CAAI Transactions on Intelligence Technology

WILEY

The Institution of Engineering and Technology

ORIGINAL RESEARCH OPEN ACCESS

Access and Privacy Control for Healthcare Decision Support System: A Smart Medical Data Exchange Engine (SMDEE)

Imran Khan[1,2] | Javed Rashid[3,4] | Anwar Ghani[5] | Muhammad Shoaib Saleem[6,7] | Muhammad Faheem[8,9] | Humera Khan[10]

[1]Department of Computer Science, International Islamic University, Islamabad, Pakistan | [2]Department of Computing, Khanpur Institute of Technology, Khanpur, Pakistan | [3]Department of IT Services, University of Okara, Okara, Punjab, Pakistan | [4]MLC Lab, Okara, Punjab, Pakistan | [5]Department of Computer Science, School of Engineering and Digital Sciences, Nazarbayev University, Astana, Kazakhstan | [6]Department of Mathematics, University of Okara, Okara, Punjab, Pakistan | [7]Center for Theoretical Physics, Khazar University, Baku, Azerbaijan | [8]VTT Technical Research Centre of Finland, Espoo, Finland | [9]School of Technology and Innovations, University of Vaasa, Vaasa, Finland | [10]Department of Information Systems, Faculty of Computing and Information Technology, Northern Border University, Rafha, Saudi Arabia

Correspondence: Muhammad Faheem (muhammad.faheem@uwasa.fi)

Received: 22 July 2024 | **Revised:** 6 May 2025 | **Accepted:** 17 July 2025

Handling Editor: Qing Liao

Keywords: data protection | decision making | information retrieval | intelligent information processing | medical applications | privacy issues | security | security of data

ABSTRACT

Secure and automated sharing of medical information among different medical entities/stakeholders like patients, hospitals, doctors, law enforcement agencies, health insurance companies etc., in a standard format has always been a challenging problem. Current methods for ensuring compliance with medical privacy laws require specialists who are deeply familiar with these laws' complex requirements to verify the lawful exchange of medical information. This article introduces a Smart Medical Data Exchange Engine (SDEE) designed to automate the extracting of logical rules from medical privacy legislation using advanced techniques. These rules facilitate the secure extraction of information, safeguarding patient privacy and confidentiality. In addition, SMDEE can generate standardised clinical documents according to Health Level 7 (HL7) standards and also standardise the nomenclature of requested medical data, enabling accurate decision-making when accessing patient data. All access requests to patient information are processed through SMDEE to ensure authorised access. The proposed system's efficacy is evaluated using the Health Insurance Portability and Accountability Act (HIPAA), a fundamental privacy law in the United States. However, SMDEE's flexibility allows its application worldwide, accommodating various medical privacy laws. Beyond facilitating global information exchange, SMDEE aims to enhance international patients' timely and appropriate treatment.

1 | Introduction

The exchange of healthcare information is critically sensitive, underscored by the risks of infringing on patient rights and privacy, as well as the substantial responsibility it entails. In many Western nations, healthcare frameworks are established to safeguard the privacy of health information. Ensuring the security of patient information is a top priority for healthcare entities in the United States. To avoid potential legal complications, the Health Insurance Portability and Accountability Act

(HIPAA) outlines thorough regulations to safeguard patient data. According to HIPAA regulations [1, 2], all stakeholders including medical professionals (doctors, nurses, laboratories, etc.), patients, other healthcare service providers (such as insurance and pharmaceutical companies) and law enforcement departments are required to follow these rules to facilitate a smooth flow of information that addresses everyone's needs. Noncompliance with HIPAA regulations can lead to penalties, including fines up to $25,000 per year and imprisonment for one to five years [3–5].

Research has highlighted the implications of using computerised clinical decision support systems in the medical field, particularly when medical regulations are violated. For example, patients can access their laboratory results as part of their protected health information (PHI). However, there are instances where hospitals are concerned about potentially violating HIPAA privacy rules and may withhold this information. Electronic medical records (EMR) have been a significant advancement in storing healthcare information and facilitating the development of comprehensive medical information systems within hospitals and clinics [6, 7]. However, more universal healthcare applications are urgently needed to close the knowledge gap between healthcare entities and laws, and to comply with HIPAA and other comparable requirements worldwide.

