

上海生物样本库
最佳实践规范及标准操作流程
文件汇编
（第二版）

2010 年 5 月

样本库最佳实践规范

第3章 信息系统

目 录

3 信息系统.....	2
3.1 样本库信息系统.....	2
3.1.1 定义.....	2
3.1.2 功能.....	2
3.1.3 信息系统建立的要素.....	4
3.2 信息系统的人员配备和管理.....	4
3.2.1 信息部.....	4
3.2.2 人员培训.....	6
3.2.3 信息系统权限管理.....	7
3.2.4 保密制度管理.....	8
3.2.5 管理文件.....	9
3.3 场地和硬件设备.....	10
3.3.1 场地.....	10
3.3.2 硬件设备.....	12
3.4 网络.....	15
3.4.1 网络系统的管理与安全.....	15
3.4.2 人员网络使用管理.....	16
3.4.3 病毒防治.....	17
3.5 软件系统.....	17
3.5.1 设计开发.....	17
3.5.2 功能模块.....	18
3.5.3 使用手册.....	18
3.5.4 软件的保管.....	18
3.5.5 软件的安装使用.....	19
3.6 数据.....	19
3.6.1 数据采集.....	19
3.6.2 数据管理.....	21

3 信息系统

3.1 样本库信息系统

3.1.1 定义

样本库信息系统是由样本库的信息部建立、维护和管理，并受到样本库中心执行委员会监督使用的信息化工作平台。

样本库内部工作人员通过信息系统开展样本库的各项日常工作，能简化工作流程，提高工作效率。

样本库外的人员通过信息系统访问样本及其相关数据，能加强信息交流，提高科学研究的效率。

3.1.2 功能

信息系统在样本库的运行中发挥着多项功能。

3.1.2.1 记录的功能

样本库信息系统最基本的功能是记录与样本库活动相关的所有信息，包括但不限于：

捐赠者的信息，包括个人身份信息、病理诊断信息、治疗信息、知情同意书等；

样本的信息，包括样本的来源、种类、数量、质量、编码、储存位置、处理和转移等；

样本库管理的信息，包括规章制度、质量管理体系文件、操作程序、监控记录和数据报告等；

样本研究的信息，包括样本的使用信息，研究的人员和项目，研究的结果和临床数据等。

信息系统记录保存这些数据信息，应该保证所有数据是完整、有效和准确的，

最重要的是保证所有数据的安全。

3.1.2.2 质量管理的功能

样本库的工作人员通过信息系统记录和管理与样本相关的活动，包括样本的采集、处理、储存、使用、运输和销毁。

信息系统基于样本相关活动过程的记录和管理来实现对过程和质量控制点的监督和控制，并作为相关活动审核和批准的依据。

3.1.2.3 样本库存管理的功能

信息系统给每个样本分配一个独立的身份标识，并建立样本的条形码管理系统。

信息系统给每个储存设备和容器分配独立的编号，在信息系统中反映出样本储存的位置。

信息系统通过样本库活动信息的记录和编码信息的关联来实现对样本的追踪。

信息系统通过实时追踪样本的位置和状态，来实现样本库存的管理。

3.1.2.4 数据管理使用的功能

信息系统在记录和管理使用样本数据时有着独特的优势。

数据的整合。样本库的信息系统记录了样本从采集到使用的所有数据，并不断收集来自捐赠者和使用者的数据。使得样本库能在更广泛的条件下储存和整合这些数据，并进行数据的审核和统计分析。

