信息安全保障人员认证培训教材

医疗服务信息安全

YILIAO FUWU XINXI ANQUAN

中国信息安全认证中心

◎ 主　编 张　剑　◎ 副主编 钱伟中 万里冰 张会平

★★★ CISAW ★★★

电子科技大学出版社

信息安全保障人员培训教程

医疗服务信息安全

YILIAO FUWU XINXI ANQUAN

中国信息安全认证中心

◎ 主　编 张　剑　◎ 副主编 钱伟中　万里冰　张会平

★★★ CISAW ★★★

电子科技大学出版社

图书在版编目（CIP）数据

医疗服务信息安全 / 张剑主编. - - 成都：电子科技大学出版社, 2017. 5

ISBN 978 - 7 - 5647 - 4502 - 8

Ⅰ. ①医… Ⅱ. ①张… Ⅲ. ①医疗卫生服务 - 信息安全 Ⅳ. ①R197. 1

中国版本图书馆 CIP 数据核字 (2017) 第 109309 号

内 容 提 要

本书以信息安全保障人员认证（CISAW）培训的需求为总纲，在配套教材《信息安全技术应用》一书介绍基本安全技术的基础上，深入诠释了医疗卫生信息系统及安全的核心概念，并结合医疗卫生信息系统的特点，阐述了医疗卫生信息系统合规要求、安全策略制定和安全风险评估方法。分析了保障机制及监测与评价方法，并对医疗卫生信息系统涉及的安全集成、安全开发和安全运维进行深入分析。介绍了医疗卫生信息系统相关领域前沿知识，最后对《网络安全法》进行解读。

医疗服务信息安全

yī liáo fú wù xìn xī ān quán

张 剑 主编

钱伟中 万里冰 张会平 副主编

策划编辑 万晓桐 徐守铭

责任编辑 万晓桐 徐守铭

出版发行 电子科技大学出版社

成都市一环路东一段 159 号电子信息产业大厦九楼 邮编 610051

主 页 www. uestcp. com. cn

服务电话 028—83203399

邮购电话 028—83201495

印 刷 成都市火炬印务有限公司

成品尺寸 185mm × 260mm

印 张 15. 75

字 数 326 千字

版 次 2017 年 5 月第一版

印 次 2017 年 5 月第一次印刷

书 号 ISBN 978 - 7 - 5647 - 4502 - 8

定 价 60. 00 元

前 言

医疗卫生信息系统的发展，从单一、本地化的运行平台，向复杂、网络化的运行平台转变，其中，涉及多个信息子系统的安全集成、安全开发和安全运维。同时，新兴的信息技术，如：移动互联网、云计算、物联网、大数据的发展，涉及医疗数据采集、存储、处理、通信到归档、销毁的各个环节，在为医疗活动带来便利的同时，其所带来或衍生的安全性问题也日益凸显。

《医疗服务信息安全》人员认证是信息安全保障人员认证（Certified Information Security Assurance Worker，CISAW）中管理级（Ⅱ级）“医疗服务”专业方向的参考用书，主要针对医疗机构不同岗位从业人员，包括相关部门领导、工作人员，各医疗卫生机构的医务人员、科室领导和院级领导以及医疗业务系统信息安全从业人员，旨在提高学员的安全意识及安全保障能力。

本书主要针对医疗卫生领域的信息安全问题展开讨论，全书共分 11 章。第 1 章概述，从医疗卫生信息系统的概念和发展出发，重点介绍医疗卫生信息安全形势及相关案例；第 2 章合规要求，介绍医疗卫生相关法律法规要求、国家标准要求及监管要求；第 3 章安全策略，定义医疗卫生信息安全要实现的目标和实现这些安全目标的途径和规则；第 4 章风险评估，介绍风险评估的相关知识，介绍风险识别和处置的方法；第 5 章保障措施，介绍医疗卫生信息安全监测与评价体系及实施方法；第 7 章、第 8 章、第 9 章，从医疗卫生信息系统主要涉及的运维、集成和开发等环节介绍安全需求和实施的过程；第 10 章从领域前沿的角度，介绍医疗卫生信息安全的前沿知识；第 11 章通过对《网络安全法》解读，分析医疗卫生领域网络安全保护的法律体系。

