

# 有关FDA 21 CFR Part 11验证咨询服务介绍

|      |                                     |
|------|-------------------------------------|
| 产品名称 | 有关FDA 21 CFR Part 11验证咨询服务介绍        |
| 公司名称 | 深圳市实测通技术服务有限公司                      |
| 价格   | .00/件                               |
| 规格参数 | 测试周期:5-7天<br>寄样地址:深圳宝安<br>价格费用:电话详谈 |
| 公司地址 | 深圳市罗湖区翠竹街道翠宁社区太宁路145号二单元705         |
| 联系电话 | 17324413130 17324413130             |

## 产品详情

FDA 21 CFR Part 11验证咨询服务Validation Consulting

Part 11

Part 11 分析和报告（根据系统后者产品）

Assessment and Report (per system or per product)

Part 11 解读及标准操作流程建设-此项需与Part 11分析报告部分结合

Interpretation/SOP- must be done in conjunction with Part 11 assessment

全套验证服务：验证计划、用户需求说明、功能需求说明、设计说明、安装验证、操作验证、性能验证、用户接受性测试、验证报告

Full Validation Package (draft): Validation plan, URS, FRS, DS, IQ, OQ, PQ, UAT, Summary

文档创制用时估计:

验证计划Validation Plan: 10 hours

用户需求说明Requirements (URS and FRS) 20 hours

测试脚本Protocols and Testing : IQ , OQ, PQ and UAT

标准操作流程SOP Creation:

IT安全和用户控制 IT Security and Access Control

用户权限设置Change Control Process

质量源于设计 Quality by Design

系统开发生命周期System Development LifeCycle

系统备份和恢复Backup and Recovery

灾难恢复Disaster Recovery

内部审计Internal Auditing

监管审计Regulatory Audits

质量体系政策Quality System Policy

培训政策Training Policy

风险分析Risk Assessment

系统设计原则System Design Policy

系统设计步骤System Testing Procedures

什么是 FDA 21 CFR Part 11 ?

美国FDA于1997年颁布21 CFR Part 11，并于2003年颁布相关行业指南来细化有关规则。在Part11规定中，电子记录被认为具有与书面记录和手写签名同等的效力。21 CFR Part 11被美国的生物医药企业、医院、研究所和实验室广泛接受和遵照执行。自颁布以来已被推广至全球，虽然没有强制性，但被欧洲、亚洲等地图和国家普遍接受和使用。美国作为全球生物医药产业\*主要组成部分影响力巨大，当你的药物、生物医药相关设备或者信息系统需要销售给美国的制药企业和研究人员都应该符合21 CFR Part 11的规定。如违反，FDA能够根据规定剥夺出口到美国的权利。

其他国家对电子记录和电子签名也有类似要求，会以21 CFR Part 11的相关规定为指导原则，来制定本国的相关法规。我国目前暂无像21 CFR Part 11这样在生物医药领域针对电子记录和电子签名的规范或标准。我国在2005年开始实施了《中华人民共和国电子签名法》，但这主要针对容易引起法律纠纷如合同、协议等的电子签名有效性的规定。根据小编了解，部分企业加入供应商也有对21 CFR Part 11的要求。

当前在GCP领域对中国来说，困扰的问题不仅在于你选择应用的信息系统是否适用于21CFR规定及是否验证，还在于如何建立一套较完善的实施GCP电子记录管理体系和电子签名有效性管理规范何时落地。

一、21 CFRPart 11涉及领域广泛(共有1499个部分)

21CFR=Food and Drugs 21CFR58=GLP

21CFR210=GMP, Drugs (General)

21CFR211=GMP, Drugs (Finished Pharmaceuticals) 21CFR312=Inv. New drug Application (GCP)  
21CFR314=FDA Approval of new drug (GCP) 21CFR6xx=GMP, biologics 21CFR820=GMP, Devices

21CFR?= Food, nutrients and cosmetics

21CFR11=Electronic Records; Electronic Signatures

其中在GCP领域主要包括中心实验室建设、数据获取和报告、远程数据录入、CRF体系、临床数据管理、AE报告、临床支持体系和统计分析体系。

## 二、21 CFR Part 11的主要内容

美国21 CFR Part 11的法律读本一共38页，除去1页封面，其中只有2页半是法规本身，其余34页半都是FDA从企业反馈中整理出来的绪论。这里主要是法规本身正文内容。从21 CFR Part 11的目录看整个法规分为3章，分别是：

TITLE 21--FOOD AND DRUGS  
CHAPTER I--FOOD AND DRUG ADMINISTRATION  
DEPARTMENT OF HEALTH AND HUMAN SERVICES

SUBCHAPTER A - GENERAL

PART 11 ELECTRONIC RECORDS; ELECTRONIC SIGNATURES

Subpart A - General Provisions § 11.1 - Scope.

