ICS 35.240.99
C 07

团　　体　　标　　准

T/GDNS 011—2023

医疗机构信息系统等级保护定级工作指南

Guidelines for classified Protection of Information System of Medical Institutions

2023－04－19 发布　　2023－04－24 实施

广东省计算机信息网络安全协会　发布

目　录

前　言

本标准按照GB/T 1.1《标准化工作导则 第1部分：标准化文件的结构和起草规则》要求编写。

本标准由广东省计算机信息网络安全协会提出并归口。

本标准起草单位：广东省计算机信息网络安全协会、广东省人民医院、中山大学附属第一医院、南方医科大学南方医院、广州市第一人民医院、中山大学附属肿瘤医院、中国人民解放军南部战区总医院、南方医科大学第三附属医院、中山大学附属第三院、中山大学附属第五医院、中山大学附属第六医院、中山大学附属第八医院、佛山市妇幼保健院、肇庆市第一人民医院、南方医科大学珠江医院、广东省妇幼保健院、广州市妇女儿童医疗中心、广州医科大学附属第一医院、广州医科大学附属第二医院、广州医科大学附属第五医院、广东药科大学附属第一医院、暨南大学附属第一医院、广州中医药大学第一附属医院、番禺区何贤纪念医院、广州市番禺区中心医院、佛山市中医院、梅州市人民医院、香港大学深圳医院、清远市人民医院、粤北人民医院、江门市中心医院、茂名市人民医院、阳江市人民医院、东莞市第六人民医院、惠州市第六人民医院、粤北第二人民医院、暨南大学附属顺德医院、广东轻工职业技术学院、广州理想资讯科技有限公司、工业和信息化部电子第五研究所(中国赛宝实验室)、广州市海珠区社区卫生发展指导中心、广州市番禺区卫生健康局、广东物壹信息科技股份有限公司、深圳市网安计算机安全检测技术有限公司、中科信息安全共性技术国家工程研究中心有限公司、深信服科技股份有限公司、广东珠江智联信息科技股份有限公司、奇安信安全技术（广东）有限公司、广州竞远安全技术股份有限公司、深圳市携网科技有限公司。

本标准起草人：杨洋、黄振毅、余俊蓉、严静东、安文琛、任忠敏、赵霞、银琳、张家庆、周欣、周邮、陈浩、马丽明、张杏华、陈翔、张巍、赖志存、曹晓均、陈智、陆慧菁、李斌、林嘉楠、钟军锐、林圻、何颖新、何耀德、梁瑞麟、叶欣、庞勤、邓联丙、廖茂成、温明锋、李卫昌、曾幸辉、熊劲光、莫谋森、吴鼎宁、吴庆斌、吴龙、张芳健、潘天祥、陈思宇、刘翰腾、曾艺、辛继胜、欧阳雪源、罗广伟、蔡伟标、张伟、陈涛、黄志群、王健英、彭丽超、龙军、胡建勋、吴瑞、陈建长、于海峰、成嘉轩、王水兵。

标准为首次发布。

医疗机构信息系统等级保护定级工作指南

1 范围

本标准给出了广东省各级各类医疗机构非涉及国家秘密的等级保护对象的安全保护等级定级方法和定级流程。

本标准适用于指导各级各类医疗机构开展非涉及国家秘密的等级保护对象的定级工作。涉及国家秘密的信息系统应根据国家保密局要求，遵循国家涉密信息系统分级保护制度进行安全防护工作。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本标准。

GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》

GB/T 22240-2020 《信息安全技术 网络安全等级保护定级指南》

GB/T 25058-2019 《信息安全技术 网络安全等级保护实施指南》

《医院信息化建设应用技术指引》

《全国医院信息化建设标准与规范(试行)》

《医院信息互联互通标准化成熟度测方案》

《医院分级管理标准》

3 术语和定义

GB/T 25069-2022界定的以及下列术语和定义适用于本文件。

3.1

网络安全（cybersecurity）

通过采取必要的措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

3.2

等级保护对象（target of classified protection）

网络安全等级保护工作直接作用的对象。（主要包括信息系统、通信网络设施和数据资源等）。

3.3

受侵害的客体（object of infringement）

受法律保护的等级保护对象受到破坏时所侵害的社会关系。（本标准中简称“客体”）。

4 基本原则

等级保护的核心是对系统分等级、按标准进行建设、管理和监督。信息系统网络安全等级保护实施过程中应遵循以下原则：

（1）法规遵从原则

信息系统网络安全等级保护工作开展应符合国家法律法规及行业主管部门相关规定，科学确定信息系统的安全等级并予以备案，按照相应等级要求组织实施安全保障。

（2）适时调整原则

由于各级各类医疗机构信息系统的应用类型、覆盖范围、外部环境等约束条件，以及加载、处理的信息处于不断变化与发展之中，因此，医疗机构需要根据内外部环境变化情况，适时重新确定信息系统的网络安全保护等级，并调整相应的保护措施。

