ICS 35.240.80
CCS C30

ZMDS

中关村医疗器械产业技术创新联盟团体标准

T/ZMDS 20007-2023

健康软件和健康 IT 系统安全性、有效性和网络安全—第 1 部分：原则和概念

Health software and health IT systems safety, effectiveness and security —Part1: Principles and concepts

（ISO 81001-1:2021, IDT）

2023-12-29 发布　　2023-12-29 实施

中关村医疗器械产业技术创新联盟　　发布

目 录

前　言

本文件按照GB/T 1.1－2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件使用翻译法等同采用IEC 81001-1:2021。

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专利的责任。本

文件由中关村医疗器械产业技术创新联盟提出。

本文件由中关村医疗器械产业技术创新联盟标准化技术委员会归口。

本文件起草单位：北京怡和嘉业医疗科技股份有限公司， 通用电气医疗系统贸易发展（上海）有限公司，飞利浦（中国）投资有限公司。

本文件主要起草人：秦川，谌达宇，陈兴文，陈蓓。

引　言

尽管数字医疗的优势已受到广泛接受，但健康软件和健康IT系统对安全性、有效性和网络安全造成的潜在的意外及负面影响也越来越明显。 当今复杂的健康软件和健康IT系统已提供了更为先进的决策支持，并在系统之间、组织之间和持续护理中各阶段间整合了患者数据。 在因此给患者和医疗系统带来的利益之外，这也增加了因软件引起的不良事件对患者和医疗机构造成伤害的可能性。 其中，设计缺陷、编码错误、实施或配置错误、数据完整性问题、决策支持工具故障、与临床工作流程不一致以及对该软件和系统的不当维护和使用都是造成伤害事件的典型示例。

管理健康软件和健康IT系统（包括医疗器械）的安全性、有效性和网络安全这三种属性，需要采取综合的和协调的方法来进行优化。 许多组织和角色参与了健康软件和健康IT系统的整个生存周期（参见图1）。 因此，对概念、原则和术语的共同理解，对于规范流程和跨组织间的沟通，以支持使用协调的方式管理安全性、有效性和网络安全就体现得至关重要。 本文件也将在医疗保健领域不断发展的复杂的内外部环境考虑在内，包括人员、技术（硬件/软件）、组织、流程和外部环境。

附录A提供了本文件、正在使用的术语和定义及其与其他健康软件和健康IT系统安全性、有效性和网络安全各方面标准有关的理论依据。

除了一套共同的术语、定义和概念外，本文件在第5条中描述了八个基本要素，它们支持第4条中阐述的主题思想。 对于每个基本要素，都包括描述要素的"声明"；解释其重要性的"理论依据"；与管理安全性、有效性和网络安全有关的"关键概念和原则"；以及有关组织可以采取的应用这些概念和原则的"方法"的高级指南。

鉴于在健康软件和健康IT系统的整个生存周期中，各组织、角色和责任间的沟通对四个跨组织基本要素的重要性，5.3.2、5.3.3、5.3.4和5.3.5节中包含了有关主要转换点的沟通和信息共享的额外子条款。

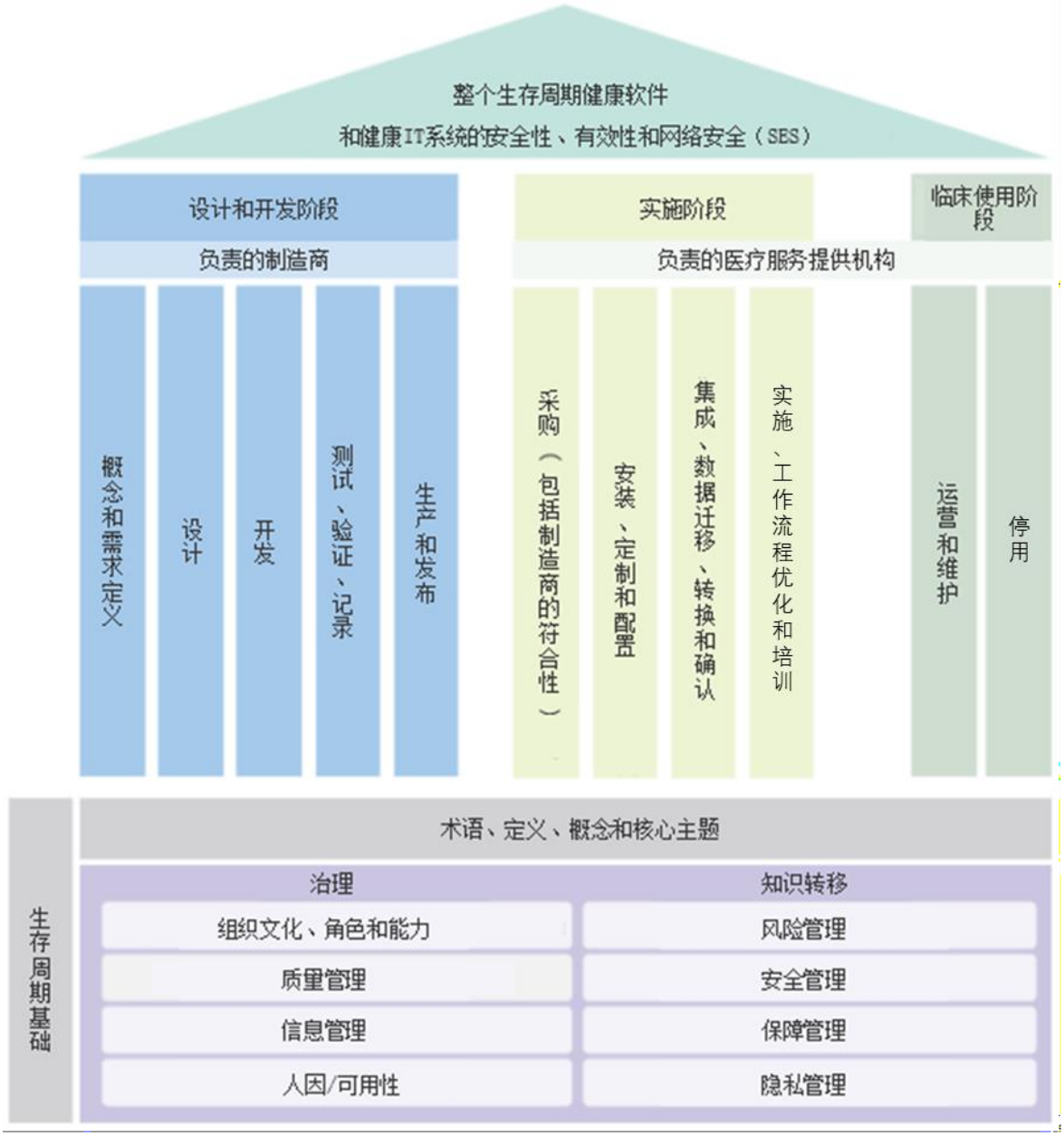

图1 涉及健康软件和健康IT系统的安全性、有效性和网络安全的生存周期框架

健康软件和健康 IT 系统的安全性、有效性和网络安全
—第 1 部分：原则和概念

1 范围

1.1 目的

本文件提供了健康软件和健康IT系统的原则、概念、术语和定义，以及从概念到停用的整个生存周期内安全性、有效性和网络安全的关键属性，如图1所示。它还确定了生存周期中发生责任转移的转换点，以及在这些转换点上有必要进行的多边沟通类型。该文件还为其他涉及健康软件和健康IT系统的安全性、有效性和网络安全（包括隐私保护）方面的专用标准建立了统一的概念和标准术语。