- (a) The regulations in this part set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.
- (b) This part applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations. This part also applies to electronic records submitted to the agency under requirements of the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in agency regulations. However, this part does not apply to paper records that are, or have been, transmitted by electronic means.
- (c) Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required by agency regulations, unless specifically excepted by regulation(s) effective on or after August 20, 1997.
- (d) Electronic records that meet the requirements of this part may be used in lieu of paper records, in accordance with § 11.2, unless paper records are specifically required.
- (e) Computer systems (including hardware and software), controls, and attendant documentation maintained under this part shall be readily available for, and subject to, FDA inspection.
- (f) This part does not apply to records required to be established or maintained by §§ 1.326 through 1.368 of this chapter. Records that satisfy the requirements of part 1, subpart J of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.

(g) This part does not apply to electronic signatures obtained under § 101.11(d) of this chapter.

(h) This part does not apply to electronic signatures obtained under § 101.8(d) of this chapter.

(i) This part does not apply to records required to be established or maintained by part 117 of this chapter. Records that satisfy the requirements of part 117 of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.

(j) This part does not apply to records required to be established or maintained by part 507 of this chapter. Records that satisfy the requirements of part 507 of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.

(k) This part does not apply to records required to be established or maintained by part 112 of this chapter. Records that satisfy the requirements of part 112 of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.

(l) This part does not apply to records required to be established or maintained by subpart L of part 1 of this chapter. Records that satisfy the requirements of subpart L of part 1 of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.

(m) This part does not apply to records required to be established or maintained by subpart M of part 1 of this chapter. Records that satisfy the requirements of subpart M of part 1 of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.

(n) This part does not apply to records required to be established or maintained by subpart O of part 1 of this chapter. Records that satisfy the requirements of subpart O of part 1 of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.

(o) This part does not apply to records required to be established or maintained by part 121 of this chapter. Records that satisfy the requirements of part 121 of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.

(p) This part does not apply to records required to be established or maintained by subpart R of part 1 of this chapter. Records that satisfy the requirements of subpart R of part 1 of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.

[62 FR 13464, Mar. 20, 1997, as amended at 69 FR 71655, Dec. 9, 2004; 79 FR 71253, 71291, Dec. 1, 2014; 80 FR 71253, June 19, 2015; 80 FR 56144, 56336, Sept. 17, 2015; 80 FR 74352, 74547, 74667, Nov. 27, 2015; 81 FR 20170, Apr. 6, 2016; 81 FR 34218, May 27, 2016; 86 FR 68830, Dec. 3, 2021]

## § 11.2 - Implementation.

(a) For records required to be maintained but not submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that the requirements of this part are met.

(b) For records submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that:

(1) The requirements of this part are met; and

(2) The document or parts of a document to be submitted have been identified in public docket No. 92S-0251 as being the type of submission the agency accepts in electronic form. This docket will identify specifically what types of documents or parts of documents are acceptable for submission in electronic form without paper records and the agency receiving unit(s) (e.g., specific center, office, division, branch) to which such submissions may be made. Documents to agency receiving unit(s) not specified in the public docket will not be considered as official if they are submitted in electronic form; paper forms of such documents will be considered as official and must accompany any electronic records. Persons are expected to consult with the intended agency receiving unit for details on how (e.g., method of transmission, media, file formats, and technical protocols) and whether to proceed with the electronic submission.

### § 11.3 - Definitions.

a) The definitions and interpretations of terms contained in section 201 of the act apply to those terms when used in this part.

(b) The following definitions of terms also apply to this part:

(1) Act means the Federal Food, Drug, and Cosmetic Act (secs. 201-903 (21 U.S.C. 321-393)).

(2) Agency means the Food and Drug Administration.

(3) Biometrics means a method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable.

(4) Closed system means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.

(5) Digital signature means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.

(6) Electronic record means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.

(7) Electronic signature means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.

(8) Handwritten signature means the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.

(9) Open system means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.

### A 章节—一般规定

11.1适用范围 (21 CFR Part 11的适用范围, 什么情况下的电子记录和电子签名是适用于21CFR Part 11的)

11.2执行（在什么情况下可以去应用本法规） 11.3定义（一些重要的定义，帮助理解本法规）

Subpart B - Electronic Records § 11.10 - Controls for closed systems.

Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:

- (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.
- (b) The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.
- (c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.
- (d) Limiting system access to authorized individuals.
- (e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.
- (f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.
- (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.
- (h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.
- (i) Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.
- (j) The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.
- (k) Use of appropriate controls over systems documentation including:
  - (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.
  - (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.

§ 11.30 - Controls for open systems.

Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and

controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in § 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.

