北京地区医院信息系统基础设施

运行与管理规范

2007 年 12 月

北京市公共卫生信息中心

北京地区医院信息化基础建设促进小组

《北京地区医院信息系统基础设施建设指南》

《北京地区医院信息系统基础设施运行与管理规范》

编委会

前　言

当前，医院信息化是医院建设的基础，是医院现代化建设的核心，是医院实现“加强管理、提高质量，优化流程、方便病人，控制成本、降低费用”的重要和有效手段，是区域卫生信息化建设的重要内容，是保证公共卫生信息系统良好运行的有力支撑。北京地区经过了二十多年的医院信息化历程，在这一历程中，政府和老百姓对改善医疗服务质量和水平的要求更加强烈，其他行业在信息化方面的成效愈加显著，特别是经历了 2003 年抗击非典的斗争，越来越多的卫生行政部门和医院管理者、卫生信息化工作人员更加清晰地认识到信息化对医院发展的重要性，对区域卫生事业发展的重要性，对满足老百姓不同层次卫生服务需求的重要性。

医院信息化建设内容庞杂，是一项非常复杂的建设和管理的系统工程，而要提高整个北京地区医疗机构的信息化水平更是一项非常艰巨的任务。北京地区有各级各类医疗机构 5903 家，还有 2834 多家村卫生室，是全国医疗卫生资源最丰富的地区。这些医疗机构不仅在规模、水平上极富差距，还隶属于不同的主管部门或实际拥有者，在信息化建设的投入、效果上也差异显著。不仅如此，医院的信息化建设还普遍面临着资金、人才、标准等难题，以及一些更为具体的困惑，如：医院信息系统的建设工作在医院如何组织，如何实施，如何保障？医院信息系统建设涵盖的内容，如何按照统一的框架结构作好整体规划？如何作好医院信息系统的运行、维护和管理？有没有统一的流程和制度？已运行的医院信息系统运行状态，按照何标准检测系统运行状况和进行安全评估？如何把风险降到最低？

这些问题在各医院信息化的实践中更为现实、具体、普遍。为统筹协调北京地区医院信息化建设，发挥北京地区专家资源的优势，为各医院的信息化建设提供支持，实现对医院信息化建设的管理、运行实现规范化和标准化。在北京市公共卫生信息中心的具体组织下，北京市卫生局成立了促进北京地区医院信息化基础建设专家小组，开展了《北京地区医院信息系统基础设施运行与管理规范》（以下简称《规范》）和《北京地区医院信息系统基础设施建设指南》（以下简称《指南》）的编制工作。

在编制过程中，专家组认真学习我国有关计算机信息系统的法规和制度，如《中华人民共和国计算机信息系统安全保护条例》、《中华人民共和国计算机信息网络国际互联网管理暂行规定》、《中华人民共和国互联网安全保护技术措施规定》（公安部令第 82 号）、《信息产业部信息系统安全等级保护条例》、《卫生部医院信息系统基本功能规范》、《国家中医药管理局中医医院信息化建设基本规范》、《北京市公共服务网络与信息系统安全管理规定》等，力图使上述法规和制度在《规范》和《指南》中得到充分的贯彻和落实。同时，专家们花费了大量的时间去了解和把握国际信息技术管理业务的发展趋势，充分学习和借鉴了 ISO/IEC20000、ISO17799、ISO27001、ITIL 等国际先进的标准和理念，并结合北京地区医院信息化建设的实际情况，努力使医院信息系统建设和管理符合国际标准化质量管理体系。

《指南》和《规范》各有不同的侧重，《指南》侧重于信息系统基础设施规划和建设的技术层面，《规范》侧重于信息系统基础设施的管理和运行维护层面，二者在内容上是相互对应的。

《指南》按照信息系统基础设施内在的逻辑层次分为四个部分，包括网络系统、基础服务、网络布线系统、机房环境建设；共七章，包括医院信息系统基础设施建设的规划、网络系统规划与设计、网络基础服务、网络系统建设、网络安全管理、网络布线系统、机房建设及相关标准。把国际相关标准与北京地区医院的基本情况相结合是《指南》内容编写的基本原则。

《规范》的内容由组织管理体系、规划与计划、规章制度、运行管理、操作规程、信息系统、突发事件应对管理等章节组成。明确了信息系统管理的组织机构和职责，制定了信息系统运行和维护的相关规章制度，优化了信息系统的管理流程，提供了信息安全的保障措施。

《指南》和《规范》适用于北京地区医院计算机通信网络、信息化基础设施应用工程系统、计算机软件等设计、安装、运行和维护，各种数据库应用和信息服务业的规范化，以及主要信息产品开发与应用的规范化，也为从事医院 IT 服务的厂商、设备供应商提供了服务标准和执行依据。《指南》和《规范》的完成，无疑将为北京市卫生系统作好信息应用工程的统一监督与管理，推进医院信息系统的质量监督和认证工作等奠定重要的技术基础。同时，也可供从事信息化的

科技与管理人员以及信息技术教学人员参考。

在编制过程中，专家与业内同行们越来越认识到《指南》和《规范》对加强医院信息系统建设和管理的重要性，在专家们各自所在医院的积极支持下，在信息中心的组织下，在部分 IT 企业的支持下，专家们分工合作，认真讨论，编制过程中共组织各类专题会 19 次，培训班 3 次，专家参与人 156 次，经过近一年的努力，最终完成了《指南》和《规范》的编制工作。

《指南》和《规范》发布的意义在于：遵循我国及国际标准，初步建立起北京地区医院信息系统的建设规范和医院信息系统服务管理规范，为构建医院信息系统的安全体系结构，细化和落实北京市卫生局开展的“人民满意医院”的评审，提升医院信息系统的整体保障能力和服务水平提供了重要的依据，为今后开展和实施医院信息服务的质量管理认证工作打下了基础。

《指南》、《规范》出台后，北京市卫生局将结合医院管理评审等工作，抓好《指南》、《规范》的宣传、贯彻。同时，在应用的过程中要针对发现的问题加以改进，针对仍有争议的问题加以验证，使《指南》和《规范》在实践中不断完善，并尝试建立起支持医院信息化基础建设规范化的专门机构和队伍，以此促进北京地区医院信息化工作在基础设施方面建立起标准规范和标准架构，实现与国际标准技术接轨，推进北京地区医院信息化工作在建设、管理、运行、维护和服务等方面全面、高效、扎实的开展。