1.2 应用领域

本文件适用于参与健康软件和健康IT系统生存周期的所有相关方如下：

a) 设计、开发、集成、实施和操作这些系统的组织、健康信息学专业人员和临床主管人员--例如健康软件开发商和医疗器械制造商、系统集成商、系统管理者（包括云和其他信息技术服务提供商）。

b) 医疗服务提供机构、医疗服务提供商和其他使用这些系统提供医疗服务的人员。

c) 寻求对组织能力有信心，能为组织持续提供安全、有效和可靠的健康软件、健康IT系统和服务的政府、健康系统资助者、监管机构、专业组织，客户；

d) 通过对安全性、有效性和网络安全管理中使用的概念和标准术语的共同理解，在管理安全性、有效性和网络安全风险的方面寻求改善沟通的组织和利益相关方。

e) 在健康软件和健康IT系统的安全性、有效性和网络安全风险管理方面可提供培训、评估或建议的提供商。

f) 安全性、有效性和网络安全标准相关的制定者。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1 组织、人员和角色

3.1.1

管理者 administrator

负责已实施的健康IT系统（3.3.8）的持续运营并确保其得到持续保护和维护的角色（3.1.10）。

3.1.2

客户 customer

可能或实际收到预期提供或者要求提供的产品（3.3.15）或服务的个人或组织（3.1.8）。

注1：客户可以来自组织内部或外部。

[来源：ISO 9000:2015，3.2.4，修改--实例删除。]

3.1.3

开发者 developer

负责执行健康软件（3.3.9）或健康IT系统（3.3.8）的设计和开发阶段（从概念到发布和维护）的实体。

注：例如，开发者可以是制造组织（3.1.8）、服务供应商或医疗保健服务组织（3.1.4）的一部分。

3.1.4

医疗服务提供机构 healthcare delivery organization HDO

提供医疗服务的场所或企业，如诊所或医院。

3.1.5

实施者 implementer

负责健康软件（3.3.9）和健康IT系统（3.3.8）的临床安装、工作流程优化和培训的实体。

注：实施者可以是制造商（3.1.7）、医疗服务提供机构（3.1.4）或第三方。

3.1.6

集成商 integrator

负责将医疗服务提供机构（3.1.4）使用的组件（3.3.5）纳入健康IT基础设施（3.3.7）的实体，包括技术安装、配置和数据迁移。

3.1.7

制造商 manufacturer

负责设计或制造产品的组织（3.1.8）（3.3.15）。

3.1.8

为实现目标，由职责、权限和相互关系构成自身功能的一个人或一组人。**注：**组织的概念包括，但不限于代理商、公司、集团、商行、企事业单位、行政机构、合营公司、协会、慈善机构或研究机构，或上述组织的部分或组合，无论是否为法人组织，公有的或私有的。

[来源：GB/T 19000-2016，3.2.1，有修改]

3.1.9

责任协议 responsibility agreement

充分界定所有利益相关方责任的文件

注：该协议可以是一份法律文件，例如，一份合同。

3.1.10

角色 role

职能或职位

[来源：GB/T 30107-2013] 。

3.1.11

护理对象 subject of care

寻求接受、正在接受或已经接受医疗服务的人员

[来源：ISO 13940:2015，5.2.1，有修改]

3.1.12

系统所有者 system owner

负责确保正在获取和实施的健康IT系统（3.3.8）能够满足其组织（3.1.8）医疗服务需求并实现其预期用途（3.2.7）的高级管理人员。

3.1.13

最高管理层 top management

行政管理层

指挥和控制组织（3.1.8）并且在组织中负有全面责任的一群人员。

3.1.14

用户 user

为满足健康相关目的使用该系统的人员（3.3.17）。

注：用户可以是直接的护理对象，也可以是协助（作为代理）护理对象的个人。

3.2 关键属性和过程

3.2.1

变更管理 change management

记录、协调、批准和监测所有变更的过程（3.2.10）

[来源：ISO/IEC TS 22237-7:2018, 3.1.3] 。

3.2.2

变更-发布管理 change-release management

确保对健康IT基础设施（及其组件（3.3.5）的所有变更以受控的方式进行评估、批准、实施和审查，并确保变更的交付、分发和跟踪，继而确保在适当的投入和产出的配置管理下，以受控的方式发布变更的过程（3.2.10）。

3.2.3

临床变更管理 clinical change management

支持人们及其组织（3.1.8）成功转换和采用电子健康解决方案的战略性和系统性过程（3.2.10）。重点关注结果，包括用户（3.1.14）采用的解决方案和受益的实现。

注1：改编自参考资料[39]。

3.2.4

配置管理 configuration management

确保健康IT基础设施（3.3.7）内组件（3.3.5）的配置信息以准确和受控的方式定义和维护，并提供一套机制来识别、控制和跟踪健康IT基础设施版本过程（3.2.10）

注1：改编自ISO/IEC 20000-1:2018，8.2.6。

3.2.5

有效性 effectiveness

产生预期效果的能力

3.2.6

实施 implementation

生存周期（3.3.12）的阶段，在此阶段结束时，系统的硬件、软件和程序（3.3.17）可以正常运行。［来源：ISO/IEC 2382:2015, 2122692, 有修改］

3.2.7

预期用途 intended use

预期目的 intended purpose

按照制造商提供的说明书、操作指南和信息，对产品（3.3.15）、过程（3.2.10）或服务的预期使用（3.1.7）。

注：预期的医学指征、患者群体、与医疗器械交互的身体部位或组织类型、用户特征、使用环境和工作原理是预期用途的典型要素。

［来源：ISO/IEC指南63:2019，3.4，有修改］

3.2.8

关键属性 key properties

安全（3.2.12）、有效性（3.2.5）和网络安全（3.2.13）三个风险管理（3.4.16）特征。

3.2.9

隐私 privacy

个人私人生活或事务不受侵扰的自由。 其侵扰主要来自不适当或非法收集和使用有关个人的数据。［来源：ISO/TS 27790:2009，3.56］。

3.2.10

过程 process

利用输入实现预期结果的相互关联或相互作用的一组活动。

［来源：GB/T 19000-2016，3.4.1，有修改］

3.2.11

质量 quality

产品（3.3.15）、过程（3.2.10）或服务的所有属性和特征满足产品、过程或服务使用目的所产生的要求的程度。

［来源：ISO/TS 13972:2015，2.45，有修改］

3.2.12

安全性 safety

免于不可接受的风险（3.4.10）

[来源：ISO/IEC指南63：2019，3.16]

