



IEEE Standard for Blockchain-Based Hepatobiliary Disease Data Extraction and Exchange

STANDARDS

IEEE Consumer Technology Society

Developed by the
Digital Finance and Economy Standards Committee

IEEE Std 3806™-2023

IEEE Standard for Blockchain-Based Hepatobiliary Disease Data Extraction and Exchange

Developed by the

Digital Finance and Economy Standards Committee
of the
IEEE Consumer Technology Society

Approved 21 September 2023

IEEE SA Standards Board

Abstract: Liver and gallbladder diseases affect more than one billion people around the world, but there is still a lack of successful experience and models in terms of data standardization, integration, and sharing. The goal of this document is to solve the above problems through blockchain-based data circulation standards. This standard mainly describes the format of the data circulation and the application process of hepatobiliary diseases, which standardize the data collection, processing, and exchange process of hepatobiliary disease data in the medical information system, aiming to bring a new data credible circulation innovation model for medical education, data sharing applications, and medical artificial intelligence product research and development of hepatobiliary disease big data.

Keywords: blockchain, data exchange, credible circulation, IEEE 3806™, liver cancer

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

Copyright © 2024 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 26 January 2024. Printed in the United States of America.

IEEE is a registered trademark in the U.S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated.

PDF: ISBN 979-8-8557-0454-9 STD26729
Print: ISBN 979-8-8557-0455-6 STDPD26729

*IEEE prohibits discrimination, harassment, and bullying.
For more information, visit <https://www.ieee.org/about/corporate/governance/p9-26.html>.
No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.*

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE Standards documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page (<https://standards.ieee.org/ipr/disclaimers.html>), appear in all standards and may be found under the heading “Important Notices and Disclaimers Concerning IEEE Standards Documents.”

Notice and Disclaimer of Liability Concerning the Use of IEEE Standards Documents

IEEE Standards documents are developed within IEEE Societies and subcommittees of IEEE Standards Association (IEEE SA) Board of Governors. IEEE develops its standards through an accredited consensus development process, which brings together volunteers representing varied viewpoints and interests to achieve the final product. IEEE standards are documents developed by volunteers with scientific, academic, and industry-based expertise in technical working groups. Volunteers are not necessarily members of IEEE or IEEE SA and participate without compensation from IEEE. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

IEEE makes no warranties or representations concerning its standards, and expressly disclaims all warranties, express or implied, concerning this standard, including but not limited to the warranties of merchantability, fitness for a particular purpose and non-infringement. IEEE Standards documents do not guarantee safety, security, health, or environmental protection, or guarantee against interference with or from other devices or networks. In addition, IEEE does not warrant or represent that the use of the material contained in its standards is free from patent infringement. IEEE Standards documents are supplied “AS IS” and “WITH ALL FAULTS.”

Use of an IEEE standard is wholly voluntary. The existence of an IEEE standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity, nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document, should rely upon their own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: THE NEED TO PROCURE SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Translations

The IEEE consensus balloting process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE is the approved IEEE standard.

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE SA Standards Board Operations Manual shall not be considered or inferred to be the official position of IEEE or any of its committees and shall not be considered to be, nor be relied upon as, a formal position of IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that the presenter's views should be considered the personal views of that individual rather than the formal position of IEEE, IEEE SA, the Standards Committee, or the Working Group. Statements made by volunteers may not represent the formal position of their employer(s) or affiliation(s).

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE or IEEE SA. However, **IEEE does not provide interpretations, consulting information, or advice pertaining to IEEE Standards documents.**

Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive the concurrence of a balance of interests. For this reason, IEEE and the members of its Societies and subcommittees of the IEEE SA Board of Governors are not able to provide an instant response to comments, or questions except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Any person who would like to participate in evaluating comments or in revisions to an IEEE standard is welcome to join the relevant IEEE working group. You can indicate interest in a working group using the Interests tab in the Manage Profile and Interests area of the [IEEE SA myProject system](#).¹ An IEEE Account is needed to access the application.

Comments on standards should be submitted using the [Contact Us](#) form.²

Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document does not constitute compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Data privacy

Users of IEEE Standards documents should evaluate the standards for considerations of data privacy and data ownership in the context of assessing and using the standards in compliance with applicable laws and regulations.

