PD ISO/IEC TS 21419:2024

BSI Standards Publication

Information technology — Cross-jurisdictional and societal aspects of implementation of biometric technologies — Use of biometrics for identity management in healthcare

Documents
Document Sharing Hub

Full document details: PD ISO/IEC TS 21419:2024

National foreword

This Published Document is the UK implementation of ISO/IEC TS 21419:2024.

The UK participation in its preparation was entrusted to Technical Committee IST/44/-/6, Cross-jurisdictional and societal aspects.

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 2024
Published by BSI Standards Limited 2024

ISBN 978 0 539 13955 6

ICS 35.240.15; 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 30 November 2024.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: PD ISO/IEC TS 21419:2024

Technical Specification

ISO/IEC TS 21419

Information technology — Cross-jurisdictional and societal aspects of implementation of biometric technologies — Use of biometrics for identity management in healthcare

First edition
2024-11

Reference number
ISO/IEC TS 21419:2024(en)

© ISO/IEC 2024

Documents
Document Sharing Hub

Full document details: PD ISO/IEC TS 21419:2024

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2024

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

Documents
Document Sharing Hub

Full document details: PD ISO/IEC TS 21419:2024

Contents

Page

Foreword ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Abbreviated terms ... **3**
5 Identity management in the context of healthcare-related implementation issues ... **3**
5.1 Problems for identity management in healthcare ... 3
5.1.1 Overview ... 3
5.1.2 Availability of essential medical records ... 3
5.1.3 Integration and acceptance of patient treatment recording in private homes ... 3
5.1.4 Medical facility verification of patient identity ... 4
5.1.5 Identity theft for access to medical treatment and related benefits ... 4
5.1.6 Proper vetting of medical and ancillary staff ... 4
5.1.7 Effective correlation of patient data needed for medical and pharmaceutical research ... 4
5.2 How this document can address these problems ... 4
6 Potential advantages of using appropriately designed biometric systems ... **5**
7 Healthcare use cases where biometrics can potentially bring value ... **5**
7.1 General ... 5
7.2 Priority group 1 ... 6
7.2.1 Use case 5: Fast checking of patient identity in a hospital ... 6
7.2.2 Use case 7: eHealth: remote monitoring of patient ... 8
7.3 Priority group 2 ... 11
7.3.1 Use case 1: Global logical access control of medical staff in the hospital ... 11
7.4 Priority Group 3 ... 12
7.4.1 Use case 2: Teleconsultation ... 12
7.4.2 Use case 8: Patient authentication for public health, vaccination ... 14
7.4.3 Use case 9: Identification of citizens in public health to monitor a pandemic situation ... 15
7.5 Priority Group 4 ... 16
7.5.1 Use case 3: Local logical access control of medical staff in the hospital ... 16
7.6 Priority Group 5 ... 17
7.6.1 Use case 4: Physical access control to restricted zones in the hospital ... 17
7.6.2 Use case 6: Registration and control of medical practitioners ... 19
8 Technical design and implementation — challenges and guidance ... **21**
8.1 Guidance on identity management in healthcare ... 21
8.2 Guidance on medical record sharing ... 21
8.3 Guidance on secure and consistent recording for patient treatment at home ... 22
9 Limitations on the use of biometrics for identity management in healthcare ... **23**
10 Coherent frameworks for identity management and use of biometrics in healthcare ... **23**
Annex A (informative) **Medical practitioners poll** ... **24**
Bibliography ... **25**

© ISO/IEC 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TS 21419:2024

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

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 document 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 or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 37, *Biometrics*.

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 and www.iec.ch/national-committees.

© ISO/IEC 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TS 21419:2024

Introduction

The purpose of this document is to raise awareness of the potential role of biometrics in identity management for medical and healthcare use, to analyze a number of use cases, and to provide feedback from healthcare practitioners on the use of biometrics in the cases selected.

To date, there has been little use of biometrics in support of healthcare provision in Western Europe. However, the use of biometrics is already starting to spread in other regions. Trials conducted in certain developing countries have shown positive trends and provided useful experience. The use of biometrics presents potentially great advantages in the following situations:

— for patients in enabling consistency of treatment between visits to different places of care;

— for hospital management in the simplification of procedures for ensuring the correct identity of patients at various stages of treatment, and in managing medical and support staff and recording their interactions with individual patients;

— in support of medical and pharmaceutical research, for the reliable correlation of anonymous records collected over time and across different locations from the treatment of consenting patients, with the assurance that these records (and the use of biometrics) cannot in context reveal the patient's personal identity.

In all of these examples, the use of biometrics should be combined with proven security techniques, and data protection procedures.

A large new field for the use of biometrics in healthcare is now opening, with the use of smartphones and other mobile devices for people monitoring their own health and physical activity at home and abroad. Used securely, with proper privacy protection for personal data, this can enable remote interaction with medical and support staff, and provide access for individuals to their own medical records.

