TECHNICAL SPECIFICATION

ISO/TS 23535

First edition
2022-01

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

Reference number
ISO/TS 23535:2022(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

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.

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, 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.

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

3.4
cloud computing
paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand

[SOURCE: ISO/IEC 17788:2014, 3.2.5]

3.5
cloud service
one or more capabilities offered via *cloud computing* (3.4) involved using a defined interface

[SOURCE: ISO/IEC 17788:2014, 3.2.8]

3.6
cloud service agreement
CSA
documented agreement between the *cloud service provider* (3.10) and *cloud service customer* (3.9) that governs the covered service(s)

[SOURCE: ISO/IEC 22123-1:2021, 3.8.8, modified – Note to entry removed.]

3.7
cloud service category
group of *cloud services* (3.5) that possess some common set of qualities

[SOURCE: ISO/IEC 17788:2014, 3.2.10, modified – Note to entry removed.]

3.8
cloud service characteristic
qualitative or quantitative property of a *cloud service* (3.5)

[SOURCE: ISO/IEC 19086-2:2018, 3.1]

3.9
cloud service customer
CSC
party (3.16) which is in a business relationship for the purpose of using *cloud services* (3.5)

[SOURCE: ISO/IEC 17788:2014, 3.2.11]

3.10
cloud service provider
CSP
party (3.16) which makes *cloud services* (3.5) available

[SOURCE: ISO/IEC 17788:2014. 3.2.15]

3.11
incident conclusion report
final report on failures submitted to the provider, organized and prepared in chronological order, specified by explanations and countermeasures

3.12
infrastructure as a service
IaaS
cloud computing (3.4) service model defined in section 2 of the NIST Definition of Cloud Computing [SP800145]

[SOURCE: ISO/IEC 19831:2015, 3.8]

3.13
measurement
set of operations having the objective of determining a *measurement result* (3.14)

[SOURCE: ISO/IEC 19086-2:2018, 3.4]

3.14
measurement result
value that expresses a qualitative or quantitative assessment of a *cloud service characteristic* (3.8)

[SOURCE: ISO/IEC 19086-2:2018, 3.5]

3.15
metric
standard of measurement that defines the conditions and the rules for performing the *measurement* (3.13) and for understanding the *measurement result* (3.14)

[SOURCE: ISO/IEC 19086-2:2018, 3.6, modified – Note to entry removed.]

3.16
party
natural person or legal person, whether or not incorporated, or a group of either

[SOURCE: ISO 27729:2012, 3.1]

3.17
software as a service
SaaS
cloud service category (3.7) in which the *cloud capabilities type* (3.2) provided to the *cloud service customer* (3.9) is an *application capabilities type* (3.1)

[SOURCE: ISO/IEC 17788:2014, 3.2.36]

3.18
target response time
maximum wait time for a response to a request

3.19
platform as a service
PaaS
cloud service category (3.7) in which the *cloud capabilities type* (3.2) provided to the *cloud service customer* (3.9) is a *platform capabilities type* (3.20)

[SOURCE: ISO/IEC 17788:2014, 3.2.30]

3.20
platform capabilities type
cloud capabilities type (3.2) in which the *cloud service customer* (3.9) can deploy, manage, and run customer-created or customer-acquired applications using one or more programming languages and one or more execution environments supported by the *cloud service provider* (3.10)

[SOURCE: ISO/IEC 17788:2014, 3.2.31]

3.21
interoperability
ability of two or more systems or applications to exchange information and to mutually use the information that has been exchanged

[SOURCE: ISO/IEC 17788:2014, 3.1.5]

3.22
service level agreement
SLA
documented agreement between the service provider and customer that identifies services and service targets

[SOURCE: ISO/IEC 17788:2014, 3.1.7, modified – Note to entry removed.]

4 Cloud computing in health and healthcare

4.1 Cloud computing in hospital

Cloud computing has been adopted in many domains. Hospital IT experts are seeking cloud services that correspond with characteristics of hospital operation. Health cloud providers should deliver services that match the demands particular to the health/healthcare industry. Hospital IT systems perform complex functions that protect patient safety and provide timely data required by healthcare practitioners. Because such systems normally operate non-stop, system stability is a critical factor. Due to the integration of various devices and hospital information systems, system sustainability is important. Healthcare service is disrupted in the event of a system breakdown. It is thus important to have stable systems as they have a direct impact on all connected equipment and devices.

4.2 Gap between CSC's expectation and CSP's solution

An important factor to consider is predictability and preciseness of the services provided by the cloud service provider. There is likely to be a gap between the expectations of a hospital as a cloud service customer and the solution offered by a cloud service provider. First, the gap can originate from the difficulty in specifying detailed requirements/characteristics from the customer to the cloud service provider or operator. Second, it can also come from the highly abstract characteristics of cloud computing, which makes it difficult to translate into functional units. And third, the range of responsibilities to be defined when implementing health cloud services can easily be unclear due to the lack of common criteria between cloud service customers and providers.

