TECHNICAL SPECIFICATION

# ISO/TS 22691

First edition
2021-05

# Health informatics — Token-based health information sharing



Reference number
ISO/TS 22691:2021(E)



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) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 215, *Health informatics*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.



 

# Introduction

The interexchange of patient health information between healthcare facilities is important for both patients and the facilities to ensure the continuity and safety of healthcare and to reduce unnecessary examinations. Exchange of health information using IHE XDS is known as an effective solution for accessing patient health information in real-time when needed to provide care.

NOTE 1 Integrating the Healthcare Enterprise (IHE) Cross-enterprise Document Sharing (XDS) architecture and specifications. See Annex A for more information.

However, the ability to share information using IHE XDS technologies tends to require high cost to build and maintain the necessary infrastructure, and it is sometimes difficult for each healthcare facility to create the operational policy for the interoperable exchange of patient health information using that infrastructure. Therefore, media such as CD / DVD continues to be used for exchanging images and other health information (e.g. examination report, lab results, prescriptions, etc.).

In token-based health information sharing, each HI-TOKEN (health information token) contains metadata of a health information document stored in a repository. The HI-TOKEN includes the document ID, which identifies the specific document to be shared. Therefore, there is no need to search for the document using, for example, patient identifying information as search keys. This saves time for the recipient to locate and retrieve the shared document.

A HI-TOKEN can be provided to the patient, who can provide it to the referred healthcare facility at his / her discretion. The referred healthcare facility can then use the HI-TOKEN to retrieve the shared document. This process has the additional advantage that it allows the patient to provide implicit consent for the information exchange in that they are in full control of providing the HI-TOKEN to the receiving care service provider.

Standardization of HI-TOKEN metadata and exchange formats minimizes the potential differences in interpretation between vendors implementing the corresponding systems, thereby contributing to the overall improvement of interoperability.

NOTE 2 Annex B provides an example implementation and data flow for a health information sharing system using HI-TOKEN based exchange, including data content and token format examples.

# Health informatics — Token-based health information sharing

## 1 Scope

This document specifies the data element content and exchange format for tokens used in token-based health information sharing. It includes

a) the data items that may be contained in a health information token (HI-TOKEN),

b) the value representation for each data item,

c) the exchange formats allowed for HI-TOKEN sharing (electronic, machine-readable symbol, print), and

d) considerations when establishing governance policies specifying how HI-TOKENs can be used within a specific group of healthcare organizations.

Provision is made for both physical media and electronic exchange media.

This document addresses the overall conceptual architecture and process for token-based health information sharing, as well as the role of patients, referring healthcare facilities, referred healthcare service providers, and health research institutions. Provision is made for pseudonymization of patient data.

This document only defines the specification of the HI-TOKEN used in token-based health information sharing. Data exchange / transport architectures, encryption methods, and specific governance policy requirements are outside the scope of this document.

## 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 3166-1, *Codes for the representation of names of countries and their subdivisions — Part 1: Country code*

## 3 Terms and definitions

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

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

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

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

**3.1**
**metadata**
attributes and related information about a set of data

**3.2**
**object identifier**
globally unique identifier for an information object

Note 1 to entry: Object identifiers are standardized by standard developing organizations such as the International Telecommunications Union (ITU), ISO or IEC.

**3.3**
**quick response code**
**QR code**
two-dimensional machine-readable optical symbol

Note 1 to entry: QR code formats are specified in ISO/IEC 18004:2015.

**3.4**
**transport layer security**
**TLS**
mechanism that enables use of a secure channel (communication path) for communication between various servers and clients using TCP/IP

Note 1 to entry: TLS is a suite of protocols managed by the Internet Engineering Task Force (IETF), with the foundational definition in RFC 1122.

**3.5**
**health information token**
**HI-TOKEN**
metadata that enables secure exchange in token-based health information sharing

Note 1 to entry: HI-TOKENs can be exchanged in electronic representation, machine-readable optical representation, or paper.

Note 2 to entry: This is a specialized use of the general term "token" in that it refers to the data items and exchange formats specified for use in token-based health information sharing applications.

**3.6**
**universal serial bus**
**USB**
digital interface for connecting up to 127 devices in a tiered-star topology

Note 1 to entry: The specification can be downloaded at www.usb.org.

**3.7**
**health information sharing community**
**health information community**
**HI-community**
group of facilities/enterprises that have agreed to work together using a common set of policies for the purpose of sharing health information using HI-TOKENs

Note 1 to entry: Membership of a facility/enterprise in one community does not prevent it from being a member of another community.

**3.8**
**demilitarized zone**
**DMZ**
logical and physical network space between the perimeter router and the exterior firewall

Note 1 to entry: The DMZ can be between networks and can be under close observation but it does not have to be so.

Note 2 to entry: They are generally unsecured areas containing bastion hosts that provide public services.

# 4 Data items in HI-TOKEN

## 4.1 Overview

Clause 4 defines the data items in a HI-TOKEN. Each HI-community shall determine which data items are mandatory, optional or extended. Extended data items allow for the addition of content that can be necessary for real-world system implementations but is beyond the scope of this HI-TOKEN document.

## 4.2 Item definitions

Table 1 shows HI-TOKEN data item definitions. In addition to data Group and Item Names, Table 1 specifies:

**Short form** Short form of an item name that may be used when long overall length of the HI-TOKEN representation is not desirable (QR code for example).

**Optionality** Two types are identified: “R: Required” and “O: Optional”. Items designated as "R" shall always be included in the HI-TOKEN. Items designated as "O" are optional items that may be included if available and appropriate.

