International Standard

ISO/IEC 5153-1

Information technology — City service platform for public health emergencies —

Part 1: Overview and general requirements

First edition
2024-03

Technologies de l'information — Plateforme de services urbains pour les urgences en matière de santé publique —

Partie 1: Aperçu et exigences générales

Reference number
ISO/IEC 5153-1:2024(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

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*.

A list of all parts in the ISO/IEC 5153 series can be found on the ISO and IEC websites.

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

Public health emergencies, particularly those caused by infectious diseases such as the COVID-19 pandemic, have unprecedented impacts on the social and economic aspect of many cities. A Public Health Emergency of International Concern (PHEIC) is a formal declaration by the World Health Organization (WHO) of "an extraordinary event which is determined to constitute a public health risk to other States through the international spread of disease and to potentially require a coordinated international response".[6]

Information technology can provide significant support in expanding city capacities to respond to such public health emergencies, in particular by providing capabilities to coordinate data, services and applications across operational domains for multiple stakeholders in smart cities.

Smart city applications can be classified into two groups: domain-specific applications and cross-domain applications. In a public health emergency scenario, various information and services are provided via different channels from different sources. It would be more convenient and simpler for users to have a single hub which can provide all necessary services at the application layer.

This document introduces a city service platform as a single hub for public health emergencies.

Information technology — City service platform for public health emergencies —

Part 1:
Overview and general requirements

1 Scope

This document specifies the general requirements for a city service platform for public health emergencies. It also specifies the requirements in terms of data, functions, security and privacy protection.

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 27701, *Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines*

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
city service
service rendered in the public interest

Note 1 to entry: This is also known as "public service" and "service of general interest".

4 Abbreviated terms

DDoS	distributed denial-of-service
PHE	public health emergency
SCDP	smart city digital platform

5 Public health emergency scenario

A public health emergency (PHE) is a typical smart city scenario which requires cross-sector and cross-department cooperation and collaboration. Controlling a public health emergency and allocating necessary emergency resources requires professional authority and enforceability, such as disease control and prevention, emergency response and management, and healthcare. Information technologies also enable accurate information collection and analysis, quick community reactions, enhancement of society cooperation and support in decision-making, thus improving city sustainability and resilience under a PHE scenario.

According to a study taken by the World Summit on the Information Society (WSIS), the main stakeholders for a PHE include academia, civil society, the government, international organizations, the private sector and others (individuals and organizations).[4] These stakeholders can be further categorized into three roles, as follows.

1) Manager and coordinator: ensures preparedness, readiness and response actions at an appropriate scale to reduce both PHE spread and economic, public and social impacts.

2) Service provider: implements and provides necessary technologies, measures, services and tools based on user demand and policies made by manager and coordinator.

3) User: follows official guidance and uses services provided to protect themselves and others with respect to public interest.

PHEs have wide impact on all aspects of city operation and public daily life. In general, the following four phases of emergency management are widely applied:

- Prevention and mitigation: cover activities or precautions for assessing and preventing the risks, vulnerabilities, threats, potential severity, likelihood, consequences and impact of a PHE for cities. With these activities or precautions, it can be ensured that cities have taken adequate steps to prevent and reduce the likelihood of occurrence or mitigate the damaging effects.

  NOTE It is necessary to consider and plan prevention and mitigation in advance of an actual emergency.

- Preparedness: covers the planning that needs to be incorporated or decided actions that will assist in successfully dealing with an emergency.

- Response: covers the reality of how to respond to an emergency scenario.

- Recovery: takes place after the emergency is over and the immediate danger has subsided.

City services are located at the smart applications layer as described in ISO/IEC 30145-3. With the common data and service capabilities provided by a smart city digital platform as described in ISO/IEC 24039, a city service platform for PHE focuses on providing scenario-specific and integrated services to improve emergency response efficiency, ensure city operation, protect public safety and continue daily life throughout the emergency prevention and mitigation, preparedness, response and recovery stages, as shown in Figure 1.