#### § 11.50 - Signature manifestations.

a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:

- (1) The printed name of the signer;
- (2) The date and time when the signature was executed; and
- (3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.

(b) The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).

#### § 11.70 - Signature/record linking.

Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.

### B章节—电子记录

11.10封闭系统的控制（只有相关权限的人才能进入并读取电子记录内容的系统）

11.30开放系统的控制

（进入时不受控制的系统，比封闭系统多了进入后安全性的要求） 11.50签名的显示  
（电子签名应显示的内容）

11.70签名/记录连接（电子签名与电子记录的连接）

#### Subpart C - Electronic Signatures § 11.100 - General requirements.

(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.

(b) Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.

(c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.

(1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office

of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857.

(2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.

§ 11.200 - Electronic signature components and controls.

a) Electronic signatures that are not based upon biometrics shall:

(1) Employ at least two distinct identification components such as an identification code and password.

(i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.

(ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.

(2) Be used only by their genuine owners; and

(3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.

(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.

§ 11.300 - Controls for identification codes/passwords.

Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:

(a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.

(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).

(c) Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.

(d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.

(e) Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.

C章节—电子签名

11.100—般要求（电子签名的基本要求，如唯一性和排他性）



- 11.200电子签名的构成及控制（电子签名的成分和应用）
- 11.300识别代码和密码的控制（电子签名的识别和密码管理）

### 三、21 CFR Part 11对系统的安全要求

#### 1.安防措施

##### 21CFR Part

11对系统的安全要求主要是防止未经授权的人进入系统接触电子记录，更改和删除电子记录和电子签名。

因此要求有系统安全进入的机制，包括物理手段和逻辑手段，传统的物理手段是制定程序阻止未经授权人员出入，但在实际情况中很难做到，现在较多的则是采取逻辑手段，即计算机系统控制的方式，包括用户ID、授权、用户配置文件的角色，密码策略、密码的安全性，合法用户的权限，共享桌面、远程登录等等，在后面详细讲述。

另外一点重要的系统评价，应定期评估和验证系统是否符合21CFR Part 11的要求。

#### 2.“许可”机制

“许可”机制确保用户能修改自己的纪录，但只能读（不能修改）其他用户的记录，通过管理个人文件和目录来实现。

“许可”机制可以通过用户配置文件来实现，在共享数据的同时，为数据提供保密性和完整性。

每个用户根据分配给其不同的权限被设定成一个特定的用户角色（如管理员、主管、技术员、操作员等），也就说定义角色时含分配权限。

#### 3.可信赖记录

可信赖记录的先决条件，除了数据安全性外，就是可追溯性。“没有写下来的东西就是谣言”在FDA检查过程中，审计员将查阅实验室日志来检查分析过程。日志的内容将不能够用普通的方法被修改或删除。要注意到包含了很多条日志信息的审核跟踪将变得难以管理，如前面提到的要定义好那些要记录，不能使日志数据冗余。

审核跟踪是确保所有的数据都具有清晰完整的记录，而不是对人员进行控制或衡量工作效率。帮助记录人和复合人理解当时为何要执行特定的操作。

#### 4.设备控制和数据采集

那些控制实验仪器但不获得数据的计算机是否需要符合21CFR Part 11的要求？共有四个级别。

级别1：使用一起本身的控制面板和键盘来进行手工参数设定，通过数模转化起记录信号，设定参数难以打印，必须手工记录。

级别2：通过逆向工程来实施仪器控制，通过分析其他供货商的\*终产品来摸索出所使用通讯协议的设计方法。如果特定的供货商没有正式公开控制代码，想要得到厂家的正式技术支持非常困难，另外对于这样的系统还要进行操作认证和其他相关验证。一起固件的升级也可能导致与数据系统的通讯失灵。无错误处理能力和日志。

级别3：创建完整的原始数据和元数据以及正确的文件变得很容易，这一级别中，错误报告与处理很完善

，很容易确认分析是否在顺利完成，出现技术错误时，很容易进行诊断。一些厂商能够实施另外一种级别的仪器控制，即由数据系统控制仪器，数据系统可以进行仪器详细全面的诊断和一些其它功能。这种控制还可以对一起进行预防性维护和早期维护反馈（EMF），能够进行完善的仪器序列号和固件的修订追踪。这种信息在做固定资产审查时非常有用。同时可以执行21 CFR Part 11所要求的功能检查。

级别4：通过握手协议来进行，一个握手协议需要接收者在收到数据后，要想发送者发确认已表明数据收到。可以防止控制着认为它已经发出指令给设备，但设备实际上没有执行。

更多关于FDA认证资讯，FDA认证如何办理，欢迎您来咨询中拓检测，我们有专业的FDA认证团队竭诚为您服务