**Type** Identifies the data type for value representation. For details of representation, see Clause 5.

**Description** Specifies the detailed meaning for each data item.

**Table 1 — HI-TOKEN data item definitions**

| Group | Item | Short form | Optionality | Type | Description |
|---|---|---|---|---|---|
| community | identifier | CMID | R | oid | The identifier assigned to the HI-community. The identifier shall be specified as an ISO OID (object identifier). |
| | name | CMNM | O | string | May contain the human-readable display name of the HI-community. |
| sender | identifier | SDID | O | id | May contain the identifier assigned to the sender organization by the HI-community or recognized in the community. |
| | name | SDNM | O | string | May contain the human-readable display name of the sender organization. |
| | contact | SDCT | O | string | May contain the contact (telephone, email etc.) of the sender organization |
| recipient [a] | identifier | RCID | O | id | May contain the identifier assigned to the recipient organization by the HI-community or recognized in the community. |
| | name | RCNM | O | string | May contain the human-readable display name of the recipient organization. |
| creation | timeStamp | CRTS | O | dateTime | May contain date and time the HI-TOKEN was created. |
| patient [b] | identifier | PTID | O | id | May contain the patient ID assigned by the sender organization. |
| | anonymized | PTAN | O | boolean | May contain “true” or “false”. "true" indicates that the information described in the patient has been anonymized while “false" indicates it has not been anonymized. If this data item is not present, or a null value is sent, the interpretation is "false" – that the patient information is not anonymized. |
| | name | PTNM | O | string or hn | May contain the patient’s full name. This data item may have a substructure defined to represent the details of a patient’s name. See chapter 5 Data types and value representations in HI-TOKEN for the format definition of the hn data type. |

[a] “recipient” group may be repeated if the sender intends to send the document to multiple recipients. In some data formats such as JSON, it can be represented as an array.

[b] “patient” group may be repeated if the document includes information of multiple patients. In some data formats such as JSON, it can be represented as an array

**Table 1** *(continued)*

| | | | | | |
|---|---|---|---|---|---|
| | gender | PTGD | O | code | May contain a code to represent the administrative gender of patient.<br>The following code is generally used:<br>female<br>male<br>other<br>unknown<br>This specification does not prevent the use of other gender codes. A HI-community may define and use other gender codes. |
| | birthDate | PTBD | O | date | May contain the patient's date of birth. |
| | nationality | PTNT | O | code | May contain the code of country for patient nationality. Shall be used specified codes in ISO 3166-1 numeric. |
| document | identifier | DMID | R | oid | Shall contain the identifier assigned to the document to be shared. The identifier shall be specified as an ISO OID (object identifier). |
| | description | DMDS | O | string | May contain the description of the document. |
| | numberOfPatients | DMNP | O | integer | May contain the number of patients whose information is included in the document. For example, a document for a clinical study related to multiple individuals.<br>0 means the document is not related to individual patients. If this data item is not sent, or a null value is sent, the interpretation is that the document is associated with ONE patient. |
| decryption | password | DCPW | O | string | May contain the password that will be used to decrypt the patient health information document. The algorithm to be used for encryption is not defined by this specification but should be decided according to the information sharing policy established between the sender and the recipient to ensure interoperability, both within a single HI-community and cross communities. |
| other | | OTXX | O | | This group may contain additional "extended" data items. These items should be included only after consultation between the sender and the recipient to ensure interoperability. |

[a] "recipient" group may be repeated if the sender intends to send the document to multiple recipients. In some data formats such as JSON, it can be represented as an array.

[b] "patient" group may be repeated if the document includes information of multiple patients. In some data formats such as JSON, it can be represented as an array



# 5 Data types and value representations in HI-TOKEN

## 5.1 Overview

Clause 5 defines data types and value representations for data items contained in a HI-TOKEN. A HI-community may define and use extended data types.

## 5.2 Data types and value representations

Table 2 provides data type definitions used for a HI-TOKEN. It speficies:

**Data type** The name of the kind of value being represented.

**Length** The maximum available data length.

**Description** Detailed description of data type content.

**Table 2 — Data type definitions**

| Data type | Length | Description |
|---|---|---|
| string | 10240 | Value representation by string. The number of characters is limited to a maximum of 10240 characters. |
| oid | 64 | An object identifier in ISO OID format [a]. The number of characters is limited to a maximum of 64 characters. |
| dateTime | 25 | Date and time representation with the form "YYYY-MM-DD" or "YYYY-MM-DDThh:mm:ss+zz:zz". The number of characters is limited to a maximum of 25 characters. |
| date | 10 | Date with a representation form "YYYY-MM-DD". |
| hn | - (No limit) | A person or "human" name.<br>Element <text> may contain a text representation of the full name.<br>Element <family> may contain family name. In element <given>, first name, middle name, etc. may also be represented. If need to contain middle name(s), use multiple elements <given>, consider the last <given> as the first name, and the other <given> as the middle name(s).<br>Other elements may be defined and used. |
| id | 64 | Identifier using a combination of upper- or lower-case ASCII letters, numerals ('0'..'9'), '-' and '.'. The number of characters is limited to a maximum of 64 characters. |
| integer | 11 | A signed integer in the range −2147483648..2147483647 (32-bit). |
| boolean | 5 | "true" or "false" that represents truth value. |
| code | 64 | A string that has at least one character and no leading or trailing whitespace.<br>The value is taken from a set of predefined strings (see Descriptions in Table 1). The number of characters is limited to a maximum of 64 characters. |

[a] See oid-info.com for information on ISO/IEC/ITU object identifier formatting and registration.

# 6 Exchange format of HI-TOKEN

## 6.1 Overview

There are three methods to represent a HI-TOKEN: electronic representation, machine-readable optical symbol, and text printed on paper. Implementations of HI-TOKEN document sharing within a HI-community may support one or more of these methods. Each method is described below.