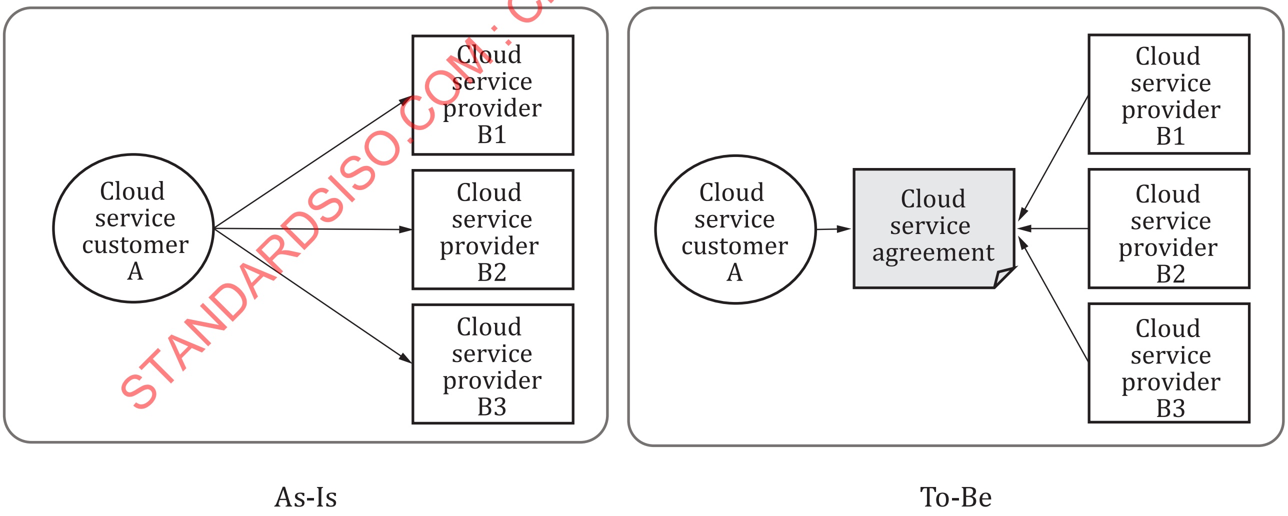
Cloud service customer A
Cloud service provider B1
Cloud service provider B2
Cloud service provider B3
As-Is
Cloud service customer A
Cloud service agreement
Cloud service provider B1
Cloud service provider B2
Cloud service provider B3
To-Be

Figure 1 — Expected role of a health cloud service agreement

These factors make it difficult to construct and put in action the measures in the event of accidents (incident recovery scenario). A list of agreements, as detailed as possible, is required to eliminate the ambiguity of the range of responsibilities. Fourth, services provided by multiple providers are not easy to compare or evaluate one against another while applying the same criteria. Fifth, it is difficult to ascertain all the facts of those services available in the real-world environment. Sixth, service contacts are not time-bound; service termination and renewal with new service details can happen over time, creating complex problems such as data security and migration. Overall, the key to successful implementation of health cloud services lies in the establishment of clear criteria between hospitals and cloud service providers (Figure 1).

A CSA defines basic common agreement requirements from the customer's perspective. Conceptual-level agreements are specified in detail to enhance understanding of service functions. General criteria of health cloud services are presented so that the customer can use the CSA in comparing and evaluating services from various providers. A detailed description of the CSA is expected to clarify the range of duties and responsibilities of the provider and the customer. The CSA is applicable to various cloud service models, such as SaaS. This document specifies general requirements, regardless of the service models in view. An example factors in a CSA to be considered are shown in Figure 2.