¹Available at: <https://development.standards.ieee.org/myproject-web/public/view.html#landing>.

²Available at: <https://standards.ieee.org/content/ieee-standards/en/about/contact/index.html>.

Copyrights

IEEE draft and approved standards are copyrighted by IEEE under US and international copyright laws. They are made available by IEEE and are adopted for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making these documents available for use and adoption by public authorities and private users, neither IEEE nor its licensors waive any rights in copyright to the documents.

Photocopies

Subject to payment of the appropriate licensing fees, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual, non-commercial use only. To arrange for payment of licensing fees, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400; <https://www.copyright.com/>. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Updating of IEEE Standards documents

Users of IEEE Standards documents should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect.

Every IEEE standard is subjected to review at least every 10 years. When a document is more than 10 years old and has not undergone a revision process, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE standard.

In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit [IEEE Xplore](#) or [contact IEEE](#).³ For more information about the IEEE SA or IEEE's standards development process, visit the IEEE SA Website.

Errata

Errata, if any, for all IEEE standards can be accessed on the [IEEE SA Website](#).⁴ Search for standard number and year of approval to access the web page of the published standard. Errata links are located under the Additional Resources Details section. Errata are also available in [IEEE Xplore](#). Users are encouraged to periodically check for errata.

Patents

IEEE standards are developed in compliance with the [IEEE SA Patent Policy](#).⁵

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has

³Available at: <https://ieeexplore.ieee.org/browse/standards/collection/ieee>.

⁴Available at: <https://standards.ieee.org/standard/index.html>.

⁵Available at: <https://standards.ieee.org/about/sasb/patcom/materials.html>.

filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE SA Website at <https://standards.ieee.org/about/sasb/patcom/patents.html>. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

IMPORTANT NOTICE

Technologies, application of technologies, and recommended procedures in various industries evolve over time. The IEEE standards development process allows participants to review developments in industries, technologies, and practices, and to determine what, if any, updates should be made to the IEEE standard. During this evolution, the technologies and recommendations in IEEE standards may be implemented in ways not foreseen during the standard's development. IEEE standards development activities consider research and information presented to the standards development group in developing any safety recommendations. Other information about safety practices, changes in technology or technology implementation, or impact by peripheral systems also may be pertinent to safety considerations during implementation of the standard. Implementers and users of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices and all applicable laws and regulations.

Participants

At the time this standard was completed, the Blockchain-Based Hepatobiliary Disease Data Extraction and Exchange Working Group had the following membership:

Jiahong Dong, *Chair*
Wai Kin (Victor) Chan, *Vice Chair*
Wei Xu, *Secretary*

<i>Organization Represented</i>	<i>Name of Representative</i>
0xSenses Corporation.....	Yu Yuan
Beijing Tsinghua Changgung Hospital.....	Jiahong Dong
Fuzhou Data Technology Research Institute Co., Ltd.....	Hairong Lyu
Huakong TsingJiao Information Science Co., Ltd.....	Wei Xu
Peking Union Medical College Hospital.....	Meng Yang
Tsinghua University.....	Wai Kin (Victor) Chan

The Working Group gratefully acknowledges the contributions of the following participants. Without their assistance and dedication, this standard would not have been completed.

Sisi Duani	Daozhuang Lin	Bin Yang
Xiaobin Feng	Minghui Liu	Yi Yang
Haitian Fu	Ligong Lu	Wei Yin
Chengquan Li	Lan Ma	Xiaomao Yu
Qiang Li	Boyuan Shi	Hongxu Yun
Yong Li	Shiyu Sun	Jiawen Zhou

The following members of the entity Standards Association balloting group voted on this standard. Balloters may have voted for approval, disapproval, or abstention.

