TECHNICAL REPORT

ISO/IEC TR 27563

First edition
2023-05

Security and privacy in artificial intelligence use cases — Best practices

Sécurité et respect de la vie privée dans les cas d'usage de l'intelligence artificielle — Bonnes pratiques

Copyrighted document, no reproduction or circulation
For review by FG on AI in healthcare
Oct 2024

Reference number
ISO/IEC TR 27563:2023(E)

Documents
Document Sharing Hub
© ISO/IEC 2023

Full document details: ISO_IEC TR 27563 WG_2023

Copyrighted document, no reproduction or circulation
For review by FG on AI in healthcare
Oct 2024

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2023
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

© ISO/IEC 2023 – All rights reserved

Documents
Document Sharing Hub

Full document details: ISO_IEC TR 27563 WG_2023

Contents

Page

Foreword ..... **iv**
Introduction ..... **v**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Abbreviated terms **2**
5 Analysis of security and privacy **3**
5.1 General 3
5.2 Application domains in ISO/IEC TR 24030:2021 use cases 3
5.3 Security in ISO/IEC TR 24030:2021 use cases 3
5.4 Privacy in ISO/IEC TR 24030:2021 use cases 4
6 Templates for analysis **5**
7 Supporting information **6**
7.1 Describe ecosystem 6
7.2 Provide assessment of systems of interest 7
7.3 Identify security and privacy concerns 7
7.4 Identify security and privacy risks 9
7.5 Identify security and privacy controls 11
7.6 Identify security and privacy assurance concerns 15
7.7 Identify security and privacy plan requirements 16
Annex A (informative) **Additional use cases** **18**
Bibliography **28**

Copyrighted document - no reproduction or circulation
For review by FG on AI in healthcare
Oct 2024

© ISO/IEC 2023 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC TR 27563 WG_2023

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 27, *Information technology, cyber security and privacy protection*.

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.

Copyrighted document, no reproduction or circulation
For review by FC on AI in healthcare
Oct 2024

© ISO/IEC 2023 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC TR 27563 WG_2023

Introduction

Artificial intelligence (AI) and machine learning (ML) are increasingly being adopted by the digital industry, using algorithms to make decisions that have the potential to negatively impact the privacy of individuals and in some cases can even cause harm to some of them, unless adequate safeguards are deployed. Such safeguards to protect privacy often depend on a variety of factors including the specific type of process, sensitivity of data used, and potential harm likely to be caused.

This concern has been expressed by:

— Practitioners, who identified 23 principles for AI at the 2017 Asilomar conference[1] covering research, ethics and values, as well as longer term issues.

— Standard developers, as evidenced by the report on ethically aligned design published by the IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems[2].

— Policy makers, as exemplified by the appointment by the European Commission of a high-level expert group on artificial intelligence and the subsequent publication of an assessment list[3].

This document provides an analysis of security and privacy of use cases provided in ISO/IEC TR 24030, which should be used in parallel. A number of additional use cases are provided in Annex A.

This document also uses concepts from ISO/IEC TR 24028, which addresses trustworthiness in AI systems, including approaches to establish trust (e.g. transparency, explainability, controllability), and to achieve trustworthiness properties (e.g. resiliency, reliability, accuracy, safety, security, or privacy).

Copyrighted document, no reproduction or circulation
For review by FG on AI in healthcare
Oct 2024

© ISO/IEC 2023 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC TR 27563 WG_2023

Copyrighted document, no reproduction or circulation
For review by FG on AI in healthcare
Oct 2024

Documents
Document Sharing Hub

Security and privacy in artificial intelligence use cases — Best practices

1 Scope

This document outlines best practices on assessing security and privacy in artificial intelligence use cases, covering in particular those published in ISO/IEC TR 24030.

The following aspects are addressed:

— an overall assessment of security and privacy on the AI system of interest;

— security and privacy concerns;

— security and privacy risks;

— security and privacy controls;

— security and privacy assurance; and

— security and privacy plans.

Security and privacy are treated separately as the analysis of security and the analysis of privacy can differ.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

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

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

3.1
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 can be directly or indirectly linked to a natural person

Note 1 to entry: The "natural person" in the definition is the *PII principal* (3.3). 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]

Copyrighted document, no reproduction or circulation
For review by FG on AI in healthcare
Oct 2024

© ISO/IEC 2023 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC TR 27563 WG_2023

3.2
PII controller
privacy stakeholder (or privacy stakeholders) that determines the purposes and means for processing *personally identifiable information (PII)* (3.1) other than natural persons who use data for personal purposes

Note 1 to entry: A PII controller sometimes instructs others [e.g. *PII processors* (3.4)] to process PII on its behalf while the responsibility for the processing remains with the PII controller.

