TECHNICAL REPORT

ISO/TR 21332

First edition
2021-04

Health informatics — Cloud computing considerations for the security and privacy of health information systems

Informatique de santé — Considérations relatives à l'informatique en nuage pour la sécurité et la confidentialité des systèmes d'information de santé

Reference number
ISO/TR 21332:2021(E)

© ISO 2021



COPYRIGHT PROTECTED DOCUMENT

© ISO 2021

All rights reserved. Unless otherwise specified, or required in the context of its implementation, 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
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 ..... **iv**
Introduction ..... **v**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Abbreviated terms **6**
5 Cloud computing **6**
5.1 General 6
5.2 Overview of cloud computing 6
5.3 Cloud computing roles and activities 8
5.4 Cloud capabilities types and cloud service categories 8
5.5 Cloud deployment models 9
5.6 Cloud computing information system security capabilities 11
6 Considerations for health information in cloud computing environment **12**
6.1 Overview 12
6.2 Health information security 14
6.2.1 Overview of Teleworking Policies and Procedures 14
6.2.2 Telework and portable devices 14
6.3 Information security policies 15
6.3.1 Overview 15
6.3.2 Information security and protection of PII and PHI 15
6.3.3 Availability 16
6.3.4 Cloud deployment models considerations 17
6.3.5 Audit trail and logs 17
6.3.6 Cryptography and obfuscation 18
6.3.7 Retention, backup, and deletion 19
6.3.8 Access control and multi-client segmentation 19
6.3.9 Change management 21
6.3.10 Disaster recovery 21
6.3.11 Testing and evaluation 22
6.3.12 Information management 22
Annex A (informative) **Example guidance from the UK for selecting and risk managing cloud based digital health services** **24**
Annex B (informative) **Detailed advice and guidance** **30**
Annex C (informative) **Service classification recommendations** **50**
Bibliography **52**

© ISO 2021 – All rights reserved

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 2021 – All rights reserved

Introduction

This document identifies core Electronic Health Record (EHR) security and privacy requirements where cloud computing services are utilized. Additional requirements may also be needed where local legal or regulatory requirements exist. Potential additions or modifications can be considered by the cloud service providers in their contractual arrangements.

Cloud computing usage and adoption is becoming popular for healthcare applications worldwide. However, there are health information systems in the market that were not originally designed to operate in such an environment. The appeal and reasons for use that lead to cloud computing adoption are varied, but the available solutions do not always take into account the necessary security and privacy precautions and the necessary measures for secure use of this platform. Migration is a key consideration, as is the design of new systems to account for this type of environment.

The security and privacy of EHRs are paramount considerations for organizations that use health information systems based on cloud services, and for the patient's trust and confidence that their information is processed and stored safely and securely.

This document includes perspective of health information on cloud computing and health informatics requirements. It also provides guidance on selecting service providers in the public cloud for safely locating healthcare data, and confidential patient information (including solutions on handling of data off-shoring).

© ISO 2021 – All rights reserved

Health informatics — Cloud computing considerations for the security and privacy of health information systems

1 Scope

This document provides an overview of security and privacy considerations for Electronic Health Records (EHR) in a cloud computing service that users can leverage when selecting a service provider.

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 terminological databases for use in standardization at the following addresses:

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

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

3.1
application capabilities type
cloud capabilities type (3.2) in which the *cloud service customer* (3.8) can use the *cloud service provider's* (3.11) 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* (3.8), based on resources used

Note 1 to entry: The cloud capabilities types are *application capabilities type* (3.1), *infrastructure capabilities type* (3.24) and *platform capabilities type* (3.31).

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

3.3
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

Note 1 to entry: Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.

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

3.4
cloud deployment model
way in which *cloud computing* (3.3) can be organized based on the control and sharing of physical or virtual resources

Note 1 to entry: The cloud deployment models include community cloud, hybrid cloud, private cloud and public cloud.

© ISO 2021 – All rights reserved

[SOURCE: ISO/IEC 17788:2014, 3.2.7]

3.5
cloud service
one or more capabilities offered via *cloud computing* (3.3) invoked using a defined interface

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

3.6
cloud service category
group of *cloud services* (3.5) that possess some common set of qualities

Note 1 to entry: A cloud service category can include capabilities from one or more *cloud capabilities types* (3.2).

[SOURCE: ISO/IEC 17788:2014, 3.2.10]

3.7
cloud service customer data
class of data objects under the control, by legal or other reasons, of the *cloud service customer* (3.8) that were input to the *cloud service* (3.5), or resulted from exercising the capabilities of the *cloud service* (3.5) by or on behalf of the *cloud service customer* (3.8) via the published interface of the *cloud service* (3.5)

Note 1 to entry: An example of legal controls is copyright.