在《指南》和《规范》任务提出和完成的整个过程中，相继得到了多家厂商、集成商的大力支持及技术方面的指导与帮助；北京市公共卫生信息中心为《指南》和《规范》的顺利编制提供了组织和工作上的保证；在《指南》和《规范》编辑过程中，先后得到了局领导及各界专家的热情支持和具体指导。在此一并表示感谢！

《指南》和《规范》的编制规模大，专业技术协调、组织工作多，编制时间紧，工作中难免出现不足之处，敬请读者指正。

北京地区医院信息化基础建设促进小组

第一章　总　则

第一条　为满足北京地区公共卫生体系对医院信息化建设和管理的要求，确保医院信息系统安全可靠地运行，提高北京地区医院信息系统管理水平，特制定本规范。

第二条　本规范是北京地区医院信息系统基础设施运行与管理的指导性文件，各医院应根据本规范的要求，并结合医院实际情况，开展医院信息系统运行管理体系的建设。本规范也是对医院信息系统运行管理体系建设的评估准则。

第三条　本规范以医院信息系统基础设施的运行与管理为中心，构建医院信息系统运行管理体系。该管理体系主要包括：组织机构、规章制度、运行管理、岗位职责与操作规程、突发事件的应对等。

第四条　本规范参照国际 ITIL/ISO20000 的 IT 服务管理的最佳实践方法与理念，并结合当前北京地区医院信息管理的实际情况，引入服务台、事件管理、问题管理、配置管理和变更管理等 ITIL 的管理思想和方法；提出以“服务台”为标志的规范化服务流程及相应的岗位职责与管理要点。

第五条　本规范中所用术语与定义参见《北京地区医院信息系统基础设施建设指南》，具体包括：安全策略、基础设施、资产、机密性、完整性、可用性、真实性、责任性、不可抵赖性、可靠性、信息安全、事件、突发事件、风险评估、用户、消失、变更等。

第二章　组织管理体系

第六条　医院信息化管理的组织体系是医院信息系统基础设施正常运行的前提和保障。医院应根据本规范的要求，并结合医院规模和信息化建设的实际情况，建立与之相适应的、运行有效的信息化组织管理体系。

第七条　医院信息化建设应坚持“一把手”负责的原则，由医院院长负责医院信息化建设工作。

第八条　医院要成立医院信息化工作领导小组（或委员会）（以下简称“领导小组”），统一领导和协调医院的信息化建设工作。领导小组成员由院长、主管副院长、信息中心主任以及人事、医务、护理、科研、教育、财务、器材（设备）等相关职能部门的正职组成。

领导小组的主要职责是：

1．制定医院信息化建设的远景目标和战略规划；

2．批准医院信息化建设的五年规划和年度计划；

3．批准医院信息化建设年度资金预算，年度预算要与五年规划和年度计划相匹配，应列入年度资金预算的项目主要包括：人员费、办公费、设备购置费、服务费、运维费、耗材费、培训费等；

4．协调解决和决定医院信息化建设中的重大问题和事项。

第九条 医院应建立信息化建设监督机制，负责评审业务科室提出的信息建设项目和需求，并监督医院信息化建设的计划执行情况及预算落实情况。

第十条 医院要设置专门的信息管理与技术部门，如信息中心、信息处等（以下统称“信息中心”）。信息中心负责将医院信息化建设的长远目标及战略规划分解到信息系统的规划、设计、实施方案中。

信息中心的主要职责是：

1．编制并落实医院信息化建设的五年规划；

2．编制并实施信息化建设的年度计划；

3．编制并执行医院信息化建设的年度资金预算；

4．协助相关部门优化流程，提高医疗服务质量、减少医疗差错；

5．制定并实施医院信息管理的规章制度；

6．制定并实施各种操作规程；

7．制定并实施各类信息规范和信息标准；

8．建设、管理及维护医院信息系统；

9．采集、整理、归集、分析医院信息资源；

10．组织相关技术培训，提供技术咨询；

11．负责医院信息系统突发事件应对的管理和协调工作。

第十一条 医院应根据上级主管部门对信息中心的定编指标，并结合实际情况，确定相应的人员编制和岗位设置，可根据实际情况定期调整。

第十二条 信息中心必须设置如下技术岗位：

1．数据库管理岗；

2．网络管理岗；

3．应用系统管理岗；

4．系统管理岗；

5．信息安全管理岗；

6．现场技术支持岗；

7．调研与实施岗；

8．技术培训岗。

第十三条 医院应在各科室设置兼职信息员，辅助信息中心对各科室的信息管理及信息技术的支持工作。兼职信息员在信息业务方面接受信息中心的指导。

第三章 规划与计划

第十四条 医院要制定信息化建设的五年规划（以下简称“五年规划”）和年度计划，以明确医院信息化建设的中长期目标和近期计划。

第十五条 五年规划的编制依据是国家和北京市卫生系统对医院信息化建设的总体要求、医院五年规划纲要中对信息化建设的要求、医院上个五年规划中信息化建设的完成情况。

五年规划的内容应包括：对上个五年规划执行情况的回顾，指导思想，规划目标，主要任务，保障措施等。

五年规划由医院信息中心负责编制，经医院信息化工作领导小组审批后执行。五年规划在实施过程中，要结合实施情况，至少进行 1 次修订。

第十六条 年度计划的编制依据是五年规划和医院年度工作计划。年度计划的编制要坚持实事求是的原则，既要保证先进性，又具有可行性，以确保计划的完成。

年度计划的内容应包括：实施项目（含子项目）、内容、阶段（季度）进度、资金预算、负责部门、协作部门等。

年度计划由医院信息主管部门编制，经医院信息化工作领导小组审批后执行。

第十七条 为确保五年规划和年度计划的执行，确保信息化建设能满足医院整体发展的要求，医院应落实信息化建设的资金。医院对信息化建设的年度投入

不应低于当年医疗总收入的 1%～2%。

第四章　规章制度

第十八条　医院信息化工作的制度建设是医院信息系统基础设施安全运行与有效管理的重要保障。规章制度与信息技术、产品同等重要，技术措施通过规章制度得以实施，规章制度通过技术手段得以贯彻执行。医院必须建立健全信息化建设相关的规章制度。