数据的互通。样本库的信息系统为使用样本的研究人员和机构提供了一个良好的获取数据和交流信息的平台，提高样本使用和研究的效率，同时还能实现不同数据库间的数据共享。

数据的合理合法。样本库法律和伦理上的职能保证了信息系统储存的数据是符合法律法规和伦理道德，保证了捐赠者和样本使用者的权利。

3.1.3 信息系统建立的要素

信息系统由样本库的信息部负责建立，建立前应进行计划和各个功能模块的需求分析。

信息系统的建立、管理和使用应设置必要的组织机构、配备适合的人员、设置访问使用权限、建立管理文件和开展人员培训。

信息系统的建立需要一定的场地和硬件设备，应按照要求建设和采购设施设备，并进行必要的维护 and 安全管理。

信息系统应建立必要的数据管理制度，加强网络和数据安全的管理，做好数据备份和恢复工作。

信息系统应开发和更新软件系统，管理好软件的安装使用，并建立软件系统的使用手册。

3.2 信息系统的人员配备和管理

3.2.1 信息部

样本库应设立信息部来建设和管理信息系统。

3.2.1.1 职能

信息部应建立安全、可靠、可用和快速的信息系统，协助样本库实现信息化管理。

信息部应建立专业的信息技术服务团队，有效整合样本库资源，实现信息部的职能。

信息部应布置专门的场地和采购、安装及维护信息系统的硬件设备。

信息部应开发整合多个功能模块的信息系统软件，利用软件系统来全面管理样本库的运行。

信息部应建立必要的信息系统管理和使用文件，培训样本库内外的人员使用信息系统。

信息部应协助数据的采集和管理，做好数据备份和恢复，保证数据的安全。

信息部应随着样本库的发展，不断更新和加强样本库信息系统的软硬件配

备，建立强大的信息技术服务团队，确保信息系统在样本库发挥应有的作用。

3.2.1.2 人员配备

信息部在主管下面设立硬件工程师、软件工程师和数据管理员，来执行不同的职能。

3.2.1.2.1 主管

负责建立信息部的技术人员团队，实现信息部的功能和样本库信息系统的运行。

负责管理信息部所有人员和软硬件设备，充分发挥他们的作用，提高工作效率。

负责配合人事部组织人员培训，并对人员的工作内容进行考核。

负责制定信息系统建立的计划，组织进行建立的可行性分析和必要的需求分析，监督和指导信息系统的建立。

负责确保样本库信息系统核心数据和设施设备的安全。

3.2.1.2.2 硬件工程师

负责构建、管理、规划和维护样本库信息系统的硬件设施和设备，确保信息系统稳定运行。

负责采购信息系统所需要的硬件设施设备，并按照规定规范管理和使用，不得擅自变更设施设备的用途，杜绝非正常使用和浪费。

负责建立设备清单，指定设备的负责人，核准设备使用的目的、部门和人员，并进行使用的培训和监督管理。

负责信息系统硬件设施设备的维护、校准和故障维修，确保设备的正常运行。

负责信息系统硬件设施设备的安全，建立必要的防护措施和设置访问使用权限。

3.2.1.2.3 软件工程师

负责根据计划开发样本库信息系统的软件系统,按照样本库和用户的需求不断维护和更新升级软件系统。