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

3.3
PII principal
natural person to whom the *personally identifiable information (PII)* (3.1) relates

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

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

3.4
PII processor
privacy stakeholder that processes *personally identifiable information (PII)* (3.1) on behalf of and in accordance with the instructions of a *PII controller* (3.2)

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

4 Abbreviated terms

CCTV	closed-circuit television
GDPR	General Data Protection Regulation
HCI	human computing interaction
LINDDUN	linkability, identifiability, non-repudiation, detectability, disclosure of information, unawareness, non-compliance
NIST	national institute of standards and technology
OEM	original equipment manufacturer
PIA	privacy impact assessment
PII	personally identifiable information
PoC	proof of concept
SDG	sustainable development goals
STRIDE	spoofing identity, tampering, repudiation, information disclosure, denial of service, elevation of privilege
UC	use case
V2X	vehicle-to-everything

Copyrighted document, no reproduction or circulation
For review by FG on AI in healthcare
Oct 2024

© ISO/IEC 2023 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC TR 27563 WG_2023

5 Analysis of security and privacy

5.1 General

This document includes a security and privacy analysis of ISO/IEC TR 24030:2021 use cases. Two electronic attachments were used:

— the first is the material used by ISO/IEC TR 24030:2021, available here: https://standards.iso.org/iso-iec/tr/24030/ed-1/en/Use+cases-v05_electronic_attachment_022021.pdf,

— the second is the material used by this document, available here: https://standards.iso.org/iso-iec/tr/27563/ed-1/en/Security-privacy-24030-ed-1-AI-use-cases.pdf.

Annex A provides a list of new use cases.

5.2 Application domains in ISO/IEC TR 24030:2021 use cases

ISO/IEC TR 24030:2021 describes 132 use cases, belonging to 22 application domains as shown in Figure 1.

NOTE 1 134 use cases are listed in this document, as use case 96 from ISO/IEC TR 24030 has been categorized into 3 application domains.

NOTE 2 The number of use cases per domain, e.g. 1 energy use case compared to 29 healthcare use cases is not an indication of the potential deployment of AI capabilities in a domain.

NOTE 3 The assignment of a use case to a domain depends on the viewpoint of experts. For instance, use case 132 (Device control using both cloud AI and embedded AI) is classified as manufacturing instead of home.

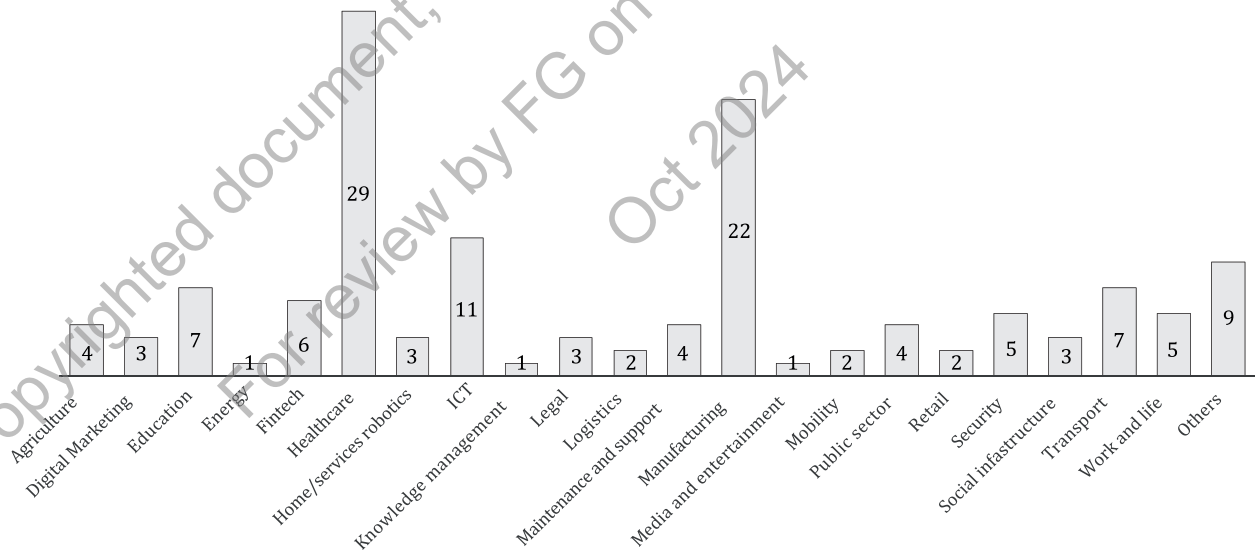

Figure 1 — Distribution of use cases by application domains

5.3 Security in ISO/IEC TR 24030:2021 use cases

Figure 2 summarizes the security analysis of ISO/IEC TR 24030 use cases in the second electronic attachment. It shows for each application domain:

— the number of use cases for which security concerns can be negligible;

— the number of use cases for which security concerns can be limited;

— the number of use cases for which security concerns can be significant; and

Copyrighted document, no reproduction or circulation
For review by FG on AI in healthcare
Oct 2024

© ISO/IEC 2023 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC TR 27563 WG_2023

— the number of use cases for which security concerns can be maximum.

NOTE 1 The assessment is based on the most critical systems of interest. For instance, use case 1 (Explainable artificial intelligence for genomic medicine) involves two systems of interest, the genomic sequence processing system for which security concerns can be maximum, and the genomic training system for which system concerns can be significant. The resulting assessment is that security concerns can be maximum.

NOTE 2 The assessment result of each domain is not an indication of the potential privacy concern of AI in a domain.

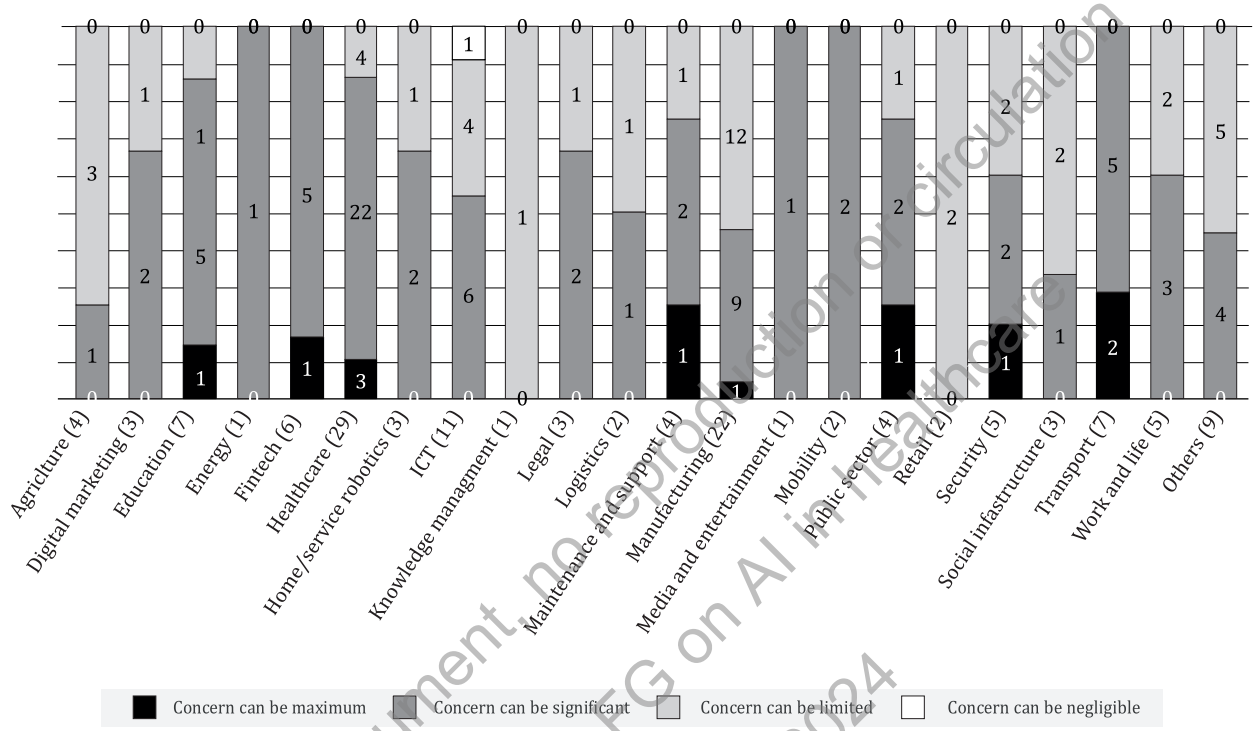

Figure 2 — Security analysis in AI use cases

5.4 Privacy in ISO/IEC TR 24030:2021 use cases

Figure 3 summarizes the privacy analysis of ISO/IEC TR 24030 use cases listed in the attachment. It shows for each application domain:

— the number of use cases for which privacy concerns can be negligible;

— the number of use cases for which privacy concerns can be limited;

— the number of use cases for which privacy concerns can be significant;

— the number of use cases for which privacy concerns can be maximum.