3.2.13

网络安全 security/cybersecurity

信息和系统（3.3.17）受到保护的状态，未经授权的活动如访问、使用、披露、破坏、修改或毁坏被限制在一定的程度，使其保密性、完整性和可得性相关的风险（3.4.10）在整个生存周期内保持在可接受的水平（3.3.12）。**注：**在信息安全领域availability译为可用性，而在医疗器械领域usability译为可用性，为避免引起歧义本标准将availability译为可得性。

3.2.14

网络安全能力 security capability

从技术方面、行政方面或组织方面对数据和系统的保密性、完整性、可得性和可问责性相关的风险（3.4.10） 进行管理的控制措施的宽泛类别（3.3.17）。管理数据和系统的保密性、完整性、可得性和责任性风险（3.4.10）的技术、行政或组织控制的大类（3.3.17）。3.2.15

可用性 usability

为了便于使用从而在预期的使用（3.2.7）环境中建立有效性（3.2.5）、效率和用户满意度的用户（3.1.14）接口的特性。

注：包括有效性、效率和用户满意度在内的可用性的所有属性会提高或降低安全性（3.2.12）。［来源：IEC 62366-1:2015，3.16］。

3.2.16

验证 verification

通过提供客观证据对规定要求已得到满足的认定。

注1：验证所需的客观证据可以是检查的结果，也可以是其他形式的判定，如进行替代计算或审查文件。

注2：为验证而进行的活动有时称为鉴定过程（3.2.10）。

注3："已验证"一词用来指定相应的状态。

3.3 **[来源：ISO 9000:2015 GB/T 19000-2016，3.8.12]健康信息和技术**

3.3.1

随附资料 accompanying information

随附文件 accompanying document

随附文档 accompanying documentation

标记在健康IT（3.3.6）、产品（3.3.15）或用户（3.1.14）附件上的随附信息，或负责安装、使用、处理、维护、停用和处置医疗器械（3.3.13）或附件的随附信息，特别是有关安全使用的随附信息。

3.3.2

资产 asset

对个人、组织（3.1.8）或政府有价值的任何物理或数字实体

[来源：ISO/IEC 27032:2012，4.6，有修改]

3.3.3

云计算 cloud computing

支持网络访问可扩展的，弹性的物理或虚拟资源共享池的范例，并可按需进行自助配置和管理。[来源：ISO/IEC 17788:2014, 3.25]

3.3.4

云服务 cloud service

通过云计算（3.3.3）使用已定义接口调用的一项或多项能力。

[来源：ISO/IEC 17788:2014, 3.2.8]

3.3.5

组件 component

系统（3.3.17）资源的集合，（a）构成系统的物理或逻辑部分，（b）具有指定的功能和接口，（c）视为（例如，通过策略或规范）独立于系统其他部分而存在。

[来源：IETF RFC 4949，有修改]

3.3.6

健康信息技术 health information technology

健康IT health IT

记录并预期应用信息技术来收集、储存、处理、检索和交流与健康、患者护理和身心健康有关的信息的技术。

3.3.7

健康IT基础设施 health IT infrastructure

个人或组织（3.3.2）可用来开发、配置、整合、维护和使用IT服务并支持健康、患者护理和其他组织目标的一套IT资产组合（3.3.2）。

注：健康IT基础设施可以包括以下内容：

a）数据和信息；

b）健康软件（3.3.9）；

c）医疗器械（3.3.13）；

d）IT硬件和服务，包括移动和桌面设备、IT网络（3.3.11）、数据中心、网络安全（3.2.13）、软件开发、IT运维和外部提供的服务，如互联网、SaaS和云计算（3.3.3）；

e）人员，以及他们的资质、技能和经验；　　f）

管理和支持健康IT基础设施的技术程序和文件；

g）通过利用上述资产（3.3.2）配置和实施，以实现组织目标的健康IT系统（3.3.8）

h）无形资产，如声誉和形象。

3.3.8

健康IT系统 health IT system

相互作用的健康IT（3.3.6）要素的组合，其配置和实施是为了支持和实现个人或组织的（3.1.8）具体健康目标。

注：这些要素包括健康软件（3.3.9）、医疗器械（3.3.13）、IT硬件、接口、数据、程序和文档）。

3.3.9

健康软件 health software

专门用于管理、维护或改善个人健康或提供护理，或为植入医疗器械而开发的软件（3.3.13）。

注：健康软件包括医疗器械独立软件。（Software as a Medical Device，SaMD）。[

来源：GB/T 42984.1-2023，3.18，有修改。]

3.3.10

互操作性 interoperability

两个或多个系统（3.3.17）或组件（3.3.5）交换信息和使用已交换信息的能力。

[来源：参考资料[50]]

3.3.11

IT网络 IT network

系统（3.3.17）或由通信节点和传输链路组成的系统，在两个或多个指定的通信节点之间提供物理连接或无线传输 注1。改编自IEC 61907:2009，3.1.1。

3.3.12

生存周期 life cycle

在产品（3.3.15）或系统（3.3.17）的生命周期中的所有阶段，包括最初构想到最后停用和处置。[

来源：ISO/IEC指南63:2019，3.5，有修改]

3.3.13

医疗器械 medical device

制造商（3.1.7）为用户单独或组合使用提供的仪器、设备、工具、机器、器具、植入物、体外使用的试剂、软件、材料或其他类似或相关的物品，用于实现以下一个或多个具体的医疗目的

- 对疾病的诊断、预防、监测、治疗或缓解
- 对损伤的诊断、监测、治疗、缓解或代偿
- 对解剖或生理过程的研究、替换、修改或支持
- 对生命的支持或维持
- 对受孕的控制
- 对医疗器械的消毒
- 通过对来自人体的标本进行体外检查来提供信息

并非通过药理学、免疫学或代谢手段在人体内外实现其主要的预期作用，但可以通过这些手段协助其实现预期功能

注：在某些司法管辖区可视为医疗器械的产品（3.3.15）但在某些司法管辖区不视为医疗器械产品，包括：

- 消毒物质；
- 残疾人的辅助工具；
- 含有动物和/或人体组织的设备；
- 用于体外受精或辅助生殖技术的设备。[

来源：ISO/IEC指南63：2019，3.7]

3.3.14

个人健康信息 personal health information

与个人身体或精神健康有关的可识别人员的信息

注1：为个人提供健康服务，其中可能包括：

a) 关于提供健康服务的个人注册信息。

b) 关于个人的医疗支付或健康服务资格信息。

c) 以满足健康目的分配给个人作为唯一识别的编号、符号或特定物品，。

d) 在向个人提供健康服务的过程中收集的有关个人的任何信息；

e) 通过身体部位或身体物质的测试或检查获得的信息。f

）确定某人（如健康专业人员）为个人的保健提供者。

注2：个人健康信息不包括本身或与持有人所掌握的其他信息相结合的匿名信息，即无法从该信息中确定作为信息主体的个人身份。

[来源：ISO 27799:2016，3.8]