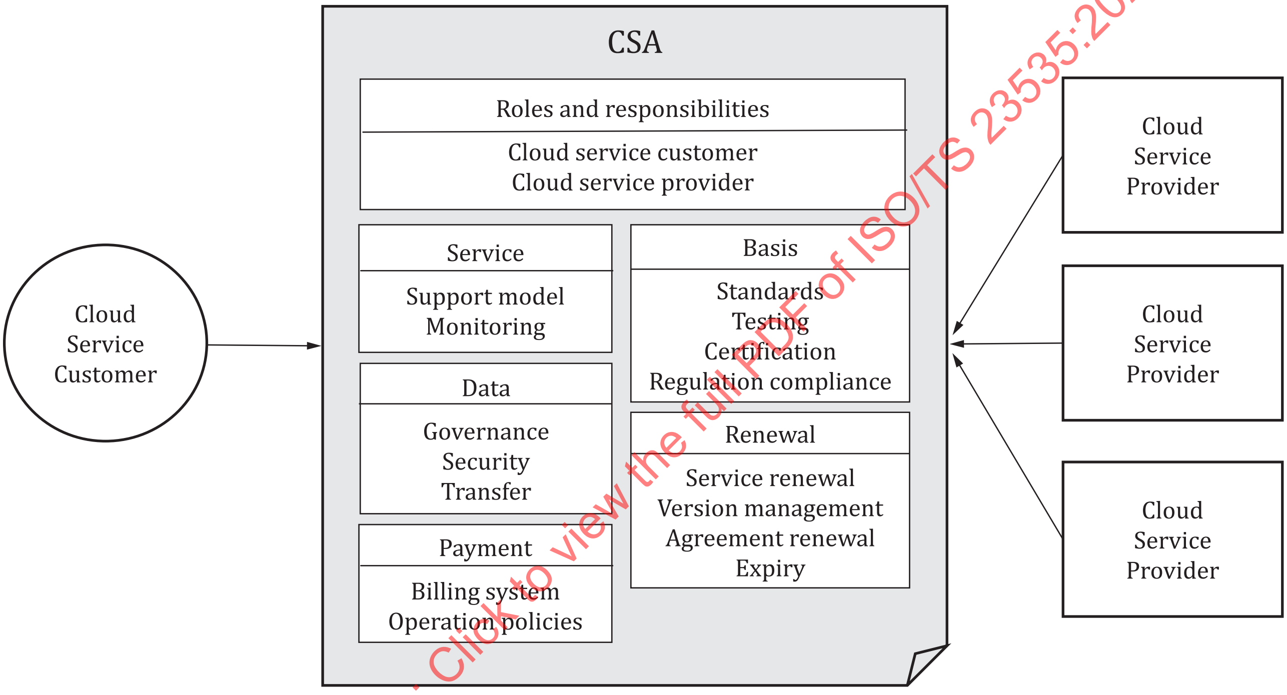

Figure 2 — CSA factors

5 CSA for health and healthcare

5.1 Roles and responsibilities

5.1.1 Cloud service customer

5.1.1.1 General

Service customers are parties that are in a business relationship for the purpose of using the cloud. They are cloud service users, cloud service administrators, and cloud service business managers.

5.1.1.2 Cloud service user

A cloud service user engages in various activities that include the services provided by the cloud service provider. The user credentials are authenticated by the cloud service provider and the user is granted access to the cloud service.

5.1.1.3 Cloud service administrator

A cloud service administrator is responsible for overseeing the operation of the customer's use of the cloud services and all operational processes associated with the customer's existing ICT systems. To ensure effective administration of the services, the cloud service administrator can engage in the following, but not limited to, activities:

a) Trial execution of the service: the cloud service provider's service may be used as a trial to check its suitability for the business needs of the customer. The trial is initiated with mutual agreement and understanding between the cloud service provider and the customer.

 1) The cloud service administrator may collect user credentials to the cloud service provider for trial services.

 2) The service is tested to see if it fits the business requirements.

b) Service monitoring: the cloud service administrator monitors the performance of the service

 1) The cloud service administrator tracks service usage to ensure that it is properly used.

 2) The cloud service administrator ensures that the integration of the existing ICT systems and the cloud service is achieved in a way that the business goals are met.

 3) The cloud service administrator checks the measurements and performance indicators related to the service (e.g., service availability, frequency of service interruptions, average help desk repair time).

 4) The cloud service administrator monitors performance indicators such as data usage.

 5) The cloud service administrator evaluates the provided service quality against the agreed service quality.

c) Security management:

 1) It is necessary to manage an appropriate security environment for cloud service customer data.

 2) Data backup and recovery, replication and failover plans may be established.

 3) Security policies are to be in place and evaluated.

 4) Encryption and integrity methods for service customer data may be employed and evaluated.

d) Billing and usage report:

 1) The cloud service administrator makes reports on the use of cloud services.

 2) The cloud service administrator makes reports on billing/invoice data related to usage.

e) Incident report processing: the cloud service administrator reports on customer-related problems.

 1) The cloud service administrator evaluates the impact of each incident.

 2) The cloud service administrator identifies the cause of the incident.

 3) The cloud service administrator checks the incident report prepared by the cloud service provider.

 4) The cloud service administrator develops alternatives to solving the incident.

5) The cloud service administrator identifies issues that may not have been resolved within an agreed-upon time frame or have a significant business impact.

f) Tenancy management: the cloud service administrator manages tenancy agreed-upon between the service customer and the cloud service provider. The tenancy agreement may include:

1) User accounts, security roles, identities, and privileges.

2) Steps to identify and control data shared among tenancy users.

3) Tenant creation and removal, and allocated resources.

4) Enforcement policies for each tenant.

5.1.1.4 Cloud service business manager

A cloud service business manager is responsible for managing the business in an efficient manner to achieve the business goals of the customer. The cloud service business manager can engage in the following, but not limited to, activities:

a) Accounting and finance: the cloud service business manager deals with accounting and financial aspects in relation to the cloud service.

1) The cloud service business manager aligns the business plans with the cloud services.

2) The cloud service business manager manages accounting and financial details in relation to cloud service usage.

3) The cloud service business manager processes the billing/invoices received from the cloud service provider and makes sure that the bills are commensurate with the usage data.

4) The cloud service business manager manages cloud service customers.

5) The cloud service business manager manages payments to the cloud service provider.

6) The cloud service business manager maintains the cloud account.

b) Service selection and purchase:

1) The cloud service business manager investigates the service offerings from cloud service providers to determine the service that corresponds with the business and technical requirements of the customer.

2) The cloud service business manager analyses services and related prices in the SLA.