负责培训和监督管理样本库内所有计算机上软件的安装使用,确保软件的安装使用符合版权和样本库规定的要求。

负责按照样本库的人员工作职能的划分,设置人员访问使用信息系统软件的权限,建立防火墙等措施,保证软件系统的安全。

3.2.1.2.4 数据管理员

负责数据的采集,确保采集的数据合理合法和符合样本库的要求,确保数据的通用性和有效性。

负责检查和审核所有数据,及时修正错误和缺失的数据。

负责监控数据的访问、使用和共享,根据数据重要程度对所有接触数据的人员设置访问使用权限。

负责确保数据的安全,严格保存保密数据,建立数据的备份和恢复机制。

3.2.2 人员培训

由于信息系统使用的特殊性,信息部不仅要对本部门内的技术人员进行必要的培训,还应对所有使用信息系统的样本库员工和外部的人员进行信息系统合理、安全和有效使用的培训。

3.2.2.1 信息部人员培训

与1.3.5中提到的人员培训一样,信息部应对部门内部的信息技术人员进行入职培训、岗位技能的培训和特殊技能的培训,使其成为胜任信息部特定岗位工作的人员。

3.2.2.2 样本库人员培训

样本库大多数人员都会使用到信息系统来进行工作,应确保所有相关人员都

接受来自信息部的培训，包括来自硬件、软件和数据等方面的培训。

由于信息系统是在计算机上运行，对于缺乏基本计算机技能的人员应首先进行计算机使用的培训。

根据人员使用信息系统的权限设置和需要进行不同模块的培训，人员岗位或者使用需要发生改变时应接受新的培训。

信息系统发生变更或者升级更新时，人员应接受新的培训。

在不影响信息系统正常运行的情况下允许人员对信息系统进行测试使用。

3.2.2.3 外部人员培训

样本库外部人员主要使用信息系统的软件系统部分，通过软件系统的使用手册和远程教学来实现培训。

发生软件系统变更或升级时，应提供外部人员培训和测试使用。

培训应使外部人员知晓其访问信息系统的目的和权限，了解必要的保密原则。

3.2.3 信息系统权限管理

3.2.3.1 权限设置

样本库的信息系统被样本库的工作人员和外部的的人员共同使用，所有人根据他们不同的需求使用信息系统的不同功能模块和访问不同的数据。

样本库在管理信息系统时应根据人员和使用需求的差异，数据和系统功能的重要程度和安全级别的不同，设置不同的软硬件访问权限。

信息系统权限管理的方式主要通过设置账户和密码来访问使用软硬件，建立账户和人员资料的列表，设置帐号的权限和有效期限，系统的管理所有使用信息系统的人员。

当使用人员的身份、个人信息和使用需求发生变化时，应该重新分配信息系统的使用权限，或者在特定情况下关闭用户的账号。

信息系统应全面进行权限管理，每个功能模块的权限分为不同的级别和范围，需要设置访问使用权限，包括但不限于：

计算机机房的访问使用权限；
计算机服务器的访问使用权限；
个人计算机的访问使用权限；
网络系统的访问使用权限；
附属设备的访问使用权限；
信息系统软件功能模块的访问使用权限；
样本数据的访问使用权限；
样本捐赠者个人资料的访问使用权限；
临床数据和样本研究结果数据的访问使用权限。

