Technical Specification

ISO/IEC TS 21419

First edition
2024-11

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

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

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) 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.

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.

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

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].

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

of patients that need to be closely monitored away from the hospital. This information could transit to the medical care team and allow them (with the patient's consent) to access it and start treatment on time and avoid possible secondary risk. Authentication, identification, record keeping or remote monitoring all help to address the same broad challenge. Medical professionals and healthcare facilities need to make the most efficient use of resources, among which space and time are premium.

5.1.4 Medical facility verification of patient identity

Current procedures for ensuring the correct identity of patients at various stages of hospital treatment are difficult to perform, notably if the patient is unconscious, and dangerous mistakes can occasionally occur.[6]

5.1.5 Identity theft for access to medical treatment and related benefits

Most healthcare systems usually provide emergency treatment without checking entitlement, but people who are not entitled to routine medical care, pharmacy provision and social security benefits can often obtain them through fraudulent claims of identity. This is difficult to detect and can cause large costs to government-provided healthcare programmes, and to companies which insure those who are actually entitled to treatment.

5.1.6 Proper vetting of medical and ancillary staff

Fraudulent identity claims by job applicants are not uncommon and can be difficult to detect, particularly when the job applicant is foreign to the place of employment. This is particularly dangerous when false medical qualifications can be claimed. Correct identification of medical staff authorized to access patient records remotely is also difficult to achieve.

5.1.7 Effective correlation of patient data needed for medical and pharmaceutical research

The reliable correlation of medical records collected over time and across different locations from the treatment of consenting patients is vitally important in supporting medical research and drug development. However, programs which anonymize medical data, thereby ensuring that patients' identity information is securely protected, have proven to be very difficult and very costly to develop and implement.

The use of real-world medical record data is essential for making the development and use of pharmaceuticals more effective and efficient, including in terms of research and development, regulatory decision making, health technology assessment, pricing, and reimbursement decisions and treatment. In order for this "learning system" to become a reality, it is necessary to establish and implement a governance security framework to encourage the availability and use of personal health data for the public interest.

5.2 How this document can address these problems

This document presents a number of different use cases in the field of healthcare for which biometrics could bring value. It analyses the value of biometrics for these use cases, and the value of biometrics for the stakeholders involved (patient, researchers, medical practitioners, etc.). A subset of use cases has been analyzed in more detail and reviewed by medical institutions to suggest a justified order of prioritization.

A clinical audit is a quality improvement process that seeks to improve patient care and outcomes through the systematic review of care against explicit criteria and the implementation of change. Such audits are important in ensuring:

1) that what needs be done is actually done, and

2) identification of the person who has performed each clinical process for a patient.

This falls within the sphere of clinical governance and forms part of the system for improving the standard of clinical practice.

6 Potential advantages of using appropriately designed biometric systems

Over time, where it is properly organized and delivered, the provision of secure biometric means for establishing and verifying human identity can help to solve many of the problems that are encountered with identity management in healthcare. The following list explains the potential contribution of biometric systems in this context.

a) Biometrics can provide the most acceptable and reliable identification method:

Different biometric modes and systems of implementation can be needed depending on the case to protect patients' privacy and the security of their associated medical data. Valuable experience is already available from trials and the deployment of biometric systems in advanced economies and in the developing world, which can enable reliable biometric technology to be chosen and applied in a way which can be safe and acceptable to most individual patients and members of medical staff.

b) Appropriately designed biometric-based systems can ensure effective anonymization:

Protection or segregation of personal data is key to the solution of several problems currently present in healthcare identity management. Use of biometric credentials, based on people's physical or behavioural characteristics, can be designed to identify them correctly without revealing their personal data to any unauthorized recipients. But a coherent, systematic and proactive threat-based security design is needed to ensure continuing effective data protection.

Biometric data, which in itself represents personal data, can also be managed is such a way that privacy is preserved (e.g. all biometric data remain under their owner's control).

c) Biometrics can enable appropriate data correlation for research needs:

Whereas the problems mentioned in Clause 5 can be tackled with systems using one-to-one matching of appropriately anonymized biometric templates, data correlation for research purposes will need successive one-to-many matching processes. The necessary computing resources do not need to be used in real time. While identification of individuals involved in ongoing operational medical procedures is required instantaneously, data for research needs will be used at a later time and can be processed more slowly.

d) Impact of secure data:

Restricted and monitored access to patient data can provide reassurance for patients, and can help to ensure data integrity across networked medial systems. This ultimately increases public trust in use of biometrics in healthcare.

e) Remote verification of identity using biometrics can be designed to work securely:

Further development work is needed to ensure the security and effectiveness of using biometrics for remote verification of identity from smartphones and other mobile devices. Technical information on this important subject is provided in ISO/IEC TR 30125.