0xSenses Corporation	Intel
Beijing Tsinghua Changgung Hospital	Shenzhen Jiatian Technology Co., Ltd.
Fuzhou Institute for Data Technology	Shenzhen University
Guangdong Zhongchuang Zhijia Research Co., Ltd.	South China University of Technology
Hangzhou Qulian Technology Co., Ltd.	Tongyuan Software Co., Ltd
Huakong TsingJiao Information Science (Beijing) Limited	Tsinghua Shenzhen International
Institute of Biomedical Engineering	Graduate School

When the IEEE SA Standards Board approved this standard on 21 September 2023, it had the following membership:

David J. Law, *Chair*
Ted Burse, *Vice Chair*
Gary Hoffman, *Past Chair*
Konstantinos Karachalios, *Secretary*

Sara R. Biyabani
Doug Edward
Ramy Ahmed Fathy
Guido R. Hiertz
Yousef Kimiagar
Joseph L. Koepfinger*
Thomas Koshy
John D. Kulick

Joseph S. Levy
Howard Li
Johnny Daozhuang Lin
Gui Lin
Xiaohui Liu
Kevin W. Lu
Daleep C. Mohla
Andrew Myles

Paul Nikolich
Annette D. Reilly
Robby Robson
Lei Wang
F. Keith Waters
Karl Weber
Philip B. Winston
Don Wright

*Member Emeritus

Introduction

This introduction is not part of IEEE Std 3806-2023, IEEE Standard for Blockchain-Based Hepatobiliary Disease Data Extraction and Exchange.

This standard is oriented to various application links such as prevention, screening, diagnosis, treatment, rehabilitation and prognosis of liver and gallbladder diseases; it establishes a service standard reference for reliable circulation of liver and gallbladder disease data for various medical institutions, research institutions, and medical and pharmaceutical companies. It uses blockchain technology to define the attributes of data, data attributes, electronic medical records, traceability certificates, and other data circulation links, and to describe the transfer of data in data circulation, the transmission of disease data, and the checking of medical record information between different applications.

This standard mainly describes the format of the data circulation and the application process of hepatobiliary diseases. When data is extracted and exchanged between different organizations and applications, the data formats, interfaces, and security algorithm standards of different organizations are inconsistent, resulting in ineffective communication between applications and organizations. The goal of this document is to solve the above problems through blockchain-based data circulation standards.

According to the standards of hepatobiliary data collection, labeling and quality control, a standard data set of diagnosis and treatment based on blockchain data structure was established. This data set focuses on adult cases diagnosed with hepatobiliary disease. The data scope is mainly based on therapeutic medical records and CT imaging examination, supplemented by full-cycle medical records and multimodal imaging examinations, and standardized data collection and exchange data standards for case data are formulated.

The classification of this standard refers to the national electronic medical records and information industry standards, as well as the latest diagnosis and treatment standards in the field of hepatobiliary diseases. It mainly includes the whole-process medical record data of 19 modules including basic information, medical records, current medical history, past history, personal history, family history, physical examination, diagnosis, laboratory examination, imaging examination, and pathological examination of patients with hepatobiliary diseases. This standard involves the group standards “Standard Data Specification for Hepatobiliary Diseases: Liver Cancer CT/MRI Image Acquisition and Processing Standards,” “Standard Data Specifications for Hepatobiliary Diseases: Liver Cancer CT/MRI Image Labeling and Quality Control Standards,” and “Standard Data Specification for Hepatobiliary Diseases: Standard Dataset of Medical Records for Liver Cancer Research” issued by the Chinese Medical Doctor Association.

Contents

1. Overview	11
1.1 General	11
1.2 Scope	11
1.3 Word usage	11
2. Normative references	11
3. Definitions, acronyms, and abbreviations	12
3.1 Definitions	12
3.2 Acronyms and abbreviations	14
4. Application framework for data extraction and exchange of hepatobiliary diseases	14
4.1 Hepatobiliary disease data extraction and exchange of the data structure	14
4.2 Data extraction and exchange process for hepatobiliary diseases	15
5. Data extraction and exchange of hepatobiliary diseases	15
6. Hepatobiliary disease data extraction and exchange attributes	16
6.1 Data definition	16
6.2 Extract and exchange properties	17
6.3 Organization definition	17
6.4 Application description	18
6.5 Application definition	18
7. Hepatobiliary disease data exchange users	19
7.1 Design guideline	19
7.2 User definition	19
8. Hepatobiliary disease data extraction and exchange statistics and traceability	19
8.1 General requirements	19
8.2 Statistics	20
8.3 Data traceability	20
Annex A (informative) Hepatobiliary disease data application panorama	21
Annex B (informative) Data set standard	23
Annex C (informative) Bibliography	57

IEEE Standard for Blockchain-Based Hepatobiliary Disease Data Extraction and Exchange

1. Overview

1.1 General

This standard mainly describes the format of the data circulation and application process of hepatobiliary diseases, so as to standardize the data collection, processing, and exchange process of hepatobiliary disease data in the medical information system.