3) The cloud service business manager negotiates terms of agreement for cloud services.

4) The cloud service business manager manages cloud service contracts and registration.

c) Audit report request: the cloud service business manager prepares reports on cloud audit requested by the customer in compliance with audit standards or systems.

5.1.2 Cloud service provider

5.1.2.1 Cloud service provider

A cloud service provider is responsible for providing cloud services and performing necessary activities for service maintenance. Cloud service providers include cloud service operation managers, cloud service deployment managers, cloud service managers, cloud service business managers, customer support and care representatives, inter-cloud providers, cloud service security and risk managers, and network providers.

5.1.2.2 Cloud service operations manager

A cloud service operations manager is responsible for operational processes and procedures and manages services and related infrastructure in accordance with operational goals.

a) System preparation:

   1) The cloud service operations manager evaluates the impact of deploying new services or expanding the use of existing services.

   2) The cloud service operations manager manages the capacities of data center resources to meet the needs of new deployments.

b) Service monitoring and management:

   1) The cloud service operations manager monitors services and infrastructure of the supplier.

   2) The cloud service operations manager identifies and maintains events and related data of importance to the supplier's business.

   3) The cloud service operations manager manages network infrastructure, including routers, domain name servers, IP addresses, and virtual individuals.

   4) The cloud service operations manager supervises storage allocation.

   5) The cloud service operations manager manages authentication and authorization of users.

   6) The cloud service operations manager configures and maintains operating systems and hypervisors.

   7) The cloud service operations manager manages virtualization environments.

   8) The cloud service operations manager ensures safe operation of the ICT environment of the supplier and that SLAs are met.

c) Asset and inventory management:

   1) The cloud service operation manager supervises computing, storage, network, and software assets and their relationships.

   2) The cloud service operations manager oversees versions, patch levels, and configuration information.

   3) The cloud service operations manager administers new assets and safely dispose of old assets.

d) Provision of audit data: The cloud service operations manager provides audit related data according to audit plans or standards.

5.1.2.3 Cloud service deployment manager

A cloud service deployment manager activates the operational processes and execute services in the early stages of service deployment.

a) Environment and process definition: the cloud service deployment manager governs the technical environment and operation for the processes employed in service deployment.

   1) The cloud service deployment manager manages software dependencies including technical environment configuration such as storage and network resources.

   2) The cloud service deployment manager governs changes in usage requirements in policies that affect resource expansion or reduction.

3) The cloud service deployment manager ensures compliance with appropriate standards for security and business.

4) The cloud service deployment manager defines the processes related to service execution and modification, service upgrade and plans.

b) Metric definition and collection: recommended components in a metric model are set forth in ISO/IEC TR 23951:2020, Annex A.2.

1) The cloud service deployment manager defines metrics used in SLAs.

2) The cloud service deployment manager develops methods for capturing metrics for each cloud service.

3) The cloud service deployment manager defines metric reporting and management methods so that SLA targets are met.

c) Deployment stage definition: the cloud service deployment manager defines service deployment stages.

5.1.2.4 Cloud service manager

A cloud service manager may ensure that the service is functioning correctly for use by the customer and that the service meets the goals specified in the SLA. The cloud service manager shall ensure stable operation of the supplier's business support systems and operation support systems and be responsible for the operation of functions provided to customers and partners.

a) Service provision: The cloud service manager may govern overall cloud services offered to the customer, including receipt and processing of service calls from customers. The cloud service manager authorizes and authenticates user identities and may be able to execute configuration and invocation of other services. The activities of the cloud service manager in this regard includes the following, but not limited to, activities:

1) The cloud service manager handles processes that deal with service defects.

2) The cloud service manager manages business support systems and operation support systems.

3) The cloud service manager manages the services and infrastructure offered to the customer.

4) The cloud service manager manages system process automation.

5) The cloud service manager supervises long-term capacity maintenance and performance trends.

6) The cloud service manager manages computing and storage requirements for maintenance updates on hardware.

7) The cloud service manager manages network functions for the data centers.

8) The cloud service manager oversees resources required to run the data centers and provide support.

b) Service arrangement and provision:

1) The cloud service manager performs network endpoint activities that the customer can access and that handle service requests of the customer.

2) The cloud service manager follows distribution processes defined for the service.

c) Service level management: the cloud service manager manages SLA target compliance. The cloud service manager monitors metrics for each service and compare them with service targets. When a metric does not meet the value required by the SLA, actions may be taken to re-deliver and deploy the service. If compliance cannot be maintained, report the issue to the relevant stakeholders.

5.1.2.5 Cloud service business manager

A cloud service business manager tracks customers' business plans, define service delivery strategies, and manage business relationships.

a) Business plans:

   1) The cloud service business manager defines service offerings that include technical details and SLAs.

   2) The cloud service business manager develops business plans for services offered to customers.

   3) The cloud service business manager oversees the financial and technical aspects of the service, defines target audiences, develops, and maintains contracts and SLAs, and handles channel markets and sales targets.

   4) The cloud service business manager endeavours to achieve planned financial goals of the cloud provider, using such means as tracking sales and boosting service usage.

b) Customer relationship management: the cloud service business manager oversees business relationship with customers.