3.2.3.2 账户安全

应加强账户的管理，分配好权限，并在使用者身份发生变化时修改相应的权限。

所有通过特定权限账户访问使用信息系统的人员必须保护好自己的账户。

账户和密码在任何情况下不得透露给第三方人员或机构。

跟随账户一起提供的初始密码应在第一次使用后立刻更换。

不使用任何保存账户和密码的自动登陆程序。

使用人员拥有多个账户不能使用相同的密码，不与任何人共享账户和密码。

不得通过电话、电子邮件或其他电子通讯方式泄漏账户和密码。

账户和密码在发生任何泄漏或者怀疑泄漏的情况下应立刻冻结账户并停止使用，更换账户名和密码。

应设置一定期限规定账号密码不得重复使用，并强制账号密码的变更。

应建立具有安全性的密码，密码长度最少要有8个字符，包含大写和小写字母、数字及特殊字符中任意三种的组合，密码不能包含账号或全名。

密码不应由可以明显获取或与所有者相关联的数字或字母组成。

3.2.4 保密制度管理

为了维护样本库、样本捐赠者和使用者的利益，制订信息系统的保密制度，样本库全体人员和使用信息系统的外部人员必须严格遵守。

严守秘密，不得以任何方式向样本库内外无关人员散布、泄漏样本库信息系统的机密和涉及样本及捐赠者的机密。

3.2.4.1 保密的内容

保密制度涉及样本库信息系统的方方面面，内容包括：

信息系统软硬件相关信息，涉及访问的账户和密码应保密；

信息系统数据库信息，样本及其活动相关的重要数据信息应保密；

信息系统所涉及的样本库职能框架信息和相关的质量管理体系文件应保密；

信息系统保存的所有捐赠者和样本使用者的个人信息应严格保密。

3.2.4.2 保密的基本准则

不得以泄露、告知、公布、发布、出版、传授、转让或者其它任何方式使任何第三方知悉属于样本库或者他人的保密信息。

所有数据信息间关联应该用没有特殊意义的数字编码进行，不应泄漏任何个人信息。

样本库人员应该遵守样本库信息系统的保密制度，在入职时应签订的员工保密协议，在1.3.4中已经提到。

严格遵守保密制度，不准携带机密文件和信息到与样本库活动无关的场所，不应在公共场所谈论保密信息和交接保密文件。

保密文本和信息资料不准私自复制、摘录和外传，也不得在公开发表的文章中引用。

人员调职、离职时，必须将自己经管的保密信息资料等交至上级主管，不可随意移交给其它人员，并在相关协议的保密期限内继续遵守保密制度的规定。

发现失密和泄密现象，应及时报告，认真处理。对失密泄密者，视情节轻重，给予一定行政处分。造成样本库或个人严重损失的，应予以赔偿。

3.2.5 管理文件

信息系统的管理是作为整个样本库质量管理体系的一部分，也应符合要求建立相应的管理文件。

依托于文件体系对样本库的信息系统进行管理，建立相应的管理规范，提供必要的技术支持和解决方案，并保证信息系统和数据的安全。

应建立必要的信息保密制度，确保所有使用信息系统的人员知晓和遵守。

应建立必要的硬件设备使用管理程序，提供给信息部和样本库相关工作人员学习和使用，规范人员的行动。

应建立信息系统软件的使用手册，提供给所有使用软件系统的人员。

应根据信息系统要求建立一些标准操作规程，包括数据采集、数据访问和数据备份等，规范信息系统的使用和管理。

3.3 场地和硬件设备

3.3.1 场地

3.1.1.1 环境条件

由于信息系统的设备包括计算机服务器在内都是精密设备，对于环境条件的要求相对严格，为确保设备正常使用年限及延长设备寿命，保证设备的正常运行，应给设备存放场所特别是机房创造良好的环境条件。

信息系统的设备会产生高温，容易损伤设备，其所处环境温度不宜超过25℃，应有空调设备保证工作温度。

长期过湿的环境会造成设备的电子零件接点生锈产生接触不良或漏电的现象，应控制环境的湿度。

良好的通风环境可以降低设备所处环境的温度和湿度。

灰尘覆盖在电子零件上会造成不易散热和增温现象，缩短设备的使用寿命。设备所处环境应避免灰尘过多，定期检查散热风口是否有大量灰尘堆积，并由专业人员将设备内外覆盖的灰尘去除。