3.3.15

产品 product

在组织和顾客（3.1.2）之间未发生任何交易的情况下，组织（3.1.8）能够产生的输出。**注1**：在供方和顾客之间未发生任何必要交易的情况下，可以实现产品的生产。但是，当产品交付给顾客时，通常包含服务因素。

注2：产品的主导因素一般是有形的。

[来源：GB/T 19000-2016，3.7.6，有修改]

3.3.16

社会技术生态系统 sociotechnical ecosystem

复杂的"生态系统"或"社会技术系统"环境，在此环境下，软件与其他系统（3.3.17）、技术、基础设施和领域（人、组织（3.1.8）和外部环境）紧密结合，并配置为支持本地临床和商业过程（3.2.10）。

3.3.17

系统 system

为实现一个或多个所声称的目标而组织的相互作用的要素组合

[来源：ISO/IEC/IEE 15288。2015年，4.1.46，有修改]

3.4 风险管理

3.4.1

保证案例 assurance case

合理、可供审核的物品，其创建是为了提供论据，以证明其顶层声称获得了满足，其中包含了系统的论点及其底层论据和支持该声称的明确假设。**注**：保证案例包含以下内容及其关系：

—— 一项或多项有关属性的声称；

——证据和任何假设与声称之间有逻辑联系的论证；

—— 支持这些论证的一系列证据和可能的假设；以及

—— 选择顶级声称和推理方法的理由。

[来源：ISO/IEC/IEEE 15026-1:2019, 3.1.2] 。

3.4.2

事件 event

某一特定情况集合的产生或变化

注1：一个事件可以是单次或多次发生，可以有数个原因。

注2：一个事件可以由没有发生的事情组成。

注3：一个事件有时可以称为"事件"或"意外事件"。

[来源：ISO指南73:2009，3.5.1.3，有修改]

3.4.3

利用 exploit

通过漏洞（3.4.22）破坏系统网络安全（3.2.13）的确定方式（3.3.17）。

[来源：ISO/IEC 27039:2015，2.9，有修改]。

3.4.4

暴露 exposure

组织（3.1.8）和/或利益相关方方受事件影响的程度（3.4.2）。

[来源：ISO指南73:2009，3.6.1.2] 。

3.4.5

伤害 harm

对人健康的损伤或损害，或对财产或环境的损害

[来源：ISO/IEC指南63：2019，3.1]

3.4.6

危险 hazard

伤害（3.4.5）潜在的根源。

[来源：ISO/IEC指南63：2019，3.2]

3.4.7

危险情况 hazardous situation

人员、财产或环境暴露于一种或多种危险（3.4.6）中的情形。

[来源：ISO/IEC指南63：2019，3.3]

3.4.8

可合理预见的误使用 reasonably foreseeable misuse

由容易预测的人的行为所引起的未按照制造商预期的方式对产品（3.3.15）或系统（3.3.17）的使用。

注1：容易预测的人的行为包括全部类型的用户（3.1.14）行为，例如非专业的和专业的用户。

注2：可合理预见的误使用可能是有意的或无意的。

[来源：ISO/IEC指南63:2019，3.8，有修改]

3.4.9

剩余风险 residual risk

实施风控（3.4.13）措施后仍存在的风险（3.4.10）。

[来源：ISO/IEC指南63：2019，3.9]

3.4.10

风险 risk

伤害（3.4.5）发生概率和严重度（3.4.20）的组合。

注：发生概率包括对危险情况的暴露（3.4.7）和避免或限制伤害的可能性。

[来源：ISO/IEC指南63：2019，3.10]

3.4.11

风险分析 risk analysis

系统性地使用可获得的信息以识别危险（3.4.6）和预估风险（3.4.10）。

[来源：ISO/IEC指南63：2019，3.11]

3.4.12

风险评估 risk assessment

包括风险分析（3.4.11）和风险评估（3.4.15）的全过程（3.2.10）。

[来源：ISO/IEC指南63：2014，3.11]

3.4.13

风险控制 risk control

做出决策并实施措施，以便降低风险（3.4.10)或将风险（3.4.10)维持在规定界限内的过程（3.2.10)。[来源：ISO/IEC指南63：2019，3.12]

3.4.14

风险预估 risk estimation

用于对伤害（3.4.5）发生概率和严重度（3.4.20）赋值的过程（3.2.10）。

[来源：ISO/IEC指南63：2019，3.13]

3.4.15

风险评估 risk evaluation

将已预估的风险（3.2.10）和给定的风险（3.2.10）准则进行比较，以确定风险可接受性的过程（3.4.10）。

[来源：ISO/IEC指南63：2019，3.14]

3.4.16

风险管理 risk management

将管理策略、程序及其实践系统性地应用于对风险（3.4.10）的分析、评估、控制和监视的活动。[来源：ISO/IEC指南63：2019，3.15]

3.4.17

风险管理文档 risk management file

由风险管理（3.4.16）产生的一组记录和其他文件。

[来源：GB/T 42062-2022 3.25]。

3.4.18

风险容忍度 risk tolerance

组织（3.1.8）或利益相关方在风险控制（3.4.13）之后，为实现其目标，做好承担风险的准备度（3.4.10）。

注：风险容忍度可能会受到法律或监管要求的影响。

[来源：ISO指南73:2009，3.7.1.3，有修改]

3.4.19

根本原因 root cause

在一系列事件（3.4.2）开始时出现的一些条件或动作，导致故障模式的启动。

[来源：ISO 13372:2012，8.9]

3.4.20

严重度 severity

对危险（3.4.6）导致的可能后果的衡量。

[来源：ISO/IEC指南63：2019，3.17]

3.4.21

威胁 threat

当可能违反网络安全并造成伤害（3.4.5）的情况、能力、行动或事件（3.4.2）存在时，存在违反网络安全（3.2.13）的可能性。

[来源：IEC指南120:2018，3.16] 。

3.4.22

漏洞 vulnerability

系统（3.3.17）设计、实施（3.2.6）或操作和管理中的缺陷或弱点（3.4.23），可被利用用于侵犯系统的网络安全（3.2.13）的策略。

[来源：IEC指南120:2018，3.18] 。

3.4.23

弱点 weakness

一种缺陷。

注1：弱点会导致网络安全（3.2.13）和/或隐私风险（3.2.9）。

注2：改编自参考资料[42]。

4 核心主题

4.1 概述

医疗保健领域的信息技术无处不在，并以复杂和相互关联的方式持续发展着。因此，随着联网设备和可互操作系统的大规模增长，所有利益相关方的活动变得更加相互依赖。对于所有参与其中的人来讲， 了解健康IT的整个生存周期非常重要。 这是为了确保他们能够对以前没有意识到的任何相互依赖性和关联做好计划和应对。 因此，这些利益相关方之间的互动对保持整个基础设施的安全性、有效性和网络安全管理的一致性必不可少。