   1) The cloud service business manager develops and maintain product catalogues (examples of product catalogues are set forth in B.1).

   2) The cloud service business manager provides a point of contact for the customers.

   3) The cloud service business manager resolves concerns or issues raised by the customers.

c) Financial management:

   1) The cloud service business manager oversees claims and resolves incidents.

   2) The cloud service business manager governs billing to the customers.

   3) The cloud service business manager manages payment and accounting in relation to the customers.

5.1.2.6 Customer support and care representative

a) Customer request processing:

   1) The customer support and care representative is responsible for handling support requests, reports, and incidents from the customers.

   2) The customer support and care representative may use various means of communication with the customers (e.g., email, web)

5.1.2.7 Inter-cloud provider

An inter-cloud provider offers part or total cloud services. The activities of the inter-cloud provider may involve working as intermediaries, aggregation, arbitrage, peering, and interfacing between cloud service providers.

a) Peer cloud service management:

   1) The inter-cloud provider selects and uses one or more services from peer cloud service providers.

2) To ensure that the cloud service meets the agreed SLA, the inter-cloud provider reports and resolves issues related to peer cloud service providers.

3) The inter-cloud provider manages business tasks, such business plans and financial processing, including those of peer cloud service providers.

4) The inter-cloud provider understands the service usage of peer cloud providers and makes sure that their services are adequate for the business plan.

5) The inter-cloud provider integrates cloud services of peer cloud service providers and monitors service implementations to ensure successful fulfilment of business objectives.

6) The inter-cloud provider coordinate identity and security credentials between the cloud service customer and peer cloud service providers.

a) Peering, federation, brokerage, aggregation, and arbitrage transactions:

1) The inter-cloud provider manages peering, which refers to the use of cloud services from peer cloud providers.

2) The inter-cloud provider manages federation provided to consumers through service integration between peer clouds.

3) The inter-cloud provider manages cloud service brokerage.

4) The inter-cloud provider oversees access management for cloud services, provision of cloud service APIs (application programming interface), ID management, performance reporting, and enhanced security.

5) The inter-cloud provider manages integration between the cloud provider and peer cloud provider.

6) The inter-cloud provider manages arbitrage transactions by selecting one of the services provided by peer cloud service providers.

5.1.2.8 Cloud service security and risk manager

A cloud service security and risk manager shall be responsible for managing risks to the services the provider offers and for making sure that security requirements in SLAs are met.

a) Security and risk management:

1) The cloud service security and risk manager defines information security policies.

2) The cloud service security and risk manager understands service requirements, statutory and regulatory requirements, and contract and SLA obligations.

3) The cloud service security and risk manager defines information security risks related to cloud services and remedies to the risks.

4) The cloud service security and risk manager develops information security controls to address risks.

5) The cloud service security and risk manager controls identity and access management.

6) The cloud service security and risk manager discovers, classifies, and protects data and information assets.

7) The cloud service security and risk manager acquires and oversees the information systems.

8) The cloud service security and risk manager protects infrastructure from threats and vulnerabilities.

  9) The cloud service security and risk manager oversees information security incidents.

  10) The cloud service security and risk manager puts in place security governance and ensures its compliance.

  11) The cloud service security and risk manager manages personal security, network and communication security, and multi-tenant issues.

  12) The cloud service security and risk manager make sure that controls are in place to safeguard against security breaches for the deployed services and infrastructure.

  13) The cloud service security and risk manager designs, implements, and evaluates system and application program security.

  14) The cloud service security and risk manager manages, designs, implements, and evaluates security.

  15) The cloud service security and risk manager evaluates and adjusts implemented controls according to outcomes.

b) Service continuity: the cloud service security and risk manager designs and implements service continuity measures. The manager considers potential failure modes of the cloud service and support infrastructure. The recovery process may be deployed so that the cloud service can be used within the terms of the SLA through failover and redundancy.

c) Conformity assurance:

  1) The cloud service security and risk manager ensures that the cloud service and support infrastructure are in line with standardized requirements such as an authentication system.

  2) The cloud service security and risk manager ensures that applicable regulatory requirements for the service or data are met.

5.1.2.9 Network provider

A network provider is an essential stakeholder in health cloud services. The services of the network provider include:

a) Provision of network connection: the network provider enables network connection and provides connection between the cloud customer and the provider in various forms (e.g., VPNs or dedicated bandwidth connections).

b) Provision of network services: the network provider provides network-related services such as firewalls.

c) Provision of network management services: the network provider offers operation and maintenance of cloud network infrastructure, traces network resources and offers resource allocation methods, and performs repairs and upgrades in the network infrastructure.

5.2 Service support

5.2.1 Service catalogue

The cloud service provider shall provide a catalogue of its services to help the customer make informed decisions.

a) The catalogue shall provide the consumer with information such as the types, performances, and prices of the cloud services to choose from

b) The catalogue shall be made available as a document on the web.

