

doi:10.3969/j.issn.1006-4931.2020.04.006

GMP 体系下 Windows 操作系统合规性探索

胡 顺¹, 郑 莹¹, 刘泽伦¹, 邓 宇¹, 安定国¹, 蒋琼霞²

(1. 湖北省食品药品监督管理局东湖新技术开发区分局, 湖北 武汉 430075; 2. 武汉华龙生物制药有限公司, 湖北 武汉 430043)

摘要:目的 为提升药品生产企业数据可靠性管理水平提供参考。方法 分析药品生产企业执行药品生产质量管理规范(GMP)及相关法规过程中在计算机化系统常用操作平台(以 Windows 7 系统为例)管控上存在的问题及其可能原因,并提出了可操作性的解决方案。结果与结论 GMP 体系中 Windows 操作平台在数据可靠性及合规性上存在一定的问题,药品生产企业应引起重视,需通过适当措施进行必要的管控,以减少药品数据在其生命周期内的风险。

关键词:药品生产质量管理规范;药品数据;可靠性;合规性;Windows 操作系统;Windows 7

中图分类号:R95

文献标识码:A

文章编号:1006-4931(2020)04-0018-04

Exploration of Windows Operation System in GMP Compliance

HU Shun¹, ZHENG Ying¹, LIU Zelun¹, DENG Yu¹, AN Dingguo¹, Jiang Qiongxia²

(1. East Lake New Technology Development Zone Branch, Hubei Food and Drug Administration, Wuhan, Hubei, China 430075; 2. Wuhan Hualong Biopharmaceutical Co., Ltd., Wuhan, Hubei, China 430043)

Abstract: Objective To provide reference for improving the level of data reliability management of pharmaceutical manufacturers.

Methods : By analyzing the problems and possible causes of the management and control of the common computer operating system (taking Windows 7 as an example) in the process of implementing Good Manufacturing Practice(GMP) and related regulations by pharmaceutical manufacturers, the operability solution was proposed. **Results & Conclusion** There are certain problems in the reliability and compliance of the Windows operating platform in the GMP system. Drug manufacturers should pay attention to this and need to adopt appropriate control measures to reduce the risk of drug data over its life cycle.

Key words: Good Manufacturing Practice; drug data; reliability; compliance; Windows operating system; Windows 7

2016年,美国食品和药物管理局(FDA)共发布了44封关于药品生产质量问题的警告信,涉及162项缺陷,其中有98项与制药企业质量控制(QC)实验室的数据可靠性问题相关,包括我国15家制药企业的38项缺陷(38.78%)^[1]。2015年11月13日,原国家食品药品监督管理总局(CFDA)在官方网站上发布了《关于8家企业11个药品注册申请不予批准的公告》,原因是在对这些企业进行现场核查时发现“原始记录缺失,隐瞒弃用试验数据,修改调换试验数据,试验数据不可溯源,分析测试数据存疑,临床试验数据存在不真实、不完整的情况”等涉及数据可靠性的问题。

近年来,数据可靠性成为药品生产领域的研究热点,国内外一系列法规指南相继出台,众多培训检查,言必提及数据可靠性。各大仪器设备开发商以此为契,加大了软硬件升级的力度,其中以 Waters, Agilent, Diamond 及 Shimadzu 为代表的设备软件开发商由于长期以来的技术优势,在数据可靠性方面占有先机,获得了巨大的经济收益,同时也极大地提高了国内药品生产企业药品数据管理质量水平。整个行业从认识到管理水平均得到了很大提升,其中以计算机化系统为代表的数据库内容发展最迅速,计算机化系统大多不可避免地