如图2所示，六个核心主题为理解如何利用生存周期框架的八个基本要素（见图1）来制定一个有凝聚力的综合方法来解决安全性、有效性和网络安全问题提供了总体基础。

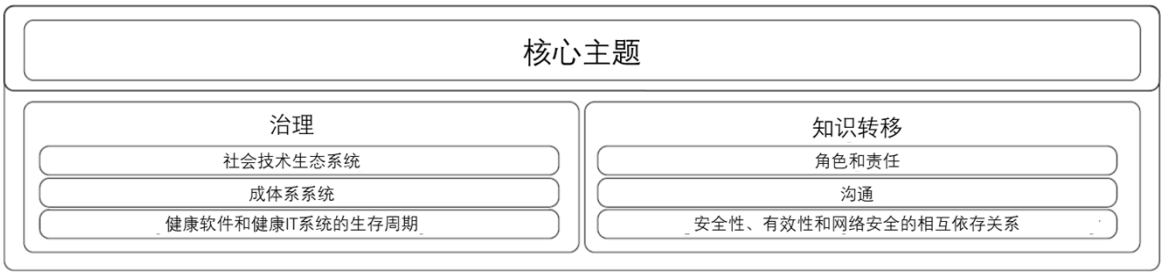

图2 核心主题

4.2 社会技术生态系统

一个互联、复杂的医疗生态系统的影响并不限于健康软件和健康IT系统。重要的是要考虑更大的社会技术环境（见图3），以及在生态系统的每个部分和通过这些部分的互动可能产生的对安全性、有效性和网络安全的潜在影响。此生态系统包括：

a) 健康IT基础设施（例如，硬件、软件、网络、与其他系统的接口、医疗器械和数据），以及参与开发、实施和运营许多健康IT组件和服务的组织。

b) 医疗服务环境（例如，临床医生、患者和其他相关人员、临床工作流程以及正在部署健康IT系统的具体组织环境），以及

c) 更广泛的医疗系统（例如，法规、资金和政策影响）；在该系统中，HDO（及其支持的健康IT系统/基础设施）必须合规运维。

注：此社会技术生态系统存在于一个外部环境中（例如，公众舆论、环境条件），因此也会受到外部的影响。

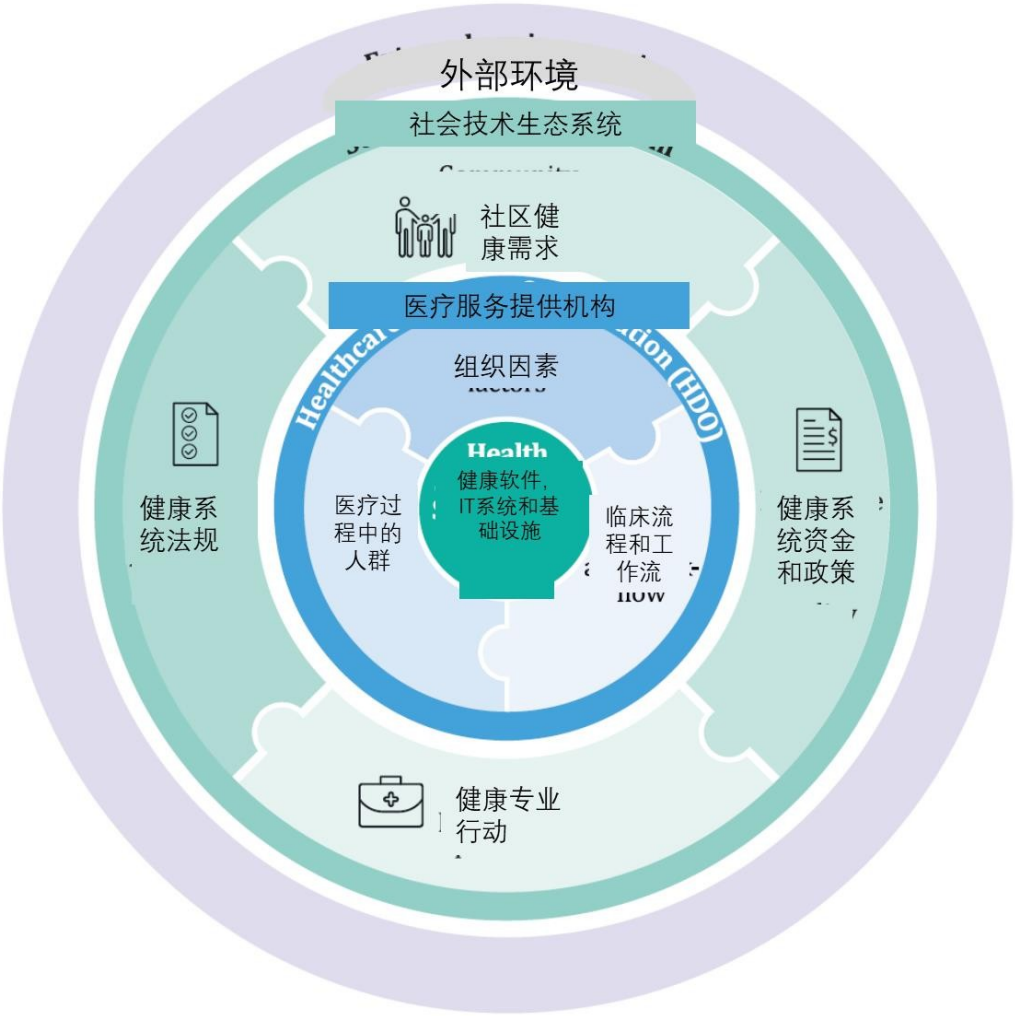

图3 健康软件和健康IT系统在其社会技术生态系统中的作用

研究表明，鉴于健康软件、健康IT系统和医疗器械在医疗保健领域的应用规模，涉及使用这些技术的安全和网络安全事件报告不足。对报告事件的定性和定量研究表明，在此生态系统中，造成患者伤害的根本原因是多样化的。此方面的示例包括软件和底层硬件的错误和故障、数据质量和完整性的缺陷、网络安全和隐私漏洞、决策支持算法上的故障、基础设施的失效、互操作性问题、记录不匹配、识别患者上的错误、人机接口错误、系统和工作过程间的不协调以及培训不足。

4.3 体系

在当今综合且复杂的健康IT基础设施中，健康软件、医疗器械、数据和其他健康IT组件的生存周期往往是相互依赖的。健康IT基础设施的所有元素都有自己的生存周期，每个健康IT系统及其子系统至少增加一个额外的生存周期。此外，每个整合的医疗器械都有自己的产品生存周期，遵循一套特定的监管要求，以保证其安全和有效使用。增加此种复杂性的是支持核心信息技术组件、服务和技术的大型基础设施，包括网络、数据中心和中间件。

