Licensed copy: Techstreet Content, ISO Exchange - Michigan, Version correct as of 27/01/2023. Licensed copy: Techstreet Content, ISO Exchange - Michigan, Version correct as of 27/01/2023.

PD ISO/TS 23535:2022



BSI Standards Publication

Health informatics — Requirements for customer-oriented health cloud service agreements

bsi.

National foreword

This Published Document is the UK implementation of ISO/TS 23535:2022.

The UK participation in its preparation was entrusted to Technical Committee IST/35, Health informatics.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

This publication is not to be regarded as a British Standard.

© The British Standards Institution 2022
Published by BSI Standards Limited 2022

ISBN 978 0 539 04777 6

ICS 35.240.80

Compliance with a Published Document cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 28 February 2022.

Amendments/corrigenda issued since publication

Date	Text affected

Licensed copy: Techstreet Content, ISO Exchange - Michigan, Version correct as of 27/01/2023. Licensed copy: Techstreet Content, ISO Exchange - Michigan, Version correct as of 27/01/2023.

Licensed copy: Techstreet Content, ISO Exchange - Michigan, Version correct as of 27/01/2023.

PD ISO/TS 23535:2022

TECHNICAL SPECIFICATION

ISO/TS 23535

First edition
2022-01-25

Health informatics — Requirements for customer-oriented health cloud service agreements

Reference number
ISO/TS 23535:2022(E)

© ISO 2022

Licensed copy: Techstreet Content, ISO Exchange - Michigan, Version correct as of 27/01/2023. Licensed copy: Techstreet Content, ISO Exchange - Michigan, Version correct as of 27/01/2023.



COPYRIGHT PROTECTED DOCUMENT

© ISO 2022, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

© ISO 2022 – All rights reserved

Contents

Page

Foreword ..... **v**
Introduction ..... **vi**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Cloud computing in health and healthcare **4**
4.1 Cloud computing in hospital 4
4.2 Gap between CSC's expectation and CSP's solution 4
5 CSA for health and healthcare **5**
5.1 Roles and responsibilities 5
5.1.1 Cloud service customer 5
5.1.2 Cloud service provider 7
5.2 Service support 12
5.2.1 Service catalogue 12
5.2.2 Service coverage 13
5.2.3 Uninterrupted service 13
5.2.4 Accountability for service interruption 13
5.2.5 Compensation for service interruption 13
5.2.6 Service downtime 13
5.2.7 Service disruption notification 13
5.2.8 Target response time 14
5.2.9 Information on subcontractors 14
5.3 Service model 14
5.4 Service monitoring 14
5.5 Incident reporting 15
5.5.1 Incident report 15
5.5.2 Incident response 15
5.5.3 Incident report delivery 15
5.5.4 Repair time 15
5.6 Standards, testing, and certification 15
5.6.1 Conformity with international standards 15
5.6.2 Guidelines for ensuring compatibility between clouds 15
5.6.3 Support data input 16
5.6.4 Adopt international standards 16
5.6.5 Compliance with non-international standards 16
5.6.6 Compliance test 16
5.6.7 Compliance with updated standards 16
5.6.8 Certification details 16
5.7 Data location 16
5.7.1 Cloud service area and location 16
5.7.2 Cloud relocation 16
5.7.3 Violation of advance notice 16
5.8 Data governance 16
5.8.1 Cloud data maintenance policy 16
5.8.2 Cloud data backup plan 17
5.8.3 Cloud data collection 17
5.8.4 Cloud data query history 17
5.9 Data security 17
5.9.1 Technical security measures 17
5.9.2 Administrative security measures 17
5.9.3 Physical security measures 18
5.9.4 Simulation for technical security measures 18

© ISO 2022 – All rights reserved

Licensed copy: Techstreet Content, ISO Exchange - Michigan, Version correct as of 27/01/2023. Licensed copy: Techstreet Content, ISO Exchange - Michigan, Version correct as of 27/01/2023.

5.9.5 Data integrity assurance 18
5.9.6 De-identification 18
5.10 Data transfer 18
5.10.1 Data transfer deadline 18
5.10.2 Data transfer method 18
5.10.3 Data transfer roles 18
5.10.4 Data deletion method 18
5.10.5 Data transfer customer approval 18
5.10.6 Approved data transfer range 18
5.10.7 Responsibilities for data transfer violation 19
5.11 Billing system and operation policies 19
5.11.1 Billing system criteria 19
5.11.2 Internal cloud operational policy 19
5.11.3 Billing for excess usage 19
5.12 Payments 19
5.12.1 Payment method/time 19
5.12.2 Payment period 19
5.12.3 Payment method 19
5.12.4 Explanation of billing details 19
5.13 Regulatory compliance 19
5.13.1 Jurisdiction compliance 19
5.14 Service update and version management 20
5.14.1 Service update notification 20
5.14.2 Change notification upon service update 20
5.14.3 Service update stability assessment 20
5.14.4 Service version management 20
5.15 Agreement renewal and expiry 20
Annex A (informative) **Summary of security and privacy and metric model components** **21**
Annex B (informative) **Service catalogues and cost estimate** **23**
Bibliography **26**

© ISO 2022 – All rights reserved

Licensed copy: Techstreet Content, ISO Exchange - Michigan, Version correct as of 27/01/2023. Licensed copy: Techstreet Content, ISO Exchange - Michigan, Version correct as of 27/01/2023.