第十九条　医院信息系统的建设及其规章制度必须遵守国家的有关法律、法规、标准与规范。

第二十条　医院应对信息资产进行风险评估，并为降低这些风险采取相应措施，包括制定规章制度、设置管理流程并采取相应的技术手段。医院要对信息资产的内容、保密程度及拥有者与责任人作出明确规定。

第二十一条　规章制度应包括如下内容：

1．信息安全管理的规章制度；

2．数据备份的规章制度；

3．机房管理的规章制度；

4．网络管理的规章制度；

5．设备管理的规章制度；

6．用户管理的规章制度；

7．值班制度；

8．应急预案；

9．培训制度。

第二十二条　医院应对规章制度的实施情况及效果作定期检查，并根据检查结果及时调整。

第二十三条　应将信息安全的规章制度纳入新职工入院教育及培训的内容当中，医院应与职工签订信息安全保密协议书。

第二十四条　信息中心必须有明确的岗位、职责、任务、操作规程及考核标准。

第五章　运行管理

第二十五条　医院要建立全院统一的用户请求服务机制。包括以下内容：

1．信息中心至少设置一部服务电话，用于用户请求服务。并设专门岗位负责服务受理（以下简称“接听员”）；

2．接听员应及时准确地回应用户请求或移交相应岗位处理；

3．接听员应对用户的服务请求进行记录。记录内容至少包括：时间，用户的详细联系方式（如：姓名、科室、所在位置、联系电话等），事件特征描述、发生时间、性质等。

第二十六条　接听员和相应岗位人员应快速响应并解决用户请求，将事件对业务的影响降到最小。

第二十七条　对移交给相应岗位处理的请求实行工作单制度。工作单至少应包含：用户详细联系方式、开单时间、事件发生时间、事件描述、处理措施、处理结果、完成时间等。事件处理完毕，经办人应将工作单交由用户确认。工作单应由专人负责收集、保管，定期统计分析，并制定改进措施。

第二十八条　所有用户请求都应有明确的结果，如：彻底解决、暂时解决、无法解决、消失等。

第二十九条　对暂时解决的事件应尽快找出问题根源，制定出最终解决方案，并采取相应措施，防止类似事件再次发生。

第三十条　对信息系统出现的重大事件要建立上报制度。明确上报流程，并根据事件的严重程度、影响范围明确上报的级别和时限。

第三十一条　信息中心应将常见问题的解决方法总结成册或公布于内部网站，供用户参考，以降低不必要的用户请求、提高工作效率。

第三十二条　信息中心的管理对象至少包括：

1．用户身份、密码；

2．用户端计算机、系统软件、应用软件；

3．服务器硬件、软件及配置；

4．网络系统、网络设备及配置；

5．机房及设备间设施；

6．布线系统和配置；

7．各类技术说明书。

第三十三条 信息中心应就所管理的对象建立相应的对象文档，并确保对象文档的准确性及完整性。对象文档至少包括：

1．管理对象的标识、位置、拥有者/责任人、购置/保修信息等；

2．管理对象的技术文档，如系统配置清单、配置参数和系统安装、配置手册、图纸以及与之相关的管理对象列表和关系等；

3．管理对象的操作手册/用户指南。

第三十四条 应设立专门的技术档案室，设专人管理对象文档。

第三十五条 医院应对信息系统的变更进行统一管理，要建立变更操作流程和相应岗位责任制度并严格落实。管理的范围至少包括软件、硬件、网络设备和文档等的变更。

第三十六条 变更前必须对潜在的风险、影响及需要的资源作周密调研，制定出实施计划、测试计划、回退计划、日程安排、任务分配等。较大的变更必须预先进行测试，并完成测试报告。

第六章 操作规程

第三十七条 医院应对信息系统的关键硬件设备、软件系统以及环境设施的操作管理制定严格的规程，包括：

1．对服务器、网络设备、存储设备的操作规程；

2．对数据库的操作规程；

3．基础数据的维护规程；

4．系统软件的安装规程；

5．用户端设备环境和应用软件的安装规程；

6．机房或设备间的空调、UPS 等设施的操作规程；

7．常见故障的处理规程。

第三十八条 操作规程必须文档化。文档至少包括：操作人员的资质要求、操作目的、操作内容、步骤、正常反应及异常反应、出现异常反应时的处理及允

许处理的时间和环境要求等。

第三十九条 所有操作过程必须文档化。文档至少包括：操作对象的技术文档，如系统配置参数和系统配置手册等；对运行系统的操作，必须准确记录操作的对象、内容、结果、时间和操作人姓名。

第四十条 应避免在业务高峰期间对窗口业务所涉及的网络设备、访问的服务器、软件系统进行任何变更操作。

第七章 信息系统突发事件应对管理

第四十一条 信息系统突发事件根据严重程度划分为三个预警等级：

1．三级预警：出现局部的、对医院信息系统或医院业务未构成严重影响的突发事件。

2．二级预警：出现局部的、对医院信息系统或医院业务构成严重影响的突发事件。

3．一级预警：出现全局的、对医院信息系统或医院业务构成灾难性影响的突发事件。

第四十二条 信息系统突发事件应对的工作原则是预防为主、健全制度、统一领导、分级控制、措施果断、快速反应、有效配合。

第四十三条 医院必须建立突发事件应对体系，主要包括：组织机构、工作职责、应急预案、通讯系统，以及必要物资储备。

第四十四条 组织机构：

1．领导小组：是医院信息系统突发事件应对工作的最高领导机构，负责批准突发事件应对的管理制度、应急预案、演练计划等。

2．工作小组：是信息系统突发事件应对工作的日常管理机构，由信息中心和相关用户部门组成，办公室设在信息中心。负责起草应急预案、演练计划及实施，负责突发事件发生后应对处理的协调工作。