（3）重点保护原则

信息系统网络安全等级保护应突出重点。对关系国家安全、公共健康安全、社会稳定等方面的重要系统，集中资源优先建设、加强管理和监督。

（4）分域保护原则

网络安全等级保护工作应根据系统的类型、重要程度、业务特点和不同发展水平，分类、分级、分阶段进行实施，并通过划分不同的安全域，实现不同强度的安全保护。

5 定级原理及流程

5.1 定级原理

根据国家 GB/T 22240-2020《信息安全技术 网络安全等级保护定级指南》的规定，医疗机构信息系统的安全保护等级分为以下五级：

a） 第一级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益；

b） 第二级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全；

c） 第三级，信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害；

d） 第四级，信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害；

e） 第五级，信息系统受到破坏后，会对国家安全造成特别严重损害。

5.2 定级过程

医疗机构信息系统定级工作的一般流程如图 1 定级流程图所示：

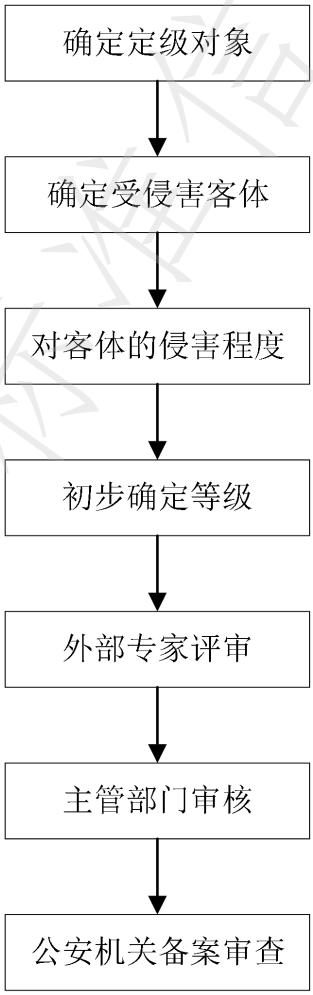

图 1 定级流程图

a） 确定定级对象

确定定级对象由信息处（科）或相关科室负责，定级对象一般为支撑医疗服务的临床服务类系统、医疗管理类系统以及医院运营管理类系统。结合医疗机构的信息化建设情况，作为定级对象的信息系统应具备以下基本特征：

1） 信息系统是由相关和配套的设备、设施按照一定的应用模板和规则组合而成，避免将某个单一的系统组件，如服务器、终端、网络设备等作为定级对象。

2） 信息系统承载“相对独立”的业务，即主要业务流程独立，但与其它业务应用有一定的数据交换、共享一些设备，例如网络传输设备。

3） 涉及区域内医疗业务信息系统数据交换和共享的平台，或承载不同系统间信息整合任务的基础网络平台。

结合各级医疗机构等级保护工作情况，医疗机构等级保护工作定级对象主要包括医院患者信息系统、电子病历系统、影像系统、检验系统、医院信息平台、门户网站、办公自动化系统和集成平台等。详见附录 A《定级对象表》。

5.2.1 确定受侵害客体

定级对象受到破坏时所侵害的客体包括国家安全、社会秩序、公众利益以及公民、法人和其他组织的合法权益。

1） 侵害国家安全的事项包括以下方面：

- 影响国家政权稳固和国防实力；
- 影响国家统一、民族团结和社会安定；
- 影响国家对外活动中的政治、经济利益；
- 影响国家重要的安全保卫工作；
- 影响国家经济竞争力和科技实力；
- 其他影响国家安全的事项。

2） 侵害社会秩序的事项包括以下方面：

- 影响医疗机构社会管理和公共服务的工作秩序；
- 影响医疗机构类型的经济活动秩序；
- 影响医疗机构的科研、生产秩序；
- 影响公众在法律约束和道德规范下的正常生活秩序等；
- 其他影响社会秩序的事项。

3） 影响公共利益的事项包括以下方面：

- 影响社会成员使用医疗机构；
- 影响社会成员获取公开信息资源；
- 影响社会成员接受公共服务等方面；
- 其他影响公共利益的事项。

4） 影响公民、法人和其他组织的合法权益：

判断定级对象受到损害后是否影响公民、法人和其他组织的合法权益，是指由法律确认的并受法律保护的公民、法人和其他组织所享有的一定的社会权利和利益。

确定作为定级对象的信息系统受到破坏后所侵害的客体时，应首先判断是否侵害国家安全，然后判断是否侵害社会秩序或公众利益，最后判断是否侵害公民、法人和其他组织的合法权益。