## 6.2 Electronic representation

This document does not define the format of an electronic representation of a HI-TOKEN. Generally, a HI-TOKEN can be represented in XML, JSON, or Plain-Text. In real-world system implementations, the format should be agreed on by the sender and the recipient (see Clause 8 for additional guidance).

Figure 1 displays an example of how a HI-TOKEN can be expressed in electronic representation using JSON.

```
{
    "community": {
        "identifier": "2.9999.1.9999",
        "name": "ISO Example DataExchangeService"
    },
    "sender": {
        "identifier": "9999000001",
        "name": "HI-TOKEN Hospital"
    },
    "creation": {
        "timeStamp": "2020-02-16"
    },
    "patient": [
        {
            "identifier": "1234567890",
            "name": {
                "family": "ISO",
                "given": [
                    "iso",
                    "Iso"
                ]
            },
            "gender": "N",
            "birthDate": "2017-09-29"
        }
    ],
    "document": {
        "identifier": "2.25.113059749145936325402354257176981405696"
    },
    "decryption": {
        "password": "13E9M5GH5M5SSWK8O8GCA0WSG"
    }
}
```


**Figure 1 — Example of JSON encoded HI-TOKEN**

## 6.3 Machine-readable optical representation

A HI-TOKEN can also be represented as a machine-readable optical symbol. Although this document does not define the type or format of a machine-readable optical symbol representing a HI-TOKEN, QR codes are widely used internationally and across industries. In order to minimize the required HI-TOKEN size in a QR code, data item “Short form” in Table 1 can be used.

The following is an example of QR code where the colon, i.e. ":", is used as a separator between item names in short form and the corresponding values while the forward slash, i.e. "/", is used as an item delimiter.

Figure 2 shows an example of how a HI-TOKEN can be expressed in machine-readable optical representation.

CMID:2.9999.1.9999 / DMID: 2.25.113059749145936325402354257176981405696 /
DCPW:13E9M5GH5M5SSWK8O8GC40WSG

**Figure 2 — Example of a QR code as a machine-readable optical representation**

## 6.4 Printed text representation

A HI-TOKEN can also be printed as text on physical paper. This document does not define a specific format or layout for printing HI-TOKEN information on paper media. Machine-readable optical symbol can also be printed on paper so that the system of the recipient can easily read a HI-TOKEN.

The following is an example of printing a HI-TOKEN on paper media with a QR code.

Figure 3 shows an example of how a HI-TOKEN can be formatted when printed.

# Health Information Token

| | |
|---|---|
| Community | ISO Example DataExchangeService<br>ID: 2.9999.1.9999 |
| Sender | HI-TOKEN Hospital<br>ID: 9999000001 |
| Date of Issue | 2020-02-16 |

| | |
|---|---|
| Patient ID | 99991203732 |
| Patient Name | ISO iso Iso |
| Patient Sex | N |
| Date of Birth | 2017-09-29 |

Community ID
Document ID
Password

CMID:2.9999.1.9999
DMID: 2.25.113059749145936325402354257176981405696
DCPW:13E9M5GH5M5SSWK8O8GC40WSG



**Figure 3 — Example of a HI-TOKEN on printed text representation**

## 7 Security considerations

### 7.1 General considerations

#### 7.1.1 Overview

Proper risk assessment should be performed when implementing an information sharing system using HI-TOKEN.

There are many formal and informal information security guidance documents and standards; however, the following subclauses identify considerations that are of particular relevance to HI-TOKEN security management.

#### 7.1.2 HI-TOKEN

Since a HI-TOKEN is the key to access the document, it should be managed properly. A HI-TOKEN should be written, retained, read and transferred in safe ways. In real-world operations, the overall management process should be designed appropriately to avoid unintended disclosure of a HI-TOKEN at any occasion. When the issuer provides the HI-TOKEN to a patient, it is recommended that the issuer tells the patient not to disclose the content of the HI-TOKEN unnecessarily and unintentionally.

#### 7.1.3 Documents stored in the information repository

A document stored in a repository should be well protected. For example, encryption / decryption passwords should not be communicated to or held in the same information exchange server as the encrypted document.

#### 7.1.4 Data transfer

The unintended disclosure of document content by interception during data transfer should be prevented. Document encryption is the primary method for ensuring confidentiality and integrity. The use of TLS in internet communication provides an additional level of data protection.

If documents are transferred using media such as USB memory devices, special handling should be followed including the complete deletion of the files after use.

#### 7.1.5 Encryption

A sufficiently strong encryption and long decryption passwords should be used to achieve better security.

#### 7.1.6 Authentication and authorization

User authentication and authorization methods are often used for access control, ensuring that the user or the client are legitimate and have the necessary permission to access data. While outside the scope of this document, HI-communities are strongly encouraged to implement appropriate authorization and authentication capabilities utilizing up-to-date methods. Authentication and authorization to access HI-TOKEN itself are also subject to be considered.

#### 7.1.7 Logging

In order to track health information document exchange activity, it is desirable to make appropriate logs with appropriate methods. For example, using the IHE ITI ATNA (Audit Trail / Node Authentication) profile is an effective option.

### 7.2 Specific requirements

There are no specific security implementation requirements, such as encryption methods or transport-specific security mechanisms.

