了解数据安全的重要性、现有的程序以及能够提供适当的安全措施和安全系统被破坏后的处理方法的系统特性。这些系统特性可包括系统访问情况的日常监督、文件校验的执行和例外情况和(或)整体趋势的报告。

5.6.4 备份

对于计算机化的系统来说,将所有的软件和数据备份是为了在任何可危及数据完整性的崩溃(例如硬盘损坏)后恢复系统而进行的标准操作。这意味着备份的数据有可能成为原始数据,因此应被当作原始数据等同对待。

5.7 计算机化的系统的确认

计算机化的系统应要满足其预期目的。下列方面应被提及:

5.7.1 可接受度

5.7.1.1 计算机化的系统应被设计为能满足GLP原则并且预先提出计划。应有足够的文件证明每个系统是在经过认可的质量和技术标准(例如GB/T 19001)下控制和开发的。更重要的是,应有证据表明这些系统在投入日常使用之前经过了试验机构严格的测试与可接受标准相一致。正式的可接受度测试要求在事先确定的计划下执行并且保留所有的操作程序、测试数据、测试结果、正式的测试摘要和正式验收记录的书面证据。

5.7.1.2 对于厂家提供的系统来说,很可能在开发中生成的大量文件证明保留于厂家那里。这种情况下,在试验机构处应有正式的评估和(或)厂家的审核。

5.7.2 回顾性评估

5.7.2.1 有一些系统并没有预期或者被指定要求遵循GLP原则。这种情况下应有书面的使用该系统的正当理由,这应包括一个对适用性的回顾性评估。

5.7.2.2 回顾性评估应首先收集涉及该计算机化的系统的所有历史记录。随后这些记录将被审查并形成一个书面的摘要。这个回顾性评估的摘要应详细说明存在何种确认证据,以及将来为了确保该计算机化的系统的确认所需进行的工作。

5.7.3 更改控制

5.7.3.1 更改控制是对在计算机化的系统的使用期间发生的任何改变的正式批准和文件。当一个改变可能会影响计算机化的系统的确认状态时,就需要有一个更改控制。一旦计算机化的系统投入运行,更改控制程序就应是有效的。

5.7.3.2 这一程序应描述这样的评估方法:该方法用于确定为了维持系统有效状态而需进行重新测试的必要程度。更改控制程序应指定人员来负责决定更改控制的必要性和批准执行。

5.7.3.3 无论改变的起因如何(源于供应商或者内部开发系统),都需要提供适当的信息作为更改控制程序的一部分。更改控制程序应能确保数据的完整性。

5.7.4 **支持机制**

为确保计算机化的系统始终适用于其预期的目的,支持机制应适当的确保系统功能正常并被正确的使用。这可以包括系统的管理、培训、维护、技术支持、审核和(或)效能评估。效能评估是对系统进行周期性的正式审查以确保它能够持续满足一定的效能标准,例如:可靠性、响应性和能力。

5.8 **文档**

下列条目的清单是关于计算机化的系统的开发、确认、操作和维护的最少文件的指导。

5.8.1 **规定**

应有有关涵盖计算机化的系统的资料收集、获取、需求、设计、确认、测试、安装、操作、维护、设置、控制、审核、监督和报废等情况的书面管理规定。

5.8.2 **应用程序描述**

对于每一个应用软件应有文档来充分地描述:

a) 应用软件的名称或者标识码,以及该应用目的的详细说明;

b) 执行应用软件的硬件(包括型号);

c) 与之共同使用的操作系统和其他系统软件(比如:工具软件);

d) 应用软件使用的语言和(或)使用的数据库工具;

e) 该应用软件执行的主要功能;

f) 与该应用软件相关的数据和(或)数据库流程设计的综述;

g) 该应用软件的文件结构、错误和报警信息以及运算法则;

h) 该应用软件的版本号;

i) 该应用软件模块与其他设备和系统间的配置和通讯连接。

5.8.3 **源代码**

某些 OECD 成员国要求应用软件的源代码应是可被试验机构使用或取得的。

5.8.4 **标准操作程序**

多数涵盖计算机化的系统使用的文件可以标准操作程序的形式存在。这些应包括,但不仅限于以下内容:

