PD ISO/TR 21332:2021

BSI Standards Publication

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



bsi.

# National foreword

This Published Document is the UK implementation of ISO/TR 21332:2021.

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.


Published by BSI Standards Limited 2021

ISBN 978 0 539 00603 2

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 31 May 2021.

**Amendments/corrigenda issued since publication**

| Date | Text affected |
|---|---|

PD ISO/TR 21332:2021

TECHNICAL REPORT

**ISO/TR 21332**

First edition
2021-03-31

# 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 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

# 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

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).

**TECHNICAL REPORT** **ISO/TR 21332:2021**

# 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.