## 8 Guidance for establishing a HI-community token sharing policy

In order to implement effective and interoperable use of HI-TOKEN sharing within a HI-community, all participants shall agree on all the details relating to the information and formatting of the tokens, as well as the procedures and expectations for how they will be used and managed. Establishing a HI-community governance policy should be completed early in any implementation project and should be reviewed and maintained regularly throughout the life of the program. Considerations should include:

**a. Data item optionality**

— Data items presented in Clause 4 may be designated as mandatory, optional or conditional

— In the case of "conditional" data items, the criteria for inclusion or exclusion should be clearly stated

— Multiplicity limitations, if any, should also be explicitly specified; for example, data items that may repeat may be limited to a maximum number of instances

**b. Data item extensions**

— Additional data items not specified in Clause 4 should be clearly specified

— Data item optionality, value representation and any limitations should be specified

**c. Data value representations**

— Additional constraints or requirements for data item values that have variable contents

— This includes specifying valid "community", "sender" and "recipient" organization identifiers and names, etc.

**d. HI-TOKEN exchange format(s)**

— Clause 6 specifies three HI-TOKEN exchange formats. A HI-community shall determine which of the three may or shall be supported

— Some formats, such as printed text, may require layout requirements, including size and location of the HI-TOKEN QR code that is printed

**e. Security and privacy management**

— Specific security mechanisms (including token encryption technology) are beyond the scope of this document; however, specific technologies (encryption / decryption methods) to achieve exchange

— Clause 7 provides some basic security considerations; however, many HI-communities operate within jurisdictions that require additional, often extensive, security measures

— Privacy should also be ensured as required by the community (legal regulations can also apply); this includes ensuring that individuals fully understand their responsibilities in reducing the unplanned disclosure of personal information

— Patient identification information often varies between HI-TOKEN sender and recipient organizations; care shall be taken to identify and reconcile these cases, ensuring that the information is properly associated on the receiving end

**f. HI-TOKEN management processes**

— Mechanisms should be established for how HI-communities will identify (e.g. periodic surveys) and resolve issues arising from HI-TOKEN usage; or

— Determine how to improve its usage (e.g. new data item usage)

**g. Mappings or mixed-architecture use support**

— Some HI-communities can use, for example, IHE XDS.b and "XDS on FHIR" infrastructure for information exchange internally or between specific organizations

— Guidance or specifications can be made to facilitate the ease of integrating information that is provided using HI-TOKEN exchange but that can ultimately be integrated into a different health information exchange architecture

Additional considerations can be required, depending on the organizational entities involved, the legal regulations that govern information management and exchange in each region, etc.

# Annex A
(informative)

# Comparison of IHE XDS/XDR and token-based health information sharing use cases

## A.1 Overview

This Annex compares the token-based health information sharing with IHE XDS and XDR profiles including XDS on FHIR, by illustrating actors and transactions.

This Annex reproduces text from the following documents:

a. IHE IT Infrastructure (ITI) Technical Framework, Volume 1 (ITI TF-1) Integration Profiles Profiles-Revision 16.0[5]

b. IHE IT Infrastructure Technical Framework Supplement Mobile access to Health Documents (MHD) With XDS on FHIR Rev. 3.1 – Trial Implementation

## A.2 Overview: IHE XDS

The Cross-Enterprise Document Sharing (XDS.b) IHE Integration Profile facilitates the registration, distribution and access across health enterprises of patient electronic health records. Cross-Enterprise Document Sharing is focused on providing a standards-based specification for managing the sharing of documents between any healthcare enterprise, ranging from a private physician office to a clinic to an acute care in-patient facility.

The XDS.b Integration Profile assumes that these enterprises belong to one or more XDS Affinity Domains. An XDS Affinity Domain is a group of healthcare enterprises that have agreed to work together using a common set of policies and share a common infrastructure.

Within an XDS Affinity Domain, certain common policies and business rules shall be defined. They include how patients are identified, consent is obtained, and access is controlled, as well as the format, content, structure, organization and representation of clinical information. This Integration Profile does not define specific policies and business rules; however, it has been designed to accommodate a wide range of such policies to facilitate the deployment of standards-based infrastructures for sharing patient clinical documents. This is managed through federated document repositories and a document registry to create a longitudinal record of information about a patient within a given XDS Affinity Domain.

The concept of a document in XDS is not limited to textual information. As XDS is document content neutral, any type of clinical information without regard to content and representation is supported. In order to ensure the necessary interoperability between the document sources and the document consumers, the XDS Affinity Domain shall adopt policies concerning document format, structure and content.

Figure A.1 shows the actors involved in the XDS.b Profile and the relevant transactions between them.