Health information technology (HIT) has demonstrated significant potential in improving the efficiency, quality and safety of medical care, reducing documentation errors and decreasing patient waiting times [8–11]. Software engineering has produced a substantial body of research over the years [12], focused on ensuring the secure exchange of healthcare information among medical entities [13–16]. Research and development of software engineering techniques that enhance privacy have received considerable attention [17], demonstrating the industry's dedication to protecting patients' privacy in the digital age.

1.1 | Motivation

In today's healthcare system, doctors need quick and accurate access to patient information to make the right decisions about treatment. However, this is often difficult because medical data are stored in different places, there are privacy concerns and there is a risk of unauthorised access. Another big challenge is that medical documents and the way data are shared are not always standardised.

The main goal of this research is to create a system where a healthcare provider can access a patient's medical data anywhere in the world through a simple request. No matter where a person travels, their health records should be easily available, just as in their hometown.

This research also focuses on building a strong and secure data exchange system that follows medical privacy laws. It should use the latest healthcare standards, like HL7, and proper medical terms (nomenclature) to share data safely and correctly.

This work is driven by the need to solve the current problems in medical data sharing. The aim is to create a system that not only protects privacy but also makes medical information sharing clear, secure and useful for both patients and doctors.

This research is dedicated to the privacy-preserved exchange of medical information internationally, strongly relying on the robust HL7 standards. These standards play a crucial role in ensuring the privacy and consistency of data exchange, which aligns with each country's medical privacy regulations. The overarching goal is to standardise medical data terminology globally. Before the exchange, the requested information is processed through the SMDEE to ensure compliance with regional rules. The data are then formatted into a standardised document based on HL7 protocols, a process that guarantees secure and consistent handling of medical data across borders.

1.2 | Research Contributions

The general contributions of the research are listed as follows:

- Formalisation of Privacy Laws into logical rules for clear decision making guidelines to help decide when medical data can or cannot be shared.
- To generate a standard medical document with standardised medical terms and names using updated HL7 formats by converting older HL7 CCR and CCD versions for global adoption.
- To allow safe sharing of medical information according to Privacy Laws, to allow for smooth medical data and patient medical history exchange, improving the quality of treatment and care.
- A prototype system (MDB with SMDEE) was built and tested at the International Islamic University Medical Centre and PIMS Hospital to check its feasibility and performance.

1.3 | Article Layout

The enforcement and interpretation of HIPAA privacy rules serve as a primary test case to substantiate this research. The remainder of this article is organised as follows: Section 2 discusses a critical literature review of state-of-the-art paradigms. Section 3 elucidates our System Methodology, Mathematical Model and Request Processing with illustrative examples. Section 3.12 focuses on the Algorithm's Results and Discussion. Section 4 covers the deployment of SMDEE with Medical Applications. Section 5 discusses our framework for converting patient information from CDA to FHIR formats, and Section 6 concludes the research findings.

2 | Related Work

Several studies have explored various approaches for translating legal texts into logical rule sets. The work by the authors in ref.

[18] leverages ChatGPT as a tool for reading and interpreting NLP-based texts. The authors in ref. [19] delve into the legal, ethical and social dimensions relevant to healthcare. Maxwell and Anton [3] transformed HIPAA legal text into Prolog statements, employing Hohfeldian concepts [20] and classifying legal rights [21] through a process akin to software engineering to create production rules. This transformation, however, often resulted in the generation of logically redundant rules. Lam, Mitchell and Sundaram [4] proposed a method for compliance verification using extracted logical rules, identifying significant conflicts and anomalies within the rule set. The rules were classified as either 'permitted by' or 'forbidden by,' with the latter typically used in decision-making situations to emphasise that prohibitions take precedence over permissions when problems arise.

DeYoung et al. [5] suggested representing legal constraints through 'positive and negative norms,' where the negative norms (prohibitions) outweigh positive norms (permissions) in the event of a conflict. To extract needs and norms from legal documents, Hashmi [22] proposed an approach. To check compliance, it uses a natural 'IF...THEN' structure to analyse legal texts and extract activities, categories of duties and the relationships between them.

O'Neill [23] proposed the Governance, Risk and Compliance (GRC) paradigm to improve businesses' compliance outcomes and governance capacities regarding data privacy threats. To derive privacy requirements from HIPAA for use in medical software, Alshugran and Dichter [24, 25] developed access modeling methods. However, they encountered limitations with these modeling techniques, leading to a revised rule extraction model [26] that expresses HIPAA rules within a service-oriented architecture, enabling its deployment as a web service.