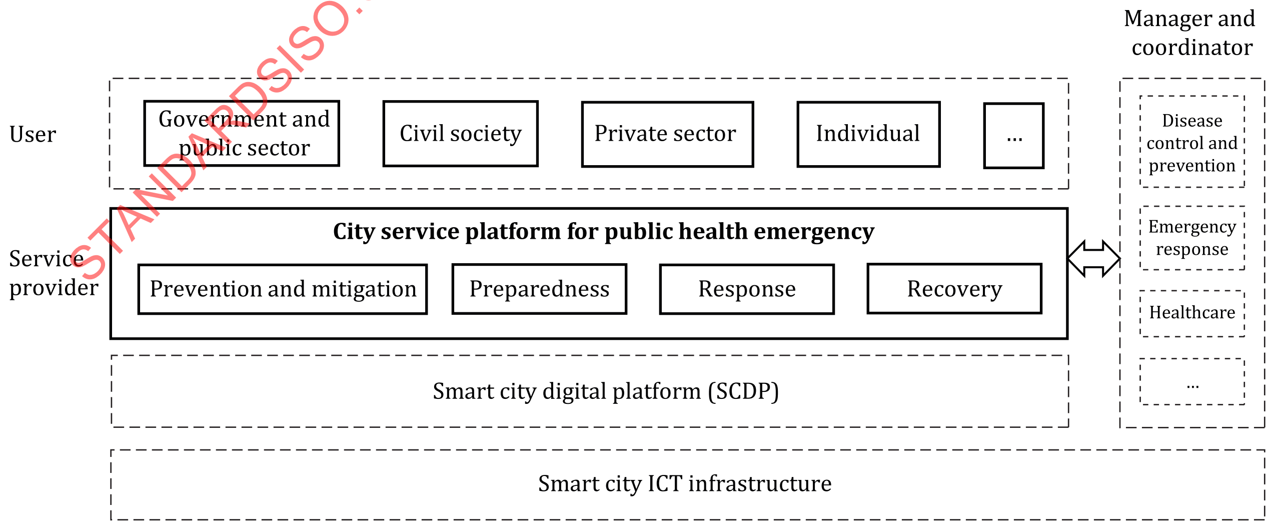
Manager and coordinator
User
Government and public sector
Civil society
Private sector
Individual
...
Disease control and prevention
Emergency response
Healthcare
...
Service provider
City service platform for public health emergency
Prevention and mitigation
Preparedness
Response
Recovery
Smart city digital platform (SCDP)
Smart city ICT infrastructure

Figure 1 — City service platform for public health emergency (PHE)

6 General requirements

6.1 Accessibility requirements

A PHE can have global impact for everyone, including people living in situations of poverty, older people, people with disabilities, young people and indigenous peoples.

Thus, a city service platform for PHE shall provide the necessary accessibility supports for people with difficulties in vision, physical ability, hearing or mobility, and people with cognitive impairments or learning disabilities. A city service platform for PHE should support and meet corresponding requirements for digital inclusion solutions and initiatives provided by government, civil society and international organizations, taking into consideration the unbalanced development of information infrastructure that can present startling digital inequalities between and within countries.

6.2 Interoperability requirements

A PHE can impact all aspects of daily life and social activities. PHE-related digital services can be delivered via various channels, such as sensors, cameras, mobile devices, tablets, smart terminals, smart screens, etc. Thus, a city service platform for PHE should enable data and system interoperability for various devices and terminals.

For example, individuals can use mobile apps to report relevant information. Professional or authorized organizations can use client web programs to confirm reported information and executive responses. Coordinators and management departments can use smart screens to visualize the overall situation and perform decision-making.

Technical requirements for a city service platform for PHE in terms of data, service and interface are provided in Clause 7 and Clause 8.

6.3 Privacy protection requirements

To control the spread of a PHE, the collection of personal information, such as health-related information, travel history and medical records can be necessary. Thus, a city service platform for PHE shall establish a complete privacy protection policy according to municipal policy and regulations, taking both technical and business aspects into consideration, such as the location of the platform, where and to whom the service is delivered, etc. Technical privacy protection requirements for a city service platform for PHE are provided in Clause 10.