电源及电压是否稳定，也影响到信息系统硬件设备的运行和使用寿命，和样本库其他设备一样也需要稳压设备和备用电源系统。

3.3.1.2 计算机房管理

计算机房是用来放置信息系统重要设备的场所，对环境与安全有着特殊的需

求。

机房内必须配备24小时运作的空调设备，确保环境温度不得超过25℃。

机房内必须配备不间断电源系统，确保15分钟的断电保护，在备用电源系统发挥作用前能不受影响。

机房内应该设置独立的门禁、安全系统，确保只有授权的人员可以出入，并确保有足够的防盗措施。

非授权工作人员不得进入机房，特殊情况需经信息部主管批准，并书面登记后方可进入。

进入机房人员应严格遵守机房管理规范。

进入机房人员不得携带任何易燃、易爆、腐蚀性、强电磁、辐射性、流体物质等对设备正常运行构成威胁的物品。

信息部工作人员应随时监控核心设备运行状况，发现异常情况应立即进行处理，及时上报信息主管并详细记录。

非信息部人员未经许可不得擅自上机操作和对运行设备的配置进行更改。

严格执行密码管理规定，对操作密码定期更改，超级用户密码由各系统管理员掌握，并报上级主管。

信息部人员应严格执行信息保密制度，不得擅自泄露机房各种信息资料与数据。

机房内不得吸烟、饮食、嬉戏等，定期对机房环境进行清洁，保持机房安静、整洁。

定期对机房内设置的消防设备及烟雾报警系统进行检查，以保证其有效性。

进出机房及监控室时，使用门禁系统严格控制进出人员的权限并保留详细记录。

非信息部人员在机房实施任何作业时，信息部人员应全程陪同，以防止任何意外状况发生。

未经机房管理人员允许，不得将机房所属物品带出机房。

3.3.2 硬件设备

3.3.2.1 计算机服务器

样本库信息系统需要配备足够运算和储存能力的计算机服务器，确保以下功能的实现：

服务器应能支持信息系统软件的运行，满足样本库内部和外部对软件系统的访问使用；

服务器应有强大的运行处理能力，满足各功能模块的流程管理和数据管理的功能实现；

服务器应有足够的储存空间，满足样本库所有数据的保存和备份；

服务器应有一定的运算能力，满足数据统计分析等特殊功能。

服务器作为信息系统的主要载体，属于共享设备，需要设定严格的访问权限。

服务器仅允许特定的管理人员或经过授权的人员操作，设有开机密码并不得擅自更改。

服务器的开机和关机应由管理人员根据规定来确定时间，特殊情况不在此限，例如宕机维修、更新系统等等。

服务器命名以安装的软件系统命名，若相同系统有多台服务器，应加上数字命名。

3.3.2.2 个人计算机

个人计算机连接服务器，由样本库工作人员使用，录入和取用信息系统的数据，使用软件系统开展样本库的日常工作和实施管理。

个人计算机包括台式计算机和笔记本计算机，一般以使用部门或者人员的名字作为计算机名。

个人计算机应设置带有一定权限的账户和密码，不得使用他人的账户或者与他人共享自己的账户和密码。

不得在个人计算机上开设任何形式的数据共享，所有共享数据都必须存放在指定服务器上，并提前通知管理人员。

3.3.2.3 计算机使用规范

不得擅自对样本库的计算机设备上更改开机密码（CMOS密码），如有特殊原因，须由信息部主管书面核准，并把所设密码报备硬件工程师。

不得擅自搬动任何计算机设备（包括打印机和扫描仪等），如需变更办公位置，必须提前一天通知信息部，以便安排人员做好必要准备和配合。

不得擅自拆装任何计算机，只有硬件工程师有权拆装电脑硬件设备。

不得擅自更改任何计算机的系统设定值（包括IP地址、计算机名称和群组名称等），只有硬件工程师有权更改。

不得擅自对样本库信息系统的计算机设备中安装任何软件。只有软件工程师或者得到信息部授权的人员有权安装。如确因工作要求，须安装特殊软件的，需要向信息部申请。

不得使用他人的用户名和密码。用户必须使用本人的用户名（一般为本人姓名）和密码来使用计算机，包括登录、上网等。每个人应妥善保管自己的密码，以防泄漏。员工不得将个人帐号密码告知他人，请他人代为操作系统。