1.2 Scope

This standard specifies the blockchain-based system architecture, interfaces, protocols, testing, and verification for the extraction and exchange of hepatobiliary disease data across multiple organizations and stakeholders.

1.3 Word usage

The word *shall* indicates mandatory requirements strictly to be followed in order to conform to the standard and from which no deviation is permitted (*shall* equals *is required to*).^{6,7}

The word *should* indicates that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required (*should* equals *is recommended that*).

The word *may* is used to indicate a course of action permissible within the limits of the standard (*may* equals *is permitted to*).

The word *can* is used for statements of possibility and capability, whether material, physical, or causal (*can* equals *is able to*).

2. Normative references

There are no normative references in this standard.

⁶The use of the word *must* is deprecated and cannot be used when stating mandatory requirements, *must* is used only to describe unavoidable situations.

⁷The use of *will* is deprecated and cannot be used when stating mandatory requirements, *will* is only used in statements of fact.

3. Definitions, acronyms, and abbreviations

3.1 Definitions

For the purposes of this document, the following terms and definitions apply. The *IEEE Standards Dictionary Online* should be consulted for terms not defined in this clause.⁸

blockchain: A chained data structure that combines data blocks in a sequential manner in chronological order, and a cryptographically guaranteed immutable and unforgeable distributed ledger.

data: A reinterpretable formalized representation of the information as applicable to communication, interpretation, or processing.

data acquisition: The data is generated by the generating device according to the data collection specification, stored in a digital format, and transmitted to the target system.

data set: The data form of the data record aggregation.

differential privacy: A data sharing method that shall only share some statistical characteristics that shall describe the database without disclosing specific information about individuals.

digital signature: Data appended to a data unit, or a cryptographic transformation made to a data unit, that allows the recipient of the data unit to confirm the origin and integrity of the data unit and protects data against falsification or repudiation by persons such as recipients.

distributed ledger: The extraction and exchange data is stored in the ledger on the blockchain. All the extraction and exchange data are digitally signed by the private key, and the data extraction and exchange records under this account are recorded in the ledger.

electronic medical record: In the process of medical activities, medical personnel use digital information such as text, symbols, charts, graphics, data, and images generated by the information system of medical institutions, and can realize storage, management, transmission, and reproduction of medical records, which is a record form of medical records.

encryption: The process of cryptographically transforming data to produce ciphertext. Generally contains a set of transformations that uses a set of algorithms and a set of input parameters. The input parameter is often referred to as the secret key.

features: The representation of the characteristics of objective things is an information unit with specific semantics. A good feature can be used as a manifestation of some outstanding properties and become the key to distinguish things.

federated learning: A distributed machine learning framework. Its core idea is that when multiple data sources participate in model training, the original data transfer is not required, and the model joint training is only performed through the intermediate parameters of the interactive model, and the original data shall not be exported locally.

hepatic and gall diseases: Common liver diseases include hepatic hemangioma, liver cyst, liver abscess, intrahepatic parasitic diseases, liver cancer, etc. Common biliary tract diseases include cholecystitis, gallbladder stones, common bile duct stones, acute suppurative obstructive cholangitis, etc.