7 Healthcare use cases where biometrics can potentially bring value

7.1 General

The following subclauses present use cases for biometrics in healthcare. They are described as user stories (or epics, because they are high level), from the point of view of the end-users, following the Agile framework.[7]

In the context of the EU project PANACEA,[11] all of the following use cases have been presented to a panel of healthcare operators, and the result of this presentation is addressed in Annex A of this document.

Use cases are presented with the same numbers used as when they were presented to the attendees of the PANACEA workshop. They are sorted by priority in this subclause based on the vote of the attendees of the panel as shown in Annex A.

1) Priority group 1:
   - Use case 5: Fast checking of patient identity in a hospital, see 7.2.1;
   - Use case 7: eHealth: remote monitoring of patient, see 7.2.2.
2) Priority group 2:
   - Use case 1: Global logical access control of medical staff in the hospital, see 7.3.1.
3) Priority group 3:
   - Use case 2: Teleconsultation, see 7.4.1;
   - Use case 8: Patient authentication for public health, vaccination, see 7.4.2;
   - Use case 9: Identification of citizens for public health to monitor a pandemic situation, see 7.4.3.
4) Priority group 4:
   - Use case 3: Local logical access control of medical staff in the hospital, see 7.5.1.
5) Priority group 5: (very low priority)
   - Use case 4: Physical access control to restricted zones in the hospital, see 7.6.1;
   - Use case 6: Registration and control of medical practitioners, see 7.6.2.

7.2 Priority group 1

7.2.1 Use case 5: Fast checking of patient identity in a hospital

7.2.1.1 Use case description

The use case can be described as follows:

As a doctor or nurse:

— I want to be certain of the identity of my patient, because in extremely rare cases treatment might be given to the wrong patient.

Currently, there are robust processes within hospitals to prevent “patient exchange” or unsuitable patient care due to wrong identification. This mostly consists of plastic wristbands attached physically to patients. Doctors and nurses have confidence in these processes. However, extremely infrequent errors can occur which can potentially ruin the reputation of the hospital, and of the person who made the mistake.

For medical practitioners, the most important use of fast patient identification is within the context of catastrophic events, for example, in situations of flooding, tsunami or earthquake. In such cases, there can potentially be no careful admission process in the hospital, no link to a patient health record, and the patient can often be unable to give their own identity. Fast patient identification also has further social benefits within this context, because during catastrophic events, there are often occurrences of identity thefts with the aim of benefitting from insurance or state help money.

In the hospital, the use case is mostly a requirement from the patient's point of view, as they can fear receiving the wrong operation or wrong treatment.

As a patient:

— I want my doctor or nurse to be absolutely sure of my identity and what operation or treatment I need, because I have heard about cases of treatment given to the wrong patient and I am scared.

The use case comes with additional requirements for the biometric system from the point of view of the patient.

— My identification needs to be linked to a description of the treatment or operation I need.

— As far as possible, I don't want to wear something that could be uncomfortable in order to be identified (this is unlikely to apply to emergency situations where the priority is receiving appropriate care).

Medical personnel want the patient identity check to be:

— fast;

— accurate (even if the patient in an operation room is unconscious);

— easy to link with the medical history of the patient (a newly created history in case of emergency, catastrophic events, but very useful to link, for instance, patients to medical exams results).

IT management can add cost constraints (the process will ideally avoid requiring very expensive equipment), and privacy concerns (as the hospital will be required to adhere to pertinent data protection regulations).

7.2.1.2 How biometrics can be applied to the use case

The most common way to identify patients in the hospital is to use a plastic wristband with a name and a barcode.

Although unlikely, these wristbands can fall or can be torn off by patients. To replace them, either more robust wristbands (e.g. with an electronic component, or made with a better baseline material than plastic), or biometrics, could be considered.

The benefit of wristbands in the hospital is that they do not contain any personal data, or any personal data they can contain is destroyed when the patient leaves: it is possible that there is no trace that any identification was ever made. This is extremely privacy preserving.