7 Data requirements

7.1 Data traceability

Data traceability requirements and recommendations of a city service platform for PHE shall include the following points.

a) Within the specified data retention period, the data should be clear, readable, understandable and traceable, ensuring that the steps and the sequence of data generation can be completely reproduced.

b) Operations such as data extraction, cleaning, loading, fusion and conversion during data processing shall be recorded through the audit trail function to ensure the traceability.

c) Alternative methods should be used for situations that do not have the audit trail function, such as log, change control, record version control or original electronic records, supplemented with paper records to ensure the data traceability.

d) The audit trail function of the platform shall not be closed and the data generated by the audit trail function shall not be modified. The frequency and the content of the audit trail review should be determined based on task risk level.

e) Data traceability analysis, auditing and tracking should be supported to improve supervision for the spread of unauthorized data.

f) The record storage duration should be determined by fully considering the municipal regulations and legal requirements.

7.2 Data exchange and sharing

The data exchange and sharing requirements and recommendations of a city service platform for PHE shall:

a) provide a variety of data sharing and exchange methods to realize data sharing and business collaboration between provincial, prefectural, county and district levels of commissions, bureaus and related organizations, and provide support for cross-departmental applications;

b) be able to exchange data across domains and network segments, access across network segments and firewalls, and provide data exchange and data forwarding functions between the same or different networks;

c) realize the exchange and sharing of a variety of information resources, including file exchange, database data exchange, and event-driven, request/response, and publish/subscribe;

d) support the convenient and rapid packaging of various databases and application systems into services, and analyze the data in various service interfaces provided by various institutions;

e) provide data exchange logs to ensure that all data exchange tasks record detailed log information, and that data exchange tasks can be tracked and audited afterwards.

7.3 Data security

The data security requirements and recommendations of a city service platform for PHE shall:

a) enable data security protection throughout the data lifecycle;

b) provide secured information inquiry, copy and share methods to ensure data security, and comply with relevant municipal policies.

c) support the complete destruction of corresponding data as local laws and regulations require data to be deleted, storage space to be released, medium to be redistributed, replaced or eliminated; appropriate destruction methods should be selected for different types of data and medium to ensure that the data are destroyed and cannot be restored.

7.4 Data quality

The data quality requirements and recommendations of a city service platform for PHE shall:

a) objectively reflect the reality (authenticity);

b) reflect the actual situation in the process of time change (timeliness);

c) take into account compliance with data standards, data models and data rules (normative);

d) ensure the completeness of data field information and metadata (integrity);

e) establish a data management mechanism from data collection, data transmission, data processing, data exchange to data destruction throughout both the data lifecycle and emergency management lifecycle;

f) ensure the integrity, standardization, consistency, accuracy, uniqueness and relevance of the internal storage, processing and external data provided;

g) provide a data validity check to ensure the input content via human-machine interface or communication interface meets system requirements.

8 Functional requirements for platform services

8.1 Prevention and mitigation

8.1.1 Emergency planning

A city service platform for PHE should be able to identify application and technical requirements based on emergency plan, including related stakeholder responsibility, data collection and processing management, data quality measurement, task handling procedure flow, access control strategy, etc.

NOTE The emergency plan at city level includes emergency management activities and responses. It identifies the objectives of emergency response and provides guidance, explaining the key issues for effective decision-making.

8.1.2 Emergency exercises

A city service platform for PHE should have the ability to carry out emergency exercises to improve awareness for all stakeholders, to intuitively understand and summarize emergency events, and to improve the vigilance of emergency risk sources.

8.2 Preparedness

8.2.1 Information release

A city service platform for PHE should support live information release from authority organizations or professional organizations. It should also provide an interactive map that allows users to select a specific county, city or area to see the number of total new confirmed cases, suspected cases and cured cases with a timeline. It should also provide tools to predict the trend of the possible spread rate.

8.2.2 Warning distribution

A city service platform for PHE should support sending emergency warnings to decision makers, other necessary relevant stakeholders and the public. It should provide warning information with emergency descriptions, emergency categorization, level of risk, name of sending authority and other related information. Warnings should be able to be distributed in various ways, depending on user needs, the urgency of the emergency information, and the available distribution channels.

8.3 Response

8.3.1 Self-quarantine monitoring

Under certain PHE situations caused by infectious diseases, self-quarantine helps to prevent the spread of the disease as it minimizes the connections of potential confirmed cases with the public. The city service platform for PHE should be able to support or connect with self-quarantine systems to collect and exchange related information and support performing data processes and analysis.

NOTE Local government and public health authorities determine and establish the self-quarantine options for their jurisdictions.