a) 操作计算机化的系统(软硬件)的程序,以及相关人员的责任;

b) 检测和防止未经授权的访问和程序更改的安全程序;

c) 程序更改的程序和授权以及更改记录;

d) 设备(软/硬件)更改的程序和授权,包括适当情况下在使用前进行检测;

e) 对整个系统或某个组件进行周期性测试,以确保其功能正常,并将这些测试进行记录;

f) 维护计算机化的系统和其他相关设备的程序;

g) 软件开发和可接受度测试的程序以及所有可接受度测试的记录;

h) 所有存储数据的备份程序以及崩溃时的应急计划;

i) 存档和恢复所有文件、软件和电子数据的程序;

j) 监督和审核计算机化的系统的程序。

5.9 **档案**

5.9.1 GLP 关于数据存档的原则应始终如一地对所有类型的数据执行。因此电子数据应具有和其他数据一样的访问控制、索引和便于取阅。

5.9.2 当多个研究的电子数据被存储在同一个存储介质时,应要求有一个详细的索引。

5.9.3 可能需要提供特殊的环境控制设备以便确保电子数据存储的完整性。如果需要额外的存档机构，那么管理者应指定专门的档案管理人员，并且确保只能由经过授权的人员访问档案。还有必要执行程序以确保不会对长期存储的数据的完整性造成危害。当需要考虑数据的长期存取问题或者当计算机化的系统需要报废时，应制定确保数据持续可读的程序。这可以包括：硬拷贝打印输出或者是将数据转移至另一个系统等。

5.9.4 电子数据的销毁应有管理者的授权和相关文件。其他用来支持计算机化的系统的数据，例如源代码和开发、确认、操作、维护和监督记录，应至少和与这些系统相关的研究记录保留相同的时间。

附 录 A
（资料性附录）
术语解释

A.1 可接受度标准(acceptance criteria)：应满足成功完成一个试验阶段或者应满足交付要求的书面标准。

A.2 可接受度测试(acceptance testing)：在预期的操作环境下对计算机化的系统的正式测试，以决定试验机构的所有可接受度标准能否被满足或者该系统对于操作使用来说是否能被接受。

A.3 备份(back-up)：当系统崩溃或者遇到灾难时用来恢复数据或软件、重启操作过程，或者供备用计算机使用的预防措施。

A.4 更改控制(change control)：在运行过程中评估和记录系统的操作和更改以决定计算机化的系统在发生任何更改后是否需要进行确认程序。

A.5 计算机化的系统(computerised system)：一组硬件和软件设计和组合在一起，执行一个或一组特定的功能。

A.6 电子签名(electronic signature)：以电磁压力或者任一符号或者一组符号编码的计算机数据的登录形式，由某人等同于其手写签名那样执行、修改或授权。

A.7 硬件(hardware)：计算机化的系统的物理设备，包括计算机本身和它的外围设备。

A.8 外围设备(peripheral components)：任何具有使用界面的仪器，或者辅助的，或者可移动的设备，例如打印机、调制解调器、终端，等等。

A.9 公认的技术标准(recognised technical standards)：由国家或者国际标准化组织发布的标准(如ISO、IEEE、ANSI 等)。

A.10 安全(security)：对计算机软硬件的保护，以避免意外或者恶意的访问、使用、修改、破坏或者泄漏。安全还包括人员、数据、通讯以及物理和逻辑上保护计算机的装置。

A.11 软件(应用软件)[software(application)]：是一个满足试验机构需要的、开发的、修改的或适合的程序，用于进行过程控制、数据收集、数据操作、数据报告和(或)存档。

A.12 软件(操作系统)[software (operating system)]：一个或一组程序、例行程序及子程序，用来控制计算机的操作。一个操作系统可以提供例如资源分配、时间调度、输入输出控制以及数据的管理。

A.13 源代码(source code)：一组最初的以人类可读形式表达的程序(程序语言)，它在被计算机执行前应转化为计算机可读的形式。

A.14 计算机化的系统的确认(validation of a computerised system)：确认计算机化的系统适用于其预期目的的验证行为。