跟电脑操作系统联系在一起,Windows 操作平台更是不可缺少的基础平台,在确保软件正常工作及数据安全上的作用不可忽视。

1 Windows 平台合规性控制的必要性

1.1 相关法规指南的要求

2003年,美国联邦法规第21章第11款(21CFRPart 11)对食品、药品生产过程数据安全性进行了要求^[2],指出应利用限制访问或防止非授权人员访问以实现对数据的保护。人员若要进入系统须经授权,且每个经过授权的人员都应有与其姓名相关联的独立用户名和密码,并具有唯一性。设置访问权限,每个用户只能访问特定的程序、文件和记录。2016年4月,美国FDA发布了《数据可靠性及其动态药品生产管理规范符合性行业指南》^[3],该指南在21CFRPart 11的基础上对数据可靠性在动态药品生产质量管理规范(CGMP)中的作用进行了进一步阐述和要求。

2015年3月,英国药品和医疗保健用品管理局(MHRA)发布了《关于GMP数据可靠性的行业指南》^[4]。该指南认为,就药品生产企业而言,最重要的是设计出一套合理的数据管理程序来降低数据可靠性的风险,而不只是对数据进行常规核对,如对带有计时功

第一作者:胡顺,男,大学本科,执业药师,工程师,主要从事药品、医疗器械技术审评工作,(电子信箱)hushun2006@qq.com。

能的计算机化系统等仪器设备进行进入权限设置,防止操作人员为了便于重复试验随意更改时间;控制计算机化系统中用户的权限,防止未经授权人员访问、修改数据等。

2015年12月1日起实施的我国药品生产质量管理规范(GMP)附录《计算机化系统》要求,计算机化系统的验证应包含应用程序的验证和基础架构确认。原CFDA食品药品审核查验中心于2016年10月10日在其官方网站上发布了《药品数据管理规范(征求意见稿)》,规定计算机化系统应按相应质量管理规范要求进行验证,并至少确认以应用程序和操作系统中保障数据可靠性的设计和配置(如审计追踪)已启用并有效运行,登录控制、权限设置及系统配置符合数据可靠性要求,应控制日期和时间的更改。

《良好自动化生产实践指南》第五版(GAMP5)认为,不同类别的计算机化系统是由不同系统组件构成的。目前,GAMP5将计算机化系统的组件分为操作系统、不可配置组件、可配置组件与定制组件。这些组件又由硬件和软件构成,其中软件分4个类别^[5]:第1类为基础设施软件,分为市场售卖的分层式软件和基础设施软件工具,包括操作系统、数据库引擎等;第2类为不可配置软件产品,分为不能通过配置以适应具体业务流程的系统或只可使用默认配置的可配置系统,包括商用货架产品(COTS)软件、仪表仪器等;第3类为可配置软件产品,此类产品提供了标准化的界面和功能,以使配置适合用户的具体业务流程,具体包括实验室信息管理系统(LIMS)、管理控制与数据获取(SCADA)、企业资源规划(ERP)等;第4类为定制应用软件,为满足客户特殊需求而开发的软件。Windows操作系统属第一类软件。

1.2 技术上有效的控制手段

按照GAMP5关于计算机化系统的分类,在GMP体系下不同级别的计算机化系统组成结构复杂程度是不一样的。如Waters色谱工作站的Power系统成熟度很高,能完全按计算机化系统关于数据可靠性的要求进行用户分级、权限控制、审计追踪、数据备份和存储。但如紫外、红外检测仪器,其应用程序本身不具备用户权限、审计追踪控制的功能,无法实现对数据安全的良好保护,除制订管理文件,通过人工记录的方式进行数据可靠的控制外,还需对软件使用平台Windows操作系统进行必要控制,在一定程度上防止无关人员登录、使用电脑对数据安全造成危害。Windows操作系统的有效控制也是保证软件安全运行的基础,若数据安全可靠保证较高的色谱工作站处在一个安全、稳定性很差的平台上,随时有错误、崩溃的风险,数据的安全可靠也就无从谈起。

2 存在的问题

从近年来国内制药行业检查情况看,国内企业在数据可靠性方面还存在很多问题。原山东省食品药品监督管理局审评认证中心2016年4月至9月开展的山东省无菌药品生产企业数据可靠性调研结果显示,目前电脑系统的账户分级工作开展较少,53家调研企业中只有6家以文件形式进行了相关规定,实际进行分级管理的仅2家^[6]。