Biometrics for patient fast identification cannot be decentralized easily (i.e. it does not rely on a device that the patient would carry). While using a centralized biometric database as the link to the patient themselves might not be considered proportional to the potential benefit it brings (e.g. for hospital follow up), a centralized database is ideal in a catastrophic event situation, where identification is useful while the patient is receiving care. It is also likely to be useful during follow up care in the aftermath of a catastrophic event. In this case, proportionality of a central biometric database is very likely.

7.2.1.3 Advantages, disadvantages, risks and priority associated to the use of biometrics in this use case

— Advantages:

  — reduces the risk of error (which can increase in relation to medical staff exhaustion levels);

  — linked to the patient themselves (i.e. not to an "added device");

  — less subject to damage (e.g. water, tearing);

  — corresponds to patient's fear and therefore increases the patient's confidence in the hospital;

  — in case of a catastrophic event, does not require any additional device;

  - in case of a catastrophic event, creates a temporary identification for the patient that can be further used.
- Disadvantages:
  - not part of the usual "routine" of medical personnel;
  - no certainty that biometrics reading is always easy, depending on where the patient is;
  - not a suitable use case for decentralized biometrics: a central data storage is probably required.
- Risks:
  - patient in hospital can choose not to accept biometrics;
  - data protection regulations can require "proportionality" to be proven:[2] in hospital for routine medicine, proving proportionality can be an issue; in catastrophic events, the use of biometric as described in this use case is certainly proportional (and already in use for refugees).
- Priority:
  - Priority group 1.
  - In hospital, for habitual planned treatment, priority is not high because current “bracelet” solutions are widely accepted and reliable. However, for provision of emergency medicine in catastrophic events, this use case has very high priority.

7.2.1.4 Analysis and recommendations

As this use case is most useful in catastrophic event cases, this is the only context taken into consideration in this subclause. In such a case, people are likely to suffer from severe wounds rendering them unconscious and unable to convey any relative information to their caregivers.

In order to maximize the chances of a correct treatment, healthcare services need to be able to use identification in line with the recommendation of international organizations such as UNHCR, and collect multiple biometrics when the person is first taken in charge by the rescue services (see for instance References [8] and [9]).

In this case, when possible, healthcare services (i.e. first responders) need to be able to accept input about patient identity from external authorities in order to enable the identification of a social security number and to enable access to people’s medical ID and health records. At a minimum, if the person is not identified by a national authority, the temporary identification will be used to start personalized health monitoring.

7.2.2 Use case 7: eHealth: remote monitoring of patient

7.2.2.1 Use case description

This use case concerns remote monitoring of patient data. The patient wants the hospital to authorize doctors “manipulating” their data from a remote location.

From the point of view of a patient at home the use case can be described as:

- I want the doctors/nurses with access to my data and treating me from a remote location to be authenticated because I cannot entrust the monitoring of my data and the mission of curing me to incompetent people.

When performing this activity, medical personnel will simply login to the hospital IT system or to a certain application of the hospital. Therefore, from their perspective, this use case resembles use case 1 or use case 3, detailed respectively in 7.3.1 and 7.5.1.

From the point of view of the IT manager of the hospital, the use case can be described as:

— I need all hospital staff using systems connected to the IT of the hospital (software, databases, medical devices, etc.) to be able to be reliably authenticated, because I do not want to have intrusion in the IT system, and because I want all changes and actions related to the IT system to be traceable to the medical person who triggered them (particularly as these changes could be related to patient data).

From the perspective of the IT manager, the use case comes with additional requirements for the biometric system:

— accuracy (including robustness to presentation attacks when biometrics is used);

— same for all access points of the IT system within the hospital.

The use case comes with additional requirements for the biometric system from the point of view of the people actually using logical authentication:

— privacy preserving;

— easy to use;

— fast and reliable (i.e. not requiring multiple attempts);

— compatible with the hardware they already carry (no new device);

— not requiring them to use their hands to do something special with an access control device (taking them out of their pockets, putting them in a specific reader, etc.).

Furthermore, remote medical devices (at the patient's home) can be connected directly to the IT of the hospital: although this is beyond the question of biometrics and access control, authentication of remote medical devices and secured data exchange is mandatory in this use case.

In addition to authentication, this use case can also include authorization.

As a doctor in charge of patient A, B and C in remote healthcare:

— I want to authorize another doctor to take care of my patients because I am going to be absent for a period of time.

However, this involves authorization mechanisms in the hospital, beyond access control and beyond biometrics.