The field of health informatics has been persistently focused on data standardisation and establishing universal communication protocols [27]. Researchers [28] have identified knowledge gaps and the burden of documentation among physicians and nurses using electronic health records (EHRs), who reportedly spend more time on electronic documentation and clerical tasks than on direct patient care [29–32]. The absence of standardisation exacerbates this situation. HL7 has introduced various models for standardising healthcare data [33–35] and exchanging clinical documents. The use of Health Information Exchange (HIE) in European hospitals was explored in ref. [36], while the authors in ref. [37] reviewed the design and implementation of clinical decision support (CDS) systems with a focus on interoperability standards like Fast Healthcare Interoperability Resources (FHIR), Substitutable Medical Applications and Reusable Technologies (SMART), Clinical Quality Language (CQL) and CDS Hooks.

The necessity for AI-based, data-driven medical diagnosis that processes vast quantities of medical data from diverse sources through a blockchain-based architecture has been underscored [38]. A blockchain-based medical data-sharing framework was proposed [39] to address technical challenges and efficiently manage outbreak records. Moreover, a holistic framework that leverages edge computing and blockchain technologies for processing large volumes of medical data was introduced [40]. Another blockchain-based data privacy framework introduced using Federated Learning for IoMT applications [41]. After closely studying research on medical data privacy and security, we found that most studies focus on using blockchain technology to protect different types of medical data. A blockchain-based system introduced to enhance the patient medical data privacy and security [42, 43] Various healthcare departments globally utilise standardised documents such as CDA and FHIR for storing and exchanging healthcare data [44–46]. Authors propose a novel Lionised remora optimisation-based serpent (LRO-S) encryption method to encrypt sensitive data and reduce privacy breaches and cyber-attacks from unauthorised users and hackers to access medical data on the cloud [47].

Authors suggest the method that uses blockchain and attribute-based search to protect medical data. The system allows data owners to set detailed access rules using special symbols (wildcards), giving them better control over who can see their data. It also uses a technique called inner product predicate to hide the access rules completely, which helps prevent any private medical information from being exposed [48].

An approach that integrates various technologies intending to fully decentralise the sharing of medical data with minimum privacy risks while maintaining high-performance medical services [49]. Authors introduce a blockchain-based system for sharing medical data. It keeps track of how the data are used and includes an automatic system to check and audit everything. The system uses smart contracts to verify search results and make sure the data stored in the cloud have not been changed. This helps ensure that the medical data stay safe and trustworthy during both sharing and storage [50].

The authors look at how AI-based security systems can help safely and ethically share medical data around the world. Their goal is to protect data accuracy, keep patient information private and make sure everyone has fair access to healthcare improvements. They suggest a security model that combines federated learning, blockchain and AI-powered threat detection to reduce the risks of sharing health data across different countries [51].

The study says that some important changes are needed to make data sharing safe, fair and useful. These include getting clear permission from patients, having clear rules about who is responsible if something goes wrong and better ways to manage data. These changes will help build patient trust, improve healthcare and support global health goals [52].

3 | Materials and Methods

Currently, different healthcare standards are used in different parts of the world; so when the record of a patient needs to be exchanged from one healthcare setting using CDA (HL7 V3) to another healthcare setting that uses FHIR as a standard, the result is a loss of information or a slight change in the meaning

due to inter-convertibility issues. This change of meaning is unacceptable in healthcare, as most information is highly sensitive. This article addresses the interconvertibility issues. SMDEE generates standardised clinical documents for information exchange according to HL7 standards.

Doctors, nurses, hospitals, laboratories, insurance firms and the like are virtually universal in the medical industry. Each participant or organisation is required to fulfil a certain function by the rules. Medical Law (HIPAA) logical rules are formalised using the World Rule Model (WRM) [53]. As a first step, it uses HIPAA to create several concept classes and then uses those classes to extract data and distribute it. The official language of the HIPAA privacy regulations is divided into eight distinct classes to facilitate compliance testing [54]. To manage electronic health records, this study used a modest experimental programme called the 'medical drop box' (MDB) [55]. Assumptions for exchanging medical data throughout the healthcare industry in compliance with privacy regulations and medical laws form the basis of the Smart Medical Data Exchange Engine Concept.

3.1 | Assumption

It is assumed that each country has medical laws in English. Requests for information exchange are always processed through the SMDEE. Each country's health department is responsible for managing patients' data with MDB and updating medical laws for formalisation and verification.

3.2 | Practical Implementation and Testing

We used the HIPAA law because it is very detailed and widely accepted as a standard in medical research. In our study, we focused only on the Privacy Rule in HIPAA, which controls how medical information is shared between different healthcare organisations.