8.3.2 Self-check and reporting

Self-check and reporting services enable individuals to record and report emergency-related symptoms. The city service platform for PHE should support or connect with self-check and reporting services with the permission of the individual or after an anonymization process. Reported information can be used to help local government, authorities, and public health providers to gain better understanding of current conditions, enabling them to prepare or respond to the situation. An example of a self-check and reporting service is provided in Annex B.

8.3.3 Graphic code

The city service platform for PHE should support health information generation and checking with a graphic code. A graphic code uses different code indicators, such as colours, to indicate the exposure risks based on factors such as travel history, duration of time spent in high-risk areas, and relationships to potential carriers. A graphic code is generated with health information which can only be accessed with user confirmation for usage permission. A graphic code can be printed or encoded as a two-dimensional graphic code, such as a QR code. An example of graphic code management is provided in Annex C.

NOTE Countries and regions can establish emergency health information authorized notarization services within their own regions. When the health information is used for cross-regional services, the service provider needs to register their service and usage via the registration framework.

8.3.4 Travel declaration

The city service platform for PHE should support the provision of necessary information to generate and check travel certification. A travel certificate can be used during the public health emergency while ensuring public health and safety corresponding to local emergency control actions. The city service platform should support pre-declaration for people planning to have cross-regional travel. Declared information includes vehicle information, passenger information and journey information. An example of a cross-regional certificate check is provided in Annex A.

NOTE "Cross-regional" refers to crossing the boundary between different authorized areas, such as city, state and county.

8.3.5 Contact tracing

Contact tracing is based on interviews of confirmed cases. To ensure the accuracy of contact tracing, technical solutions are recommended to compensate for omission or errors caused by incomplete recollection of the route or any possible intent for hiding the route of the patient or contacts. The city service platform should support contact tracing with additional collected information, such as location information and visitor information with the permission or confirmation from the individual or authority.

8.3.6 Public health resources management

A city service platform for PHE should support collaboration and interaction among different stakeholders, such as medical facilities, manufacturers and governments, who work together and interact with each other to manage the public health resources. Medical facilities provide the current information such as usage and stock status. Manufacturers provide stock status and production capacity. Based on the collected information, governments can plan for production and distribution of emergency resources.

8.4 Recovery

After the emergency situation is lifted, a city service platform for PHE should support investigation and evaluation for PHE events, including impact and loss assessment, event response, on-site analysis, incident follow-up processing, etc. Problem analysis and suggestions for improvement should also be provided.

9 Security requirements

9.1 Access security

Within the context of access security, city service platforms for PHE shall:

a) support user identification and authentication, and establish an identity lifecycle management mechanism;

b) be able to handle login failures, such as a limited number of illegal logins and automatic logout when the login connection excesses time limitation;

c) enable a centralized and unified identity management mechanism with multiple dimensions, establish corresponding identity management specifications, and provide an account validation management mechanism for different user systems;

d) enable user authority management mechanisms with authority classification and hierarchical management;

e) support security monitoring based on audit logs, including but not limited to administrative activity audit logs, data access audit logs, system event audit logs and policy denied audit logs.

9.2 Operation security

Within the context of operational security, city service platforms for public health emergencies shall:

a) enable necessary measures and have the ability to identify security risks and vulnerabilities of the platform;

b) ensure timely vulnerability repairment and risk mitigation after sufficient testing and evaluation;

c) follow the minimal installation principle and shut down unnecessary system services and ports;

d) enable intrusion detection capabilities at network boundaries and key nodes;

e) enable the ability to detect and prevent DDoS attacks;

f) be able to identify, alarm and analyze various security attacks.

10 Privacy protection

A city service platform for the collection and processing of personal information in the context of a public health emergency shall (when necessary):

a) ensure personal information is collected directly from the individual only when it is needed, and with the consent of the individual and in accordance with relevant municipal policies;

b) clearly provide a statement to declare the purpose of collection and use of information before collecting, including the usage scope, identity and contact information of the platform, and the consequences of not providing information; the platform shall not collect personal information beyond the usage scope;

c) eliminate information which can directly disclose or imply personal identities during processing and apply de-identification or anonymization techniques to avoid disclosure of personal information during data analysis;

d) ensure that the collection and use of personal information is limited only to public health purposes, unless required by local regulations or laws with the consent of the individual from whom the personal information is collected;

e) meet related requirements identified in ISO/IEC 27701 concerning personal information.