⁸*IEEE Standards Dictionary Online* is available at: <http://dictionary.ieee.org>. An IEEE account is required for access to the dictionary, and one can be created at no charge on the dictionary sign-in page.

hidden query: Also known as private information retrieval, it means that the query party hides the keywords or customer ID information of the query object, and the data service provider provides matching query results but cannot know which query object corresponds to it. The data does not go out and can be calculated, eliminating the possibility of data caching.

homomorphic encryption: A form of encryption that allows one to perform certain forms of algebraic operations on ciphertext to obtain results that are still encrypted, and decrypt it to obtain the same result as performing the same operation on plaintext.

hospital information system: Using electronic computers and communication equipment, it provides various departments of the hospital with the ability to collect, store, process, extract, and data exchange patient diagnosis and treatment information and administrative management information, and to meet the functional requirements of authorized users.

laboratory information system: A type of software used to process laboratory process information, usually connected with other information systems; consists of a variety of laboratory process modules, which can be selected and configured according to the actual situation of the user.

machine learning: A method in which a computer simulates or implements human learning behaviors to acquire new knowledge or skills, reorganize existing knowledge structures, and continuously improve its own performance.

medical data: The data generated during the patient's medical treatment process that mainly includes basic patient information, disease complaints, test data, imaging data, diagnosis data, treatment data, etc.

oblivious transfer: A type of protocol in cryptography that enables the sender to transmit one of many possible pieces of information to the receiver, but keeps the information received by the receiver unknown, thereby protecting the privacy of the sender and receiver.

picture archiving and communication system: The main function of the system applied in the imaging department of the hospital is to digitally store various medical images generated daily through various interfaces, which shall be quickly recalled for use when needed. It also has some auxiliary diagnostic management functions.

private set intersection: A cryptographic technology that shall be used to help ensure that the two parties participating in the calculation shall obtain the intersection of the two parties' data without revealing their information except the intersection.

secret sharing: A security computing algorithm. By dividing the secret, each divided share is shared with different participants for management, so that only more than a certain number of participants can cooperate to reply to the secret message, so as to disperse the risk of intrusion.

smart contract: A computer protocol designed to communicate, verify, or enforce contracts in an informational manner. It allows trusted transactions without third parties that are traceable and irreversible.

software development kit: A collection of development tools for creating application software for a specific software package, software framework, hardware platform, operating system, which facilitates the creation of applications through compilers, debuggers, software frameworks, etc.

3.2 Acronyms and abbreviations

API	application programming interface
CA	certificate authority
HIS	hospital information system
LIS	laboratory information system
NFC	near field communication
PACS	picture archiving and communication system
SDK	software development kit

4. Application framework for data extraction and exchange of hepatobiliary diseases

4.1 Hepatobiliary disease data extraction and exchange of the data structure

Each medical institution forms a network for the sharing and use of specialized disease data by establishing a blockchain-based medical data private network. The definitions listed in [Clause 3](#) are applied to the platform and the alliance hospital units, scientific research cooperation units and construction units in the network, in the process of docking, extracting, and processing medical data from hospital information systems (HIS), laboratory information systems (LIS), picture archiving and communication systems (PACS) and other information systems in the hospital to form a standard data sub-database for liver and gallbladder diseases, to realize the transformation of medical sensitive data into de-private clinical scientific research data through measures such as standard grading and classification systems, security measures and technical requirements, de-identification schemes, grading application and effect evaluations, and to provide research applications in a safe and reliable environment.

This standard defines a scene as an application, for example, hepatobiliary CT/MRI image acquisition and processing scene, liver cancer CT/MRI image labeling and quality control scene, liver cancer scientific research medical record standard data set, etc. Each scene is defined as an application. Different applications have different scheduling processes. One application shall have multiple users; one user shall belong to multiple organizations; one organization shall have multiple patients or multiple users; one patient has multiple assets in one organization; and each asset is stored in the blockchain. Each asset forms a unique AssetID on the blockchain. The access right of AssetID is verified during circulation, and the specific attributes are described and explained in [Clause 6](#) and [Clause 7](#). The data structure is shown in [Figure 1](#).