NOTE 1 The assessment is based on the most critical systems of interest. For instance, use case 1 (Explainable artificial intelligence for genomic Medicine) involves two systems of interest, the genomic sequence processing system for which privacy concerns can be maximum, and the genomic training system for which system concerns can be negligible. The resulting assessment is that privacy concerns can be maximum.

NOTE 2 The assessment result of each domain is not an indication of the potential privacy concern of AI in a domain.

Copyrighted document, no reproduction or circulation
For review by FG on AI in Healthcare
Oct 2024

© ISO/IEC 2023 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC TR 27563 WG_2023

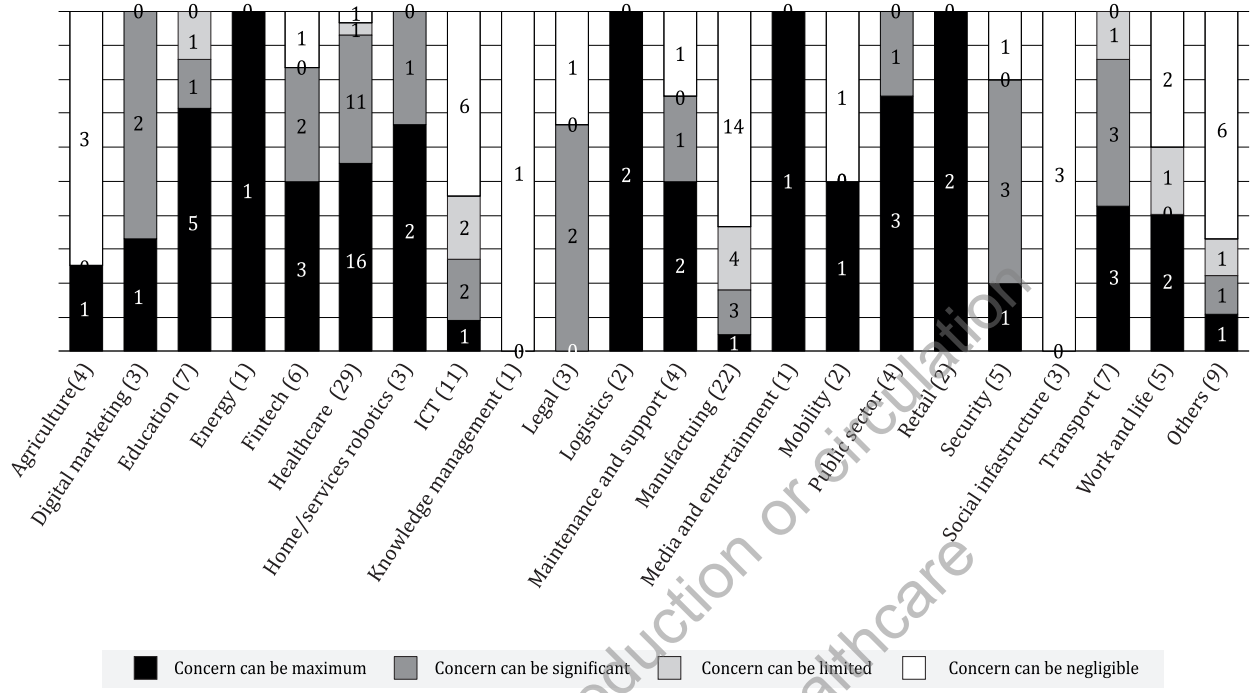

Figure 3 — Privacy analysis in use cases

6 Templates for analysis

The template used to collect material is shown in Table 1. It includes three types of table cells:

— title cell (e.g. use case name);

— instruction cell (e.g. describe the ecosystem);

— example cell (e.g. System of interest: < use case system of interest >).

Example cells can include texts in brackets, e.g. < asset A > . They are intended to be replaced by a specific text related to the use case.

NOTE 1 The proposed texts in example cells use vocabularies and concepts which are aligned with existing security and privacy references (See [7][8][9][10][13][16][17][18][19][24][15][14]).

NOTE 2 A use case can involve several systems of interest.

Copyrighted document, no reproduction or circulation
For review by FG on AI in healthcare
Oct 2024

© ISO/IEC 2023 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC TR 27563 WG_2023