3．专家组：是信息系统突发事件应对工作的决策参谋机构，为应急管理提供决策建议，必要时参加突发事件的应急处置工作。

第四十五条 应急启动：信息系统突发事件发生后，相关人员要立即上报工作小组；工作小组要立即确定突发事件等级，根据等级启动相应的应急预案。

对一、二级预警要立即向领导小组报告。

第四十六条 应急预案至少包括：

1．预警级别；

2．相关部门的职责和人员分工；

3．突发事件的预防和应急处理方案；

4．突发事件发生的现场控制，应急设施、设备，以及物资等；

5．突发事件信息的收集、分析、报告、通报等；

6．人员培训。

第四十七条 应急预案中的应急处理方案可采用任何可使业务持续运行的手段，包括手工、半手工、备用系统等；对关键业务的处理流程要制定相应的操作步骤，并确保数据的安全。

第四十八条 应加强信息系统突发事件应对工作的宣传、技术培训等工作，要保证应急预案的有效实施，不断提高信息系统的应急能力。对同一个应急预案每年要至少进行一次演练，并根据演练情况修订应急预案。

第八章 附 则

第四十九条 本规范自 2008 年 3 月 1 日起执行。

第五十条 本规范的解释权归属于北京市公共卫生信息中心。

附录一：医院信息化建设五年规划编制提纲

编制医院信息化建设五年规划（以下简称“五年规划”）要运用科学的发展观，深入研究医院五年发展期间发展战略，形成一个具有时代特点的、符合医院实际情况的、体系完善的五年规划。

五年规划的编制要树立实事求是、突出重点的思想；坚持主动、及时、客观、前瞻、真实的工作原则；坚持集思广益，以求共识的实现途径；处理好局部与全局、近期与长期、重点与一般的关系。五年规划要具备战略性、创新性、协调性、政策性和实用性。

要认真研究和总结上个五年规划的成功经验，客观分析所面临的问题及外部环境，提出发展目标、思路和措施等建议。

要提高规划编制的科学化，尽量采取科学的方法和手段，科学计算、科学分析，重大项目必须进行技术经济论证，具有目标量化，任务明确，重点突出等特点。

一、五年规划的编制依据

1．国家和北京市卫生系统对医院信息化建设的总体要求

2．医院五年规划纲要中对信息化建设的要求

3．医院上个五年规划中信息化建设的完成情况

二、规划编制的主要内容

1．对上个五年规划执行情况的回顾

简要回顾网络基础设施建设、应用系统开发、信息管理水平、信息人才队伍建设、制度建设、标准与规范的执行情况、技术业务水平、服务意识、投资情况、建设成效的评价等。

2．面临的形势及主要问题

对内部和外部环境进行分析，从政策、人才、资金、技术、硬件设施等方面分析优势及存在的问题。

3．五年规划的指导思想和规划目标

指导思想应阐述信息化建设对医院中心工作的作用、信息化建设的总方针，

坚持的原则等。

规划目标是对规划期末信息化建设的总体实现描述。

4．主要任务

明确规划期间的主要任务包括网络环境的建设、信息安全、信息资源的整合与共享、应用系统及技术框架的建设与开发、信息标准化规范的贯彻、人力资源的开发、文化建设。根据发展目标，明确任务以及任务完成的阶段和途径。

经营、医疗、教学、科研的任务。包括：医疗规模、市场开发、固定资产投资、人力资源开发与管理、管理与改革、党建与医院文化建设等方面。

5．保障措施

实现规划目标和主要任务应采取的措施，要突出体制建设、机制建设、制度建设、资金保障、新技术的应用、管理创新、交流与合作、结构调整等方面的措施。

6．建议

为实现规划目标，在操作过程中对医院的政策建议。

三、五年规划编制的计划安排

1．提出五年规划编制工作的方案

2．形成五年规划建议，报医院信息化工作领导小组通过

3．编制五年规划草案，报医院信息化工作领导小组通过

4．完成五年规划，报医院信息化工作领导小组通过

5．以正式文件的形式下发执行

附录二：医院网络系统安全管理制度

第一条 为了保证医院网络的正常运行，保护医院网络系统的安全和网络用户的使用权益，特制定本安全管理制度。

第二条 本管理制度所称的医院网络系统是指在医院信息系统中，由计算机及配套设施构成的，按照医院网络信息系统的应用目标和规定，对数据进行采集、加工、存储、传输、检索等处理的人机系统。

第三条 医院网络系统安全管理是通过实施身份认证、访问控制与授权管理、数据备份和灾备系统、安全分域及边界防护、防病毒系统、入侵检测、补丁管理、邮件安全网关、远程接入等安全技术和与之相配套的管理制度，保障网络主机及配套设备、设施的安全，网络运行环境的安全，从而达到保障计算机网络系统安全运行和信息安全的目的。

第四条 信息中心负责医院计算机网络系统的安全管理工作。应建立健全相应的规章制度和岗位职责，以确保对计算机网络系统安全管理的有效性。

第五条 计算机网络系统的建设和应用应遵守上级主管部门颁发的行政法规、用户手册和其他相关规定。

第六条 计算机网络系统实行安全等级保护和用户使用权限划分。安全等级和用户使用权限的划分和设置由信息中心负责制定和实施。

（注释：以下为身份认证）

第七条 计算机入网运行必须经信息中心批准备案，分配 IP 地址后，方可接入网络。

第八条 要对重要主机的用户名、开机口令、应用口令和数据库口令实施重点管理，严格控制设备存取及加密，未经允许严禁外来盘片带入机房对服务器进行安装等，不准将机器设备和数据带出机房。

第九条 未办理入网手续，任何单位和个人不得非法私自将计算机接入医院网络，不得以不真实身份使用网络资源，不得窃取他人账号、口令使用网络资源，不得盗用未经合法申请的 IP 地址入网。未经信息中心允许，任何单位或个人不得擅自接纳网络用户。

（注释：以下为访问控制与授权管理）

第十条 应根据网络主机不同的安全级别采取相应的访问控制、数据保护、

保密监控管理和系统安全等技术措施。

第十一条 信息中心应定期对网上用户的访问及授权情况进行检查，及时发现和限制非法用户和非授权访问。

第十二条 要按要求对数据进行日备份、月备份和年备份。严格按操作规程进行数据备份工作，确保备份数据的完整和准确性，做好备份数据的审核工作，并做好相应记录。要确保导出、导入数据的完整和准确，并做好导出、导入数据的审核工作和相应记录。