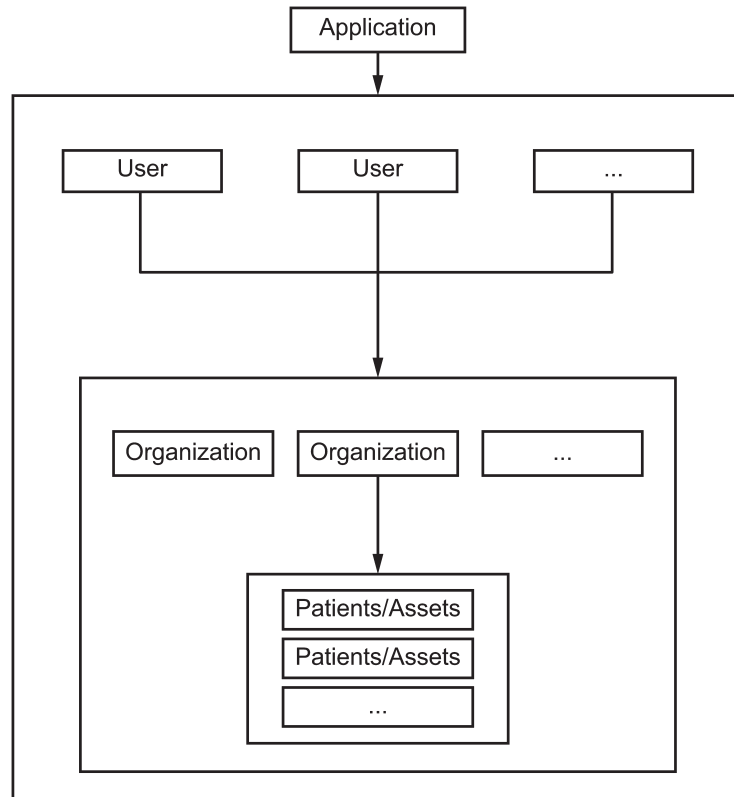


Figure 1—Data structure diagram

4.2 Data extraction and exchange process for hepatobiliary diseases

The process of data circulation digitally signs and encodes the data message. The specific circulation process of this document is as follows:

- According to the medical record data of liver and gallbladder patients, create a patient in the blockchain, create a patient asset under the patient's name, and store the patient's medical record data in the asset.
- Create an organization and the patient authorizes assets to the organization.
- Create a user, the user joins the organization, and the user has permission to access the assets authorized by the organization.
- Users access assets, through authentication, to determine whether they shall access.

5. Data extraction and exchange of hepatobiliary diseases

On the basis of trusted interconnection, the department where the data source is located, the data demand department (hospital), the regulatory department, and the medical data sharing platform are connected to complete the privacy and security circulation of medical data.

The process should adopt secure computing technology that are mainly homomorphic encryption algorithm, and blockchain technology, combined with algorithm frameworks such as federated learning, hidden query, and privacy set intersection.

Operation requests are first made by block chain approval, the data source is combined with hidden query, privacy collection exchange algorithm for federal learning after global machine learning model by homomorphic encryption, secret sharing, casual transfer security computing technology after processing form the ciphertext transmission to the data demander. The data demander collects all the ciphertext results of each data source for ciphertext calculation to form an aggregation of machine learning models, and transmits the ciphertext calculation results to the “medical data sharing platform.” The platform decrypts and returns the plaintext machine learning model to the data demander. The data demander updates the global results. All major links of data circulation are traced on the blockchain, which is convenient for auditing and tracking. In addition, third-party big data apps shall obtain data authorization based on software development kits (SDK)/application programming interfaces (API) and use data in compliance. The platform architecture is shown in Figure 2.

Based on blockchain technology and combined with trusted privacy protection computing technologies such as homomorphic encryption, federated learning, differential privacy, secret sharing, inadvertent transmission, hidden query, and privacy set intersection, data sources, data demanders and regulatory authorities are connected on the basis of trusted interconnection, and inter-agency hepatobiliary disease data extraction and exchange are completed to help ensure that the original data is not leaked in the process of analysis, calculation, circulation and integration. First, the data demander initiates a data extraction and exchange request to the blockchain platform. The request includes AssetID, key, (and/or query statement). Then, the corresponding fields in the assets maintained in the blockchain platform are authenticated, and after the rights are confirmed, the blockchain platform sends data extraction and exchange requests to the corresponding data sources. Finally, the data source forms ciphertext of the corresponding asset and transmits it to the data demander, completing a cross-institutional liver and gallbladder data extraction and exchange. All the main links of data extraction and exchange are traced on the blockchain, which is convenient for auditing and tracking.