3.3.2.4 附属设备

附属设备应包括网络相关的设备，如网络路由器、交换器等，保证样本库信息系统网络的运行。

附属设备应包括样本活动环境监控的设备，主要是传感器来接收冰箱门开关、温度等信息，收集相关的数据，进行记录和报警。

附属设备还应包括输出的设备，如条形码标签打印机等，实现信息系统功能的输出。

附属设备通常都是配合计算机主机使用，激活与关闭与计算机同步，如不是在使用手册上应有特别说明。

附属设备应该有专门的管理人员进行维护，设置不同的使用权限保证设备的正常运行。

不得擅自将外来的附属设备连接到信息系统的计算机或者其他硬件设备和网络上，避免信息安全问题的发生。

不得随意拆卸信息系统的附属设备，特别是与其他设备成套的附属设备，以

免影响正常的维护和维修。

3.3.2.5 硬件使用手册

硬件设备应建立使用操作手册，使用手册包括硬件的使用指南、维护方法和安全管理。

硬件设备在购入时应附有相应的说明书或技术操作手册，样本库也应根据实际需要购买或编写额外的使用说明书。

硬件的使用手册用于人员的培训，帮助充分了解硬件的使用，在解决设备出现的问题时进行指导。

硬件的使用手册应指定专人负责保管，使用时分发到人员手中或者易于获取，记载借出及归还日期和借阅人，如有遗失应立即补购遗失的使用手册。

3.3.2.6 硬件设备安全

所有信息系统的硬件设备应该在干净、整洁的环境中安置和使用，保证安全和避免设备的损坏。

硬件设备特别是计算机设备应装设不间断电系统(UPS)，以防电源不稳造成设备损坏和数据的丢失。

除信息部的专业人员外，任何人都不得自行拆装或者搬动任何信息系统的硬件设备。

服务器、路由器、交换机等重要设备须放置在专门的机房内。

信息部必须安排人员密切监视中心设备运行状况以及各网点运行情况，确保设备安全、高效地运行。

3.3.2.7 硬件设备的维护

信息系统的硬件设备和样本库的其他硬件设备一样，都需要一定的维护。大多设备在购入时都有特定的维护要求，应至少每半年进行一次维护，由专人按照特定的标准操作程序进行。

计算机和服务器的维护需要清除机体内外之尘屑，包括散热风扇部份，附属设备需要清除设备外部及散热风口尘屑。

特殊的设备应该按照维护手册的指导进行保养,或者由厂商派来的专业人员进行维护。

因设备维护造成设备停止使用的,应提前通知信息部和相关管理人员,安排停机维护的时间和配合的人员。

硬件设备维护后原有的工作环境会改变,应重新测试设备运行的稳定性,确认无误后再正式使用。

制定维护的计划,维护的过程和结果应被记录,并归档保存。

3.3.2.8 硬件设备的维修

与样本库其他设备不同,信息系统的设备故障应由信息部的人员来判定,对于判定不了的故障应及时通知厂商。

故障判定后的设备维修由信息部派遣专业人员进行维修,无法修理的由厂商派人修理或者送修,需要厂商修理的情况应该由信息部的人员陪同进行,保障设备中的数据安全和保密。可以的话应先转移出所有保密和敏感的数据。

应配备必要的数据库备份系统和备用设备,当硬件设备维修时保证样本库信息系统的正常运行,不影响样本库日常活动的开展。

3.4 网络

3.4.1 网络系统的管理与安全

信息系统应建立安全、可靠和快速的网络系统。信息系统的使用,数据的采集和管理都是通过网络系统开展的,此外电话、传真、互联网、远程会议和教学、电子邮件、数据库远程管理也都需要通讯网络的支持。

通讯的硬件设备,有线及无线通讯的收发设备、讯号处理的设备、传输的线路、讯号接收及转换的设备,以及信息系统直接运行的设备,都须要保持其正常的运作。

所有网络通讯设备应由专人管理,按照使用说明指示操作,环境和电源系统都应支持通讯设备的正常运作。

不得擅自调整和移动网络相关的路由器、交换器等硬件设备,避免造成任何

网络问题。

不得擅自将外来的设备连接到信息系统的硬件设备和网络上，避免信息安全问题的发生。

所有新的网络和通讯方式的使用必须由信息部审核，未经书面许可任何人都不得变更样本库网络通讯的现状。

信息系统的任何网络通讯均有相应的权限设置和密码访问通行。

信息部应调配使用各类网络资源，使网络系统发挥最佳效率。

发生网络通讯故障时，应迅速通知信息部硬件工程师，及时排除故障。

3.4.2 人员网络使用管理

使用样本库信息系统的网络系统的人员应遵守《计算机信息网络国际联网安全保护管理办法》所规定的要求。

一般使用人员不得擅自调整、移动办公区内的网络交换机、路由器等设备。不能私自更换网络交换器的连接端口，以免造成任何网络问题。

不得私自架设测试服务器或硬件设备连接至正式作业环境的网络中，以免干扰正常网络运行。

未经信息部检测合格，不得擅自将外来人员所携私人电脑连接到样本库的网络，以免造成病毒、木马等感染网络内的个人计算机和服务器。

除信息部外，一般网络使用人员不得利用任何工具软件进行扫描计算机主机、服务器和端口，不得使用任何工具软件窃取主机本地管理员权限。

样本库内不得私自架设有线或无线网络，必须通过信息部的批准。

信息系统所在网络系统主要为样本库活动使用，使用人员不得访问或下载与样本库活动无关的网站及内容。

人员不得随意开启内含宏的档案，同时不得开启来路不明的电子邮件的附件档案。

信息部使用过滤及监控设备或软件，不定期监控并过滤使用人员上网浏览、邮件内容、MSN、BBS发帖、FTP等的信息。不得私自下载MP3或色情图片、影片等不合法或有版权疑虑的软件。

3.4.3 病毒防治

信息系统内部的计算机必须使用标准的防毒系统，确保网络的安全

计算机病毒对信息系统和数据的破坏很大，再好的预防病毒系统也不能保证可以抵御所有新生的计算机病毒，除了使用好的防病毒系统降低感染机会外，还要有正确使用软件的概念，以及良好的计算机使用习惯。

