【综述】

GLP机构中计算机化系统的安全性概述

张 頔#，李芊芊#，霍桂桃，屈 哲，杨艳伟，李 琛，张 曦，吕建军*，林 志*
中国食品药品检定研究院 食品药品安全评价研究所，北京 100176

摘 要： 采用计算机化系统进行数据采集和分析是目前药物临床前安全性评价研究的趋势，由此产生的计算机化系统安全性问题成为GLP机构以及行政管理监督部门关注的重点。作者从计算机化系统安全性的概念及范围、安全要素以及安全事件的管理等方面进行了简要阐述，以期为我国药物临床前安全性评价GLP机构中计算机化系统的广泛应用提供支持和帮助，从而促进我国药物研发以及安全性评价策略与国际接轨。

关键词： 临床前安全性评价；计算机化系统；药物安全；药物临床前评价
中图分类号： R951 **文献标志码：** A **文章编号：** 1674-6376（2020）01-0153-04
DOI： 10.7501/j.issn.1674-6376.2020.01.029

Brief introduction of security of computerized system in GLP facilities

ZHANG Di, LI Qianqian, HUO Guitao, QU Zhe, YANG Yanwei, LI Chen, ZHANG Xi, LV Jianjun, LIN Zhi
National Center for Safety Evaluation of drugs, National Institutes for Food and Drug Control, Beijing 100176, China

Abstract: The use of computerized system for data acquisition and analysis is currently the trend of preclinical safety evaluation of drugs, so the security of computerized system has become the focus of GLP institutes and administrative supervision department. The author of the paper briefly introduces the concept, scope, security elements of computerized system and management of security incidents so as to provide supports and help for the wide application of computerized system in GLP institutes for preclinical safety evaluation of drugs in China, and thus promoting the research and development and safety evaluation strategy of drugs in line with international standards.

Key words: preclinical safety evaluation; computerized system; security of drug; preclinical evaluation of drug

随着药物研发的快速发展，药物临床前安全性评价中采用计算机化系统采集、处理以及分析实验数据越来越普及，由此产生的计算机化系统安全性问题也就受到各个药物非临床研究质量管理规范（good laboratory practice，GLP）机构以及行政管理监督部门的关注[1]。目前，计算机化系统安全的重要性已经被大大提升，安全是在GLP中必不可少的基本要求[2-3]，涉及到整个计算机化系统如何设计、构建、安装，检测及使用。同时也必须和其他所需的系统或业务的安全需求相兼容。

1977年美国食品药品监督管理局（US food and drug administration，FDA）制定了《联邦法规21（CFR）》的第11部分提出了电子记录存储、安全、系统检查、审计跟踪和变更控制的具体要求[2,4-5]。其中在计算机安全性部分中指出，所有计算机化系统都应该有安全控制，授权用户应该在研究记录中明确标识出来。监管机构要求具有物理安全和逻辑安全，例如使用者有唯一的用户名及密码。此外，还必须具有恰当的程序来记录对密码的定期检查以及修改情况，并且对于不再访问系统的用户删

收稿日期： 2019-09-21
基金项目： 十三五重大新药创制专项（2018ZX09201-017）
#第一作者： 张 頔，女，学士，主管技师，研究方向为毒性病理学技术。Tel：（010）67872233 E-mail：skystar.night@163.com
李芊芊，女，博士，副研究员。研究方向为毒理学。Tel：（010）67872233 E-mail：liqianqian@nifdc.org.cn
***通信作者：** 林 志，博士，研究方向为药物临床前安全性评价。Tel：（010）67872233 E-mail：linzhi@nifdc.org.cn
吕建军，博士，研究方向为药物临床前安全性评价。Tel：（010）67872233 E-mail：lujianjun@nifdc.org.cn

除密码。安全程序则必须包括防止未经授权使用密码、系统诊断、操作检查、权限检查以及设备检查。总之，计算机化系统的安全性涉及多个方面。本文从GLP条件下计算机化系统安全性的概念及范围、安全要素以及安全事件的管理等进行简要论述，以期为我国药物临床前安全性评价GLP机构中计算机化系统的广泛应用提供支持和帮助。