To test how these privacy rules work, we used a small dataset of 1000 student medical records from the International Islamic University Medical Centre and Pakistan Institute of Medical Sciences (PIMS) with dummy identities. We checked how the data could be accessed by different types of medical entities, such as doctors, patients, labs, researchers, law enforcement agencies and pharmacies. Each one had different levels of access, based on the HIPAA privacy rules.

3.3 | Key Functionality of (SMDEE)

Some key features are explained about SMDEE functionality:

- SMDEE sets up the privacy rules of each country's medical law. These rules are added to the system by that country's healthcare department when the MDB system is first set up.
- We used natural language processing (NLP) techniques to read and understand the medical laws. Then, we turned them into clear rules that SMDEE can follow when deciding whether to release data.
- For our research, we used the HIPAA law (from the USA) because it is very detailed and commonly used. We only focused on the part of HIPAA that deals with sharing private medical data.
- We did not use machine learning (ML) because every country has its laws. So, we needed to manually turn those laws into fixed rules that SMDEE can follow.
- Whenever someone (like a doctor or lab) asks for medical data through MDB, SMDEE checks and handles that request.
- When a request comes in, SMDEE first checks if the requester (like a doctor or pharmacy) is allowed to ask for that data, based on the privacy rules.
- It also checks the patient's personal privacy settings to see what they agreed to share.
- SMDEE decides whether to allow or block the sharing of medical information, based on the country's privacy rules.
- If the request is approved, SMDEE creates a medical document using standard formats like HL7 FHIR (used worldwide in healthcare).
- SMDEE can also work with other global medical formats like CDA, CCR, CCD and FHIR because different places use different formats.
- It also fixes the problem of different medical terms (nomenclature) used in different countries by converting them into a standard format, so everyone understands the same thing.

3.4 | Smart Medical Data Exchange Engine (SMDEE) With MDB

Every country has its medical laws, and SMDEE is used to make sure these laws are followed. Each person has a personal medical drop box (MDB), which stores their health records. People can use their MDB to see their medical information, share it with doctors and set their privacy preferences. All healthcare providers (like doctors, labs and pharmacies) must use the MDB system. They can only access a person's medical data if they follow that country's medical laws, which SMDEE checks. SMDEE controls who can see what information, based on privacy rules. An overview model of SMDEE is shown in Figure 1 with MDB.

When a healthcare provider wants to access or update someone's data, they use a simple drag-and-drop action in the MDB. SMDEE then checks if the request follows the patient's local medical privacy laws. It looks at things like who is asking, why they want the data, what type of data they need and whether they are allowed to have it.