Note 2 to entry: It may be that the *cloud service* (3.5) contains or operates on data that is not *cloud service customer* data; this might be data made available by the *cloud service providers* (3.11), or obtained from another source, or it might be publicly available data. However, any output data produced by the actions of the *cloud service customer* (3.8) using the capabilities of the *cloud service* (3.5) on this data is likely to be *cloud service customer data* (3.7), following the general principles of copyright, unless there are specific provisions in the *cloud service* (3.5) agreement to the contrary.

[SOURCE: ISO/IEC 17788:2014, 3.2.12]

3.8
cloud service customer
CSC
party which is in a business relationship for the purpose of using *cloud services* (3.5)

Note 1 to entry: A business relationship does not necessarily imply financial agreements.

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

3.9
cloud service derived data
class of data objects under *cloud service provider* (3.11) control that are derived as a result of interaction with the *cloud service* (3.5) by the *cloud service customer* (3.8)

Note 1 to entry: *Cloud service* (3.5) derived data includes log data containing records of who used the service, at what times, which functions, types of data involved and so on. It can also include information about the numbers of authorized users and their identities. It can also include any configuration or customization data, where the *cloud service* (3.5) has such configuration and customization capabilities.

[SOURCE: ISO/IEC 17788:2014, 3.2.13]

3.10
cloud service partner
party which is engaged in support of, or auxiliary to, activities of either the *cloud service provider* (3.11) or the *cloud service customer* (3.8), or both

[SOURCE: ISO/IEC 17788:2014, 3.2.14]

© ISO 2021 – All rights reserved

3.11
cloud service provider
party which makes *cloud services* (3.5) available

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

3.12
communications as a service
CaaS
cloud service category (3.6) in which the capability provided to the *cloud service customer* (3.8) is real time interaction and collaboration

Note 1 to entry: CaaS can provide both *application capabilities type* (3.1) and *platform capabilities type* (3.31).

[SOURCE: ISO/IEC 17788:2014, 3.2.18]

3.13
community cloud
cloud deployment model (3.4) where *cloud services* (3.5) exclusively support and are shared by a specific collection of *cloud service customers* (3.8) who have shared requirements and a relationship with one another, and where resources are controlled by at least one member of this collection

[SOURCE: ISO/IEC 17788:2014, 3.2.19]

3.14
compute as a service
CompaaS
cloud service category (3.6) in which the capabilities provided to the *cloud service customer* (3.8) are the provision and use of processing resources needed to deploy and run software

Note 1 to entry: To run some software, capabilities other than processing resources may be needed.

[SOURCE: ISO/IEC 17788:2014, 3.2.20]

3.15
cyber-incident
cyber-event that involves a loss of information security or impacts business operations

[SOURCE: ISO/IEC 27102:2019, 3.1]

3.16
cyber-insurance
insurance that covers or reduces financial loss to the insured caused by a *cyber-incident* (3.15)

[SOURCE: ISO/IEC 27102:2019, 3.2]

3.17
cyber-risk
risk caused by a *cyber-threat* (3.18)

[SOURCE: ISO/IEC 27102:2019, 3.4]

3.18
cyber-threat
threat that exploits a *cyberspace* (3.19)

[SOURCE: ISO/IEC 27102:2019, 3.5]

3.19
cyberspace
interconnected digital environment of networks, services, systems, and processes

[SOURCE: ISO/IEC 27102:2019, 3.6]

© ISO 2021 – All rights reserved

3.20
insured
entity that shares or considers sharing *cyber-risk* (3.17) with an insurer

[SOURCE: ISO/IEC 27102:2019, 3.7]

3.21
data storage as a service
DSaaS
cloud service category (3.6) in which the capability provided to the *cloud service customer* (3.8) is the provision and use of data storage and related capabilities

Note 1 to entry: DSaaS can provide any of the three *cloud capabilities types* (3.2).

[SOURCE: ISO/IEC 17788:2014, 3.2.22]

3.22
hybrid cloud
cloud deployment model (3.4) using at least two different *cloud deployment models* (3.4)

[SOURCE: ISO/IEC 17788:2014, 3.2.23]

3.23
infrastructure as a service
IaaS
cloud service category (3.6) in which the *cloud capabilities type* (3.2) provided to the *cloud service customer* (3.8) is an *infrastructure capabilities type* (3.24)

Note 1 to entry: The *cloud service customer* (3.8) does not manage or control the underlying physical and virtual resources, but does have control over operating systems, storage, and deployed applications that use the physical and virtual resources. The *cloud service customer* (3.8) may also have limited ability to control certain networking components (e.g. host firewalls).