Annex A
(informative)

Certificate check

This annex provides an example of a cross-regional certificate check under PHE which functions in the public interest by checking related health certification information via information code.

The verification client displays the local information code of user A in the information code display interface.

NOTE 1 The local information code of user A indicates the local user identification of user A. The local user identification of user A is used for the registration of the local information platform (see local information platform in Figure A.1).

NOTE 2 The local information platform collects and stores local user information within the managed region. The local user information of one user can be different for different local regions.

The background server corresponding to the verification client sends an information query request with the local information code of user A. Then, the background server corresponding to the verification client sends a request with the local user identification provided by the local information platform (local information platform A in Figure A.1), which does not include health-related information.

The feedback information, such as health certification information provided by the integrated information platform, is sent to the verification client to display in the information checking interface. The health certification information includes the health certification information of user A.

NOTE 3 The health certification information is based on local user information provided by other local information platforms.

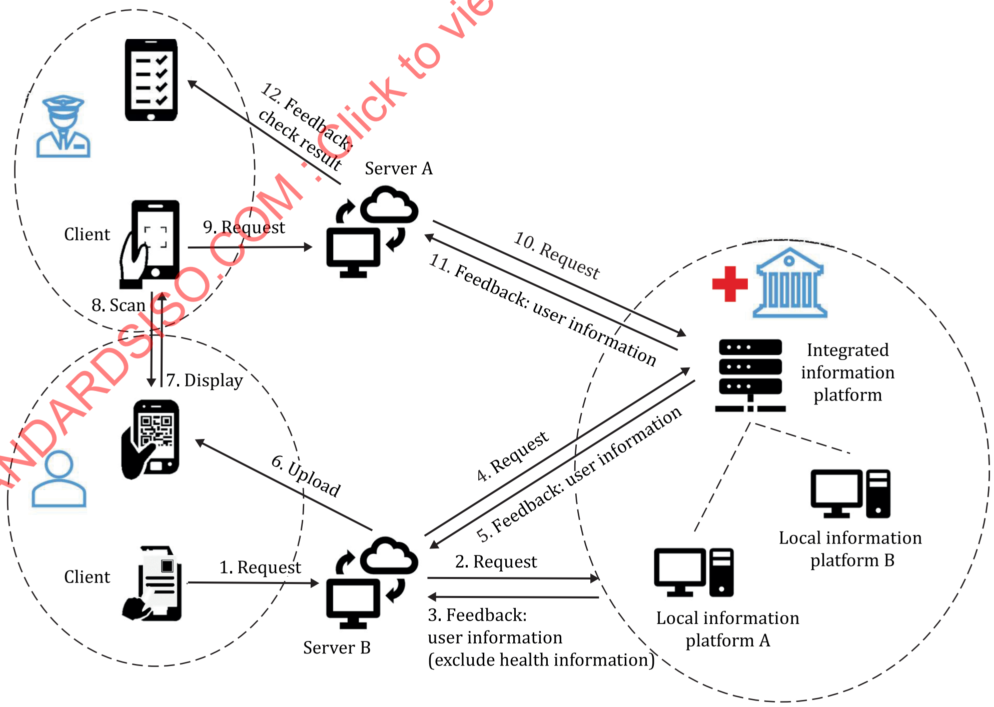

Figure A.1 — Certificate check

The certification client is deployed on code scanner. The registration interface of the certification client includes information required for the code scan control function.

User B activates the scan action by sending a trigger signal to the code scanner, then the code displayed by user A with a generic information code or a local information code is scanned.

NOTE 4 The generic information code of user A indicates the generic user identification of user A. The generic user identification of user A is used for the registration of the integrated information platform, which provides user information in at least one local managed region.

NOTE 5 For scenarios of PHE, the user information includes health-related information.

Then, the request of information query is sent to the integrated information platform with the generic user identification or local user identification of user A. The request is sent to the background server corresponding to the client that has scanned code displayed by user A, i.e server A in Figure A.1.

Feedback of the information query request is provided by the integrated information platform to server A. The feedback includes the user information of user A, which is provided by at least one of the local information platforms which have a connection with the integrated information platform. Then the queried user information of user A, such as whether user A has exposure risks, is forwarded to the certification client for the information checking interface to display.