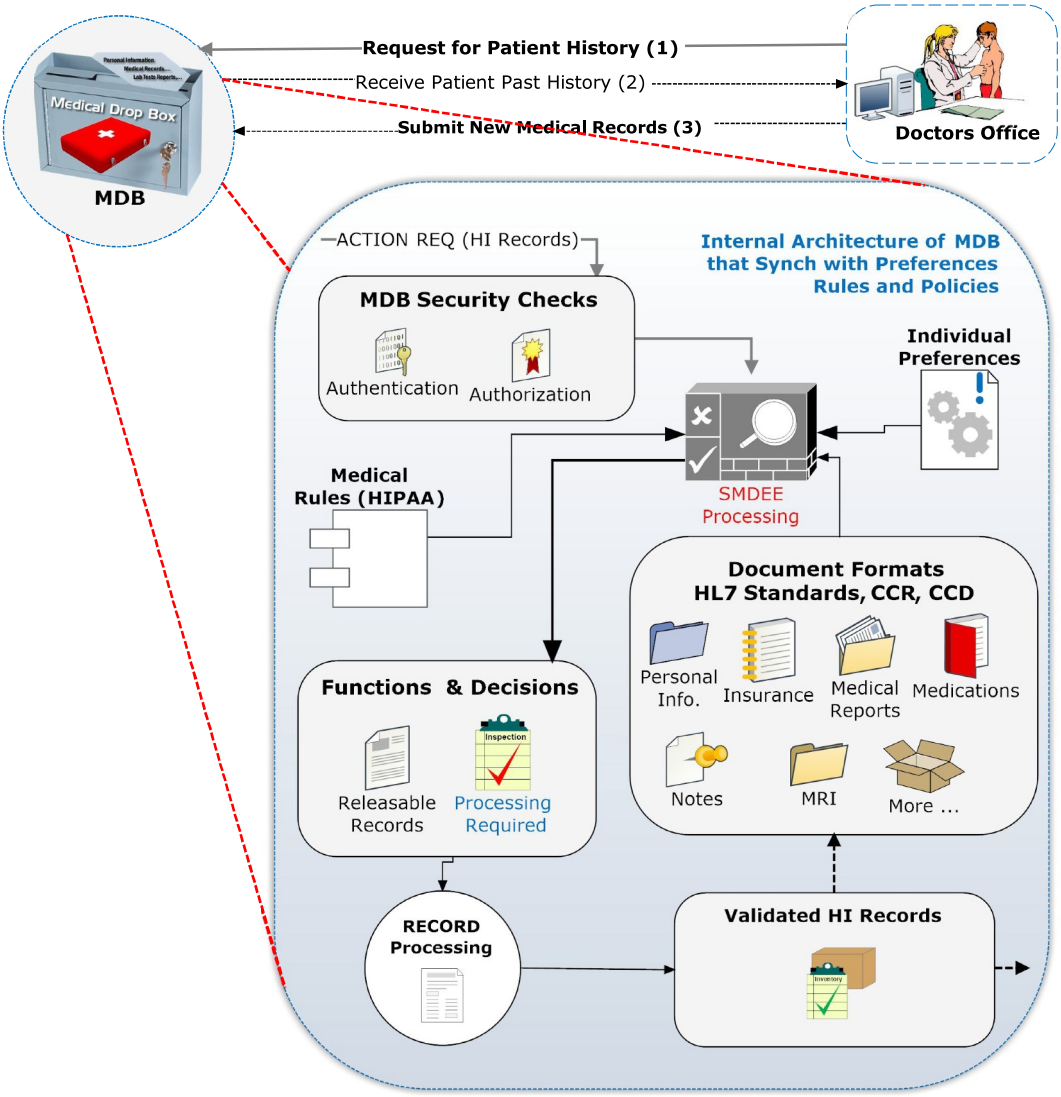

FIGURE 1 | An internal working model of SMDEE with MDB.

SMDEE then makes a decision. It decides if the request should be allowed or not, and what specific information can be shared. For example, when a patient visits a doctor, the doctor gives a small password for their MDB. The doctor can then view only the allowed medical information. After the visit, any new medical records are added to the MDB.

This process repeats every time the patient visits a new healthcare provider, so their MDB keeps growing with updated and accurate medical information.

Every person's information is saved in a clinical document file formatted as XML by the MDB [56]. The data from XML files can be accessed through any web-based or desktop medical applications so that it can be easily exchangeable among different networks. Similarly, role-based logical rules are generated in XML for each medical entity [57].

3.5 | Mathematical Model for Privacy Rules Extraction

Assume that D_i is a legally binding document. To begin, sentence tokens S_T are taken from D_i in the following way: $S_T = \{S_{T_1}, S_{T_2}, ..., S_{T_n}\}$, where n is the phrase token count. The term '.' is a stop word for sentence tokens. Creating a word token W_T requires every sentence token S_T. To compute word tokens, the following relation in Equation (1) is used.

$$W_T = \bigcup_{j=1}^{n} \left\{ \bigcup_{k=1}^{s} \text{The token for each phrase is} \left(S_{T_j}\right) \right\} \quad (1)$$

where s is the word count.

For rule generation, the POS tagging method (Algorithm 1) and the Access Level dictionary AL_D to produce a set of part-of-

speech (POS) tags are employed. Table 1 presents an example of data from the Access Level dictionary.

Here, $l = 8$, we must build rules for a set of classes $C = \{C_1, C_2, ..., C_l\}$. The rules are categorised into eight groups, denoted as

$$C = \{\{C_{1_{ReqT}}\}, \{C_{2_{PPT}}\}, \{C_{3_{PRI}}\}, \{C_{4_{CT}}\}, \{C_{5_{AT}}\}, \{C_{6_{TFT}}\}, \{C_{7_{IPT}}\}, \{C_{8_{RRT}}\}\} \tag{2}$$

Section 3 explains the specifics of these classes.