5.2.2 Service coverage

Services, both included and excluded, shall be specified in the form of a list.

a) The cloud service provider specifies both covered and uncovered service items in a list format.

b) The cloud service provider provides details for each item in the list.

c) The cloud service provider provides details on additional service options, if available.

5.2.3 Uninterrupted service

The cloud service provider shall ensure continuous operation of the service (e.g., 24-hour operation) to the customer 365 days a year.

a) The cloud service provider should monitor and measure service availability and inform the customers of the service status quo.

b) The cloud service provider should monitor and manage availability rate maintenance capability, availability monitoring support, and availability rate measurement.

c) The cloud service provider shall specify compensation for failure in case of unmet availability as agreed-upon with the customer.

5.2.4 Accountability for service interruption

The cloud service provider shall specify responsibilities assumed by the cloud service provider for end of service in caser of service interruptions.

5.2.5 Compensation for service interruption

The cloud service provider shall compensate for service interruption. The cloud service provider shall specify compensation in ways agreed-up with the customer (e.g., monetary compensation or an extension of subscription period, or credits to the customer account).

5.2.6 Service downtime

The cloud service provider shall announce service downtimes, which are periods in which the cloud services are unavailable, for planned maintenance or as required for specific purposes.

5.2.7 Service disruption notification

The cloud service provider shall notify the customer of service disruptions due to:

a) power outage.

b) network connectivity issues.

c) scheduled or unscheduled maintenance.

d) failure in backup operation.

e) natural disasters.

f) software malfunctioning (e.g., software bugs).

g) a hacking or denial of service attack.

h) human errors.

5.2.8 Target response time

The cloud service provider shall provide target response times for services, which include response measurements, levels of response times for different services. Standards for performance benchmarking (e.g., TPC, SPEC) should be used in performance benchmarking.

5.2.9 Information on subcontractors

The cloud service provider shall disclose the obligations and tasks of a subcontracted provider, if applicable.

a) When the cloud service provider consigns the service, in whole or in part, the scope and business details of the consignment shall be disclosed.

b) The cloud service provider shall ensure that the consignee adheres to the original contract during consignment.

c) When consignment recurs, or changes occur from the original contract, the cloud service provider should obtain prior consent of the customer. The customer may be able to disagree with the consignment or terminate the contract in consideration of its impact on services (e.g., increased security risks).

d) When information protection is concerned, the tasks related to it shall not be consigned to a subcontractor.

5.3 Service model

a) The cloud service provider and the customer may specify the cloud service model (e.g., IaaS, SaaS, PaaS) to be used.

b) The cloud service provider should specify whether the cloud is private, public, or hybrid in the service catalogue

5.4 Service monitoring

The cloud service provider shall provide indicators and parameters related to service monitoring based on the metric model employed.

a) The cloud service provider should provide a webpage or a program by which to monitor services.

b) Indicators for system resource monitoring should be provided that include:

- CPU utilization
- network traffic volume
- amount of traffic loss
- data transfer rate
- resource utilization rate
- disruption frequency

5.5 Incident reporting

5.5.1 Incident report

An incident report format shall be determined in mutual agreement between the cloud service provider and the customer.

a) The incident report should contain incident types (e.g., natural disaster, provider error, user error, unknown cause, etc.).

b) The incident report should contain the cause of the incident and the measures taken to for the incident.

c) The incident report shall contain compensation criteria (e.g., based on disruption duration, service credits) for each incident.

d) After resolving the incident, the cloud service provider shall submit a follow-up report to the customer.

5.5.2 Incident response

The cloud service provider should develop a manual that details the response procedures and provide it to the customer.

5.5.3 Incident report delivery

a) The cloud service provider shall provide documented response and management plans for the incident.

b) The means by which the report should be delivered should be agreed upon between the customer and the cloud service provider.

5.5.4 Repair time

A target mean time to repair (MTTR) should be determined and included in the SLA.

5.6 Standards, testing, and certification

5.6.1 Conformity with international standards

The cloud service provider shall conform to the international standards related to cloud services.

a) The cloud service provider shall conform to the ISO/TC 215 international standards on medical data and information.

b) The cloud service provider shall conform to ISO/IEC JTC 1 international standards on cloud computing.

c) The cloud service provider shall conform to ISO/IEC JTC 1 international standards on information protection.

5.6.2 Guidelines for ensuring compatibility between clouds

Guidelines shall be available to ensure compatibility between in-house systems and cloud systems. There shall be a standard that ensures compatibility between private clouds and public clouds.

5.6.3 Support data input

The cloud service provider shall support data input based on healthcare informatics international standards.

5.6.4 Adopt international standards

Health-informatics international standards (e.g., HL7 FHIR) shall be adopted.

5.6.5 Compliance with non-international standards

Standards set by each country, region, or jurisdiction shall be observed.

5.6.6 Compliance test

Official tests for standard compliance may be performed and made available to the customer.

5.6.7 Compliance with updated standards

Processes by which to inspect compliance with updated standards shall be provided.

5.6.8 Certification details

The cloud service provider may provide details of certification obtained from a third party institution to the customer.

5.7 Data location

5.7.1 Cloud service area and location

The cloud service provider shall specify the area/location of the cloud service used by the customer.