（注释：以下为安全分域及边界防护）

第十三条 加强边界安全的防护，应根据安全区域划分情况明确需进行安全防护的边界，并实施有效的访问控制策略和机制。

第十四条 应在网络系统或安全域边界的关键点采用严格的安全防护机制，如严格的登录/链接控制，高性能的防火墙、防病毒网关、入侵防范、信息过滤、边界完整性检查等。

第十五条 要实施必要的边界访问、违规外联的审计和控制。

（注释：以下为入侵检测）

第十六条 应采用必要的手段（如入侵检测系统、日志分析、网络取证分析等）对系统内的安全事件进行监控，检测攻击行为并能发现系统内非授权使用情况。

第十七条 应禁止系统内用户非授权的外部链接（如自动拨号、违规链接和无线上网）。

（注释：以下为防病毒系统）

第十八条 应部署有效的网络病毒防范软件系统和相应的网络病毒防范管理办法，实施对计算机网络病毒的有效防范。

第十九条 要制定文档化的明确的计算机病毒和恶意代码防护策略，以及确保策略有效实施规章制度。

第二十条 应在系统内关键的入口点以及各工作站、服务器和移动计算机设备上采取计算机病毒和恶意代码防护措施。

（注释：以下为备份和恢复）

第二十一条 应制定文档化的信息系统备份和恢复的策略，建立健全备份和恢复的管理制度和操作规程。

第二十二条 备份包括关键业务数据的备份、关键业务设备（如服务器、交换机等）的备份和电源备份。对重要信息系统（如 HIS 系统）的关键设施（如服务器）采取热备份。

第二十三条 应定期备份和对恢复策略进行测试，以保证其有效性。要有系统恢复的预案和演练。

第二十四条 应根据业务的重要程度、信息系统的资产价值等进行相应的需求分析，确定系统恢复的目标，如：关键业务功能、恢复的优先顺序、恢复的时间范围。

（注释：以下为远程接入）

第二十五条 为确保医院计算机局域网络运行安全，要在有效部署防火墙、入侵检测和防病毒系统的情况下，实施远程接入。在有条件的情况下，也可实施医院业务网（内网）与远程接入（外网）业务的物理隔离。凡涉密的计算机主机不得与互联网（Internet）链接。

第二十六条 任何部门和个人使用医院网络提供的远程接入服务必须向信息管理中心申请。入网用户的用户名和 IP 地址是用户在医院局域网上的合法标识，也是对用户收费的重要依据，一经指定不得擅自更改。

第二十七条 未经信息中心批准，任何个人或部门不得为外单位人员提供电子邮件或其他网络服务。

第二十八条 所有入网用户，应当遵守国家有关法律、法规及医院的有关规章制度，严格执行安全保密制度，不得利用计算机网络从事危害国家安全、损害医院利益等违法、违规活动，不得制作、查阅、复制和传播扰乱社会治安、有伤风化、淫秽色情等信息，不得利用网络攻击、损害公用网络和其他用户。否则，医院有权停止对其提供的服务；由此造成的不良后果由用户承担。

第二十九条 使用计算机网络系统的部门和个人必须遵守计算机安全使用的规定，对计算机网络系统发生的问题和故障要立即向信息中心报告。

第三十条 用户不得从事下列危害计算机网络安全的行为：

1．未经允许，进入计算机网络系统或使用网上信息资源；

2．私自转借或转让用户账号，盗用他人账号或 IP 地址；

3．未经允许，对网上应用系统的功能进行删减或更改；

4．未经允许，对计算机网络的存储、处理或传输数据和应用程序进行删减或更改；

5．故意制作、传播计算机病毒等破坏程序，使用任何工具破坏网络正常运行；

6．破坏、盗用计算机网络中的信息资源和危害计算机网络安全；

7．其他危害计算机网络安全的行为。

上述违规造成医院损失的，依照有关法律、法规及《医院计算机网络管理以及处罚规定》进行处理，情节严重者移交公安机关处理。

第三十一条 本管理制度中由医院信息中心负责解释。

第三十二条 本管理制度自公布之日起实行。

附录三：岗位职责

一、数据库管理岗

1．负责服务器（磁盘阵列）硬件的管理，定期观察、监测设备运行状况。设备出现异常及时处理，并向上级主管汇报情况。

2．负责服务器系统软件的管理。严格执行参数设置和调整的审批手续，按要求对系统参数进行设置和调整，并按规定登记参数设置和调整记录。

3．负责数据库的管理。严格执行参数进行设置和调整的审批手续，按要求对系统参数进行设置和调整，并按规定登记参数设置和调整记录。

4．负责服务器、数据库安全的管理。负责对设备的用户名、开机口令、应用口令和数据库口令的管理和使用。严格控制设备存取及加密，未经允许严禁外来盘片带入机房对服务器进行安装等，不准将机器设备和数据带出机房。

5．负责数据的备份工作，按要求对数据进行日备份、月备份和年备份。严格按操作规程进行数据备份工作，确保备份数据的完整和准确性，做好备份数据的审核工作，并做好相应记录。