7.2.2.2 How biometrics can be applied to the use case

Authentication can rely on what a person knows (password), has (personal token) and is (biometrics). In the medical domain, for medical practitioners, the use of biometrics is preferable to the other solutions.

a) What a person knows (i.e. passwords) is difficult to use in the medical domain for multiple reasons:

   — the user needs to remember passwords and find them under stressful conditions;

   — as the set of machines that a medical practitioner uses includes terminals of the IT system with the patient records, but also medical devices which are mostly independent machines relying on proprietary authentication schemes, numerous passwords could be required for the same doctor, nurse or laboratory technician;

   — safe password management relies on changing passwords regularly, not writing them down so they can be copied or stolen, inclusion of complex combinations of upper case and lower case letters, with numbers and special characters, not corresponding to any dictionary entry, etc. This drastically complicates the question of memorization;

   — passwords can take a long time to type when they are complex;

— one-time passwords could be considered, but these necessitate a time-consuming dialogue (and a device to receive and display these passwords).

Therefore, solutions involving passwords (even multifactor) are not acceptable. Some hospitals are facing such situations where credentials are printed on post-it notes close to the medical terminals, to "fight" against the complexity of passwords: these situations are best eliminated to limit the confidentiality risks on medical records and to ensure patient safety.

b) What a person has (i.e. something a person is carrying) is not safe by itself, because a person can lose the item, and it can then be used by any intruder.

c) On the contrary, authentication with biometrics (i.e. what a person is) enables:

— ease of use: this is extremely important, especially for medical personnel mainly focused on patient care;

— speed for authentication: this is key when medical personnel have to work in emergency situations with time constraints;

— accuracy: avoiding unauthorized user access to a medical device or an account without permission.

The use of two factors for authentication (biometrics and one hardware token) is becoming of more general use because it makes access control more reliable and it enables decentralization of biometric storage on a piece of hardware that the owner of the biometrics carries at all time.

7.2.2.3 Advantages, disadvantages, risks and priority associated to the use of biometrics in this use case

— Advantages:

— easy to use;

— fast (for suitable biometrics);

— remove the need of passwords (except for people not willing to use biometrics) and their associated drawbacks (transferable, difficult to maintain at the same time simple and robust, etc.);

— can be privacy preserving if properly implemented;

— can be contactless to avoid disease transmission by contact;

— can rely on existing hardware and not mean additional costs;

— well-suited for shared devices and terminals.

— Disadvantages:

— biometrics is never 100 % accurate;

— selection of suitable biometrics vendors and biometrics settings are not obvious for IT managers.

— Risks:

— As a backup strategy without biometrics is mandatory, this could lead to poor adoption (at least in the early stage).

— Priority:

— Priority group 1.

— The priority is very high for medical staff because they log into workstations and devices many times per day, and they will "contribute" to better security only if this also improves their life.

— Priority is especially high for eHealth because this is a growing trend and telehealthcare is at present a threat to security.

This use case is in priority group 1, higher than the priority for use case 1 and use case 3, because eHealth is a growing practice. But from the biometric perspective it only uses biometrics for medical personnel logical access control.

7.2.2.4 Analysis and recommendations

Not all biometrics are suitable for medical staff. Fingerprints can be inconvenient for people wearing gloves. Biometric techniques requiring contact are not advisable in an environment where diseases are potentially present. Biometric techniques which require a long acquisition time (e.g. behavioural) are simply not acceptable. In a noisy environment, speaker recognition can be unsuitable. If face recognition is selected, it has to be robust to people wearing masks. The selection of the biometrics to use warrants careful consideration to fit the constraints of medical work.

The selection of the token is equally important. A smartphone seems attractive at first glance, but in some hospitals, doctors are not allowed to carry a smartphone (in order not to be disturbed). Therefore, the selection of the hardware token should be carefully considered.

Finally, it should be considered that hospitals are often also universities, and doctors can be teachers. Due to this specificity, session management should be carefully designed. In order to ensure that a session is not left open by an authorized person, and further used by another not authorized and potentially malicious person, face biometrics can be simply used to make a periodic check (e.g. every 10 s) that the face in front of the computer or medical device is still the same. However, this will not necessarily work in the teacher/student context, where the "official doctor" allows a student to use a device for training purposes, for example. Therefore, session management should consider this constraint.

7.3 Priority group 2

7.3.1 Use case 1: Global logical access control of medical staff in the hospital

7.3.1.1 Use case description

The use case can be described as follows.