广东省各级医疗机构信息系统受到破坏后，一般侵害的客体主要包括社会秩序、公共利益和公民、法人和其他组织的合法权益。

5.2.2 对客体的侵害程度

从业务信息和系统服务两方面分别遭到破坏可能造成的影响程度，受侵害程度分为三种，分别是一般损害、严重损害和特别严重损害。

1） 一般损害

医疗机构工作职能受到局部影响，业务能力有所降低但不影响主要功能的执行，出现较轻的法律问题，较低的财产损失，有限的社会不良影响，对其他组织和个人造成较低损害。

2） 严重损害

医疗机构工作职能受到严重影响，业务能力显著下降且严重影响主要功能执行，出现较严重的法律问题，较高的财产损失，较大范围的社会不良影响，对其他组织和个人造成较严重损害。

3） 特别严重损害

医疗机构工作职能受到特别严重影响或丧失行使能力，业务能力严重下降且功能无法执行，出现极其严重的法律问题，极高的财产损失，大范围的社会不良影响，对其他组织和个人造成非常严重损害。

医疗机构的业务信息安全或系统服务安全受到破坏时，对客体的侵害程度与信息系统所属机构的行政级别、服务地区范围、服务人群规模、服务量大小、信息重要程度等有关。

5.2.3 初步确定等级

从系统类别、服务对象、影响范围、影响程度、承载数据量及数据级别等多个维度，确定受侵害客体及对客体的侵害程序，初步确定安全等级，填写《信息系统安全等级保护备案表》2 份和定级报告 1 份。确定信息系统等级可按照附录 B 信息系统定级指引。定级报告模版见附录 C.1 信息系统安全等级保护定级报告。

定级要素与安全保护等级的关系表

受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

5.2.1 外部专家评审

组织第三方信息安全专家和业务专家等专家，对初步确定的安全等级开展专家评审，出具专家评审意见；

5.2.1 主管部门审核

各级医疗机构根据专家评审意见，报送各级卫生健康委员会（局）；

5.2.2 公安机关备案

将初步定级结果盖单位公章，提交省（市）公安关机网监部门进行备案审查，审查不通过，医疗机构应组织重新定级；审查通过后最终确定定级对象的安全保护等级。

附 录 A
（资料性）
定级对象表

序号	信息系统分类	定义
1	临床服务系统	门急诊挂号系统、门诊医生工作站、分诊管理系统、住院病人入出转系统、住院医生工作站、住院护士工作站、电子化病历书写与管理系统、急诊临床信息系统、消毒供应系统、合理用药管理系统、临床检验系统、医学影像系统、超声管理系统、内镜管理系统、核医学管理系统、放射治疗管理系统、临床药学管理系统、手术麻醉管理系统、临床路径管理系统、输血管理系统、重症监护系统、心电管理系统、体检管理系统、其他功能检查管理系统、预住院管理系统、病理管理系统、移动护理系统、移动查房系统（移动医生站）、输液系统、病历质控系统、血透系统、康复治疗系统、专科电子病历系统（眼科、产科、口腔等）
2	医疗管理系统	门急诊收费系统、住院收费系统、护理管理系统、医务管理系统、院感/传染病管理系统、科研管理系统、病案管理系统、导诊管理系统、危急值管理系统、预约管理系统、抗菌药物管理系统、互联网医院管理系统、静脉药物配置管理系统、应急事件监测管理系统、手术分级管理系统、医联体管理系统、GCP、管理系统、教学管理系统、医保管理系统、随访系统、电子签章系统、职业病管理系统接口、食源性疾病上报系统接口、不良事件报告系统
3	运营管理系统	人力资源管理系统、财务管理系统、药品管理系统、医疗设备管理系统、固定资产管理系统、卫生材料管理系统、物资供应管理系统、预算管理系统、绩效管理系统、DRG、管理系统、楼宇智能管理系统、后勤信息管理系统、OA、办公系统、投诉管理系统、客户服务管理系统
4	集成平台	临床数据中心、主数据管理、患者360视图、患者主索引、精细化运营管理、信息系统集成引擎
5	接入上级信息平台	上级和医院间的信息共享、区域一卡通、区域远程医疗、区域医疗公众服务、双向转诊、区域病理共享、区域检验共享、区域影像共享

6	接入外部机构的系统	接入公安系统、接入急救中心系统、接入CDC（疾控中心）系统、接入血液中心系统、接入银行支付系统、接入非银行支付系统、医保及新农合、接入保险机构系统、第三方挂号平台、第三方药品配送机构、外部数据上报平台或监管平台
注：为方便管理，上述对象可合并管理的，建议合并定级。		