重要的是，要确保生存周期的管理过程共同起作用，为每个患者提供有效的临床实践经验。图4强调了"体系"的复杂性，说明了典型的医疗交付机构健康IT基础设施中多样元素的相互依存关系，也展示了与互联网、云服务和经常涉及的其他组织的外部连接范围。

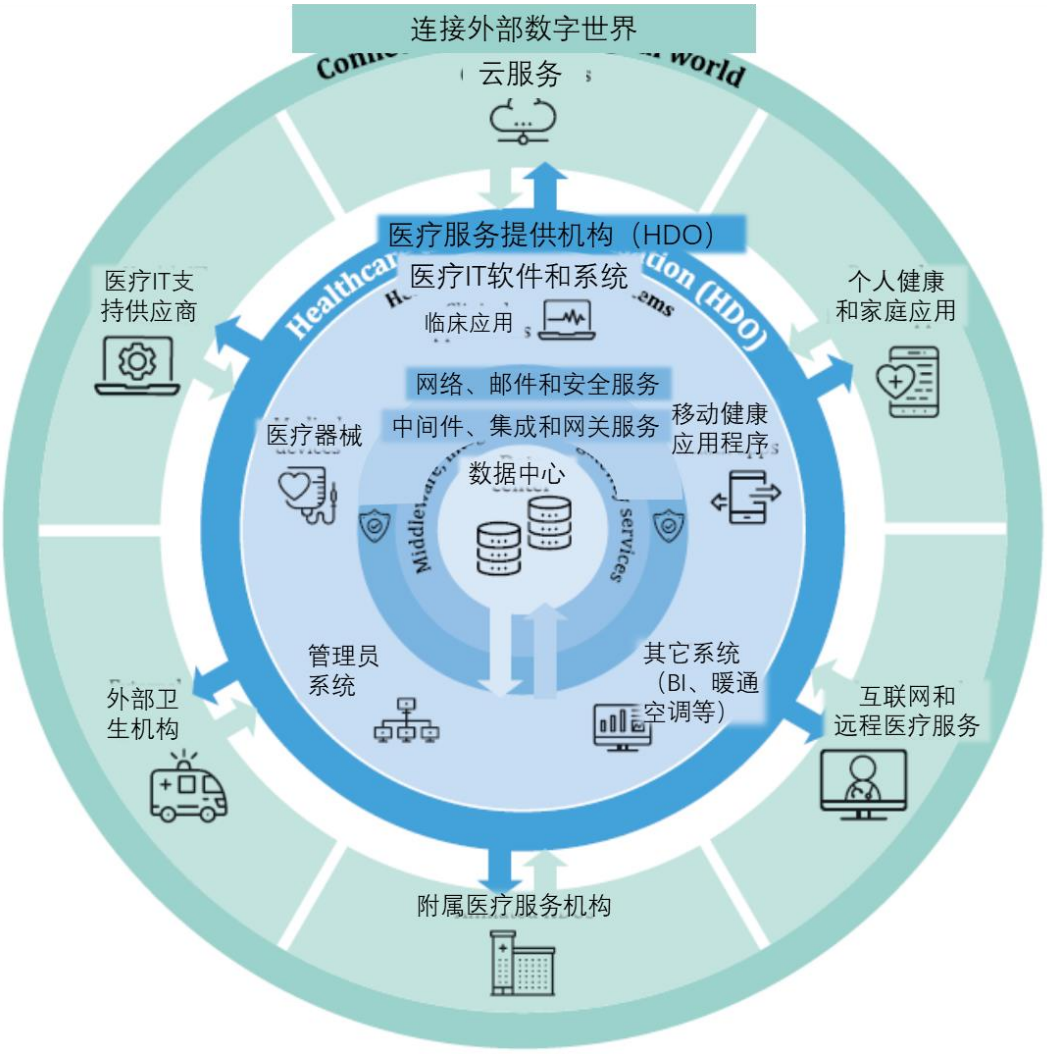

图4 体系

4.4 健康软件和健康 IT 系统的生存周期

健康软件和健康IT系统的生存周期涉及许多阶段和数个不同的角色和责任（如第4.5节中的描述）。所有角色和责任都需要共同合作，分担优化安全性、有效性和网络安全的责任。

尽管所有生存周期可能有所不同，但各阶段是相似的，在概念上可以分解为一系列活动。这既适用于整个生存周期，也适用于持续维护子周期循环，如图5所示。

图5 生存周期阶段 – 健康软件和健康IT系统

健康软件和健康IT系统通常以敏捷、迭代或递归的方式开发，范围可以从大型云计算解决方案到较小的健康IT组件（例如，通过在线商店提供的个人医疗应用程序）。虽然规模可能不同，但健康IT组件和系统可以频繁迭代，并且几乎是连续的开发周期，以满足软件维护、不断变化的业务需求和顾客期望。维护和设计/开发周期的频率，以及诸如"获得"等阶段所需的程度，也因具体的健康软件和健康IT系统、其社会技术生态系统以及其生存周期内所需的适应性变化程度而不同。在此生态系统中，诸如变更-发布管理和配置管理等过程是非常重要的。

健康IT基础设施以及“体系”中的所有健康IT系统和健康IT子组件都有自己的生存周期，因此在任何时候下列设备中都会有多个重叠的生存周期发生：

a) 健康IT系统、软件及其组件； b)

医疗器械及其相关软件和硬件；

c) 终端用户工作站、平板电脑、智能手机和其他访问设备；

d) 信息技术网络、接口和网络安全子系统；

e) 支持通用的信息技术，包括硬件和软件；

f) 数据、信息和支持性术语、算法和编码系统。

例如，网络交换机上的软件有自己的生存周期，网络交换机的硬件也有自己的生存周期，网络交换机所处的基础设施也有自己的生存周期等。

图6说明了健康IT基础设施是如何由一系列不同的系统组成的，这些系统相互连接以共享数据，相互操作并使用共同的基础设施。每个系统通常由多个健康IT组件组成，这些组件本身由数据和多个子组件组成，每个组件都有自己的生存周期。