For every class $\forall C \in D_i$ accessible in D_i, we create R_{pq} rules using the POS-Tags. In R_{pq}, the value of p is $1 \le p \le 8$ for many classes, and the value of q is $1 \le q \le t$, where t is the number of rules generated for each class. This means that

$$R_{pq} = \mathbf{T}^f(CT(POS - Tag)) \tag{3}$$

when b is the occurrence of Rule-Id and a is the occurrence of the next Rule-Id, and CT is in the set of all possible values for b. Currently, the rule is Rule-Id. The function $\mathbf{T}^f$ transforms XML's specified rules, pattern or template. The transformation function in XML tags produces rules like

$$T(x) = \bigcup_{o=1}^{6} (< tag_o > CT_o < /tag_o >) \cup \left(\bigcup_{o=7} \left(\bigcup_{u=1}^{r} (< tag_o > CT_o < /tag_o >) \right) \right) \tag{4}$$

$$tag_8 \iff \exists CT_8 \in tag_1 \cup \left(\bigcup_{o=8} \left(\bigcup_{u=1}^{s} (< tag_o > CT_o < /tag_o >) \right) \right) \tag{5}$$

In cases where $tag_8 \Leftrightarrow \exists CT_8 \in tag_1$, the existence of rule Id in tag_1 is necessary for tag_8 to generate CT_8 'CrossReference,' as stated in $CT_8 \in tag_1$. In Table 2, you may find the definitions, descriptions and examples of the XML tags.

The incoming request should be processed by the query Q_i using the algorithm shown in Figure 2. The equation $Q_i = \{Q_{C/E} \cup Q_A\}$ where $Q_{C/E} \cap Q_A = \varphi$ is based on whether the query should be processed or not. This is represented by the following Equations (6) and (7).

$$P_c(Q_{C/E}) = \{\text{Requester Pre-Conditions, Purpose Pre-Conditions, Record Items, Request Pre-Conditions}\} \tag{6}$$

$$P_c(Q_A) = \{\text{Requester Authentication}\} \tag{7}$$

$R = \{R_1, R_2, ..., R_k\}$ represents the collection of rules R_k for each entity E_x, where R_x is defined as $1 \le x \le k$. Whenever an entity E_x is queried using query Q_i, the rules for that entity are extracted by the request processing function. Considering all R_x being in E_x, if $(Purpose\ (R_x) \wedge Condition(R_x) \approx (Purpose(Q_i) \wedge Condition(R_i)$.

Two files can be input into the POS tagging algorithm: 2) The word dictionary W_{td}, which includes the Access Level dictionary AL_D and 1) the file to be tagged D_i.

TABLE 1 | A dietary sample for Access Level (AL).

AL-types	AL-value	Examples of matching words
Rule ID	Rl	Rule No.: e.g., 164.128.2, 164.126.1 etc.
Permission	Pm	Might, may, could, would, can etc.
Obligation	Ob	Must, shell, should etc.
Action	Ac	Not allow, release, deny, allow etc.
Record items	RI	Infection, heart, HIV etc.
Negation	Ne	Shall not, would not, should not etc.
Condition	Co	Permission, authorisation etc.
Cross reference	Cr	This regulation currently references other rules (164.128.1.a, etc.).
Purposes	Pr	Treatment, access, amendment etc.

TABLE 2 | Information on tags and their illustration with an example.

Tags	Tag-description	Example description
tag_1	Ruleid	For example, 164.1 is the document's rule number.
tag_2	Request	Request objectives, such as treatment, access etc.
tag_3	Requester	Individuals making the request, such as doctor, researcher etc.
tag_4	Entity	Data providing entity, like hospital etc.
tag_5	Record items	Type of data required, such as heart patients, HIV etc.
tag_6	Access level	Required actions, such as denial, release etc.
tag_7	Condition	Conditions for request, record, requester
tag_8	CrossReference	Refer to other rules in the current rule.