本书按照信息安全保障人员认证考试大纲的要求进行编写，适合广大申请认证考试的人员使用的同时，也适合所有从事与医疗卫生信息安全有关的工作人员、期望了解相关安全相关知识的人员使用。本书配套教程《网络安全意识提升》详细介

绍相关信息安全基础知识及在安全意识方面的素养提升，可供相关人员参考。

本书由张剑、钱伟中、万里冰、张会平、张徐亮、程瑜琦、吴凤翼、赵平等共同编写完成，在此对各位的辛勤付出表示感谢。

本书在成书过程中得到了《信息安全保障人员认证考试用书》编委会的指导，得到了中国信息安全认证中心、四川省中认信安技术服务有限公司的大力支持，在此表示衷心感谢。

本书作者力图以明确的思路、清晰的结构和流畅的语言来展现本书的知识体系，但也难免会出现疏漏、差错和不足，在此，恳请广大读者和同行批评指正，以便我们再版修订时加以改正和完善。

是为序。

张　剑

2016 年 10 月 31 日

丛书编委会

医疗服务信息安全

主　编：张　剑

副主编：钱伟中　万里冰　张会平

编　委：张徐亮　程瑜琦　吴凤翼　赵　平

目 录

第1章 概 述

近年来，在《2006—2020年国家信息化发展战略》的指导下，医疗卫生信息化作为国家信息化建设的重要组成部分得到了快速的发展。医疗卫生信息安全问题也随之成为该领域讨论的热点之一。

本章从医疗卫生信息化相关的基本概念出发，讲述医疗卫生信息化建设的历史、现状及发展趋势，分析医疗卫生信息化面临的安全风险，并利用实际案例来分析和讨论相关安全技术在医疗卫生信息系统中的应用。

医疗卫生信息化离不开计算机及通信技术的发展及相关领域的标准和协议的建设开发。随着医疗卫生信息化进程的推进，形成了医疗卫生信息系统的基本框架，同时在医疗卫生领域涌现了诸多的信息化相关的新概念。

在进一步阐述医疗卫生信息化相关安全问题之前，我们首先介绍一些基本概念。

1.1 基本概念

作为非医疗卫生专业的技术人员，首先要了解一些该领域的基本概念，如：医疗卫生、病历、健康档案等。

1. 医疗卫生

医疗卫生可分为医疗和公共卫生两个方面。一个国家的医疗卫生包括该国家内所有保障和提高人民的健康、治疗疾病和受伤的人员、组织、系统、过程。医疗卫生机构包括医院、卫生院、社区卫生服务中心、疾病预防控制中心等各类组织。

《中共中央国务院关于深化医药卫生体制改革的意见》中提出的：大力推进医药卫生信息化建设。此处“医药卫生”不仅包括了医疗和公共卫生，同时也包括了药品的监督管理方面的工作。

2. 健康档案

卫生部发布的《健康档案基本架构与数据标准》中定义："健康档案是居民健康管理（疾病防治、健康保护、健康促进等）过程的规范、科学记录。是以居民个人健康为核心，贯穿整个生命过程，涵盖各种健康相关因素、实现多渠道信息动态收集，满足居民自我保健和健康管理、健康决策需要的信息资源。"

3. 病历

卫生部信息化领导小组《基于健康档案的区域卫生信息平台建设技术解决方案》中指出："病历"是医疗机构对门诊、住院患者（或保健对象）临床诊疗、指导干预的卫生服务工作记录。健康档案与"病历"既有区别、更有联系。"病历"是健康档案的主要信息来源和重要组成部分，健康档案对"病历"的信息需求并非"病历"的全部，而是具有高度的目的性和抽象性。