5.7.2 Cloud relocation

a) The cloud service provider shall inform the customer of cloud relocation.

b) If there will be a change of the physical location of the cloud service, a prior agreement between the cloud service provider and the customer shall be in place.

c) The cloud service provider shall provide an advance notice to the customer in case of cloud relocation.

5.7.3 Violation of advance notice

Liabilities shall be established for the violation of the advance notice period.

5.8 Data governance

5.8.1 Cloud data maintenance policy

The cloud service provider shall provide data maintenance policies to the customer.

a) The policy includes information on data retention periods.

b) The policy ensures compliance with applicable legislation or guidance (e.g., GDPR)

NOTE Local, regional, or national guidance or legislation can apply.

5.8.2 Cloud data backup plan

The cloud service provider shall provide data backup plans to the customer that include:

a) Backup media shall be specified (e.g., physical or virtual media).

b) Backup periods shall be specified.

5.8.3 Cloud data collection

The cloud service provider shall comply with rules concerning data collection, storage, and queries.

5.8.4 Cloud data query history

The cloud service provider shall deliver data query history to the customer in the forms that can be as:

a) a web server UI.

b) e-mail.

c) texts service.

d) phone.

e) The history shall be delivered in at least one of the forms, or via a similar method on which the cloud service provide and the customer agree.

5.9 Data security

General considerations for security and privacy of data in cloud computing is summarized in A.1.

5.9.1 Technical security measures

The cloud service provider shall establish technical security measures.

a) Network security: it is necessary to put in place access controls to user terminals used.

b) System and virtualization security: user session management plans should be in place.

c) Data storage and management: standard practices of managing customer-owned data should be in place.

d) User authentication and access management: user accounts and access management policies, and user rights for specific information and situations shall be established.

5.9.2 Administrative security measures

The cloud service provider shall establish administrative security measures.

a) Personnel security: comply with management and security responsibilities of internal and external personnel.

b) Classification and control of information assets: asset lists with ownership and management responsibilities, definitions, and control measures should be prepared.

c) Emergency response system and accident management: emergency response systems and recovery plans should be prepared.

d) The cloud service provider should conform to laws and regulations on service provisions.

5.9.3 Physical security measures

The cloud service provider shall establish physical security measures.

a) The cloud service provider shall secure data by keeping the geographical locations of the data centers where the data are housed.

b) The cloud service provider should put in place rules and regulations for anyone accessing to data, and should establish countermeasures when they are breached,

5.9.4 Simulation for technical security measures

The cloud service provider may conduct a series of simulations to help customers make informed decisions on technical security measures.

5.9.5 Data integrity assurance

The cloud service provider shall provide data integrity assurance methods to the customer.

5.9.6 De-identification

Anonymized or aliased personal information is applicable in cloud services. The cloud service provider shall provide a way to ensure anonymity of customer data.

a) The cloud service provider shall provide the level of anonymity applied to customer data.

b) The cloud service provider shall gain prior consent of the customer for the information to be de-identified.

c) De-identification techniques (e.g., encryption, pseudonymization) should be employed.

d) The cloud service provider should evaluate whether de-identification is properly performed.

5.10 Data transfer

5.10.1 Data transfer deadline

The cloud service provider shall specify a deadline for data transfer upon expiry of the agreement.

5.10.2 Data transfer method

The cloud service provider shall specify methods of data transfer upon expiry of the agreement

5.10.3 Data transfer roles

Roles concerning data transfer upon expiry of the agreement shall be specified.

5.10.4 Data deletion method

Methods of data deletion upon expiry of the agreement shall be specified.

5.10.5 Data transfer customer approval

Data transfer shall be made after the cloud service provider gains explicit approval of the customer.

5.10.6 Approved data transfer range

Data transfer shall be performed within the range approved by customers.

5.10.7 Responsibilities for data transfer violation

Liabilities shall be established for any violation of data transfer approved by the customer.

5.11 Billing system and operation policies

5.11.1 Billing system criteria

The cloud service provider shall present clear criteria for its billing system.

5.11.2 Internal cloud operational policy

The cloud service provider should provide internal cloud operation policies to the customer.

5.11.3 Billing for excess usage

The cloud service provider shall explain its billing policy for excess usage to the customer and the policy should be specified in the service catalogue.

5.12 Payments

5.12.1 Payment method/time

The cloud service provider should provide details on the method and time for payment and payment information should be made available to the customer in real time.

5.12.2 Payment period

The cloud service provider shall specify the payment period (e.g., monthly or yearly) for services used by the customer. The cloud service provider shall provide details on service payment when signing a contract.

5.12.3 Payment method

The cloud service provider shall provide payment methods (service unit) for services used by the customer.

a) Detailed service fees shall be posted on the company's website.

b) The fees should be calculated for each calendar month, from the first day of a month to the end of the month.

5.12.4 Explanation of billing details

The cloud service provider shall provide billing that details charges (or discount) for any excess use of services. If the customer has used the cloud service more than the contracted service range, it is necessary to calculate and present the overuse in detail.