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 215, *Health informatics*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

© ISO 2022 – All rights reserved

Licensed copy: Techstreet Content, ISO Exchange - Michigan, Version correct as of 27/01/2023. Licensed copy: Techstreet Content, ISO Exchange - Michigan, Version correct as of 27/01/2023.

Introduction

Healthcare services go beyond the boundaries of physical providers, such as clinics or hospitals. Cloud computing, cognitive computing, virtual reality/augmented reality, IoT, robot and wearable devices have contributed to enhanced accessibility and provide value to customer health, addressing customer demand for tailored healthcare services. Modern ICT is the catalyst to the promotion of customer engagement and empowerment, especially through cloud-based services.

Cloud computing offers shared and configurable collections of computing resources and services that, typically over the Internet, are made available with minimal management effort. It eliminates the distinction between the physical and virtual resources by providing access from various devices such as wearable, wellness devices and mobile phones. There are six key characteristics of cloud computing:

— broad network access,

— measured service,

— multi-tenancy,

— on-demand self-service,

— rapid elasticity and scalability, and

— resource pooling;

and three service models:

— Software as a Service(SaaS),

— Platform as a Service (PaaS), and

— Infrastructure as a Service (IaaS).

Cloud computing is expected to bring substantial and practical impact to healthcare services from a customer perspective. Customers may enjoy by a contract customer-centric health services from the cloud provider. The cloud provider offers a variety of benefits to its customers, such as predictive disease analytics and evidence-based management of chronic diseases.

Health cloud services have evolved into a knowledge platform on which customer health data, including generic data, are collected through multi-model data collection channels, and are made accessible anywhere by any device or application. These data are analysed by sophisticated analytical techniques such as artificial intelligence and inform personalized health-related advice and insights.

Health cloud services deal with critical and sensitive information related to life and health and are subjected to regulations such as HIPPA and GDPR. The quality and quantity of services vary, depending upon operating environments, supported devices, available intelligent analysis capacities, and service level agreements. Regardless of the duration of a service contract with the health cloud provider, it is important to establish standards for a minimum set of cloud service functions that ensures customer protection.

When a customer holds contracts with multiple health cloud service providers, it is important to ensure consistency of shared data between the providers. A clear demarcation of liability may be hard to obtain in a disastrous event when the customer subscribes to various cloud service models. In case of migrating from one service provider to another, there should be a method to validate the migration is carried out in compliance with health-industry-specific criteria (e.g., rules on customer health data transfer or deletion).

Healthcare is under transformation - manifested by the departure from the traditional face-to-face healthcare services between stakeholders, such as hospitals, caregivers, and patients. In addition, the general acceptance of customer empowerment is enabled by widespread dissemination of web technology and cloud computing, creating various healthcare services such as virtual hospitals,

© ISO 2022 – All rights reserved

Licensed copy: Techstreet Content, ISO Exchange - Michigan, Version correct as of 27/01/2023. Licensed copy: Techstreet Content, ISO Exchange - Michigan, Version correct as of 27/01/2023.

telehealth, online visit, and mobile health management. Health cloud services offer computer-customer interviewing, home telehealth, and health monitoring through wearable/wellness devices.

The purpose of this document is to classify key characteristics of a cloud service agreement from the perspectives and interest of the customer and to provide an agreement list pivotal to the provision of customer-oriented healthcare service.

Please note that any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

Licensed copy: Techstreet Content, ISO Exchange - Michigan, Version correct as of 27/01/2023. Licensed copy: Techstreet Content, ISO Exchange - Michigan, Version correct as of 27/01/2023.

© ISO 2022 – All rights reserved

TECHNICAL SPECIFICATION ISO/TS 23535:2022

Health informatics — Requirements for customer-oriented health cloud service agreements

1 Scope

This document describes a core set of cloud service agreements for customer-oriented health cloud services.

This document covers a customer-oriented cloud service agreement that can be used in healthcare organizations and public health centers that use health cloud services.

This document defines key characteristics in the health cloud service agreement that are indispensable in providing optimal health/healthcare management functionalities. Privacy and security features are considered outside the scope of this document and are covered in ISO/TR 21332.

The purpose of this document is to present matters to be considered (e.g., cloud type, components, key characteristics) by stakeholders involved in the implementation of cloud computing in hospitals or healthcare organizations. The potential users of this document are mainly 1) IT managers of hospitals, 2) hospital management, and 3) cloud service providers and cloud partners that provide services to healthcare institutions.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
application capabilities type
cloud capabilities type (3.2) in which the *cloud service customer* (3.9) can use the *cloud service provider's* (3.10) applications

[SOURCE: ISO/IEC 17788:2014, 3.2.1]

3.2
cloud capabilities type
classification of the functionality provided by a *cloud service* (3.5) to the *cloud service customer* (3.9) based on resources used

[SOURCE: ISO/IEC 17788:2014, 3.2.4]

3.3
customer-oriented
relating to the needs and interests of individual customers, including businesses

© ISO 2022 – All rights reserved

Licensed copy: Techstreet Content, ISO Exchange - Michigan, Version correct as of 27/01/2023. Licensed copy: Techstreet Content, ISO Exchange - Michigan, Version correct as of 27/01/2023.