1 安全性的概念及范围

安全的目的是将危险降到一个可接受的水平，安全管理的要素包括3个方面[3,6]：(1)保密性(confidentiality)，即确保信息只能由有权限的人员访问；(2)完整性(intergrity)，即确保信息以及处理方法的准确性和完整性；(3)可用性(avaliability)，即确保需要时，有权限的用户能够访问信息及相应的设备。每个GLP机构都应该根据其需求进行风险评估并且建立相应的安全程序，包括身份识别以及内部和外部风险的管理控制。所谓的风险是指内部员工通过已感染媒介引入病毒，或者外部黑客、社会工程病毒、蠕虫病毒、木马病毒等对系统的攻击[7]。此外，电力中断、删除文档、过度权限、“只读文件”可被修改等也属于技术意外的风险。上述的安全概念应该应用于计算机化系统的所有方面。

安全范围也就是安全区域应该涉及不与网络连接的孤立系统的单机、局域网、内部连接的局域网、公共网络以及因特网的区域网络[3]。安全区域不一定非要连续的，也不是所有方面都需要，一台单机电脑可以与因特网直接相连而不一定必需通过中间区域的连接。同时不一定是连续的，安全考虑是相互关联的，当跨越多个安全区域时，安全考虑事项将增多。安全控制的决定性要素依赖于多种因素。这些因素比如与其他系统的连接级别、用户的数量、互联网与非互联网的比例等都会决定安全管理的漏洞，因此必需对这些漏洞进行修复。尽管与计算机化系统相关的链接和技术很多，但是监管对于技术类型不会有特定的要求。因此，无论是何种类型的链接或技术考虑都应该应用相同的安全原则。

2 计算机化系统的安全要素

2.1 一般要求

一些安全要素是在所有区域及系统模型中普遍存在的，需要不同层级的规定和程序。因此，需要考虑以下共同要素，包括业务影响、记录管理、检查准备、与业务流的关系、保密性、长期可用性、通用格式、默认拒绝，以及培训所有用户及支持人员，让其认识到安全的重要性。除此之外，如果服务是外包的，则需解决支持来源。

2.2 一般基础设施的考虑

基础设施包括网络硬件组件和操作系统，关于基础设施的安全考虑包括以下几方面[6]：(1)随时打补丁确保操作软件为最新版本；(2)处理并保持这些补丁为最新版；(3)关闭以保证仅启动必要的服务；(4)使用杀毒程序防止病毒或其他恶意软件的侵入；(5)账户管理；(6)密码管理；(7)漏洞通知。

2.3 应用程序的安全性考虑要点

每家公司都应该确定其风险承受能力以及应用程序的安全需求。在使用之前，需要进行应用程序的安全风险评估。在评估过程中需要考虑的项目包括[2,8]：(1)哪些应用程序步骤需要记录和登记；(2)是否执行安全编码；(3)应用程序之间或者应用程序与服务之间的相互作用，比如DNS、目录服务、数据库等；(4)应用程序的安装对基础设备或其他应用程序的影响；(5)需要哪种支持过程；(6)在风险评估中需要考虑哪个区域及用户使用环境。安全风险评估可促使定义应用程序的安全性需求，这些需求应包括在系统功能需求中，并通过适当的检测验证其功能。

2.4 附加网路的考虑要点

对于联网系统必须界定好业务需求和流程，在制定需求时要考虑控制和允许通过此控制的个人或团体，允许连接的协议、服务以及节点，时间限制需求，组织机构网络基础设施的哪个等级可以进行连接，以及进行连接的业务需求和通讯的技术规则[3]。联网系统的危险是多来源及多级别的，安全方法要多维考虑。当多个保护机制相互协调应用时则称为“深层防护”，包括杀毒软件、反间谍软件、防火墙、代理服务器、传输和存储的加密、程序账户禁用、职能、入侵防御系统(intrusion prevention system，IPS)、入侵检测系统(intrusion detection system，IDS)、访问控制列表(access control lists，ACLs)、系统超时、屏幕保护、个人用户账号、流量控制、传送及代码认证、物理权限。