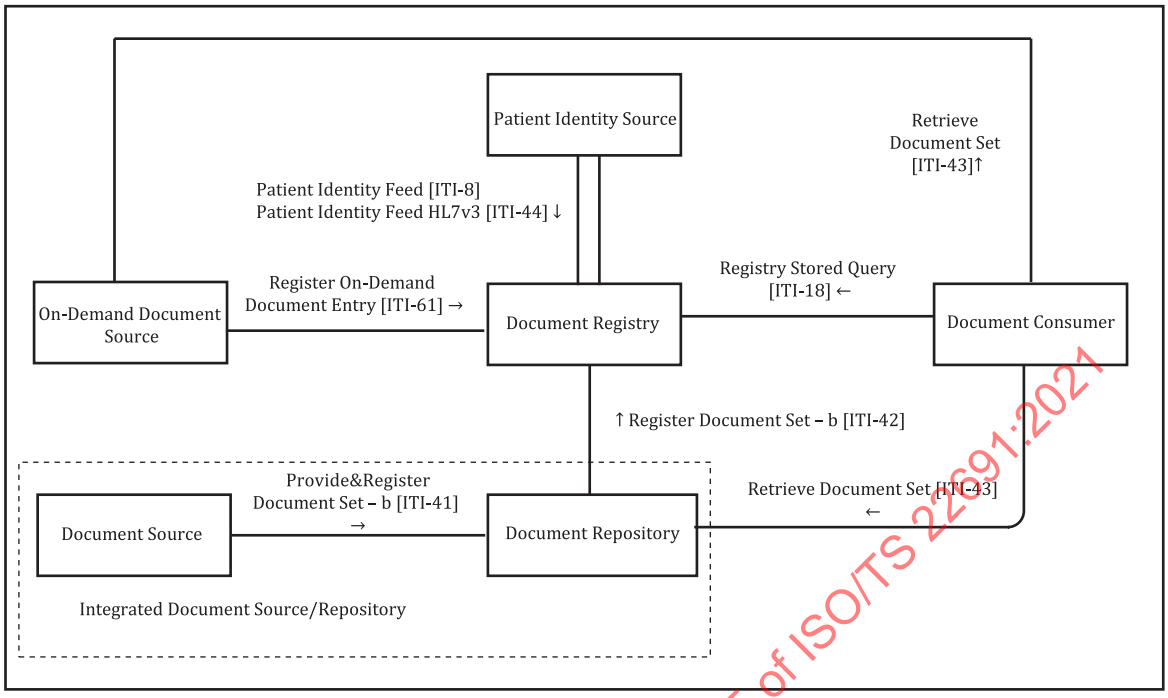


**Figure A.1 — Cross-enterprise document sharing – b (XDS.b) diagram**

## A.3 Overview: IHE XDR

Cross-Enterprise Document Reliable Interchange (XDR) provides document interchange using a reliable messaging system. This permits direct document interchange between EHRs, PHRs, and other health IT systems in the absence of a document sharing infrastructure such as XDS Registry and Repositories.

XDR provides a reliable and automatic transfer of documents and metadata for one patient between EHR systems even in the absence of an XDS infrastructure. XDR supports the reuse of the Provide and Register Set transaction-b with Web-Services as transport. Transfer is direct from source to consumer; no repository or registry actors are involved.

XDR is document format agnostic, supporting the same document content as XDS.

Figure A.2 shows the actors involved in the XDR Integration Profile and the relevant transactions between them.

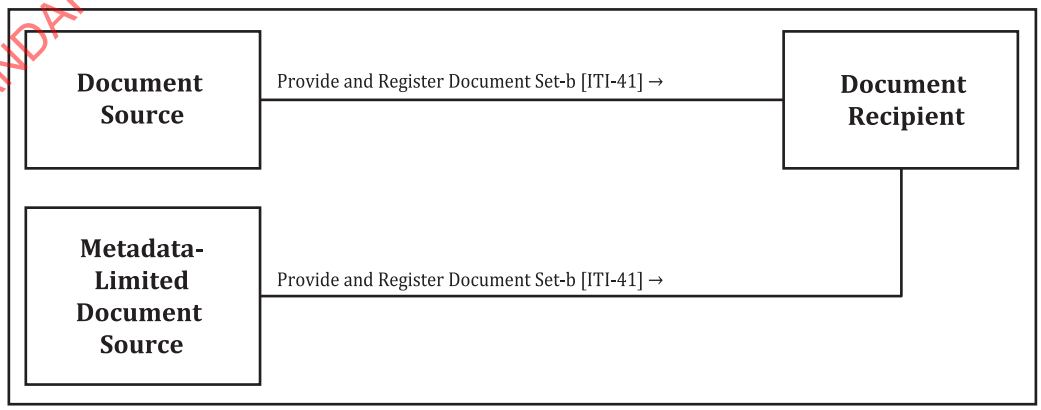


**Figure A.2 — XDR actor diagram**

XDR describes the exchange of a set of a patient's documents between healthcare providers, such as: physicians, hospitals, special care networks, or other healthcare professionals.

Where XDS Registry/Repositories are not yet implemented or available for the exchange of information, XDR is the viable approach.

In a situation where the information is going to an automated application or robust system capable of automated storage or processing of documents relative to one patient, XDR is the appropriate profile.

The XDR Integration Profile is intended only for exchange of patient related medical documents and not intended to address all cross-enterprise EHR communication needs.

## A.4 Overview: IHE MHD and "XDS on FHIR"

The Mobile access to Health Documents (MHD) Profile defines one standardized interface to health documents (a.k.a. an Application Programming Interface (API)) for use by mobile devices so that deployment of mobile applications is more consistent and reusable.

The MHD Profile does not replace XDS. Rather, it enables simplified access by mobile devices to an XDS (or a similar) document management environment containing health information.

Figure A.3 shows the actors involved in the MHD Profile and the relevant transactions between them.

