



中华人民共和国国家标准

GB/T 38631—2020

信息技术 安全技术 GB/T 22080 具体行业应用 要求

Information technology—Security techniques—
Sector-specific application of GB/T 22080—Requirements

(ISO/IEC 27009:2016, Information technology—Security techniques—
Sector-specific application of ISO/IEC 27001—Requirements, MOD)

2020-04-28 发布

2020-11-01 实施

国家市场监督管理总局 发布
国家标准化管理委员会

目 次

前言	I
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 概述	1
4.1 总则	1
4.2 本标准结构	2
4.3 扩展 GB/T 22080 要求或 GB/T 22081 控制	2
5 补充、细化或解释 GB/T 22080 要求	2
5.1 总则	2
5.2 补充要求	3
5.3 细化要求	3
5.4 解释要求	3
6 补充或修改 GB/T 22081 指南	3
6.1 总则	3
6.2 补充指南	4
6.3 修改指南	4
附录 A (规范性附录) 制定与 GB/T 22080—2016 或 GB/T 22081—2016 相关的 具体行业标准的模板	5
附录 B (资料性附录) 面向医疗行业的信息安全管理体系指南示例	8
参考文献	11

前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准使用重新起草法修改采用 ISO/IEC 27009:2016《信息技术 安全技术 ISO/IEC 27001 具体行业应用 要求》。

本标准与 ISO/IEC 27009:2016 的技术性差异及其产生的原因如下：

- 范围增加“本标准适用于制定与 GB/T 22080 相关的具体行业标准”(见第 1 章)；
- 4.1 删除“ISO/IEC 之外的组织也制定了实现具体行业需求的标准”；
- 增加“依据附录 A,面向医疗行业的信息安全管理体系指南示例参见附录 B”(见 4.2)；
- 附录 A 的 A.1 删除“具体行业标准宜命名如下:面向〈行业〉的信息安全管理体系”；
- 附录 A 的 A.2 模板中,4.2 和 5 的〈控制目标号〉〈控制目标标题〉和〈控制号〉〈控制标题〉改为〈控制目标号〉[〈控制目标标题〉]、〈控制号〉[〈控制标题〉],以避免标题与其后文字混淆；
- 附录 A 的 A.2 模板中,4.2 和 5 中,“对行业至少使用三个字母作为前缀”改为“对行业使用国民经济行业名称(见 GB/T 4754—2017)作为前缀”,4.2 中强制实施的控制,“使用(M)作为控制编号的前缀”改为“使用(强制)作为控制编号的前缀”。

本标准做了下列编辑性修改：

- 增加了参考文献 ISO 27799:2016 和 ISO 22600；
- 增加资料性附录 B“面向医疗行业的信息安全管理体系指南示例”,有利于标准落地实施。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:山东省标准化研究院、中国网络安全审查技术与认证中心、成都秦川物联网科技股份有限公司、陕西省网络与信息安全测评中心、山东崇弘信息技术有限公司。

本标准主要起草人:王曙光、魏军、王庆升、公伟、张斌、来永钧、邵泽华、赵首花、杨锐、尤其、郭杨、权亚强、李怡、何果、路津、李红胜、路征、陈慧勤、刘勘伪、于秀彦、胡鑫磊、王栋、刘鑫。

信息技术 安全技术

GB/T 22080 具体行业应用 要求

1 范围

本标准规定了 GB/T 22080 应用于具体行业(领域、应用)时的要求。本标准解释了如何在 GB/T 22080 要求上包含补充要求,如何细化 GB/T 22080 的要求,以及如何包含 GB/T 22080—2016 附录 A 之外的控制或控制集。

本标准确保补充的或细化的要求与 GB/T 22080 的要求不冲突。

本标准适用于制定与 GB/T 22080 相关的具体行业标准。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。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)适用于本文件。

GB/T 22080—2016 信息技术 安全技术 信息安全管理体系 要求(ISO/IEC 27001:2013, IDT)

GB/T 22081—2016 信息技术 安全技术 信息安全控制实践指南(ISO/IEC 27002:2013, IDT)

GB/T 29246—2017 信息技术 安全技术 信息安全管理体系 概述和词汇(ISO/IEC 27000:2016, IDT)