6．负责数据的导出、导入工作。要确保导出、导入数据的完整和准确，并做好导出、导入数据的审核和相应记录工作。

7．负责填写“服务器维护月报表”，要及时、真实、完整地反映系统的运行状况、配置变更和资产变更情况。

8．负责监督和督促系统维护商按照合同的规定对系统进行维护和保养。

9．负责按期对系统情况进行分析，并按月提交分析报告。

二、网络管理岗

1．协助主管领导制订网络建设规划；

2．负责各项网络工程的实施；

3．负责协调解决各联网单位网络使用中的问题；

4．负责网络中心资产的管理工作；

5．监督机房网络设备及软件的正常运行；

6．拓展网络业务范围，发挥网络的作用；

7．负责网络文档管理。

三、应用系统管理岗

1．记录用户使用中出现的问题；

2．负责应用系统出现故障的排查；

3．用户提出的程序新功能的确认；

4．根据应用系统使用情况，提出修改意见；

5．负责新程序的测试；

6．负责风险分析、问题分析，根据分析结果制定应用系统优化方案；

7．对数据进行分析，为医院提供分析报告；

8．利用原始数据，根据需求编写专门程序；

9．负责软件版本管理；

10．负责软件文档管理。

四、系统管理岗

1．负责服务器操作系统的基本安装和调试；

2．负责服务器硬件和系统软件的日常维护；

3．负责存储设备硬件的日常维护；

4．负责服务器、存储设备等监测项目的确定；

5．参与新购服务器和存储设备的选型；

6．负责服务器和存储设备的文档管理。

五、信息安全管理岗

1．负责医院信息系统的日常安全维护；

2．负责病毒库定期升级；

3．负责 HIS 安全检测；

4．定期分析信息安全风险；

5．提出安全解决方案；

6．负责安全文档管理。

六、现场技术支持岗

1．接到维修申请后及时到达现场；

2．尽量在最短时间内恢复设备和软件正常工作；

3．负责医院科室设备、软件的现场维修；

4．指导用户正确使用设备和软件；

5．负责设备文档管理。

附录四：运维记录单

信息中心维护维修登记表

日 期：　　编 号：

报修科室：　　联系电话：　　报修人：

报修时间：

用户描述：

需求时间：　时　分　　到达现场：　时　分　　结束时间：　时　分

机器品牌：Lenovo□　Epson□　Canon□　HP□　DELL□　IBM□　其他□　主机型号：

机器名称：计算机□　一体机□　笔记本□　打印机□　　序列号：

软件情况：

硬件情况：

故障处理及结果：

1. 重装系统：Win98□　Win2000□　WinXP□　WinME□　WinServer□
2. 安装软件：瑞星□　Office□　WinRAR□　ACDSee□　打印机驱动□　其他□
3. 数据处理：数据备份□　数据恢复□
4. 系统修复：重启机器□　更改设置□　操作系统□　注册表□　查杀病毒□
5. 更换部件：CPU□　风扇□　主板□　硬盘□　内存□　显卡□　网卡□　声卡□　光驱□
   软驱□　电源□　电源线□　IDE 线□　并口线□　串口线□　USB 线□
   打印头□　分页器□　传感器□　定影组件□　挫纸轮□　进纸器□　硒鼓□
   加墨粉□　离合器□　皮带轮□　鼓芯□　喷嘴□　手轮□　其他□
6. 报修品牌：Lenovo□　Epson□　Canon□　HP□　DELL□　IBM□　其他□

信息中心：　　部门：

数据操作申请及记录

文档编号：

申请科室		提交日期	
数据操作 修改内容			
数据操作 申请原因	科室负责人签字：　　年　月　日		
信息中心 意见	负责人签字：　　年　月　日		
操作记录	执行人签字：　　年　月　日		
备 注			

数据查询申请及记录

文档编号：

申请科室		提交日期	
查询内容			
数据查询申请原因	科室负责人签字：　　年　月　日		
信息中心意见	负责人签字：　　年　月　日		
查询记录	执行人签字：　　年　月　日		
备 注			

程序安装申请表

文档编号：

申请科室		申请人员		提交日期	
安装程序					
程序安装 申请原因	科室负责人签字：　　年　月　日				
信息中心 意见	负责人签字：　　年　月　日				
备注					

程序安装记录表

文档编号：

安装科室		安装日期	
安装程序			
安装记录	安装人签字：　　年　月　日		
验收记录	验收人签字：　　年　月　日		
备 注			

机房巡检表

巡查时间	机房	温度	湿度	巡查设备状态	巡查人
				数据库服务器□ 域控服务器□ 磁盘列阵□ 中间层服务器□ 作业备份□ 任务□ UPS□ 内网交换机□ 外网交换机□ 诊区大屏监控机□ 计算机室网页服务器□趋势服务器□	
巡查记录						
巡查时间	机房	温度	湿度	巡查设备状态	巡查人
				数据库服务器□ 域控服务器□ 磁盘列阵□ 中间层服务器□ 作业备份□ 任务□ UPS□ 内网交换机□ 外网交换机□ 诊区大屏监控机□ 计算机室网页服务器□趋势服务器□	
巡查记录						
巡查时间	机房	温度	湿度	巡查设备状态	巡查人
				数据库服务器□ 域控服务器□ 磁盘列阵□ 中间层服务器□ 作业备份□ 任务□ UPS□ 内网交换机□ 外网交换机□ 诊区大屏监控机□ 计算机室网页服务器□ 趋势服务器□	
巡查记录						
注:在□内打√为设备状态正常						

网络接入申请及执行单

文档编号：

<table>
<tr><td>申请科室</td><td></td><td>提交时间</td><td></td></tr>
<tr><td>联系人</td><td></td><td>联系电话</td><td></td></tr>
<tr><td colspan="4">开通或变更需求：
1. 原因:

2. 房间号及特殊需求:

科室负责人签字：　　年　月　日</td></tr>
<tr><td>院方批复</td><td colspan="3"></td></tr>
<tr><td colspan="4">调研过程：

</td></tr>
<tr><td colspan="4">执行反馈：

执行人签字：　　年　月　日</td></tr>
<tr><td colspan="4">备注：

</td></tr>
</table>

程序功能修改申请表

文档编号：

申请科室		申请人员		提交日期	
修改内容					
申请修改原因	科室负责人签字：　　年　月　日				
信息中心意见	负责人签字：　　年　月　日				
备注					

程序功能修改记录表

文档编号：

修改模块		**修改日期**	
数据库变更	是□　　否□	**修改难度级别**	1□　2□　3□　4□　5□
修改记录	**执行人签字：　　年　月　日**		
备 注			