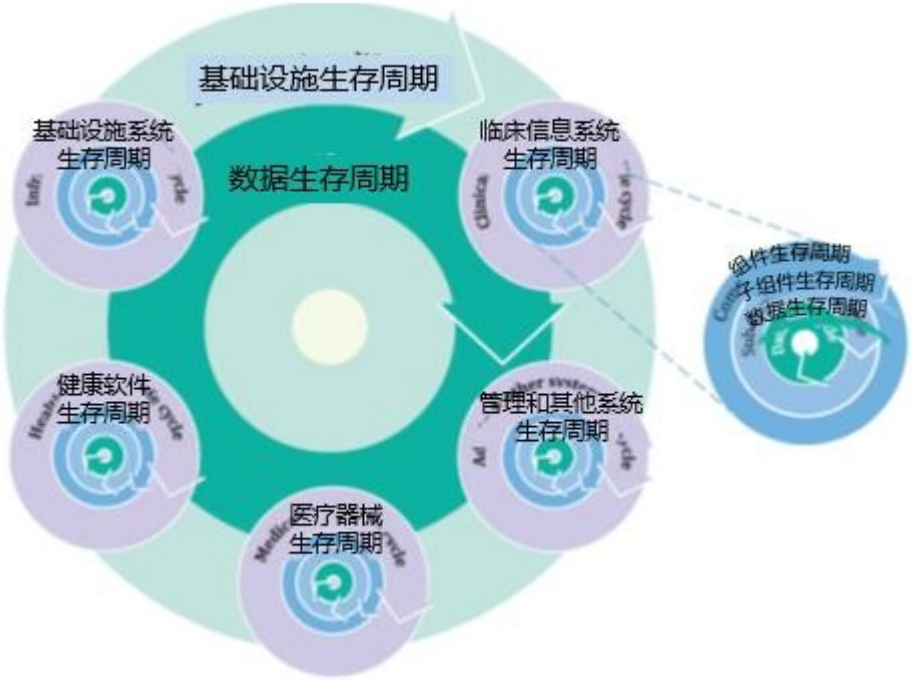

图6 生存周期内的生存周期

每组数据也有生存周期。数据会创建、使用，并可与其他数据重新编译以创建新的数据集。如果管理不善，数据来源可能会丢失，因此数据的完整性可能难以验证。数据完整性是网络安全的一个基本要素，如果数据在整个生存周期内没有得到适当的管理和维护，就会对安全性和有效性产生严重影响。主数据管理和元数据管理等技术，对于医疗信息遵守授权、同意和其他隐私原则特别有价值。此外，在多种医疗环境中收集的数据，以及之后整合并转化为对患者护理决策至关重要的信息，也需要适当管理。

4.5 角色和责任

安全性、有效性和网络安全的责任由许多角色共同承担（参见表1）。

表1 生存周期角色

角色	描述
最高管理层	指导和控制组织并在组织中负有全面责任的一群人。
系统所有者	高级管理人员，负责确保获取和实施的健康软件和健康IT系统能够满足其组织预期用途的医疗交付需求。
开发者	负责执行健康软件或健康IT系统的设计和开发阶段（概念到发布和维护）的实体。

	备注：例如，开发者可以是制造商组织的一部分，也可以是服务供应商或HDO。
集成商	负责将组件纳入医疗交付机构织所使用的健康IT基础设施的实体，包括技术安装、配置和数据迁移。
实施者	负责临床安装、工作流程优化和临床培训的实体（实施者可以是开发者或所有者）。
管理者	负责已实施的健康IT系统的持续运行并确保其得到持续保护和维护的人员。
用户	在临床环境中使用该系统的人，例如个人健康档案下的消费者。
备注：经许可改编自参考文献[38]。	

这些角色不是针对某个组织类型。例如，医院可以整合、实施和运营他们所使用的系统，但他们也可以选择内部开发自己的软件，因此医院可扮演多重角色。同样地，医疗器械公司和健康软件及系统制造商可以作为他们开发系统的集成商、实施者或管理者（如基于云的软件）。如果一个系统有多个健康IT组件构成，不同组织可以负责系统的不同方面。例如，医院可以将其信息技术运营的某些方面，如网络或服务器运营外包给第三方云服务提供商。

在组织内，管理安全性、有效性和网络安全等关键属性的责任分配，不一定要用专门的职位头衔来体现，但可以作为个人正式拥有的具体责任来列入。在某些情况下，角色的具体活动可以由不同的人分担，这取决于组织的结构，在某些情况下，取决于有关的具体健康IT组件或系统。

图7概述了角色、生存周期阶段和转换点间的关系，其中会出现责任转移和信息共享，以保持关键属性管理的连续性。

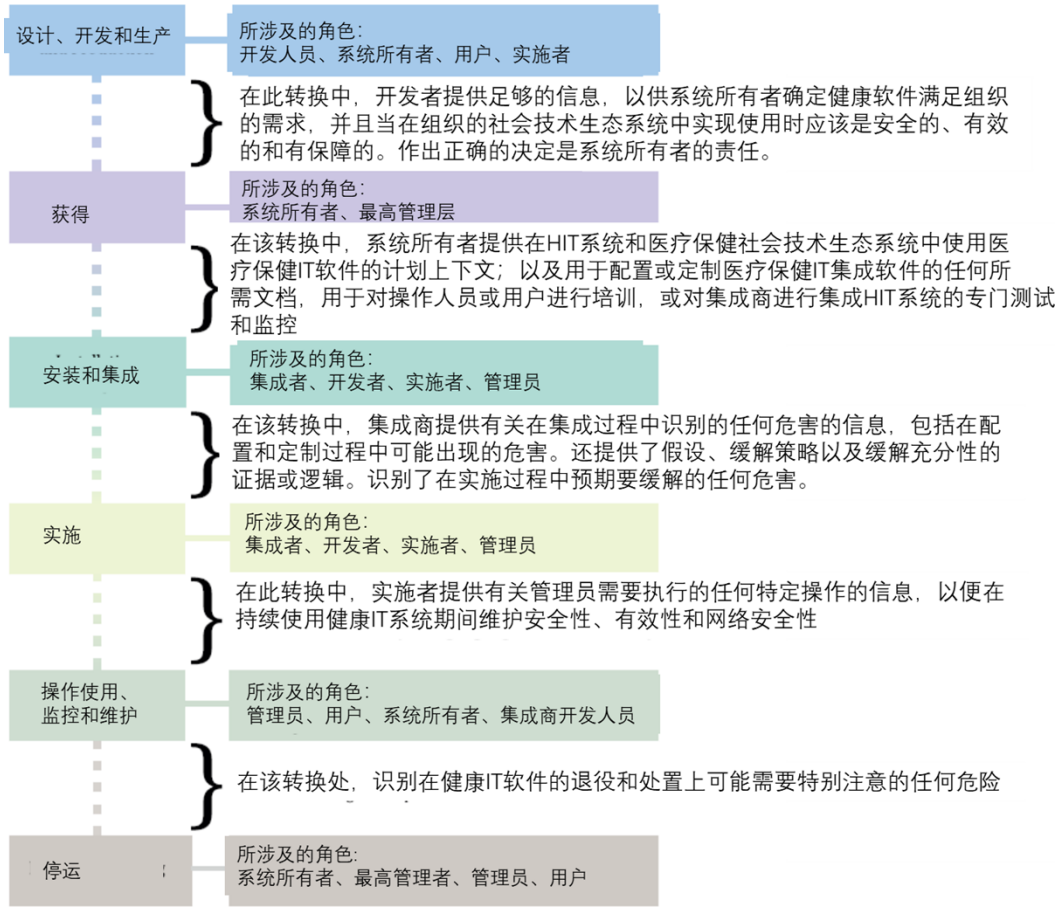

图7 健康软件的角色、生存周期阶段和转换点

注：经许可改编自参考文献[38]