机构控制内的网络会增加对于系统操作的危险。网络会形成意想不到的或有时不可预测的通路，如果没有很好的控制，会导致网络可用性的降低或网络拥堵[6,8]。使用公共因特网络将会增加安全风险。因特网本质上不可控的，任何情况都可能发生。整个机构应该定义、记录及沟通对因特网使

用的商业安全需求。除了上面所列的维护要素，对于操作系统和网络浏览器的配置设定可能需要特殊考虑。

3 安全事件的管理

安全事件有很多类型，通常认为属于违反典型的安全政策的行为包括以下几种[6]。第一，无论成功与否的试图进入未授权系统或者数据；第二，意外的中断或拒绝服务；第三，未授权使用系统对数据进行传输、处理或存储；第四，未得到所有者的授权、介绍和同意的情况下，对系统硬件、防火墙或软件进行更改。

当系统或设施出现非计划的不可用即发生安全危害时，GLP机构应该有3个层面的组织来保持GLP数据和计算机化系统的验证状态，即机构层面的高级管理职责[具有机构的业务连续计划（business continuity plan，BCP）]、区域层面[具有信息技术（information technology，IT）、实验室和动物房的灾难恢复计划（disaster recovery plan，DRP）]、系统层面[9]。BCP的制定可以作为一个整体在重大灾难期间确定机构如何运行以保持业务的完整性[10-11]。BCP给予了机构层面的方向和不同功能的优先性顺序以保持机构正常运行。为了达到BCP的目标，机构也需要有自己的DRP，写明在极端情况期间其基本功能如何继续运行。不同部门和不同实验室类型会有各自相应的DRP来符合他们公司业务BCP中“保持运行”的目的。从极端条件下恢复既需要从机构整体层面（如BCP）也需要从局部运行层面（如DRP）来计划其策略。BCP应得到区域层面的灾难恢复计划的支持[11]。在每一个区域内，每一个独立系统都应该有各自的灾难恢复（disaster recovery，DR）标准操作规程（standard operating procedure，SOP），用来描述如何完成恢复以及GLP数据的处理方法。当计算机化系统突然无法使用时，需要遵循DR标准化操作规程。通常机构应急小组等实体担任机构和组织之间的联络人，应急响应部门可以使用事故指挥模式，允许机构部门和领导层之间进行沟通[10]。视情况而定，接下来可以是进行事故报告或者相应的变更控制程序。DRP和BCP然后进行更新，反映从该事件汲取的新系统经验。

信息技术的DRP指的是数据中心和支持实验室基础设施的DR。实验室DRP是指针对特定灾难条件恢复实验室设备及服务的局部区域计划。当在GLP的法规和指导下运行的设施不是唯一需要业务连续性计划时，则必须在发生灾难期间增加附加文档方面的关注，并与专题负责人和质量保证（quality assurance，QA）人员加强沟通以保证研究数据的完整性[6,11]。动物房DRP需写明在相关动物房内饲养动物的安全性，包括环境和给药系统，以及如何减缓灾难事件对于正在进行的动物研究带来的影响[13]。无论是美国还是其他国家中只要具有动物福利保证的机构都会制定并维护现行的应急响应计划[13-14]。总之，DRPs是用来实施BCP的局部区域性文件。当灾难发生时执行恢复程序，BCP提供了临时使用手工方法操作的程序。DRP提供了通知过程来宣布灾难开始，之后宣布灾难结束。DR的SOP会描述如何操作恢复系统、设施和数据。BCP也应该提供从灾难到恢复期间合适的数据库所采取的临时记录采集方法。同时应该测试此类数据的完整性。

因此，在危机中确保动物的人道待遇、人员安全、数据安全，并且应尽快回复正常，这是非常紧迫并重要的[15]。危机中BCP计划不仅有助于保护组织机构免受灾难的影响，还为动物护理人员和其他关键部门应对任何灾难做好准备[10]。