3 术语和定义

GB/T 29246—2017 界定的以及下列术语和定义适用于本文件。

3.1

解释 interpretation

在具体行业背景下对 GB/T 22080 要求的说明(以要求或指南的形式),该说明不会使 GB/T 22080 的要求失效。

3.2

细化 refinement

GB/T 22080 要求在具体行业的详述,该详述不会删除 GB/T 22080 任一要求或使其失效。

4 概述

4.1 总则

GB/T 22080 规定了建立、实现、维护和持续改进信息安全管理体系的要求。这些要求是通用的,适用于各种类型、规模或性质的机构。

注:ISO 管理体系标准的建立依据 ISO/IEC 导则 第 1 部分 融合的 JTC1 补充部分(2016)。

GB/T 22081 为信息安全管理实践提供了指南,考虑了机构信息安全风险环境下控制的选择、实施和管理。该指南采用分层结构,包括章节、控制目标、控制、实现指南以及其他信息。指南是通用的,适

用于各种类型、规模或性质的机构。

GB/T 22081 的控制目标和控制以规范性附录形式列在 GB/T 22080—2016 的附录 A 中。GB/T 22080—2016 要求机构确定信息安全风险处置选项所必需的所有控制[见 6.1.3 b)],并将 6.1.3 b) 确定的控制与附录 A 中的控制进行比较,并验证没有忽略必要的控制[见 6.1.3 c)]。

随着 GB/T 22080 和 GB/T 22081 在企业、政府机构和非营利组织中的广泛应用,需要开发针对这些具体行业的标准,主要完成的标准包括:

- GB/T 32920,信息技术 安全技术 行业间和组织间通信的信息安全管理;
 - ISO/IEC 27011,基于 ISO/IEC 27002 的电信组织信息安全管理指南;
 - ISO/IEC 27017,基于 ISO/IEC 27002 的云服务信息安全控制实践指南;
 - ISO/IEC 27018,可识别个人信息(PII)处理者在公有云中保护可识别个人信息的实践指南。
- 具体行业标准需要与信息安全管理要求相一致。本标准主要从以下两方面规定了相关要求:
- 具体行业如何补充、细化 GB/T 22080 的要求或对其作出解释;
 - 具体行业如何补充或修改 GB/T 22081 的指南。

本标准假定所有来自 GB/T 22080 未被细化的或未作出解释的要求、所有来自 GB/T 22081 未被修改的控制,将不加修改的适用于具体行业环境。

4.2 本标准结构

第 5 章提供要求和指南,给出如何在 GB/T 22080 要求上确定补充要求、细化要求或作出解释。

第 6 章提供要求和指南,给出如何在 GB/T 22081 内容上补充或修改控制目标、控制、实现指南或其他信息。

附录 A 给出与 GB/T 22080 和(或)GB/T 22081 可用于具体行业标准的模板。

依据附录 A,面向医疗行业的信息安全管理体系指南示例参见附录 B。

本标准使用如下概念以使 GB/T 22080 的要求适用于具体行业:

- 补充:见 5.2
- 细化:见 5.3
- 解释:见 5.4

本标准使用如下概念以使 GB/T 22081 的指南适用于具体行业:

- 补充:见 6.2
- 修改:见 6.3

注:遵循本标准要求和指南而制定的具体行业指南不可包含在技术报告中。ISO/IEC 导则将技术报告定义为不含要求的文档,而任一依据本标准开发的具体行业标准,特别是附录 A,都将至少包含一个最小的要求集合(见 A.2 中模板的 4.1)。

4.3 扩展 GB/T 22080 要求或 GB/T 22081 控制

与 GB/T 22080 相关的具体行业标准可以对 GB/T 22080 或 GB/T 22081 进行补充,可将信息安全之外的要求或指南纳入具体行业之中。

示例:ISO/IEC 27018:2014 附录 A 包含一组旨在保护可识别个人信息的控制,从而使 ISO/IEC 27018 的范围除信息安全外还涵盖可识别个人信息的保护。