4.6 沟通

生存周期中各转换点的沟通对任何管理过程都非常重要，尤其在有不同利益相关方的复杂系统中变得至关重要。随着健康软件和健康IT系统在其生存周期中经历不同的阶段，一些重要的信息，如果能够共享，就会显著加强对所涉及的许多角色和组织之间的基本要素的管理。

在生存周期的所有阶段，必须清楚地确定负责管理安全性、有效性和网络安全方面的组织的角色。随着健康软件和健康IT系统在其生存周期阶段的发展（见图8），这些组织需要早期生存周期阶段的特定信息，以正确评估和管理安全性、有效性和网络安全问题，帮助履行其职责。此外，他们可以将维护和监测的信息分享给在生存周期其他阶段发挥作用的组织。

图8 – 连续沟通中转换点的信息转移

在制定沟通计划时，三个重要问题需要解决：

a) 要沟通的信息内容；

b) 接收和转移沟通信息的人员；

c) 如何充分地沟通信息。

在许多情况下，处于生存周期不同阶段的角色也需要收回流程中的信息。例如，当医疗器械制造商向客户出售医疗器械时，该制造商应监测该设备的上市后性能，收集客户的反馈，并重新评估现场发生问题的风险。在某些情况下，这些信息可以用来修改设备，以帮助维护该医疗器械的安全性、有效性和网络安全。在其他方面，如果有必要采取额外的风险控制措施或进行改变，制造商将会鱼先与客户进行沟通；在某些情况下，进行正式的召回，对现场设备进行修正维护。鉴于所涉及的角色和转换点数量， 健康软件和健康IT系统也存在类似的沟通需求。正如图7和图8所描述的那样，此种沟通可能涉及多方和阶段。

重要的是，此种知识和信息的传递是足够正式和可预测的，以便不同利益相关方能够在不同的生存周期阶段和角色之间及时有效地沟通。使此种沟通和信息传递正式化的一种方法是使用保证案例。保证案例可以用来向其他角色传达有关不同风险的信息和知识。附件C对此方法进行了进一步探讨。

另一种方法是责任协议，利益相关方在协议中规定哪些任务是由特定的一方负责。在某些情况下，这些责任是有时限的，在一定时间后就会失效。

随附的信息和标签是另一种类型的沟通，有助于将制造商的具体信息传递给客户。标签对于连接的和互操作的系统可能特别重要，制造商可以在这些系统中传达非标准的接口要求和特征、功能和性能要求以及电子接口的目的。对于集成商和实施者来说，这会是来自制造商的关键信息，以确保设备按预期执行。

另一个重要的沟通渠道是对安全和安全性事件的回顾性报告和管理，包括未遂事故。这涉及到操作层面不同角色间的沟通（如支持信息技术单位、服务承包商和受影响的临床部门），以及健康软件、健康IT系统和基础设施组件的制造商、监管者和参与汇总病例报告的机构。

4.7 安全性、有效性和网络安全的相互依存关系

同样的风险（及其风险控制措施）会影响安全性、有效性和网络安全。 在评估和管理这些风险及其风险控制措施时，必须认识到这三个关键属性的相互依赖性（图9）。例如，系统或数据在医疗点无法使用的风险不仅是网络安全风险。 如果患者护理决策受到损害，它可能对安全性产生重大影响，因为这可能影响系统的有效性（及其优势），打击临床医生对使用系统作为临床工具的信心。

图9 – 安全性、有效性和网络安全的相互依存关系

安全性、有效性和网络安全相互依存的一个后果是，针对某些风险精心设计的风控措施会对其他属性中的一个或两个产生不利影响。例如，增加控制措施以减少未经授权的访问所带来的风险，可能会影响系统的实用性和可用性，从而损害系统的有效性（和有效性的实现）。它还可能导致系统的权变措施， 对安全产生不利影响。

在解决安全性、有效性和网络安全风险，以及实现预期有效性以支持对健康软件和健康IT系统的持续投资方面，全面方法的关键是优化三个属性之间的协同和平衡作用。重要的是要确保该系统的有效性（总利益）始终超过其实施过程中的剩余风险。

5 基本要素

5.1 概述

涉及健康软件和健康IT系统的安全性、有效性和网络安全的生存周期框架有八个基本要素（图10),它们支持第4条所阐述的六个总体主题（图2）。这八个要素让整个健康软件和健康IT系统生存周期的利益相关方了解如何以综合和知情的方式解决安全性、有效性和网络安全问题。这些基本要素分为两类— 治理和知识传递。

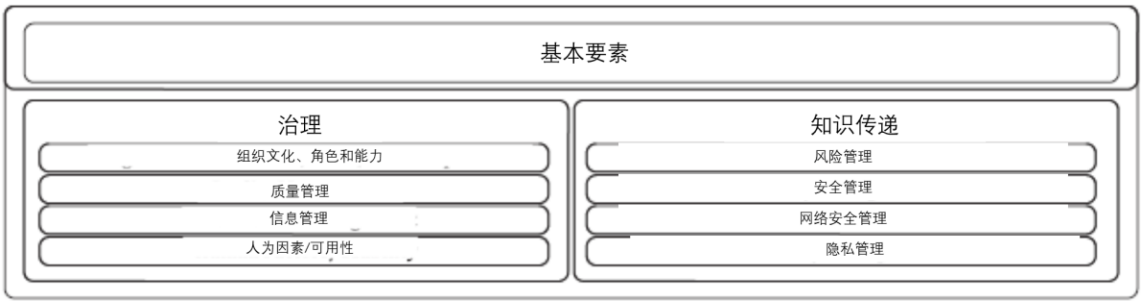

图10 基本要素

治理包括四个基本要素，涉及的活动通常是每个利益相关组织的责任，但对在所有生存周期阶段确保安全性、有效性和网络安全至关重要。这些要素应在制造商、HDO和其他支持组织的管理结构中得到解决，并且这些组织将用此来维护关键属性。这些要素在组织内的应用会因利益相关方的类型和生存周期阶段不同而有所不同。

知识传递包括四个基本要素，它们在企业层面非常重要，但也涉及到跨组织、角色和生存周期阶段的沟通。从制造商或开发商的角度来看，该类要素涉及许多评估风险的活动。这些活动产生的信息对设计和维护产品很重要，并将这些信息的子集传达给获得产品的人员。从HDO的角度来看，所涉及的角色随后将继续传递这些基本信息，以帮助指导这些产品在其生存周期后期的整合、实施、使用和停用工作。这些信息会整合到企业级的风险、安全性、隐私性和网络安全的管理过程中，这些过程用于管理每个阶段及每个阶段负责人的活动。信息可以通过不同的方式进行交流。一种方式是使用保证案例组织和传递信息。附录C展示了如何使用保证案例报告来获取和交流信息。

5.2 治理（组织内重点）

5.2.1 概述

图11显示了与治理有关的四个基本要素。

图11 基本要素-治理

5.2.2 组织文化、角色和能力

5.2.2.1 声明