4 结语

GLP机构数据的安全性是临床前药物安全性评价研究至关重要的方面。它既包括了物理安全（进入设施区域使用密码或其他身份信）也包括逻辑安全，还有数据完整性及备份安全[16]。安全性是GLP的一个重要方面，它要求对GLP机构所有人员都进行连续的监控。工作人员还应根据本研究机构制定的业务连续性计划以及灾难恢复计划等积极准确地应对突发的安全事件，以确保计算机化系统所产生实验数据的完整性。

总之，临床前药物安全性评价的计算机化系统化是信息化社会发展的必然趋势，良好的系统可促使药物研发过程更符合GLP机构的管理规范，以确保实验数据的准确性和可靠性，同时也通过工作流程的优化降低运行成本并提高工作效率[17]。所以，采用计算机化系统的GLP机构应该在管理政策制定、各项操作方法执行的标准、执行任务的方法及建议、计算机相关SOP制定等方面均遵从参考有关标准的最低安全要求[18]。只有时刻关注并认识计算机化系统安全的重要性，密切关注国际发展水平，才能促使我国临床前药物安全性评价中计算机化系统的广泛应用，从而加快药物研发以及药物安全性评价策略与国际接轨。

参考文献

[1] 张 曦, 沈连忠, 李保文, 等. GLP实验室计算机化系统的安全讨论 [J]. 中国药事, 2011(7) :670-673.

[2] Brodish D L. Computer validation in toxicology: historical review for FDA and EPA good laboratory practice [J]. Qual Assur, 1998, 6(4): 185-199.

[3] Ulma W, Schlabach D M. Technical Considerations in Remote LIMS Access via the World Wide Web [J]. J Autom Methods Manag Chem, 2005, 2005(4): 217-222.

[4] Donawa M E. FDA draft guidance on computerised systems used in clinical trials [J]. Med Device Technol, 2005, 16(1): 24-27.

[5] Bansal A, Chamberlain R, Karr S, et al. A 21 CFR Part 11 compliant graphically based electronic system for clinical research documentation [J]. J Med Syst, 2012, 36(3): 1661-1672.

[6] Hulihan E, McComack J, Newman M. *Computerized systems used in nonclinical safety assessment* [M]. Horsham, P A: Drug Information Association. 2008.

[7] 黄星儒. 分析计算机网络信息安全的影响因素及常用的防护策略 [J]. 通讯世界, 2017, 13: 46-47.

[8] 柯争先, 贾晓艳, 徐禾丰. 基于风险的计算机化系统合规管理—新修订«计算机化系统»附录解析 [J]. 中国医药报, 2015-01-03(4).

[9] Donaho. Building the human component into contingency plans [J]. Lab Anim (NY) J, 2014, 43 (1): 27-32.

[10] Dupepe L M, Donaho J C, Roble G. *Emergency Response and Management. Management of Animal Care and Use Programs in Research, Education, and Testing* [M]. 2nd edition. Boca Raton (FL): CRC Press/Taylor & Francis. 2018. Chapter 17.

[11] Ikeda T. Crisis management and recovery from the damage to the laboratory animal production facility due to the Great East Japan Earthquake [J]. Exp Anim, 2012, 61 (1): 1-11.

[12] Mortell N, Nicholls S. Practical considerations for disaster preparedness and continuity management in research facilities [J]. Lab Anim (NY), 2013, 42(10): F18-F24.

[13] National Research Council. *Guide for the Care and Use of Laboratory Animals* [M]. 8th edition. Washington DC: National Academies Press (US). 2011.

[14] Jensen J, Thompson S. The incident command system: A literature review [J]. Disasters, 2016, 40(1): 158-182.

[15] Ikeda T. Crisis management and recovery from the damage to the laboratory animal production facility due to the Great East Japan Earthquake [J]. Exp Anim, 2012, 61 (1): 1-11.

[16] Keatley K L. A review of US EPA and FDA requirements for electronic records, electronic signatures, and electronic submissions [J]. Qual Assur, 1999, 7(2): 77-89.

[17] Walter H, Henricks M D. Laboratory information systems [J]. Surg Pathol, 2015, 8: 101-108.

[18] 霍桂桃, 张 曦, 吕建军, 等. 药物临床前安全性评价机构计算机化系统的验证 [J]. 药物评价研究, 2017, 40 (11): 1525-1530.