5 补充、细化或解释 GB/T 22080 要求

5.1 总则

图 1 阐明了如何构建与 GB/T 22080 相关的具体行业要求。

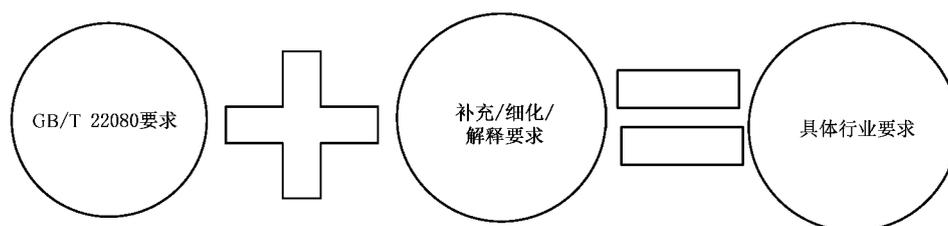


图 1 具体行业要求的构建

5.2 补充要求

允许给出补充要求的规范。

示例：对信息安全方针有补充要求的行业，可将其补充到 GB/T 22080—2016 的 5.2 规定的要求中。

对 GB/T 22080 要求进行补充不应删除 GB/T 22080 确定的任一要求或使其失效。具体行业对 GB/T 22080 要求的补充，应按照附录 A 给定的要求和指南进行。

5.3 细化要求

允许对 GB/T 22080 的要求进行细化。

注：细化不会删除 GB/T 22080 的任一要求或使其失效(见 3.2)。

GB/T 22080 要求在具体行业的细化，应按照附录 A 给定的要求和指南进行。

示例 1：具体行业标准可能包含对 GB/T 22080—2016 附录 A 的补充控制。在这种情况下，GB/T 22080—2016 的 6.1.3 c) 和 d) 中与信息安全风险处置相关的要求，需进行细化，以包含具体行业标准中给出的补充控制。

允许给出符合 GB/T 22080 要求的特定方法的规范。

示例 2：特定行业有规定的方法确定在具体行业管理体系范围内工作人员的能力。这一要求能细化 GB/T 22080—2016 的 7.2 中的通用要求。

5.4 解释要求

允许对 GB/T 22080 的要求作出解释。

注：解释不会使 GB/T 22080 的任一要求失效，只是对其作出解释或将其放入具体行业背景中(见 3.1)。

对 GB/T 22080 要求在具体行业作出解释，应按照附录 A 给定的要求和指南进行。

6 补充或修改 GB/T 22081 指南

6.1 总则

图 2 阐明了如何对 GB/T 22081 的指南进行补充和修改。

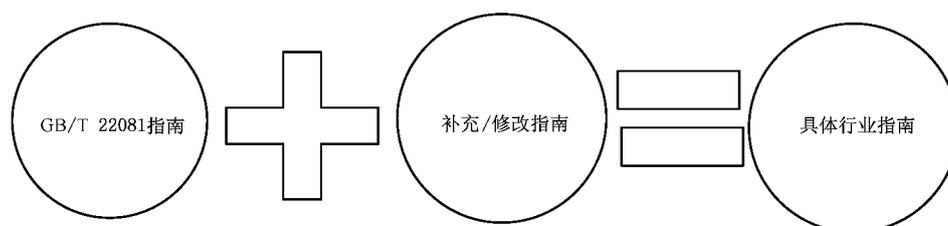


图 2 具体行业指南的构建

每项控制应仅包含一个“宜”。

注：在 GB/T 22080—2016 中，信息安全风险处置要求组织陈述所选择的控制及其选择的合理性说明，以及对附录 A

控制删减的合理性说明。在控制描述中只使用一个“宜”，可明确控制的范围。

6.2 补充指南

允许对 GB/T 22081 的章节、控制目标、控制、实现指南和其他信息进行补充。

对 GB/T 22081 补充章节、控制目标、控制、实现指南和其他信息，应按照附录 A 给定的要求和指南进行。

在规定补充章节、控制目标或控制之前，制定与 GB/T 22080 相关具体行业标准的机构宜考虑是否有更有效的方法来修改 GB/T 22081 已有内容，或是否有更有效的方法在 GB/T 22081 已有内容之上补充具体行业控制目标、控制、实现指南和其他信息来达成期望的结果。

6.3 修改指南

允许对 GB/T 22081 的章节、控制目标、控制、实现指南和其他信息进行修改。

任何修改不应删除 GB/T 22081 的控制、使其失效或减弱。

对 GB/T 22081 章节、控制目标、控制、实现指南和其他信息的修改，应按照附录 A 给定的要求和指南进行。

附 录 A (规范性附录)