所有计算机主机应安装常驻的防毒软件，以便随时侦测软件或数据文件是否存在病毒，并预防外来病毒的入侵。

计算机接触外来媒介时，应检测确定该媒介并无病毒存在后才能使用。

计算机数据文件通过网络传送时，必须以防毒软件加以检测，以免计算机不慎感染病毒。

应使用正版合法软件或在授权下根据规定合理使用信息系统，能避免感染病毒。

3.5 软件系统

3.5.1 设计开发

样本库信息系统的软件开发应根据功能、运行模式、技术构架等做出框架性的设计，然后进行可行性分析和具体的需求分析。

软件系统的设计在信息部主管的主持下进行，寻求样本库各部门和使用者的意见，设计结果进行评审，通过后进行软件的开发。

软件工程师根据设计的要求进行软件的编写，编写的软件应进行必要的测试。

软件工程师根据测试的结果反馈对软件进一步修改和测试，直到软件通过全部的测试任务。

信息系统软件的编写如决定外包，应签署相应的保密协议，并跟踪协调软件开发的进度。

编写完成的信息系统软件应进行安装验证、功能验证和性能验证。

对软件进行评估，并给出后续版本的建议，做出总结，结束当前版本信息系统软件的开发。

开发完成的信息系统应编写相应的使用手册，指导用户安装、使用和维护信息系统。

3.5.2 功能模块

软件系统由多个模块组成来具体实现样本库样本管理和信息管理的各项功能，包括但不限于：

用户账户管理；

文件查看使用；

样本查看搜索；

储存设备容器管理；

样本类型管理；

条码分配管理；

捐赠者信息管理；

样本采集管理；

数据统计分析和数据共享。

软件系统应该根据样本库的发展，不断进行升级更新，满足使用需求和硬件升级的需求。

3.5.3 使用手册

编写信息系统的用户使用手册，为用户使用信息系统提供必要的技术支持，帮助用户及时解决使用过程中出现的问题。

使用手册不仅是信息系统的使用说明，还为用户提供了问题出现时的解决方法，和样本库管理的方案和策略。

信息系统软件的使用手册请参见《样本信息管理系统使用手册》。

3.5.4 软件的保管

软件在购入或者开发完成之后，应由信息部负责保管，避免软件的丢失和随意安装使用，软件所附带的说明文件或手册也应该保管。

软件应在获得后立即复制一份，对于单一软件应随时保持两份可用状态，以

免软件媒介损坏时无法进行安装。

软件必须依托于储存媒介，储存媒介较为脆弱，对温度、湿度、烟尘等环境条件敏感，须避免日照及远离磁场过高场所或对象，如有媒介的品质出现瑕疵，必须立刻制作新的软件备份。

3.5.5 软件的安装使用

软件必须安装在计算机上才能使用，软件的安装应该遵守一定的规范。

应遵守软件版权的限制，不得在超出软件版权允许范围或者样本库规定的范围之外的场合进行安装和使用。

软件安装应由信息部管理，安装成功后，软件储存媒介须归还保管人员，保管人员对于软件媒介的借出及归还应做记录。

未经许可，样本库信息系统的计算机上不得擅自安装软件，如需要安装应通知管理人员并得到批准。

安装信息系统规定外的软件必须考虑其安全性、实用性、版本升级和售后服务能力，及与现有信息系统的兼容性。

3.6 数据

3.6.1 数据采集

样本库信息系统软件的开发应该满足数据的采集和管理的要求。

3.6.1.1 数据采集的内容

样本库信息系统采集的数据主要来自捐赠者、样本、样本使用者，在符合法律法规和伦理道德的要求下，应尽可能采集完整有效的数据，并进行数据库间的合作共享。同一批样本应指定一人进行统一随访和联系，未经授权的人员不得与样本捐赠者进行联系。