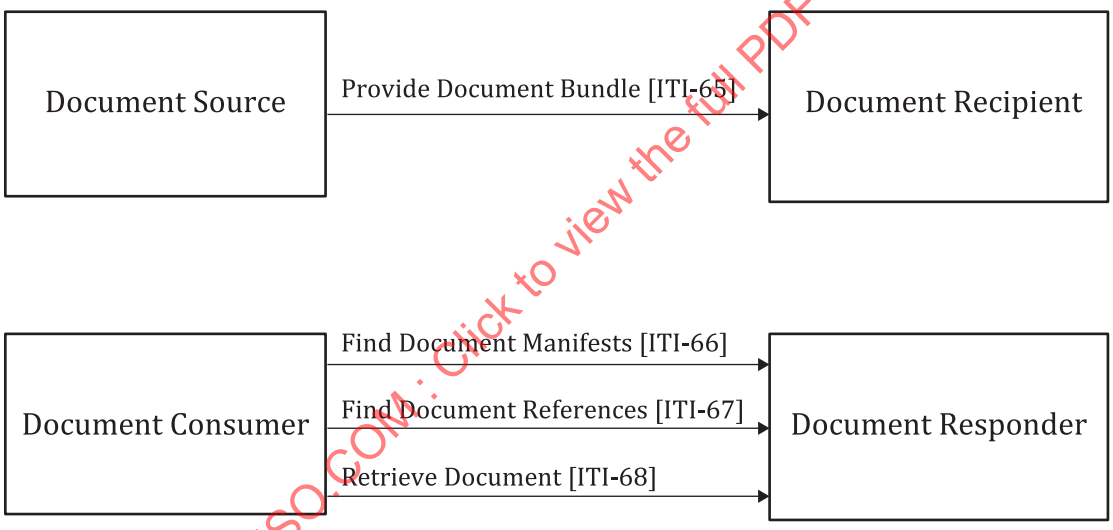


**Figure A.3 — MHD actor diagram**

When the MHD Document Recipient is acting as a proxy for an XDS environment, it could be grouped with an XDS Document Source as the "XDS on FHIR" Option defines. In this way, a received Provide Document Bundle [ITI-65] transaction would be converted by the grouped system into an XDS Provide and Register Document Set-b [ITI-41] transaction. The MHD Document Recipient, acting as a proxy, could be configured to support only a designated set of mobile devices authorized by the hosting organization and use the security model defined by that hosting organization.

Other proxy architectures to XDS are possible such as grouped with an XDS Integrated Document Source/Repository.

When the MHD Document Responder is acting as a proxy for an XDS environment, it could be grouped with an XDS Document Consumer. In this way, the MHD Find Document Manifests [ITI-66], Find Document References [ITI-67], and Retrieve Document [ITI-68] transactions will be supported in the system using the appropriate XDS Registry Stored Query [ITI-18] and Retrieve Document Set-b [ITI-43] transactions. This proxy would be configured to support a designated set of mobile devices and the security model defined by the hosting organization.

Figure A.4 illustrates MHD Actors grouped with XDS.

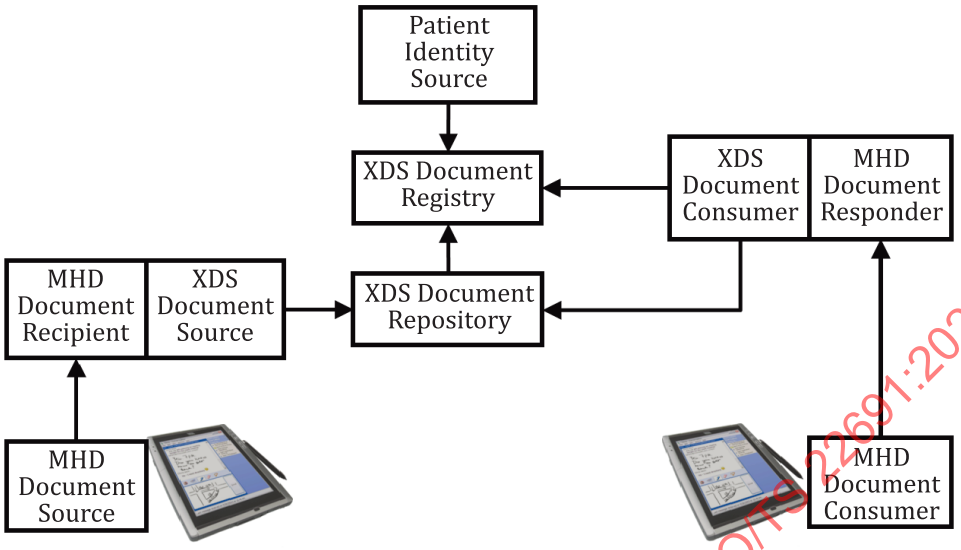


**Figure A.4 — MHD actors grouped with XDS**

## A.5 Token-based health information sharing

Token-based health information sharing supports document exchange using HI-TOKENS. The architectural approach is considerably simpler than XDS and does not have the constraints of XDR. Although XDS supports a very wide set of use cases, it also has significant infrastructure requirements that impact implementation complexity and cost. XDR is simpler than XDS; however, it also requires synchronous exchange between sender and recipient, and requires other out-of-band means for ensuring patient consent.

Token-based health information sharing has additional features, including:

**a. No patient query requirements**

Since the document is identified directly by the document ID, there is no need to make a query with patient as a search key. Therefore, there is reduced risk that the recipient downloads the wrong document.

A document can contain information of multiple patients or can not be related with individual patients since the patient is not a key to retrieve the document.

**b. Coexistence with other sharing methods**

Since this document does not define the communication method, any exchange method may be used as long as security and reliability requirements are ensured.

Token-based health information sharing does not replace XDS, MHD, etc.; rather it may can with these existing system solutions.

For example, communication can be implemented with those defined in IHE ITI, thus allowing token-based health information sharing to coexist with XDS. For example, the sender uploads a document to the repository with ITI-41 transaction (the sender as the document source), and the recipient downloads the document with ITI-43 (the recipient as the document consumer). However, in this implementation the recipient directly accesses the Repository without need of querying a Registry to locate the needed documents.

Figure A.5 shows an example using XDS transactions.