5.13 Regulatory compliance

5.13.1 Jurisdiction compliance

The provisions in the agreement should describe activities falling under the range of responsibilities of the customer and of the cloud service provider regarding laws and regulations.

5.14 Service update and version management

5.14.1 Service update notification

The cloud service provider shall give a prior notice of service renewal to the customer.

5.14.2 Change notification upon service update

The cloud service provider shall inform the customer of expected changes with service update.

a) Service version upgrades should be announced in advance.

b) Updated content shall be announced in advance.

c) Information on changes made (e.g., service addition, deletion, modification) shall be made available to the customer.

5.14.3 Service update stability assessment

The cloud service provider shall assess whether service stability is affected by updates and provide the assessment results to the customer. Assessment metrics should be used in ways that make it possible to ascertain service stability.

5.14.4 Service version management

The cloud service provider shall make available (e.g., via documents, email or website) the service version history to the customer

5.15 Agreement renewal and expiry

When the customer seeks to renew the agreement with the same cloud service provider, any change or variation in the pricing/billing should be provided to the customer in advance before the contract is finalized. It would be desirable for the cloud service provider to provide a means to the customer by which to estimate costs related to services to be subscribed to, as shown in B.2.

Annex A
(informative)

Summary of security and privacy and metric model components

A.1 ISO/TR 21332

ISO/TR 21332 provides an overview of security and privacy considerations for Electronic Health Record (EHR) in a cloud computing service. From the vantage point of organizations and patients using health information systems on cloud services, security and privacy protection of EHRs are one of the key factors for consideration.

Security features of a cloud system take into consideration multiple factors (6.6) such as auditability, availability of information, governance, and maintenance. Information security policies an organization adopts should reflect such considerations as business strategies, applicable laws and regulations, and present and future security threats. Topic-level policy considerations (7.1) are also presented in the document. Security policies should be accessible and understandable in formats that do not risk disclosure of confidential information. The document also provides some precautionary notes specific to telework and use of portable devices (7.2.1) such as distribution of malicious code, unauthorized access to sensitive data, attach-vulnerable software/system, possibility of excluding critical security applications, danger of malwares in the devices and others.

The document describes various aspects to consider in relation to information security policies (7.3), such as information security concerns (e.g., resource redundancy) that may impact service availability (7.3.2); security measures to consider in line with different cloud deployment models (7.3.3) (e.g., public, private, community and hybrid clouds); use of security information and event management (SIEM) capability (7.3.4); considerations to be taken when introducing cryptography policies (7.3.5).

Other aspects in relation to information security polies relate to data retention, backup and deletion (7.3.6), especially when the data contain personally identifiable information (PII) or personal health information (PHI); policies that govern access control (e.g., control rules and access rights) to information assets (7.3.7); considerations on legal accountability in case of data breach (7.3.7.2), disaster recovery (7.3.9).

A.2 ISO/IEC TR 23951

ISO/IEC TR 23951 introduces guidance for using the ISO/IEC 19086-2 metric model.

The service provider uses various indicators in the metrics such as service volume. They are presented as service-level objectives, which should be described, measurable and guaranteed in the SLA.

The metrics in an SLA are often ambiguous or incomplete and ways to solve the ambiguity were suggested. The document also introduces examples showing how to configure cloud service performance measurement using templates. Service level objectives are assessed by measurable characteristics. Tables are used to make detailed and practical templates with examples. Table A.1 shows the metric model index components in the document.

Table A.1 — Metric model index components [SOURCE: ISO/IEC TR 23951]

Metric (id)	
attribute	Value
id	(1..1) A unique identifier for the metric.
description	(0..n) A description of the metric. A case where several instances of this attribute are used is when descriptions are provided in multiple languages.
source	(1..1) The individual or organization that created this metric definition.
scale	(1..1) Classification of the type of measurement result when using the metric. The value of scale is one of: nominal, ordinal, interval, or ratio.
category	(0..1) A grouping of metrics of similar characteristics or intent (e.g., “cloud elasticity” or “cloud service availability”) and sharing comparable expressions, rules or parameters.
Note	(0..n) additional information about the metric and how to use it.
associated element	Reference
Expression	(0..1) id of the main expression of the metric (the expression of the calculation of the metric). Expressions can reference other expression ids, metric ids, and parameter ids. This field represents a relationship to the main expression element (identified by its id) described in a separate table (see the “Set of Expressions” table).
Parameter	(0..n) id of a parameter used by the metric. This field represents a relationship to a parameter (identified by its id), described in a separate table (see the “Set of Parameters” table).
Rule	(0..n) id of a rule used by the metric. This field represents a relationship to a rule (identified by its id), described in a separate table (see the “Set of Rules” table).
Underlying Metric	(0..n) id of another metric used in support of this metric. This field represents a relationship to the underlying metric (identified by its id). To each referenced underlying Metric corresponds a set of tables {Metric, Set of Expressions, Set of Rules, Set of Parameters}.
Underlying Expression	(0..n) id of an expression used in support of the main expression of this metric. This field represents a relationship to an expression (identified by its id), described in a separate table (see the “Set of Expressions” table).