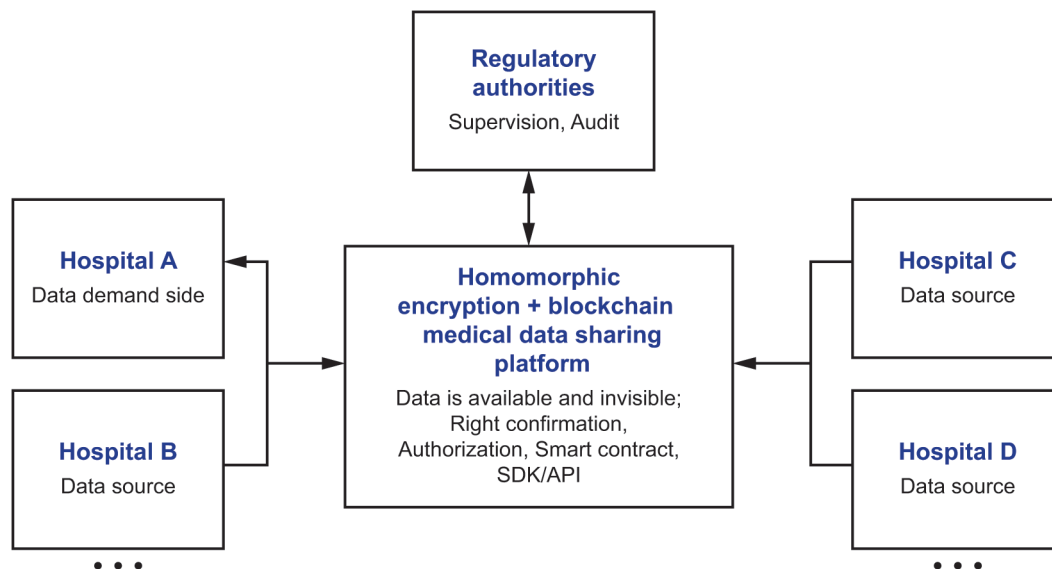


Figure 2—Data extraction and exchange diagram

6. Hepatobiliary disease data extraction and exchange attributes

6.1 Data definition

Each patient’s medical record data uniquely corresponds to the AssetID of one on the blockchain. See Table 1 for the format requirements.

The identification of data is realized based on the unique device identification (UDI) of medical data objects—“data fingerprint.” By formulating the data fingerprint of the medical data object and constructing a unique identifier, each stage of the data performs mathematical hash algorithm processing and is correlated. In this process, from the implementation of modal standardization, intelligent grading and classification, grading de-identification, and federated computing analysis, to the original medical data and the final realization of the result set exchange application, correspondingly generate the original hash value, standardized hash value, and hierarchical classification hash value, privacy comparison hash value, proof hash value, and exchange process hash value. This forms a “one number and multiple codes” identification structure, so that each link shall generate a unique fingerprint corresponding to the original data and process data, forming a medical data global unique certification mark. It involves data version history, data registration certification, data exchange and use records, data digital signature verification, data reference query, etc.

Table 1—Extract and exchange definitions

Attribute	Content
Data type	Type of data
Data ID	Data AssetID
Owner ID	Owner ID
Application number	The code of the application to which this data belongs, which is convenient for searching according to the application
Expiration time	Data expiration time
Private or not	Describes whether the data is privatized by an organization
Shared or not	Describe whether the data shall be shared
Shared content	The content that needs to be shared is protected by the user’s shared key
Sharing scope	The scope of data sharing, which shall be shared within a certain institution or within an organization
Encryption algorithm	Algorithm for data sharing encryption
Tracing history list	Describes the history of data tracing, and lists the address information of users who own data

6.2 Extract and exchange properties

Describe the attribute information that each data should have. Format requirements are provided in [Table 2](#).

Table 2—Extract and exchange properties

Attribute	Content
Data ID	Asset AssetID
Attribute name	A description of the attribute name
Attribute value	Specific attribute value

6.3 Organization definition

An organization shall include multiple assets and users, and the organization shall be understood as a collection with multiple assets, and each asset will correspond to an AssetID (data identification). The ontology structure diagram is shown in [Figure 3](#). See [Table 3](#) for format requirements.