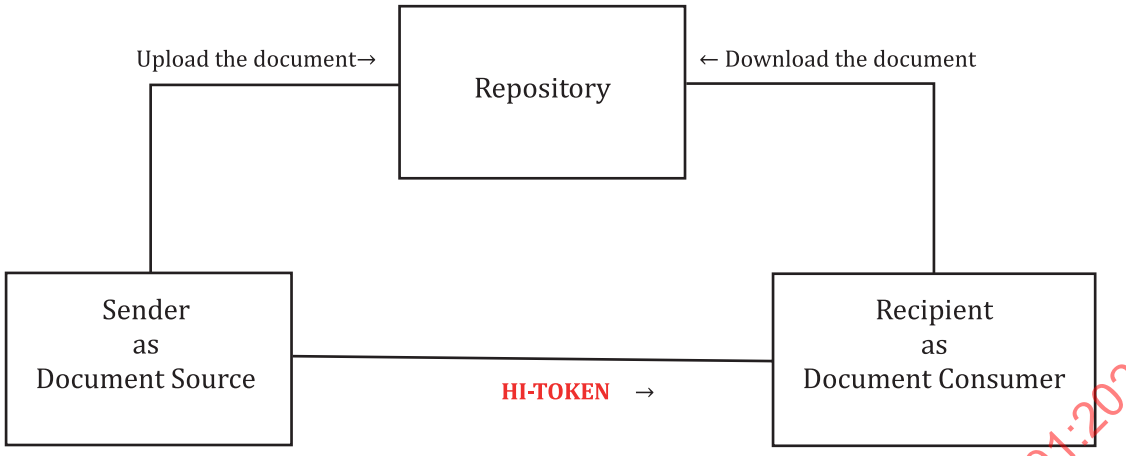


**Figure A.5 — Token-based health information sharing diagram**

Token-based health information sharing can also coexist with IHE MHD. Figure A.6 shows an example using MHD transactions. HI-TOKENs can be used as a substitute of MHD Find Document Manifests [ITI-66]. Since HI-TOKENs can directly identify the document with Document ID, there is no need to search for data using Find Document Manifests with patient information as a search key.

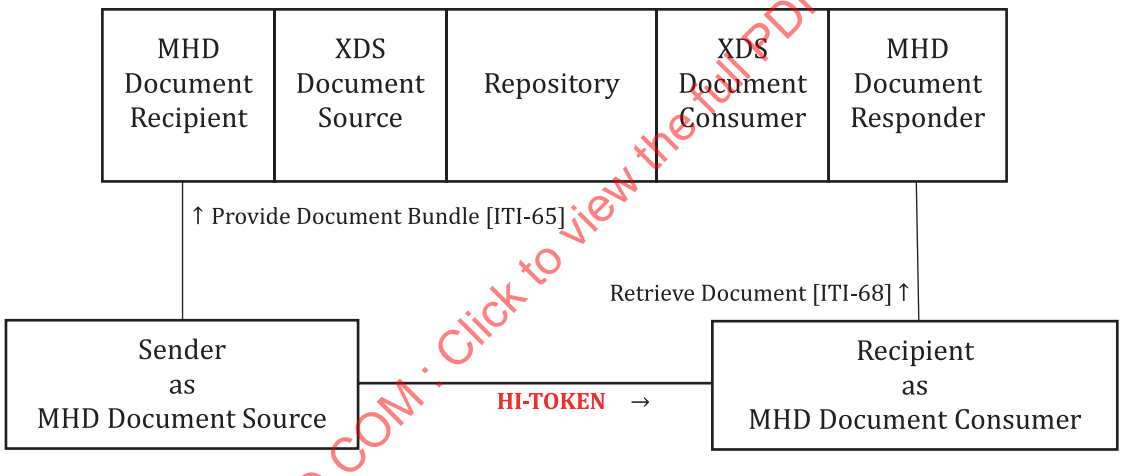


**Figure A.6 — Token-based health information sharing with MHD transactions diagram**

**c. Access is inherently controlled by the HI-TOKEN holder**

A document can be encrypted since the HI-TOKEN can contain the decryption password. When encryption is applied, the HI-TOKEN holder (patients for example) has the access control to the document since no one can access the shared document without HI-TOKEN that includes the decryption password.

Since the sender and the recipient work separately, the policies to be shared between the sender and the recipient can be minimum.

# Annex B
(informative)

# Data flow of token-based health information sharing

## B.1 Overview

This annex provides an example implementation and data flow for a health information sharing system using HI-TOKEN based exchange, including data content and token format examples. There are various other implementation approaches that can be utilized, and the examples below are only for illustrative purposes.

## B.2 Dataflow

Figure B.1 illustrates diagram on system configuration and connection.