As the IT manager of the hospital:

— I need it to be possible for all hospital staff using systems connected to the IT of the hospital (software, databases, medical devices, etc.) to be reliably authenticated, because I do not want to have an intrusion in the IT system, and because I want all changes and actions related to the IT system to be traceable to the medical person who triggered them (particularly as these changes could be related to patient data).

The use case brings additional requirements for the biometric system from the point of view of the IT manager:

— accuracy (including robustness to presentation attacks when biometrics is used);

— same for all access point of the IT system within the hospital.

The use case brings additional requirements for the biometric system from the point of view of the people actually using logical authentication:

— privacy preserving;

— easy to use;

— fast and reliable (i.e. not requiring multiple attempts);

— compatible with the hardware they already carry (no new device);

— not requiring them to use their hands to do something special with an access control device (taking them out of their pockets, putting them in a specific reader, etc.).

7.3.1.2 How biometrics can be applied to the use case

The way biometrics can be applied to this use case is as described in use case 7 (see 7.2.2.2).

7.3.1.3 Advantages, disadvantages, risks and priority associated to the use of biometrics in this use case

Advantages, disadvantages, drawbacks and risks of this use case are as described for use case 7, (see 7.2.2.3). However, use case 1 has been given a slightly lower priority group than use case 7.

7.3.1.4 Analysis and recommendations

Analysis and recommendations for this use case are as described for use case 7 (see 7.2.2.4).

7.4 Priority Group 3

7.4.1 Use case 2: Teleconsultation

7.4.1.1 Use case description

This use case can be described as follows:

From the perspective of the expert of the medical IT system:

— I want any patient who connects for telehealthcare assistance to be authenticated, so that the doctor can be sure of which patient they are talking to, and have their medical record available for consultation, and because external connections are a threat to the security of my medical IT system.

Additionally, if the authentication links the patient with a social security number or a health insurance, financial and case management can be facilitated (if required).

As a patient in teleconsultation, possibly under telehomecare:

— I want to make sure that the medical staff, located remotely, accessing my health data or taking care of me are authenticated, because I do not want to put my health at risk and give access to a medical practitioner I do not want, or to a person who is possibly not a medical practitioner.

The use case brings additional requirements for the system from the perspective of the IT manager:

— accuracy (including robustness to presentation attacks when biometrics is used);

— the patient needs to be able to authenticate themselves with a device they have themselves (PC, smartphone, etc.); the hospital will not provide them with devices.

The use case brings additional requirements for the system from the perspective of the patient:

— privacy preserving;

— easy to use;

— where possible, not requiring specific devices that they do not already have, and using the same hardware as that used for medical data recording and exchange.

Medical personnel require the system to be fast and convenient, but can be reluctant to adopt another new authentication method.

7.4.1.2 How biometrics can be applied to the use case

For medical personnel: same authentication as the logical authentication for the hospital proposed in use case 7 (see 7.2.2; one biometric criterion, with a second factor).

For patient: biometric authentication that uses their smartphone or their PC, for example, without any specific additional sensor, i.e. using a webcam and/or a microphone.

7.4.1.3 Advantages, disadvantages, risks and priority associated to the use of biometrics in this use case

This subclause mainly considers patient authentication in a healthcare scenario; the medical personnel side is already addressed in use case 7 (see 7.2.2.3).

— Advantages:

  — telehealthcare lowers occupancy rates in hospital and conditions for patients are usually better, but unprotected telehealthcare could be a threat to medical data;

  — easy and safe access to patient records and patient “monitored data” for medical personnel;

  — patient or medical operator can extend the safe sharing to additional practitioners to improve efficiency;

  — possibility of direct connection to social insurance for safe and fast consideration of care cost;

  — more reliable than evidence of a social security card, as such a card can be given to someone else;

  — can be implemented in a privacy preserving manner (no central biometric database), however this requires a hardware token and, in most countries, the social security card is insufficient: a hardware token should exist on the patient’s computer or smartphone.

— Disadvantages:

  — patient potentially does not own a computer or smartphone;

  — patient ability can vary, so specific biometrics or specific implementation can need to be considered (see ISO/IEC TR 30110 for guidance on biometrics used with children);

  — young patients need parent/guardian authorization or will have their parent/guardian going through access control for them (i.e. multiple people under a single identity).

— Risks:

  — patients will potentially not want to use biometrics or not be able to use biometrics, but still deserve telehomecare. Therefore an alternative is required, which can cause a security risk;

  — malicious usage will be reduced but not eradicated because “tricks” like presentation attacks, etc. will be used.