程序发布记录表

文档编号：

发布程序		发布日期	
发布版本号		发布人	
配置信息			
发布情况记录	执行人签字：　　年　月　日		
备 注			

信息中心值班记录

日期 ：　　值班人员：

时间	部门	事件	解决情况	备注

附录五：计算机网络系统突发事件应急预案

一、本预案适用于因网络故障、设备故障、恶意攻击、计算机病毒以及其他突发事件致使医院信息系统不能正常运行，影响医院局部或整体业务运转的二、三级突发事件。

二、组织指挥体系及职责任务

1．应对组织领导机构

（医院组织领导机构参见本规范第七章的相关内容）

计算机网络系统突发事件应对办公室（以下简称：应对办公室）设在信息中心（咨询机构、现场指挥机构），非在班时间设在院总值班室。

2．应对办公室的成员

主　任：信息中心主任

组　员：信息中心相关人员

计算机中心负责对计算机网络的小修与日常保养维护。对使用周期届满的原材料、配件进行采购及定期更换。

3．应对办公室的职责

（1）信息中心 24 小时专人值班，监控网络运行。发现问题及时处理，同时迅速向科室领导汇报。故障排除后，应完成故障报告，并在技术研讨会上汇报。

（2）详细检查故障设备，消除再发事故的可能性。

（3）负责网络的抢修。遇到较大故障，工程技术组应迅速集合，集体攻关，并做好以下工作：

故障检修：集中系统管理人员分析故障、查找原因、修复系统。

技术联络：迅速与系统承包商取得联系，采取有效手段获得技术支持。

院内协调：通知全院各科室故障情况，并到关键科室协助数据保存。

（4）负责事故的调查和报告。

三、应急响应通讯系统

1．分级响应程序

三级预案处置：发现者立即通知信息中心维修人员，信息中心须马上组织恢复工作，要充分考虑到节假日、病员量大、人员外出及医院的重大活动等特殊情况对故障恢复带来的影响。

二级预案处置：发现者立即通知信息中心，值班人员迅速判断事故的原因，并作简单的处理。当发现网络整体故障时，根据故障恢复时间的程度将转入手工工作的时限明确如下（具体实行时间及步骤由信息中心通知）：

15 分钟内不能恢复：门诊挂号、住院登记、门诊收费、急诊登记、急诊收费等工作转入手工操作。

3 小时内不能恢复：原则上将护士工作站、手术室、医技检查转入手工操作。

信息中心应将突发事件（二级）的基本情况向相关部门通报，向院突发事件应对领导小组报告。相关部门人员迅速到达现场，查明事故原因，提出解决方案。根据突发事件的实际情况和危害程度启动相应的应急保障小组程序。

2．信息报送与处理

（1）计算机网络重大事故的接报及信息传递。

①发生计算机网络重大事故突发事件后，发现人应立即向信息中心报告。

②信息中心接到突发事故报告后，应立即了解突发事故的基本情况（发生事故的部门、时间、地点，简要经过，损失情况，采取应急措施及现场情况，事故原因的初步判断，报告部门、报告人、报告时间及联系方式）并进行记录，有关人员应立即到达现场处理，根据事故的具体情况（二级突发事件）向医院突发事件应对办公室报告，并通知相关人员到岗开展应急处置工作。

成员到场后要立即检查，在截断危险源后采取果断措施防止事故的扩大后，要留下第一手资料。根据事故现场的调查情况及时向主管部门通报。

③应对办公室接到报告后，根据事件具体情况（二级突发事件）决定是否向突发事件应对领导小组报告。领导小组接到报告后，判定突发事件程度，决定是否启动应对指挥部，批准部分或全面启动二级突发事件领导机构的运行。

3．指挥与控制

（1）医院突发事件应对领导小组根据事故情况（二级突发事件）决定是否启动相关的应急预案，作出响应决定。

①召开应对领导小组会议，研究处置工作。

②传达上级领导指示精神。

③听取事故现场情况的汇报，决定处置意见。

④决定是否启用应急准备金及其数额。

⑤决定是否向社会公布消息并审批公布稿件。

⑥其他需要决定的事项。

（2）应对办公室立即到现场开展以下工作：

①落实赴现场指导处置工作及人员。

②根据处置工作的进展情况协调相关支援事项。

③跟踪事故处置工作进展情况并及时向领导小组报告。

④做好其他处置工作。

4．紧急处置

（1）紧急处置工作的原则应本着先重后轻、先人后物，最大程度减少损失。

（2）当遇有重大灾害或人员伤亡时，应上报院应对响应领导机构和相应的预案小组处理。

（3）在处置紧急抢修过程时，应提出最佳的解决方案。

（4）协助有关卫生部门进行现场处置。

5．事件的调查、处理和检测

计算机网络重大事故发生后，由信息中心会同其他相关部门成立现场调查组，负责对事故现场的调查、处理和检测工作。

6．应急人员的安全防护

应急人员在现场进行干预处理时，应注意设备维修时可能发生的危险（如爆炸、漏电等），在确保自己人身安全的情况下开展工作。

7．新闻报道

作好宣传报道工作，动员职工战胜困难；作好新闻报道工作，统一口径，及时向公众发布有关信息，平息谣传或误传，安定人心。

8．应急响应终结

计算机网络重大事故（二级突发事件）处置工作完成，经医院领导小组批准，宣告应急响应程序终结。由突发事件应对领导小组向上级主管部门报告，本次应

急工作结束。

四、应急保障

1．通信与信息保障

由信息中心负责，保证通信联系线路畅通，组织力量抢修通信设备和线路，充分利用无线通讯设备，明确各地各部门的突发事件应急值班电话。必要时要确定联络信号（例如火堆或信号弹等）。

2．治安保障

由保卫处负责，组织协调力量维护社会治安，打击违法犯罪活动。负责重要机关、部门、重要建筑设施和财产的安全保卫工作。负责交通安全管理工作，确保交通干线畅通无阻。

3．设备物资保障

由设备物资处负责，提供相关抢险设备，提供专业技术人员和维修人员，提供器材以及临时电源供给，保证抢救工作顺利进行。

4．资金保障

由财务处负责，根据本部门的应对工作任务拟定计划，管理应急准备金，定期检查，以确保应急工作的需要。

五、培训和演习

1．培训

信息中心负责对有关人员平均每季度进行 1 次相关知识培训。

2．演习

信息中心负责，至少每半年组织 1 次计算机网络重大事故预案的模拟演练。届时，信息中心和相关科室应配合完成演练，并在演练结束后，对演练作出评价。对演练中存在的问题应总结、记录，并调整不合实际的方案。

六、后期处置

1．事故调查

根据第一时间现场留下的资料进行事故的分析调研。

2．责任追究

根据事故调查处理报告书的意见对有关责任人进行处理。

3．纠正及预防措施

认真执行计算机网络的管理制度和设备使用操作常规。作好设备技术性能的点检和测试，及时发现设备故障隐患。对超出点检安全运行的数据，应分析原因、及时排除。对供水、供电系统有故障时，禁止强行启动机组运行。