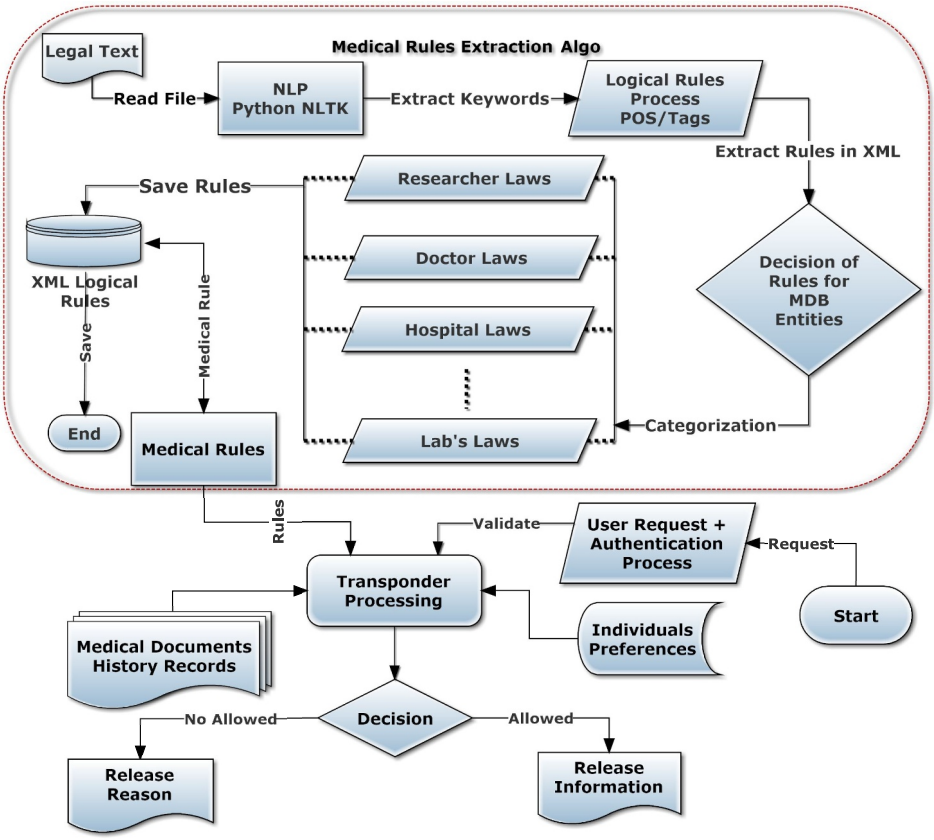

FIGURE 2 | Model for the extraction of medical rules and the processing of requests.

Python is used to implement the method in Figure 2, and the BaseX database is utilised to store rules derived from XML. XML 'rule' tags separate each clause in the HIPAA. The logical rules provided within each clause contain all information regarding the requester, the reason for accessing the information and any conditions, actions or rules that are cross-referenced. Each 'rule' tag might have a unique set of keywords utilised in the XML tags. We organise these rules into several medical entities and store the XML logical rules independently for each entity, making it easier to retrieve this information. Marks indicate the conditions of the various actors.

```
<rules>
  <rule ruleid = '164.1'>
    <Request>access</Request>
    <Requester>patient</Requester>
    <Entity>hospital</Entity>
    <AccessLevel>permission</AccessLevel>
    <Condition>hospital_Law_2</Condition>
    <CrossReference>164.5</CrossReference>
    <CrossReference>164.8</CrossReference>
  </rule>
</rules>
```

The algorithm is programmed to release or refuse information based on predefined 'Access Level' keywords. These levels are part of the action class when responding to a request. An example of the different 'Access Levels' is shown in Figure 3.

3.6 | Request Processing Through SMDEE for Privacy Rules

The input data from a request is pre-processed by applying the parsing algorithm. Alternative scenarios are evaluated, and these inputs render judgements.

Example: A requester who is a researcher is illustrated in Figure 4 as a result of the HIPAA. The example provides a detailed explanation of the rules' flow in a modal format. When any researcher requests it for research purposes, HIPAA provides full advice.

Researchers are expected to outline the intended data usage, provide a brief description of the patient data required and specify whether the data should be in electronic or paper format when submitting a request. Entities are required to make medical records available for research under HIPAA regulations. HIPAA needs authorisation before sharing any individual's health information for research purposes. The record-releasing entity or covered entity (hospital) must enquire about the researcher's authorisation before using the information for research purposes. Once the patient gives consent, the researcher obtains approval from the institute. If the researcher