附 录 B
（规范性）
信息系统定级指引

B.1 受侵害客体业务信息安全赋值

广东省各级医疗机构信息系统受到破坏后，其**业务信息安全**仅对区域内的社会成员接受公共卫生服务造成影响，或影响公共利益，以及可能对公民、法人和其他组织的合法权益造成不良影响，不对国家安全造成损害。

表 B.1 受侵害客体业务信息安全赋值表

受侵害客体	损害程度	赋值
国家安全	不适用	-
社会秩序、公共利益	一般	2
	严重	3
	特别严重	4
公民、法人和其他组织的合法权益	一般、严重、特别严重	1
各医疗机构结合定级对象被侵害后影响的受侵害客体进行赋值。		

B.2 受侵害客体系统服务安全赋值

广东省各级医疗机构信息系统受到破坏后，其**系统服务安全**应从信息系统服务对象、影响范围、影响程度多个维度，确定受侵害客体系统服务安全数值，具体划分方法见表 B.2。

表 B.2 系统服务安全赋值表

服务对象	影响范围	医院级别	赋值
公共服务	临床服务系统、集成平台	一级	1
		二级	2
		三级	3

公共服务	医疗管理系统、接入外部机构的系统	一级	1
		二级	2
		三级	2
组织内部	全院级运营管理系统、接入上级信息平台	一级	1
		二级	1
		三级	2
	科室级运营管理系统	一级	1
		二级	1
		三级	1

注：对于县（市）级统一支持辖区内基层医疗机构（一级及二级）运行的集中部署信息系统，应参照三级医院级别按不同影响范围进行取值。

B.3 初步确定等级

根据**受侵害客体业务信息安全数值**与**受侵害客体系统服务安全数值**情况，取最高值确定保护对象等级。

定级对象取值=max{受侵害客体业务信息安全数值，受侵害客体系统服务安全数值}。最终根据表 B.3 初步确定定级对象等级。

表 B.3 定级对象值与定级对象等级关系表

定级对象数值	定级对象等级
4	第四级
3	第三级
2	第二级
1	第一级

附 录 C
（资料性）
信息系统安全等级保护定级报告模板

B.1 信息系统安全等级保护定级报告

一、XXX 信息系统描述

简述确定该系统为定级对象的理由。从三方面进行说明：一是描述承担信息系统安全责任的相关单位或部门，说明本单位或部门对信息系统具有信息安全保护责任，该信息系统为本单位或部门的定级对象；二是该定级对象是否具有信息系统的基本要素，描述基本要素、系统网络结构、系统边界和边界设备；三是该定级对象是否承载着单一或相对独立的业务，业务情况描述。（注意：如果是网站的话需要提供网站域名和 IP 地址）

二、XXX 信息系统安全保护等级确定（定级方法参见国家标准《信息系统安全等级保护定级指南》）

（一）业务信息安全保护等级的确定

1、业务信息描述

描述信息系统处理的主要业务信息等。

2、业务信息受到破坏时所侵害客体的确定

说明信息受到破坏时侵害的客体是什么，即对三个客体（国家安全；社会秩序和公众利益；公民、法人和其他组织的合法权益）中的哪些客体造成侵害。

3、信息受到破坏后对侵害客体的侵害程度的确定

说明信息受到破坏后，会对侵害客体造成什么程度的侵害，即说明是一般损害、严重损害还是特别严重损害。

4、业务信息安全等级的确定

依据信息受到破坏时所侵害的客体以及侵害程度，确定业务信息安全等级。

（二）系统服务安全保护等级的确定

1、系统服务描述

描述信息系统的服务范围、服务对象等。

2、系统服务受到破坏时所侵害客体的确定

说明系统服务受到破坏时侵害的客体是什么，即对三个客体（国家安全；社会秩序和公众利益；公民、法人和其他组织的合法权益）中的哪些客体造成侵害。

3、系统服务受到破坏后对侵害客体的侵害程度的确定

说明系统服务受到破坏后，会对侵害客体造成什么程度的侵害，即说明是一般损害、严重损害还是特别严重损害。

4、系统服务安全等级的确定

依据系统服务受到破坏时所侵害的客体以及侵害程度确定系统服务安全等级。

（三）安全保护等级的确定

信息系统的安全保护等级由业务信息安全等级和系统服务安全等级较高者决定，最终确定XXX系统安全保护等级为第几级。

信息系统名称	安全保护等级	业务信息安全等级	系统服务安全等级
XXX信息系统	第X级	第X级	第X级