[SOURCE: ISO/IEC 17788:2014, 3.2.24]

3.24
infrastructure capabilities type
cloud capabilities type (3.2) in which the *cloud service customer* (3.8) can provision and use processing, storage or networking resources

[SOURCE: ISO/IEC 17788:2014, 3.2.25]

3.25
network as a service
NaaS
cloud service category (3.6) in which the capability provided to the *cloud service customer* (3.8) is transport connectivity and related network capabilities

Note 1 to entry: NaaS can provide any of the three *cloud capabilities types* (3.2).

[SOURCE: ISO/IEC 17788:2014, 3.2.28]

3.26
personally identifiable information
PII
any information that (a) can be used to establish a link between the information and the natural person to whom such information relates, or (b) is or can be directly or indirectly linked to a natural person

Note 1 to entry: The “natural person” in the definition is the PII principal. To determine whether a PII principal is identifiable, account should be taken of all the means which can reasonably be used by the privacy stakeholder holding the data, or by any other party, to establish the link between the set of PII and the natural person.

[SOURCE: ISO/IEC 29100:2011/Amd.1:2018, 2.9]

© ISO 2021 – All rights reserved

3.27
PII controller
privacy stakeholder (or privacy stakeholders) that determines the purposes and means for processing *personally identifiable information (PII)* (3.26) other than natural persons who use data for personal purposes

Note 1 to entry: A PII controller sometimes instructs others (e.g. *PII processors* (3.29)) to process *PII* (3.26) on its behalf while the responsibility for the processing remains with the PII controller.

[SOURCE: ISO/IEC 29100:2011, 2.10]

3.28
PII principal
natural person to whom the *personally identifiable information (PII)* (3.26) relates

Note 1 to entry: Depending on the jurisdiction and the particular *PII* (3.26) protection and privacy legislation, the synonym "data subject" can also be used instead of the term *"PII principal"* (3.28).

[SOURCE: ISO/IEC 29100:2011, 2.11]

3.29
PII processor
privacy stakeholder that processes *personally identifiable information (PII)* (3.26) on behalf of and in accordance with the instructions of a *PII controller* (3.27)

[SOURCE: ISO/IEC 29100:2011, 2.12]

3.30
platform as a service
PaaS
cloud service category (3.6) in which the *cloud capabilities type* (3.2) provided to the *cloud service customer* (3.8) is a *platform capabilities type* (3.31)

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

3.31
platform capabilities type
cloud capabilities type (3.2) in which the *cloud service customer* (3.8) 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* (3.11)

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

3.32
private cloud
cloud deployment model (3.4) where *cloud services* (3.5) are used exclusively by a single *cloud service customer* (3.8) and resources are controlled by that *cloud service customer* (3.8)

[SOURCE: ISO/IEC 17788:2014, 3.2.32]

3.33
public cloud
cloud deployment model (3.4) where *cloud services* (3.5) are potentially available to any *cloud service customer* (3.8) and resources are controlled by the *cloud service provider* (3.11)

[SOURCE: ISO/IEC 17788:2014, 3.2.33]

© ISO 2021 – All rights reserved

3.34
software as a service
SaaS
cloud service category (3.6) in which the *cloud capabilities type* (3.2) provided to the *cloud service customer* (3.8) is an *application capabilities type* (3.1)

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

3.35
reversibility
process for *cloud service customers* (3.8) to retrieve their *cloud service customer data* (3.7) and application artefacts and for the *cloud service provider* (3.11) to delete all *cloud service customer data* (3.7) as well as contractually specified *cloud service derived data* (3.9) after an agreed period

[SOURCE: ISO/IEC 17788:2014, 3.2.35]

4 Abbreviated terms

EHR Electronic Health Record

NHS National Health System

PHI Personal Health Information

SDO Standard Development Organizations

SIEM Security Information and Event Management

WAN Wide Area Network

5 Cloud computing

5.1 General

Cloud computing is an evolving paradigm. This is not intended to prescribe or constrain any particular method of deployment, service delivery, or business operation.

There are known risks to confidentiality and security using a cloud computing environment. However, the use of a cloud computing architecture over advanced technologies can produce valuable benefits. The challenge for health informatics is what deployment method to use with the available resources to maintain a trusted yet useful service.

5.2 Overview of cloud computing

This overview introduced the following.

a) **Six key cloud computing characteristics:**

   i) Broad network access

   It is a feature where the physical and virtual resources are available over a network and accessed through standard mechanisms that promote use by heterogeneous client platforms. The focus of this key characteristic is that cloud computing offers an increased level of convenience in that users can access physical and virtual resources from wherever they need to work, as long as it is network accessible, using a wide variety of clients, including devices such as mobile phones, tablets, laptops, and workstations.

   ii) Measured service

 © ISO 2021 – All rights reserved