以上是医疗卫生领域的基本概念。在医疗卫生信息化的建设过程中有以下一些基本概念和信息系统。医疗已生信息系统框架如图1－1所示。

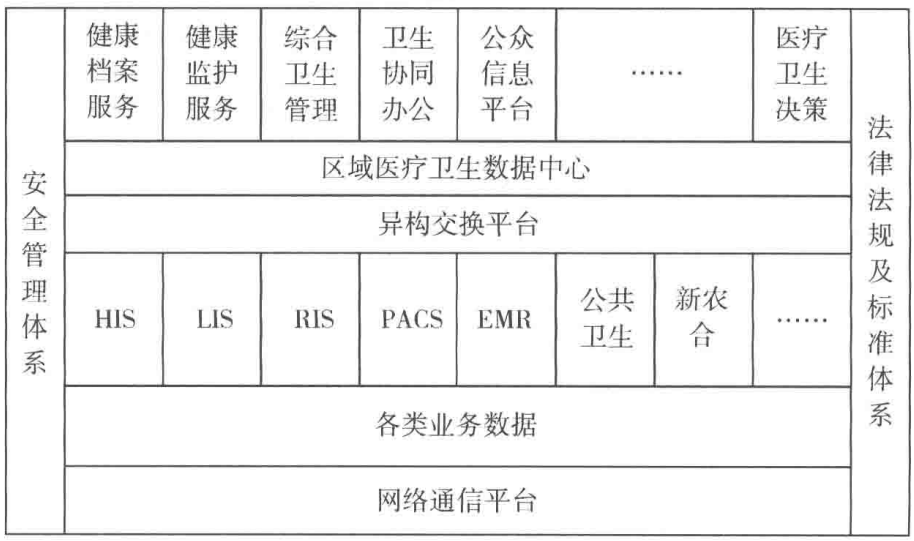

图 1－1 医疗卫生信息系统框架

1. 数字化医院

数字化医院简单讲就是利用计算机及网络通信技术，将患者的诊疗信息、卫生信息、档案信息与医院管理信息等进行有效的采集、传输、储存，并与社会医疗保健数据库互联互通的医院。

2. 数字化医院系统

数字化医院系统是包含了医院业务管理系统、临床信息系统等组成的复杂的综合信息系统。它通过资源整合和流程优化，降低了运行成本，提高了服务质量、工作效率和管理水平。患者及用户在任何能够访问互联网的地方，都能够轻松查询个人的健康档案、进行健康咨询等操作。

3. 区域医疗卫生信息化平台

卫生部《区域医疗卫生框架》中，将区域医疗卫生信息化平台定义为："连接区域内的医疗卫生机构基本业务信息系统的数据交换和共享平台，是不同系统间进行信息整合的基础和载体。从业务角度看，平台可支撑多种业务，而非仅服务于特定应用层面。"

4. 医疗保险

医疗保险是为补偿疾病所带来的医疗费用的一种保险。职工因疾病、负伤、生育时，由社会或企业提供必要的医疗服务或物质帮助的社会保险。如中国的公费医疗、劳保医疗。中国职工的医疗费用由国家、单位和个人共同负担，以减轻企业负担，避免浪费。发生保险责任事故需要进行治疗是按比例付保险金。

5. 临床信息系统

卫生部《基于电子病历的医院信息平台建设技术解决方案》中指出：临床信息系统（Clinical Information System，CIS）是数字化医院系统的组成部分，它对在医疗活动各阶段产生的数据进行采集、储存、处理、提取、传输、汇总并加工生成各种信息，支持医院医护人员的临床活动，丰富和积累临床医学知识，并提供临床咨询、辅助诊疗、辅助临床决策，以提高医疗质量和工作效率。主要包括医嘱处理系统、病人床边系统、医生工作站系统、检验医学信息系统、药物咨询系统等。

6. 医院信息系统

医院信息系统（Hospital Information System，HIS），是指利用计算机软硬件技术、网络通信技术等现代化手段，对医院及其所属各部门的人流、物流、财流进行综合管理，对在医疗活动各阶段产生的数据进行采集、储存、处理、提取、传输、汇总、加工生成各种信息，从而为医院的整体运行提供全面的、自动化的管理及各种服务的信息系统。