权限控制的关键是权限分配的合理性。目前企业对电脑系统权限分配工作开展较少,原云南省食品药品监督管理局食品药品审核查验中心选取云南省12家制药企业开展了现场调研^[7]。结果显示,83.33%的企业建立了检验仪器工作站的权限分级管理,有利于对检验数据操作人进行追溯。但对于计算机设备本身(特别是检验仪器工作软件不具备审计追踪或权限分级的计算机设备),仅1/4的企业开展了计算机系统权限分级管理;其余企业存在的主要问题包括共用用户登录计算机系统、对修改系统时间或删除文件等权限未进行限制管理等,多数企业未考虑计算机系统的权限管理,操作人员可以修改删除电脑硬盘中的数据,不符合数据可靠性的管理要求,数据归属至人是数据可靠性管理的基本要求。其实现的基础是清晰的用户划分及权限管理。这些问题也是原CFDA开展跟踪检查过程中计算机系统数据可靠性方面的常见问题^[8]。

3 原因分析

3.1 对相关法规指南理解的误区

现场检查中发现,不少制药企业人员在计算机化系统管理方面平时的培训学习流于形式,未按相关法规指南如GMP计算机化系统附录、GAMP5的相关规定对GMP相关的计算机化系统软硬件进行分级,认为电脑Windows操作系统平台与GMP体系无关,或按照GAMP5电脑操作系统作为基础设施软件,不作为验证控制对象,只对GAMP5中不可配置软件、可配置软件、定制软件进行数据可靠性的要求管理。

3.2 专业技术人员的缺失

原CFDA2015年5月26日公告《关于发布〈药品生产质量管理规范(2010年修订版)〉计算机化系统和确认与验证公告两个附录的公告》中明确规定,应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。计算机化系统的要求,验证、使用等方面涉及多学科计算机、GMP的综合知识,相当部分中小企业执行GMP的药学人员对涉及IT的相关知识知之甚少,以至于企业花重金购买了价值不菲的计算机化系统。关于仪器设备的工作软件计算机化系统验证确认,厂商一般会提供相应的培训、验证服务,

而电脑操作系统的安全权限设置不在服务范围。另外,即使有企业配备有专门的 IT 部门人员,具备专业的 IT 知识,但其对 GMP 的相关要求学习不够,不能按 GMP 要求对涉及的电脑操作系统进行有效管控。

4 符合 GMP 要求的 Windows 操作系统控制

Windows 操作系统符合数据有效性的设置同样重要,内容分为用户分级、权限分配及审计追踪,通过 Windows 操作系统提供的“本地安全策略”功能,可为计算机创建出不同安全级别的环境,在一定程度上有效、完整、安全地保护信息。安全策略是影响计算机安全性的安全设置组合,通过本地安全策略可以控制访问计算机的用户及是否在事件日志中记录用户或组的操作,也可有效限制用户访问权限,阻止潜在的破坏者对系统进行恶意改动;通过建立用户职能,将权限进行分级管理,设定不同的用户组、用户级别,赋予不同的权限,并对权限级别进行受控管理;通过审计跟踪记录不同用户的行为活动,记录并保存用户对电子数据改动前和改动后的情况,以有效鉴别对数据的不恰当改动^[9-10]。基于安全风险考虑,制药行业 GMP 体系下大部分搭载设备仪器软件的电脑操作系统一般是单机或局域网环境,很少有连接互联网的。在此也是基于单机版系统进行说明,下面只提供一种基于 Windows 7 专业版操作系统下可行的操作方法(某些设置可能对家庭版无效),对涉及的专业深层 IT 知识不过多介绍。