— Priority:

  — Priority group 3.

  — This use case extends and complements use case 7 (see 7.2.2) by enabling communication from the patient to the doctor. Telehealthcare is currently a threat to security.

7.4.1.4 Analysis and recommendations

General consideration on authentication methods are as indicated in use case 7 (see 7.2.2.2).

One reason for using biometrics for patient authentication is to prove that the person requesting a remote consultation is really who they claim to be (and not a person using the social security number of a friend or relative, or a stolen social security card). Even though the patient and the doctor will see one another during a teleconsultation, the doctor potentially has many patients, and does not recognize each of them

individually, or the doctor can be temporary replaced (e.g. due to maternity leave). Being sure of patient identity is mandatory for the following reasons:

— to obtain the correct patient history (health record, current treatment, result of last medical exams, etc.);

— (to a lesser extent) to limit social security fraud.

Password or tokens can be freely exchanged and will cause uncertainty concerning patient identity (even one time passwords that can be given to a friend or relative). Of course, it is possible that a person will authenticate and will then give the floor to someone else, this is easily addressed by showing a picture of the authenticated person and the patient side by side.

Biometrics also presents an easy means of authentication, as many people are used to such authentication thanks to their smartphones.

However, not all biometric modalities are suitable for patients. The biometric modality used should:

— not require any other equipment than a camera or microphone;

— be in line with pertinent data protection regulations, and its usage should be proportionate to the benefit that the patient has using it;

— be decentralized (no biometric data stored out of the patient owned devices); therefore trust mechanisms need to exist to make sure that authentication really took place on the user's devices (FIDO, proof of computation, etc.);

— be revocable;

— not be easily spoofed: unlike the medical staff zones of a hospital, which are already filtered in access, and which mostly include people that will not make malicious attempts against the healthcare IT, patient are external, and can be malicious individuals trying to fool the system;

— according to the data minimization principle, data controllers should ensure that data extracted from a digital image to build a template will not be excessive and will only contain the information required for the specified purpose, thereby avoiding any possible further processing. Measures should be put in place to guarantee that templates cannot be transferred across biometric systems.

A variety of solutions can be required to cover:

— all ages;

— all kinds of illness (e.g. a person with Parkinson's disease will not necessarily be able to provide a sharp image of their face or fingers; a person with bandages on fingers cannot provide fingerprints; etc.);

— all kinds of equipment (perhaps not very old computers or smartphones, but at least not only the latest generations).

7.4.2 Use case 8: Patient authentication for public health, vaccination

7.4.2.1 Use case description

This use case can be described as follows:

The use case concerns large scale vaccination in case of pandemic. It consists of patient authentication to help in monitoring the vaccination process, i.e.:

— setting an initial appointment;

— accessing the social security number of the patient and their medical record to make sure the patient is eligible for vaccination, and from the medical conditions, assess any risks to the patient;

— keeping track of vaccination and allowing for delivery of certificates (for use in travel, accessing public places, etc.);

— managing multiple injections initially, and vaccination renewal.

As a health authority:

— I want to follow up the vaccination process with patient authentication because it makes the process far more reliable and easier to track over time.

From the patient perspective, the goal is the same as in use case 2: it involves patient access control to make an appointment, and patient authentication is performed in the same way upon vaccination. This use case also represents patient access control to obtain a certificate proving that that patient has had a vaccination.

7.4.2.2 How biometrics can be applied to the use case

For making an appointment, this is as in use case 2 (see 7.4.1.3).

For the actual vaccination, the same checks could be completed as in use case 2, but with no biometric data exchanged at the points of vaccination (e.g. hospital computers).

7.4.2.3 Advantages, disadvantages, risks and priority associated to the use of biometrics in this use case

The advantages, disadvantages and risks of this use case are mostly as in use case 2 (see 7.4.1.3), except that the "business benefit" is not enabling telehomecare, but rather:

— for the patient: receiving assistance for vaccination and an easy and reliable source for a certificate;

— for the national medical authority: having a more reliable vaccination process, thereby optimizing the service offered to citizens.

7.4.2.4 Analysis and recommendations

The analysis and recommendations for this use case are similar to those described in use case 2 (see 7.4.1.4), with a specific focus on patient authentication on the place where they are authenticated: this should be done in such a way that no biometric data is used on the computers of the vaccination place (e.g. using trusted computation on the patient device).