制定与 GB/T 22080—2016 或 GB/T 22081—2016 相关的具体行业标准的模板

A.1 起草说明

A.2 中使用了如下格式规则：

——尖括号〈〉中的文本需用适宜的具体行业文本代替；

示例：对于电信行业，A.2 模板中第 4 章的标题，“〈行业〉—具体要求...”宜变为“电信行业具体要求...”。

——花括号 {} 中斜体的文本表示如何使用模板的此部分；本部分文本在具体行业标准发布版本中需删除；

——没有特殊格式的文本可逐字复制。

A.2 模板

0 引言

{包含：本标准中的要求和(或)指南，如何与 GB/T 22080 中规定的要求及 GB/T 22081 中的指南相关联。}

1 范围

{包含：适用范围的声明，该声明包含了本标准与 GB/T 22080 及 GB/T 22081 的关系。}

2 规范性引用文件

{插入相关的规范性引用文件，包含 GB/T 22080 和 GB/T 22081。}

3 术语和定义

{确保包含 GB/T 29246。}

4 与 GB/T 22080 相关的〈行业〉具体要求

{插入以下文本。}

4.1 本标准结构

本标准是与 GB/T 22080 相关的〈行业〉标准。

{如果具体行业标准有在 GB/T 22081 基础上补充或修改的具体行业章节、控制目标或控制，插入以下文本。}

〈行业〉具体参考控制目标和控制参见附录 A。

{如果有，插入描述具体行业 ISMS 问题的子章节。}

4.2 〈行业〉具体要求

{在适当的情况下，插入下列两段文本中的一段。}

对 GB/T 22080—2016 第 4 章到第 10 章的所有要求，仍适用。{或}

对 GB/T 22080—2016 第 4 章到第 10 章的所有要求，未在下面列出的，仍适用。

{补充具体行业要求。对补充要求，使用与 GB/T 22080—2016 相同格式的章节(子章节)号，并对行业使用国民经济行业名称(参见 GB/T 4754—2017)作为前缀。当补充一项要求时，首先检查它是否与 GB/T 22080—2016 中已有要求相关。如果是相关的，将新要求补充到相关的章节中并给予恰当序号。如果不相关，将补充要求置于 GB/T 22080—2016 相关要求之后，在章节中引入一个适宜的新子章节号。}

{通过插入以下文本来表示补充到 GB/T 22080—2016 要求上的具体行业要求。}

GB/T 22080—2016 要求(章节(子章节)号)补充如下:

{通过插入以下文本来表示对 GB/T 22080—2016 要求进行细化的具体行业要求。}

GB/T 22080—2016 要求(章节(子章节)号)细化如下:

{通过插入以下文本来表示对 GB/T 22080—2016 要求作出解释的具体行业要求。}

GB/T 22080—2016 要求(章节(子章节)号)解释如下:

{如果可能,请使用斜体表示补充、细化或解释的内容。}

{如果具体行业标准有针对具体行业的控制,则插入以下文本。}

GB/T 22080—2016 中 6.1.3 c)的要求细化如下:

将 6.1.3 b)确定的控制、GB/T 22080—2016 中附录 A 以及本文件附录 A 中的控制进行比较,并验证没有忽略必要的控制。

GB/T 22080—2016 中 6.1.3 d)的要求细化如下:

制定一个适用性声明,包含:

——必要的控制[见 GB/T 22080—2016,6.1.3 b)和 c)];

——选择这些控制的合理性说明(无论这些必要的控制是否已实现);

——对 GB/T 22080—2016 中附录 A 或本文件附录 A 中的控制删减的合理性说明。

{要强制应用某些特定控制,请在 GB/T 22080—2016,6.1.3 d)之后插入以下文本,并以恰当的方式识别强制控制,建议使用(强制)作为控制编号的前缀。}

组织应实现由(行业)识别的强制控制。

5 与 GB/T 22081—2016 相关的(行业)具体指南

{如果具体行业标准有在 GB/T 22081—2016 基础上补充或修改的具体行业章节、控制目标、控制、实现指南或其他信息,在本章节插入它们。补充章节、控制目标或控制的序号与 GB/T 22081—2016 采用相同格式,并对行业使用国民经济行业名称(参见 GB/T 4754—2017)作为前缀。当对 GB/T 22081—2016 控制目标、控制、实现指南和(或)其他信息补充或修改时,首先检查它是否与 GB/T 22081—2016 中已有控制目标、控制、实现指南和(或)其他信息相关。如果是相关的,补充或修改新控制目标、控制、实现指南和(或)其他信息到 GB/T 22081—2016 相关的章节中并相应编号。如果不相关,将补充条目放置到 GB/T 22081—2016 已有章节、控制目标或控制之后。}