用户分级:系统的常用用户一般有管理员用户(Administrator),普通用户或标准用户(User),以及来宾用户(Guest)。目前与制药设备仪器配套的商用电脑出厂基本已经安装好了 Windows 操作系统,系统默认账户为管理员账户,账号名为 Administrator,密码为空。使用管理员账户进行必要的工作站软件安装调试后,即可配置电脑普通操作人员账户。创建账户时,选择密码并保证密码的安全。按数据可靠性的要求,账户密码的设置要求和方法如下,在 Windows 7 桌面左下角打开“开始”菜单,选择“控制面板”,在弹出窗口中,依次点击“控制面板”“管理工具”“本地安全策略”“本地策略”“账户策略”“密码策略”,此时可见界面右边对应的内容,密码须符合复杂性要求,需开启;密码长度最小值,一般 6~8 位;密码最长使用期限,可设置 3 个月;密码最短使用期限,设为默认;强制密码历史,可默认;用可还原的加密来储存密码,可默认。

创建操作人员账户:一般有 2 种方法。方法 1,桌面左下角打开“开始”菜单,选择“控制面板”,在弹出的控制面板窗口选择“添加或删除用户账户”,在弹出的管理账户窗口中可看到现有账户,在“新增账户”选择下面的“创建一个新账户”,在弹出的创建用户窗口选择“创建

标准用户”即可,点击新创建的账号,接下来可设置登录密码等其他操作。方法 2,在桌面右键单击“计算机”,选择“管理”,在弹出的计算机管理窗口,选择“本地用户和组”,选择用户,这时可在右侧看到计算机里已有的电脑账号,在下面的空白处点击右键,选择创建新用户即可。在弹出的新用户窗口,输入新用户的信息,然后点击“创建”,点击后创建成功,这时窗口上还有一个创建新用户的窗口,可以接着创建,若不用可直接关闭。账户策略,可以不管。需注意的是,通过账户管理来添加 Windows 新用户对于普通 Windows 7 家庭版操作系统并不适用,需要 Windows 7 专业版或 Windows 7 旗舰版高级版本等才可行。

权限分配:权限管理是计算机化系统验证和法规的基本要求。默认情况下,Administrator 用户对计算机/域有不受限制的完全访问权。分配给该组的默认权限允许对整个系统进行完全控制。所以,管理员账户一般应由与计算机化系统使用、操作无关的人员掌控,如 IT 部门。标准账户为受控账户,其权限因受到限制,以杜绝标准账户可能的违反规定的操作。如禁止修改系统日期、事件、删除数据等。这些权限控制也需通过本地安全策略来实现。同上文操作依次点击“本地安全策略”“本地策略”“用户权限分配”,找到“更改系统时间”将标准账户所在的组(Users)删除,即取消了标准用户更改系统事件的权限;接下来在“本地策略”下的安全选项中,找到“交互式登录,不显示用户名”,安全设置中选择开启(防止使用已有账号列举式试密码)。重要数据通常会保存在电脑某个盘下的某个文件夹内,为了防止删除数据的操作,可控制不同账户操作相应文件夹的权限。具体方法为,鼠标右键单击相应文件夹,选择“属性”,在弹出的对话框中选择“安全”标签,点击“高级”,在弹出的对话框中会看到不同用户组对文件夹的不同操作权限,选中标准用户所在组,点击“更改权限”,在弹出的对话框中选择组进行编辑,这时会看到选中用户对该对象拥有的操作权限,在“删除”“删除子文件夹及文件”项勾选拒绝,点击“确定”。即完成了禁止标准用户对特定保存数据的删除权限。

审计追踪:计算机化系统中的关键数据操作(如参数修改、录入关键数据)等通常考虑建立数据审计追踪系统,用于记录数据的输入人员的身份和修改数据。Windows 7 系统事件日志是以特定的数据结构的方式存储有关系统、安全、应用程序的记录,每个记录事件的数据结构中包含了 9 个元素(可以理解成数据库中的字段),即日期/时间、事件类型、用户、计算机、事件 ID、来源、类别、描述、数据等信息。通过事件日志,可以了解计算机上发生的具体行为^[11]。开启审核追踪功能,配合事件查看器中事件日志记录,可达到审计追踪的目的。