Annex B
(informative)

Self-check and reporting

A self-checking and reporting mobile application has at least two types of functional user interfaces for the client, and a management platform for management and control:

- a client user functional interface for an individual to fill in required information and get graphic code;
- a client user functional interface for an information manager to record the information of visitors;
- a user information management platform to store and process information.

The process occurs as follows.

1) The client displays the self-checking and information reporting functional interface for the user to fill-in their required information.

2) The filled-in information is uploaded to the management platform with the instruction to submit to the management platform.

3) The management platform processes the received user information and acquires the history storage information of the user to verify the uploaded information and generate verified user information. The graphic code for the submitted user information is generated based on the code generation rule and verified user information. Then, the graphic code will be sent back to the client from where the information is uploaded.

   NOTE 1 The management platform updates the information code generation rule according to obtained epidemic statistical data.

   NOTE 2 The management platform generates the statistic information of the user, which is used to provide instruction of the statistic result of the use information for the user.

4) The user triggers the signal from the user interface of the mobile application to display the graphic code.

5) The manager triggers the signal from the information management user functional interface to scan the displayed graphic code from the user.

6) The information recording interface is displayed with decoded user information from the graphic code.

7) A response is provided to the submission instruction to submit the user information to the management platform.

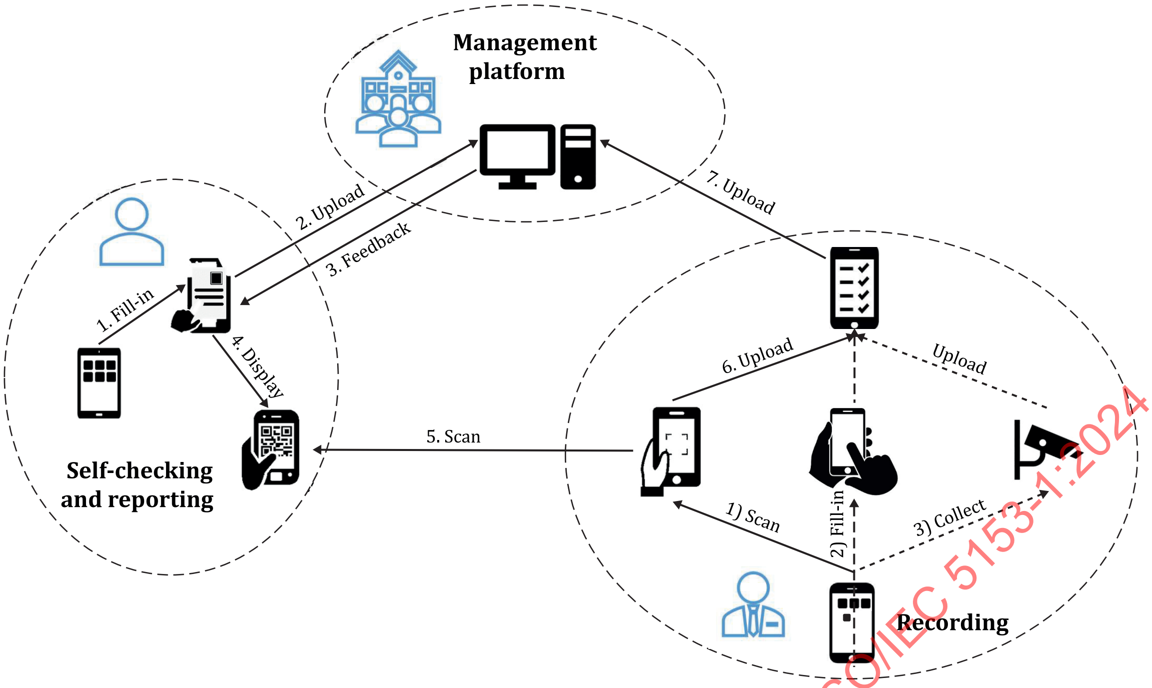

Figure B.1 — Self-check and reporting

The client for the information manager also supports another user functional interface to manage and report personnel information. The manager triggers the signal from the personnel management interface of the mobile application, including a list of managed personnel which contains at least one managed person. If the scanned information code is from a person who is listed in the managed personnel list, an interface for the manager to show the personal information of the person is displayed. Then, a selection signal with the instruction for submission of user information of the managed person to the management platform is triggered. The management platform stores the received user information of the managed person.