{插入以下文本。}

对 GB/T 22081—2016 所有的章节、控制目标、控制、实现指南和其他信息,未在下面列出的,仍适用。

{通过插入以下文本来表示补充到 GB/T 22081—2016 的具体行业章节。}

GB/T 22081—2016 的章节补充如下:

{通过在恰当章节之后插入以下文本来表示补充到 GB/T 22081—2016 的具体行业控制目标。}

GB/T 22081—2016(章节号)[(章节标题)]的控制目标补充如下:

{通过在恰当的控制目标之后插入以下文本来表示补充到 GB/T 22081—2016 的具体行业控制;确保控制目标反映补充的具体行业控制,并确保该补充不会使任何已有控制失效。}

补充到 GB/T 22081—2016(控制目标号)[(控制目标标题)]的控制补充如下:

{当修改控制目标、控制、实现指南或其他信息时(例如通过修改或补充到已有文本),根据 GB/T 22081—2016 要求重新进行理解。根据需要插入以下任一项来表示对 GB/T 22081—2016 中控制目标或控制的具体行业修改。}

(控制目标号)[(控制目标标题)]修改如下:

{或}

(控制号)[(控制标题)]修改如下:

{如果已有控制未被修改,仅给出补充的指南,根据需要插入以下标题之一。}

GB/T 22081—2016<控制号>[<控制标题>]的实现指南补充如下:

GB/T 22081—2016<控制号>[<控制标题>]的其他信息补充如下:

{建议使用斜体表示补充的或修改的文本。}

{如果具体行业标准具有根据 GB/T 22081—2016 补充的或者修改的具体行业章节、控制目标或控制,以与 GB/T 22081—2016 附录 A 相同的方式构建规范性附录 A,并在适用时用“应”代替“宜”。附录的名称和标题如下。}

附录 A

(规范性附录)

<行业>-具体参考控制目标和控制

{下面介绍表 A.1。}

表 A.1 中所列的补充或修改的控制目标和控制,是直接来源于本标准并与之相对应,并用于本标准细化的 GB/T 22080—2016,6.1.3 环境中。

附 录 B

(资料性附录)

面向医疗行业的信息安全管理体系指南示例

B.1 说明

本附录参考 ISO 27799:2016,依据信息安全管理体在医疗行业具体应用实践,形成面向医疗行业的信息安全管理体系标准。其中“5 与 GB/T 22081—2016 相关的医疗行业指南”中,从 ISO 27799:2016 的 5.1.1、6.1.5 和 9.1.1 选取部分控制、实现指南和其他信息,补充或修改后作为医疗行业指南示例。

本附录的目的不是为了形成完善的面向医疗行业的信息安全管理体系指南,仅是给出面向行业的信息安全管理体系指南的示例,便于理解本标准并推动本标准落地实施。

B.2 面向医疗的信息安全管理体系

如下为依据附录 A 选取医疗行业给出的面向医疗行业的信息安全管理体系指南。

1 范围

本标准规定了 GB/T 22080 应用于医疗行业时补充、细化和作出解释的要求,以及和 GB/T 22081 应用于医疗行业时补充和修改的指南。

本标准适用于医疗行业构建包含其特定要求的信息安全管理体系。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。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)适用于本文件。

GB/T 22080—2016 信息技术 安全技术 信息安全管理体 要求(ISO/IEC 27001:2013, IDT)

GB/T 22081—2016 信息技术 安全技术 信息安全控制实践指南(ISO/IEC 27002:2013, IDT)

GB/T 29246—2017 信息技术 安全技术 信息安全管理体 概述和词汇(ISO/IEC 27000:2016, IDT)

3 术语和定义

GB/T 29246—2017 界定的术语和定义适用于本文件。

4 与 GB/T 22080 相关的医疗行业要求

4.1 本标准结构

本标准是与 GB/T 22080 相关的具体行业标准。

医疗行业具体参考控制目标和控制参见附录 A。

4.2 医疗行业要求

对 GB/T 22080—2016 第 4 章~第 10 章的所有要求,未在下面列出的,仍适用。

GB/T 22080—2016 要求 7.1 解释如下:

在医疗行业,机构应提供信息安全管理体所需的医疗专业人员、医疗设备、场地、医疗信息系统、办公设备等医疗资源。

GB/T 22080—2016 要求 7.2 细化如下：

医疗行业机构工作人员应：

- a) 定期核查经过专业认证的医疗专业人员的能力,可通过测试、现场操作等方式进行；
- b) 定期组织相关医疗专业能力培训、进修等相关活动,组织新进人员参加相关培训、进修活动,并对参加活动人员进行考核后方可进行上岗；
- c) 对医疗专业人员的考核成绩进行定期分析,作为后续开展核查、培训等工作的依据。

GB/T 22080—2016 中 7.3 补充如下：

医疗行业机构工作人员应了解个人医疗信息保护的相关政策和要求。

GB/T 22080—2016 中 6.1.3 c) 的要求细化如下：

将 6.1.3 b) 确定的控制、GB/T 22080—2016 中附录 A 以及本文件附录 A 中的控制进行比较,并验证没有忽略必要的控制。

GB/T 22080—2016 中 6.1.3 d) 的要求细化如下：

制定一个适用性声明,包含：

- 必要的控制[见 GB/T 22080—2016, 6.1.3 b) 和 c)]；
- 选择这些控制的合理性说明(无论这些必要的控制是否已实现)；
- 对 GB/T 22080—2016 中附录 A 或本文件附录 A 中的控制删减的合理性说明。

5 与 GB/T 22081—2016 相关的医疗行业指南

对 GB/T 22081—2016 所有的章节、控制目标、控制、实现指南和其他信息,未在下面列出的,仍适用。

GB/T 22081—2016 中 5.1.1[信息安全策略]修改如下：

处理医疗信息(包括个人医疗信息)的组织,需有书面的信息安全策略,由管理者批准,并发布传达给所有医疗人员和外部相关方。

GB/T 22081—2016 中 6.1.5[项目管理中的信息安全]的控制补充如下：

在涉及个人医疗信息处理的项目中,医疗项目管理宜将患者安全视为项目风险。

GB/T 22081—2016 中 6.1.5[项目管理中的信息安全]实现指南补充如下：

在涉及个人医疗信息处理的项目中,患者安全是项目风险评估的重要组成部分。需对患者安全的风险进行仔细的分析 and 明确的处理。

GB/T 22081—2016 中 9.1.1[访问控制策略]的其他信息补充如下：

关于医疗保健相关应用程序的访问控制的补充指南参见 ISO 22600。

附录 A

(规范性附录)

医疗行业具体参考控制目标和控制

表 A.1 中所列的补充或修改的控制目标和控制,是直接来源于本标准并与之相对应,并用于本标准细化的 GB/T 22080—2016, 6.1.3 环境中。

表 A.1 补充或修改的控制目标和控制

A.5 信息安全策略		
A.5.1 信息安全管理指导		
A.5.1.1	信息安全策略	<p>医疗行业控制(修改)</p> <p>处理医疗信息(包括个人医疗信息)的组织,需有书面的信息安全策略,由管理者批准,并发布传达给所有医疗人员和外部相关方。</p>

表 A.1 (续)

A.6 信息安全组织		
A.6.1 内部组织		
A.6.1.1	项目管理中的信息安全	医疗行业控制(补充) 在涉及个人医疗信息处理的项目中,医疗项目管理宜将患者安全视为项目风险。

参 考 文 献

- [1] GB/T 4754—2017 国民经济行业分类
- [2] GB/T 32920—2016 信息技术 安全技术 行业间和组织间通信的信息安全管理 (IEC 27010:2012;IDT)
- [3] ISO/IEC Directives, Part 1, Consolidated ISO Supplement, 2016
- [4] ISO 22600 Health informatics—Privilege—Management and access control
- [5] ISO/IEC 27011:2008 Information technology—Security techniques—Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
- [6] ISO/IEC 27017:2015 Information technology—Security techniques—Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- [7] ISO/IEC 27018:2014 Information technology—Security techniques—Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- [8] ISO 27799:2016 Health informatics—Information security management in health using ISO/IEC 27002
-

中 华 人 民 共 和 国
国 家 标 准
信 息 技 术 安 全 技 术
GB/T 22080 具体行业应用 要求
GB/T 38631—2020

*

中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)

网址:www.spc.org.cn

服务热线:400-168-0010

2020年4月第一版

*

书号:155066·1-64416

版权专有 侵权必究



GB/T 38631-2020