应根据样本库工作人员和样本使用人员的需求扩充数据采集的范围。

样本库信息系统采集的数据应包括但不限于如下内容：

捐赠者的身份信息，包括身份证号、出生日期、性别、民族、出生地、住所、

家族史等；

捐赠者的生活习惯，包括饮酒和吸烟史，环境与职业暴露等；

捐赠者的知情同意书，包括知情同意书的电子副本和编号等；

捐赠者的病理诊断，包括诊断的数据、肿瘤的形态、大小和级别等；

捐赠者的治疗和手术，包括治疗方法、用药情况、治疗地点、手术类型和恢复情况等；

样本的采集，包括样本的来源、采集方法、采集样本的数量和质量、采集后处理等；

样本的储存，包括样本的储存样本的类型、条形码编号、储存位置、储存条件和冻融纪录等；

样本的运输，包括运输的时间、目的和接收方等；

样本的使用，包括使用样本的条形码编号、样本使用的人员、项目和研究结果等。

3.6.1.2 数据采集的要求

信息系统对数据的采集必须满足数据的特性。

数据的合法性，在知情同意书签订之后再采集数据，必须符合法律的要求。

数据的通用性，用通用的术语和共同的元素描述数据，保持文字内容的标准格式，方便数据的共享和理解。

数据的有效性，只有经过培训的人员才能采集、输入、转移数据并使之生效，监控采集数据的质量，保证数据的长期有效。

数据的可追溯性，数据应通过样本条形码编号的唯一性进行追溯。

数据的完整性，多方面收集数据，加强数据库间的交流合作和数据共享。

数据的安全性，安全保存采集的数据，限定使用者的权限，阻止数据的非法获取。

3.6.2 数据管理

3.6.2.1 数据的维护

为了确保数据的完整性、一致性和准确性，应定期对信息系统的数据进行维护

进行月度和年度的数据审核，找出有疑问和不完整的数据。

问题数据将被重新核对，进行补充和修改，确保数据得到修正。

3.6.2.2 数据的删除

当捐赠者取消知情同意后，在销毁样本的同时应删除与该捐赠者和来自其样本的一切相关数据。

删除所有个人数据和电子信息档案，包括个人信息、知情同意书、调查问卷、临床报告和病理诊断等，如果软件不支持信息删除则将所有数据标记为“无知情同意”，禁止访问和使用。

回收和删除发放给研究者和保存在信息系统中的与样本相关的所有数据和记录，包括样本类型、形态和质量，样本采集、处理、储存、运输和使用的的所有相关纪录。

3.6.2.3 数据访问

数据访问应针对使用样本库信息系统的内部员工和外部使用者，设置不同的访问权限。当使用者的角色发生改变时，相应的访问权限也应改变。

允许访问的数据必须得到审核和监控，确保只有授权的用户才能访问。

发布可以访问的数据与样本采用一致的原则，不能透露任何捐赠者的个人信息或者关联的信息。

数据访问应设置硬件和软件的防火墙，确保敏感信息在网络中得到保护，在没有足够级别防火墙的情况下数据访问必须被监控，在有非法入侵时应报警。

数据访问应减少保密信息的出现，外部用户不被授权访问敏感和保密信息。

不得擅自下载和刻录信息系统的数据，数据的转移必须得到授权和监督，数据的使用必须有目的性并符合获取时的规定要求。

3.6.2.4 数据备份

为了应对可能出现的信息系统故障、数据库错误、系统更新、火灾和自然灾害等造成的重要数据丢失，样本库的信息系统应做好数据备份的工作。

建立适合样本库信息系统的数据库备份计划和方法，由信息部执行和监控。

定期进行数据备份，间隔根据所要备份数据的重要性的和数据恢复的需要决定。

数据库备份的媒介选择应基于数据的重要性、数据的大小、媒介保存的条件、以及数据恢复的方法。

信息系统如有条件应建立数据的异地备份，异地备份的机构必须被授权保存敏感和保密信息。

信息系统数据的备份最好是自动的，不需要人工干预，以减少错误的发生。

3.6.2.5 数据恢复

数据管理员应建立数据恢复的预案，确定需要数据恢复的情况，制定数据恢复的程序和安排执行的人员。

应至少每3个月做一次恢复测试，抽查核对部分数据，确保备份数据的完整性和有效性。

需要数据恢复时，按照预案从备份媒介中恢复数据，并对恢复的数据和系统进行测试。

应通知相关的使用人员，恢复后数据的备份时间点，并启用恢复后的系统。

应对恢复的数据进行质量控制，审核数据的完整性和准确性。

3.6.2.6 数据保密

信息系统的数据库保密应采用多种方式进行，根据数据的重要性而不同。

计算机保密，为使用者设定不同的开机密码，或者直接设定管理员的权限。

文件保密，对储存在信息系统服务器或个人计算机中的重要数据文件加密，必须输入正确密码才能使用。

媒介保密，为储存数据的媒介设置密码，取用媒介内的数据时必须输入正确

密码。

系统保密，为信息系统设置密码和访问权限，必须输入正确密码才能进入系统。

数据保密一般采用账号密码的方式，也可以采用硬件设备或者其他特殊的加密方法。