7.4.3 Use case 9: Identification of citizens in public health to monitor a pandemic situation

7.4.3.1 Use case description

This use case is again about the management of pandemics, but without being limited to vaccination: it is a way to extend the data available in the aftermath of the pandemic by relying on the citizens, when researchers and doctors can no longer provide enough data and large scale information is required. Input of data after patient discharge or from homecare is difficult, and in these cases the patient's correct identification is mandatory.

The principle is to rely on authenticated citizens giving their health data (i.e. their self-test data) online.

The use case can be described as follows:

As the health authority:

— I want citizens to reliably be able to login to a pandemic follow up application and give their own data, because I want to follow the pandemic data at a larger scale, and for this purpose I need the help of citizens.

Other than wanting to follow the data at a larger scale, at the authentication level, the use case is the same as use cases 2 and 8 (see 7.4.1.4 and 7.4.2.1); only its business benefit changes.

7.4.3.2 How biometrics can be applied to the use case

Application of biometrics in this use case is the same as for use case 2 (see 7.4.1.2).

7.4.3.3 Advantages, disadvantages, risks and priority associated to the use of biometrics in this use case

Advantages, disadvantages, risks and priority in this use case are the same as for use case 2 (see 7.4.1.3).

7.4.3.4 Analysis and recommendations

The analysis and recommendations for this use case are the same as for use case 2 (see 7.4.1.4).

7.5 Priority Group 4

7.5.1 Use case 3: Local logical access control of medical staff in the hospital

7.5.1.1 Use case description

This use case can be described as follows:

The use case is similar to use case 1 (7.3.1) and use case 7 (7.2.2). The principle is that access control is limited to one or more applications within the hospital, rather than being generalized. The benefit is that, in comparison to a situation where everything is suddenly to be changed at the same time, as in use case 1, a progressive transition is possible. The drawback is that only part of the hospital is protected, and doctors and nurses still need to remember multiple ways of accessing hospital IT systems.

As the IT manager of the hospital:

— I need all hospital staff using Application A to be able to be reliably authenticated, because this application can be used to make an intrusion in the IT system of the hospital, and because I want all changes and actions related to Application A to be traceable to the medical person who triggered them.

The use case brings additional requirements for the biometric system from the point of view of the IT manager:

— accuracy (including robustness to presentation attacks when biometrics is used);

— if some applications are already "access controlled", use of the same access control for other applications.

The use case brings additional requirements for the system from the point of view of the people actually using logical authentication:

— privacy preserving;

— easy to use;

— fast and reliable (i.e. not requiring multiple attempts);

— no new device to carry (the worst case scenario being that each application comes with a need for a specific non-shared device);

— not requiring them to use their hands to do something special with an access control device (taking them out of their pockets, putting them in a specific reader, etc.).

7.5.1.2 How biometrics can be applied to the use case

Two-factor authentication with one factor being biometrics and the other being a hardware token in line with the working practices of the hospital is considered appropriate. The use of biometrics for one or several applications has no reason to be different from one hospital department to another.

7.5.1.3 Advantages, disadvantages, risks and priority associated to the use of biometrics in this use case

The advantages, disadvantages, risk and priority for this use case are very similar to those of use case 1 and use case 7. They are repeated here, with changes labelled as such.

- Advantages:
  - easy to use;
  - fast (for suitable biometrics);
  - removes the need for passwords (except for people not willing to use biometrics) and their associated drawbacks (transferable, difficulty in remaining simultaneously simple and robust, etc.);
  - can be privacy preserving if properly implemented;
  - can be contactless to avoid disease transmission by contact;
  - can rely on existing hardware and not equate to additional costs;
  - well suited to shared devices and terminals;
  - (additional advantage) flexible: applications and systems can be moved progressively;
  - (additional advantage) makes it possible to measure acceptability by medical staff.
- Disadvantages:
  - biometrics is never 100 % accurate;
  - selection of suitable biometrics vendors and biometrics settings are not obvious for IT managers;
  - (additional disadvantage) if one application uses a certain hardware token, then this token could be used for other applications moving forward.
- Risks:
  - as a backup strategy without biometrics is mandatory, this could lead to poor adoption (at least in the early stage);
  - (additional risk) difficult to agree on a common strategy between application vendors.
- Priority:
  - Priority group 4.
  - As medical staff login to selected applications multiple times per day, they will contribute to better security only if this also improves their life. However, use case 1, where the whole hospital migrates to two-factor authentication for logical access control, is considered higher priority.