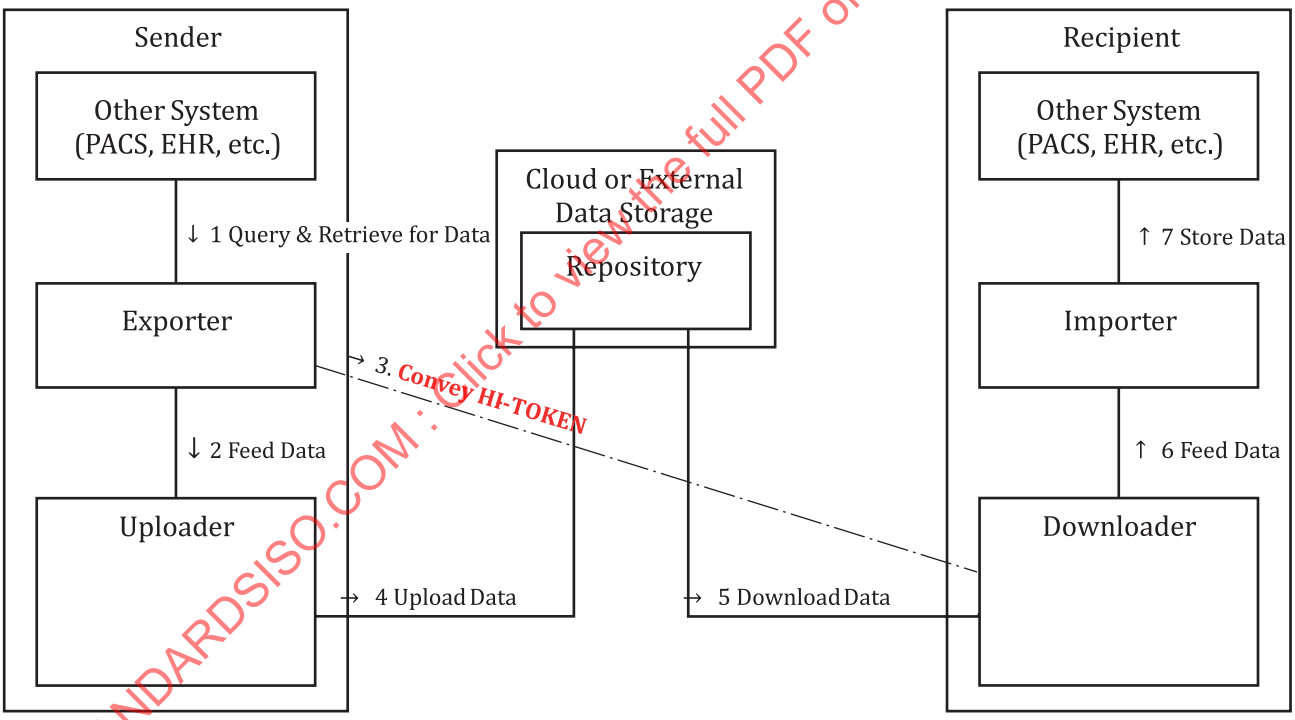


**Figure B.1 — Dataflow of token-based health information sharing connection diagram**

Figure B.2 illustrates sequence diagram of data flow.

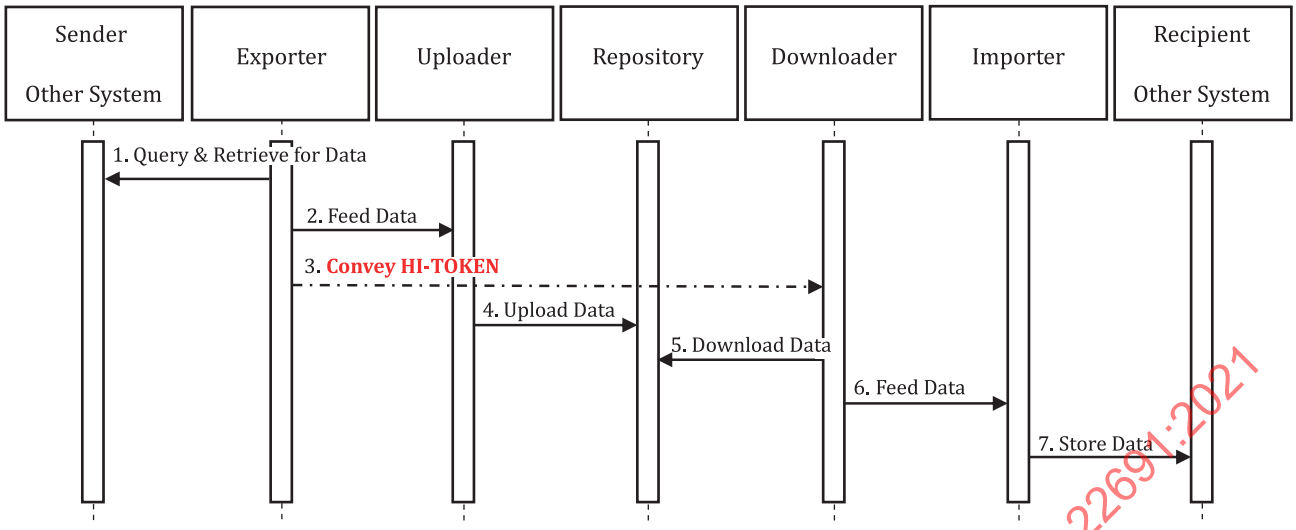


**Figure B.2 — Dataflow of token-based health information sharing sequence diagram**

1. The Exporter queries and retrieves data related to a specific patient from an information system in its own facility.
2. The Exporter creates a single archive file with a unique document ID, encrypts the retrieved data and sends it to the Uploader. If the Uploader is not directly connected to the facility's internal network (i.e. it is located on the DMZ), it is assumed to be delivered using media such as a USB memory device.
3. The Exporter creates a HI-TOKEN. The HI-TOKEN can be stored on the electronic media such as patients' smartphone or printed on paper media. The HI-TOKEN is conveyed (e.g. "sneaker-net") to the Recipient.
4. The Uploader sends the document archive with the document ID to the Repository.
5. When the Downloader receives a HI-TOKEN, it reads the content of the HI-TOKEN. The Downloader retrieves the document archive file from the Repository using the document ID in the HI-TOKEN.
6. The Downloader sends the retrieved data to the Importer, delivered either directly online or delivered offline via media. If the Downloader is not directly connected to the facility's network (i.e. it is located on the DMZ), the file(s) are assumed to be delivered using media such as a USB memory device.
7. Retrieved data should be reconciled and sent to other systems in the recipient facility or stored for future access. Note that the patient ID and other attributes are those of the sender facility and might not be the same as those used at the recipient facility. In that case, patient attributes should be reconciled to ensure that it is properly applied in the recipient facility.



## B.3 Examples of the using token-based health information sharing

### B.3.1 Sender facility:exporter / uploader

In the example displayed in Figure B.3, the Uploader is not directly connected to the facility's network. This can be the result of a security strategy often employed by organizations to "air gap" networks, removing any connection and thus any possibility for systems from one network compromising those on another. In these cases, the document can be transported using USB memory devices, the HI-TOKEN with the document's metadata is printed to a "token sheet"