© ISO/IEC 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TS 21419:2024

Documents
Document Sharing Hub

Full document details: PD ISO/IEC TS 21419:2024

Information technology — Cross-jurisdictional and societal aspects of implementation of biometric technologies — Use of biometrics for identity management in healthcare

1 Scope

This document describes potential applications of biometrics in identity management systems used for medical and healthcare purposes. It provides feedback from healthcare practitioners on the advantages, disadvantages, risks and priority of implementing certain use cases of healthcare with biometrics. For those use cases, information related to the selection of biometric type and associated measures related to security and privacy protection is provided to system designers.

The document concentrates on aspects of the subject which apply to the good management of healthcare services for patients who need monitoring, treatment and care in hospitals, clinics or at home, but can be incapacitated. It does not cover the measurement and interpretation of symptoms and biological data for the purposes of medical treatment or research.

The document is intended to be useful for the management of public and private healthcare systems anywhere in the world, and to commercial providers of identity management services and equipment. It is also potentially relevant to regulatory stakeholders addressing issues of privacy and legality, and the assessment of potential vulnerabilities in biometrics and identity management systems applied in the healthcare sector.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 2382-37, *Information technology — Vocabulary — Part 37: Biometrics*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 2382-37 and the following 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
identity management
processes and policies involved in managing the lifecycle and value, type and optional metadata of attributes in identities known in a particular domain

[SOURCE: ISO/IEC 24760-1:2019, 3.4.1, modified — Notes to entry have been removed.]

3.2
biometrics
automated recognition of individuals based on their behavioural and biological characteristics

© ISO/IEC 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TS 21419:2024

3.3
mobile device
compact, handheld, lightweight computing device

EXAMPLE Laptops, tablet PCs, wearable ICT devices, smartphones and USB gadgets.

3.4
personally identifiable information
PII
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 might 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 29100:2024, 3.7]

3.5
personal data
any information relating to an identified or identifiable natural person ("data subject")

Note 1 to entry: An identifiable natural person is one who can be identified, directly or indirectly (see ISO/IEC 24760-1).

Note 2 to entry: In the data protection requirements defined in ISO/IEC 24760-1, "biometric data" refers to personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images.

3.6
processing
any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

3.7
data controller
natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data

3.8
consent
any freely-given, specific, informed and unambiguous indication of the data subject's wishes by which they signify agreement, by a statement or by a clear affirmative action, to the processing of personal data relating to them

3.9
anonymization
process by which personally identifiable information (PII) is irreversibly altered in such a way that a PII principal can no longer be identified directly or indirectly, either by the PII controller alone or in collaboration with any other party

Note 1 to entry: See Reference [5] for further information.

[SOURCE: ISO 29100:2024, 3.2, modified — Note 1 to entry has been added].

© ISO/IEC 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TS 21419:2024

4 Abbreviated terms

FIDO Fast Identity Online (open industry association)

GP general practitioner

ICT information and communication technology

PII personally identifiable information

UNHCR United Nations Refugee Agency, formally known as the Office of the High Commissioner for Refugees

5 Identity management in the context of healthcare-related implementation issues

5.1 Problems for identity management in healthcare

5.1.1 Overview

Secure and effective identification of individual people is generally essential for the management of any healthcare system. However, this is difficult to achieve in large complex systems, such as the United Kingdom of Great Britain and Northern Ireland's National Health Service, or in North America where many different commercial organizations provide healthcare services.

The following subclauses present notable problems related to identity management in healthcare.

5.1.2 Availability of essential medical records

Data protection regulations significantly limit the sharing of personal medical information without the specific consent of the patient (see ISO/IEC 24760-1). This makes it difficult to ensure consistency of treatment between patients' visits to different places of care. For example, staff in hospitals are often unable to gain quick and full access to the relevant records of the patients they are treating.

The rapid advancement of ICT has shifted the performance of healthcare. In this context, some of the major concerns are related to the security, privacy, confidentiality and integrity of patients' data. Controlled access to medical records and medical information management systems is of paramount importance. The use of biometrics for authentication can play an important role in sustaining privacy and confidentiality for secure access of patients' medical records. It can also simplify access control processes currently in place. The objective in this context is to develop a healthcare information management system that embeds biometrics, as part of a multi-factor user authentication, where users are medical personnel.

It is sometimes necessary to transfer medical records between hospitals (e.g. when patients need assistance abroad). This is potentially best achieved under the control of the patients themselves, implying a need for access control for patients, so that they can access and transfer their own medical records. For this purpose, at the patient level, access control would benefit from biometric protection, as biometrics is the only thing patients carry with themselves at all times, even in the case of an accident occurring on the beach or in the context of a sporting activity, for example.

5.1.3 Integration and acceptance of patient treatment recording in private homes

Hospital and GP medical costs can often be saved by care or self-treatment at home, but secure remote access to consistent records by medical staff and by patients themselves cannot yet be organized, in spite of the increasing availability of sophisticated smartphone applications enabling people to monitor their own health.

Modern tele-homecare aims to create tele-care pathways able to enhance the quality and continuity of care by improving risk-adjusted patient outcomes, promoting patient safety, empowering patients, and optimizing the use of resources. In this respect, an envisaged remote monitoring system would need to be able to detect and identify, in a timely manner, possible pathological conditions critical for the progression

© ISO/IEC 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TS 21419:2024