7. 检验医学信息系统

检验医学信息系统（Laboratory Information Management System，LIS）是临床信息系统的一个重要的组成部分，它的主要功能是将检验仪器传出的各类检验数据经分析、处理，生成检验报告，并通过网络及时将结果反馈给临床医生及患者。它的功能还包括标本流管理、报告管理、仪器设备质量控制及设备实时控制等。

8. PACS 系统

影像归档与传输系统（Picture Archiving and Communication Systems，PACS）是应用在医院影像科室的信息系统，主要任务是把各种医学影像（包括核磁，CT，超声，各种 X 光机，各种红外仪、显微仪等设备产生的图像）通过各种接口（模拟，DICOM，网络）以数字化的方式利用海量存储设备进行保存，便于调回使用和辅助诊断。它在各种影像设备间传输数据和组织存储数据具有重要作用。

9. 放射信息系统

放射信息系统（Radiation Information System，RIS）是放射科的登记、分诊、影像诊断报告以及放射科的各项信息查询、统计等工作的管理系统，RIS 系统与 PACS 系统紧密相连，构成医院数字医疗设备、影像及报告管理的解决方案。

10. 电子病历

电子病历（Electronic Medical Record，EMR），也叫计算机化的病案系统或称基于计算机的病人记录（Computer-Based Patient Record，CPR），是用电子设备（计算机、健康卡等）保存、管理、传输和重现的数字化的病人医疗记录。美国国立医学研究所将其定义为："基于一个特定系统的电子化病人记录，该系统提供用户访问完整准确的数据、警示、提示和临床决策支持系统的能力。"与传统病历相比，电子病历不仅指静态病历信息，还包括提供的相关服务。它是以电子化方式管理的有关个人终生健康状态和医疗保健行为的信息，涉及病人信息的采集、存储、传输、处理和利用的所有过程信息。

11. 新型农村合作医疗卫生信息系统

新型农村合作医疗卫生信息系统，简称新农合，主要功能包括新型农村合作医疗的费用测算、基金收缴、支付补偿、监督审计、决策分析和政策公告等功能。它是公共卫生建设的重要组成部分。

1.2 发展

医疗卫生信息系统随着计算机技术及通信技术的应用而产生，在相关技术的推动下不断发展，并在新时期呈现出新的特征。

1. 医疗卫生信息系统发展历程

医疗卫生信息系统的发展，从体系结构上来看，经历单机阶段、网络互联阶段、数字化阶段和区域共享阶段 4 个阶段，如图 1－2 所示。

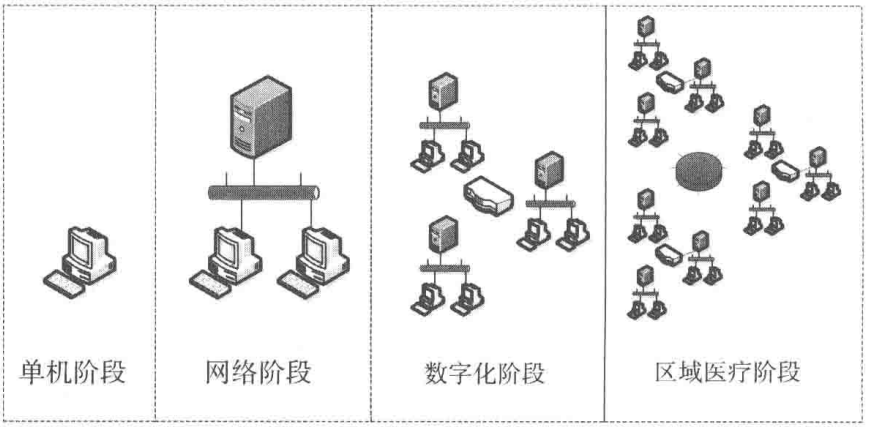

图 1－2 发展历程图