4．奖励与处罚

对在处理处置事故中表现突出的人员给予奖励，对事故中的有关责任人给予相应的处罚。

附录六：ITIL 简介

ITIL 是英文 Information Technology Infrastructure Library 的缩写，通常被译为“信息技术基础架构库”。ITIL 是一套由英国商务部（OGC）开发、出版的书籍，ITIL 描述了一套集成的流程，是面向 IT 服务管理的最佳实践。

早在上个世纪 80 年代中期，英国政府为了提高政府部门 IT 服务的质量启动了一个项目，邀请国内外知名 IT 厂商和专家共同开发一套规范化的、可进行财务计量的 IT 资源使用方法。这种方法应该是独立于厂商的并且可适用于不同规模、不同技术和业务需求的组织。这个项目的最终成果就是现在被广泛认可的 ITIL。目前，ITIL 的最新版是 3.0 版。

ITIL 2.0 主要包括六个模块，即业务管理、服务管理、ICT 基础架构管理、IT 服务管理规划与实施、应用管理和安全管理。其中服务管理是其最核心的模块，该模块包括“服务提供”和“服务支持”两个流程组，共包括了十个流程和一项职能。见下表：

IT 服务支持（Service Support）	IT 服务提供（Service Delivery）
服务台功能（Service Desk）	
事件管理流程（Incident Mgmt）	服务级别管理（Service Level Mgmt）
问题管理流程（Problem Mgmt）	可用性管理流程（Availability Mgmt）
配置管理流程（Configuration Mgmt）	持续性管理流程（Continuity Mgmt）
变更管理流程（Change Mgmt）	IT 能力管理流程（Capacity Mgmt）
发布管理流程（Release Mgmt）	服务财务管理流程（Financial Mgmt）

各流程的具体作用如下：

服务支持（Service Support）

服务台	IT 服务的单点入口、受理服务请求和突发事件
事件管理	有效解决突发事件可用性管理，尽快恢复 IT 服务
问题管理	找寻问题的根源和解决方案连续性管理，消除或减少问题事件的发生
变更管理	管理变更的实施过程能力管理，避免或减小变更带来的影响

发布管理	控制 IT 系统和软件的发布过程管理软件版本
配置管理	管理 IT 系统的所有元素及相关信息，描述 IT 元素之间的相互关系

服务提供（Service Delivery）

服务级别管理	提供与服务级别对等的服务内容，完成量化服务管理
可用性管理	监控 IT 重要资源和运行指标，保证整个业务系统的可用性
连续性管理	建立业务持续计划，实现业务的持续运行
容量管理	监控和提高系统性能，进行性能规划
财务管理	IT 服务的预算管理、成本管理，计算 IT 服务价值

ITIL 除了为 IT 部门的所有活动提供了一个通用框架外，对医疗行业来说，更重要的是“IT 服务”这一重要理念。ITIL 将 IT 部门所做的工作看成是向医院提供服务，而 IT 部门本身不是一个单纯的成本中心，医院在 IT 方面的投资本质上是花钱买服务。因此，医院在考虑投资与回报时不仅要计算信息系统为医院节省了多少钱、堵了多少漏洞，还要考虑这些服务自身的价值，而这些服务价值的计算是与医院战略目标的实现联系在一起的。这也是 ITIL 3.0 将信息技术提高到组织的战略资源高度的原因。

2007 年 5 月 30 日 ITIL V3.0 发布。ITILV 3.0 在 IT 服务管理流程方面沿用了 2.0 的所有内容，但在整个框架上有了很大改进，这些改进包括：

1．用了服务生命周期的循环、而非流程的线性概念；

2．增加了与其他标准框架的融合，如 Cobit、CMMI 及 Six Sigma 等；

3．提供了丰富的新资源。2.0 只告诉大家应该“做什么”，而 3.0 中针对“怎么做”给出了很多行业案例和一些具体实施方案。

ITIL 3.0 的核心包括五部分：服务策略（Service Strategy），服务设计（Service Design），服务转换（Service Transition），服务运行（Service Operations），持续的服务改进（Continuous Service Improvement）。

ITIL 认证

ITIL 认证一共有三种级别，分别为 ITIL 基础（ITIL Foundation）、ITIL 从业

者（ITIL Practitioner）和 ITIL 服务经理（ITIL Service Manager）。其中 ITIL 基础认证主要针对从事 IT 服务管理的人员，要求了解 ITIL 的基本术语、概念、流程之间的关系和掌握 IT 服务管理的基本原理；ITIL 从业者认证针对从事 IT 服务管理特定流程的人员，要求掌握运作某一个或几个特定 ITIL 流程的能力和经验；ITIL 经理认证针对高层的 IT 服务管理人员，考核其实施和运作 IT 服务的能力。

ITIL 的版本变迁

ITIL 自英国中央计算机和电信局(CCTA)提出至今共经历了三个主要版本：

V 1.0：持续时间从 1986 到 2001 年。第一版的 ITIL 开发了 40 多卷图书，主要是基于职能型的实践。

V 2.0：持续时间从 2001 年到 2007 年，主要是基于流程型实践，总结为 9 卷，并成为 IT 服务管理领域全球认可的最佳实践框架。2.0 版中的 ITIL 主要包括六个模块，即业务管理、服务管理、ICT 基础架构管理、IT 服务管理规划与实施、应用管理和安全管理。其中服务管理是其最核心的模块，该模块包括“服务提供”和“服务支持”两个流程组。

V 3.0：2007 年 5 月 30 日发布，基于服务生命周期的 ITIL V3.0 整合了 V 1.0 和 V 2.0 的精华，并融入了 IT 服务管理领域当前的最佳实践。5 本书构成了 ITIL V 3.0 的核心，这 5 本书籍分别是《服务策略》(Service Strategy)、《服务设计》(Service Design)、《服务导入》(Service Transition)、《服务运营》(Service Operation)及《持续性服务改进》(Continuous Service Improvement)。

致　谢

在《指南》和《规范》任务提出和完成的整个过程中，相继得到了以下多家厂商、集成商的大力支持及技术方面的指导与帮助，在此表示感谢！

国际商业机器全球服务（中国）有限公司

美国康普国际控股有限公司北京办事处

微软(中国)有限公司

中国网通(集团)有限公司北京市分公司

北京联信永益科技有限公司

北京博望恒信智能系统有限公司

杭州华三通信技术有限公司

北京金山软件有限公司

航天四创科技有限责任公司