7.5.1.4 Analysis and recommendations

The recommendations are the same as in use case 7 (7.2.2.4). It is up to the IT service of a hospital to decide which strategy is better: migrating to safe access control for all IT directly or progressively by application.

7.6 Priority Group 5

7.6.1 Use case 4: Physical access control to restricted zones in the hospital

7.6.1.1 Use case description

The use case can be described as follows.

As the manager of the hospital:

— I want to protect the access to certain restricted zones in the hospital that are critical (pharmacy, operating room, intensive therapies, sterile wards and rooms, radiotherapy rooms, biobanks, IT hospital servers, etc.), because unauthorized people can cause very important damages in these zones, i.e. endanger safety by theft, unauthorized access to data, violation of sterility measures, threatening of medical personnel and patients.

This use case brings additional requirements for the biometric system from the point of view of the hospital manager:

— accuracy (including robustness to presentation attacks when biometrics is used);

— potentially suitable for external access that can correspond to outdoor locations;

— same for all points of access within the hospital.

The use case brings additional requirements for the biometric system from the point of view of the people actually using logical authentication:

— privacy preserving;

— easy to use;

— fast and reliable (i.e. not requiring multiple attempts);

— compatible with the hardware they already carry (no new device).

The use case also needs to consider people who are not authorized but can come close to the access control point: their privacy should not be violated (i.e. none of their personal data should be caught without their explicit consent when they come close to a point of physical access control).

7.6.1.2 How biometrics can be applied to the use case

Physical access control offers the same choice of "factors" as logical access control: what a person knows (i.e. a password), what a person has (i.e. a key, etc.) and what a person is (biometrics). The usual benefits of biometrics apply:

— a person's password can be stolen (just by looking at what they type), and a key or any other piece of hardware can also be stolen, but "stealing" biometrics is far more difficult (although 3D masks and fake fingers do exist);

— biometrics cannot be forgotten and most people find their use easy;

— most biometrics will give extremely fast answers.

7.6.1.3 Advantages, disadvantages, risks and priority associated to the use of biometrics in this use case

— Advantages:

  — makes access control simple, fast and reliable;

  — no risk of lost or stolen badge, password, etc.;

  — easy to accept by most people;

  — can be privacy preserving if properly implemented;

  — with the development of contactless biometrics: safe from a "hygienic" perspective;

- most systems come with countermeasures for usual attacks (e.g. presentation attacks, tailgating).

- Disadvantages:
  - biometrics is never 100 % accurate.
  - it can be necessary to monitor for specific attacks (e.g. an authorized person presents their own biometrics, but provides access to an unauthorized person).

- Risks:
  - as a backup strategy without biometrics is mandatory, this could lead to poor adoption or be a weakness in the reliability of the system;
  - access for visitors also needs to be considered, and this could create weaknesses;
  - criticism of the new system from patients could have a negative impact on the hospital image.

- Priority:
  - Priority group 5.
  - Physical access control for critical places in the hospital is essential: from medical practitioners' feedback, it seems that this is already in place in most large hospitals.

7.6.1.4 Analysis and recommendations

In using biometrics for physical access control, visitors need to be given access as well. Rules can exist concerning visitors (e.g. they can need to be accompanied at all times during visits, with a "tutor") and the access control system needs to take such associated rules into account.

A characteristic specific to hospitals is that hospitals are public places, and they are widely open to visitors. Only some parts are restricted. Visitors to the hospital can be upset because they are visiting a person who has severe health problems; this makes them vulnerable. It is extremely important to consider biometric access control that will not register data from a visitor "by chance", without the visitor being aware of it.

Another specific characteristic of hospitals is that they are places where infections are more common. Therefore, it is imperative that access control be contactless (e.g. a touch pad to type a code is not recommended).

Furthermore, as with logical access control:

- the people to be controlled can be in a hurry because of an emergency situation and therefore access control should not delay their work (e.g. by default open doors could be considered; the use of behavioural biometrics or access control using voice involving long sentences are not appropriate);
- inside the hospital, medical personnel might wear gloves, masks, etc., and biometrics considered need to be robust to these attributes.

Finally, physical access control is usually accompanied by barriers, turnstiles, etc. For busy medical personnel, where speed is key, opening the barriers by default and closing them on unsuccessful access attempt only could be considered to facilitate access.

7.6.2 Use case 6: Registration and control of medical practitioners

7.6.2.1 Use case description

The use case can be described as follows.