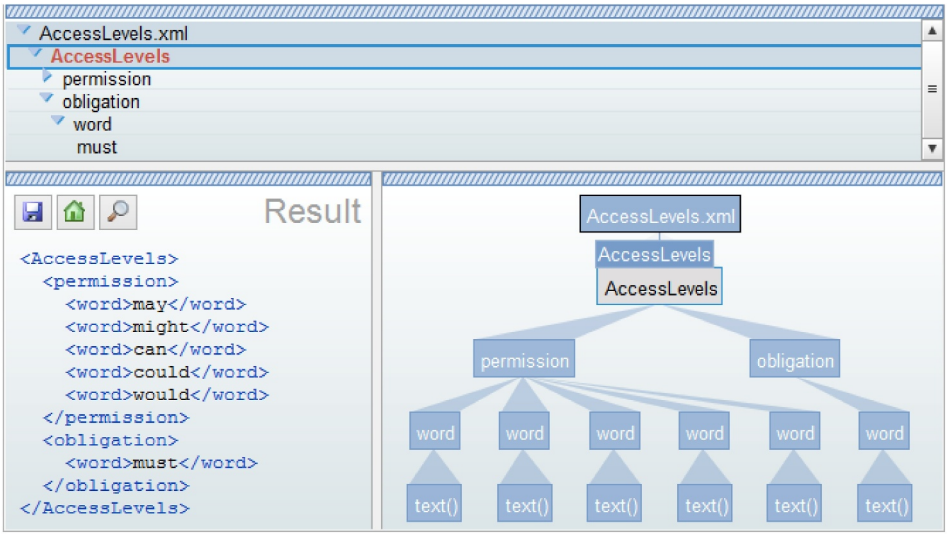

FIGURE 3 | Access levels from action class in XML logical rules.

does not give authorisation, there are rules to ensure the request is legitimate. For research purposes, the releasing entity must make de-identified or restricted data available. For de-identifiable and limited data, Table 3 contrasts data pieces that should be kept or excluded.

ALGORITHM 1 | The POS tagging algorithm.

Input: Legal Text File D_i, Tag Dictionary File $W_d + A_L$
Output: Generate Tagged Data

Convert the sentence into a list of characters: `str`
Prepare a list to store candidate sentences citem as (word, tag) pairs
Determine the maximum length for each tag `max_len`
Initialise a list `rulesTemp` for tagging rules
Load the tag dictionary `tagdict`
Set `start_index` for the current word to 0
Set `end_index` for the current word to 0
Initialise `rulesTemp[0]` = [] for $p \neq 0$
Tokenise the text `str` ← `String_Tokenised` (D[i])
Processing:
`end_index` = 1
while `end_index` < `str.length` **do**
    for all `tag` **do**
        for `start_index` = `max(1, end_index − max_len[tag] + 1)` **to** `end_index` **do**
            Extract word `w = str[start_index ... end_index`
            if `(word, tag) exists in tagdict` **then**
                Create a copy `item` ← `citem`
                Append `(word, tag)` to `item`
                Insert `item` into `rulesTemp [end_index]`
            end if
        end for
    end for
    Increment `end_index` by 1
end while
Output:
`return` the best tags from `rulesTemp [str.length]`

The request processing algorithm handles the request in the example shown in Figure 4. Data formats for releasing records, purpose lists, patient record components and the identity of the requester are all part of the parsing process that should be executed upon request. Following request parsing, the Medical Law Engine tests rules under various scenarios about the requester's authorisation and authentication, the purpose, and the record items. We will release the requested data in the appropriate format if the researcher meets all the prerequisites. If a waiver is not attached to the request, the SMDEE will proceed. The request will only be rejected if none are found.

The SMDEE will decide to implement a procedure for preparing a response. This method specifies the data that will be released and how it will be released if the request is authorised. The response will also provide the reason for denial, if applicable.

3.7 | Results and Discussion for Privacy Rules Extraction

Three algorithms were implemented to create SMDEE. The POS tagging process is handled by Algorithm 1, the XML logical rules are generated by Algorithm 2 and the outcome is produced by Algorithm 3, which explains the processing of a request.

3.8 | Decoding Algorithm

One of the primary obstacles in creating the SMDEE is the decoding algorithm for the segmentation and POS tagging system, as the speed and accuracy of the decoder are of utmost importance. With its many combinations of candidates, the algorithm searches a vast area for point-of-speech tagging. Obtaining precise recommendations for the POS tags is not straightforward, and our system operates linearly, utilising rule templates. With the help of learning algorithms and additional feature selections, this can be accomplished in the future.

3.9 | Optimisation

Coding approaches optimise the programme's performance, even when handling massive amounts of data. Strings represent POS tags, and algorithms are required to compare multiple tags. To make this work faster, we gave each tag an integer or index number. Similarly, rule templates were used for the evaluation. Regarding POS tagging, the built-in NLTK packages in Python are also really useful.

ALGORITHM 2 | XML logical rule generation algorithm.

Input: Rule Pattern File $R_{P,f}$, POST Data File $POS_{tag,f}$
Output: Generated XML Logical Rules
1: **Step 1:**
2: Read $R_{P,f}$ to extract R_P (Rule Pattern)
3: Read R_P and place it in a list R_c
4: **Step 2:**
5: Create lists L_m where $2 \leq m \leq n$ is the number of

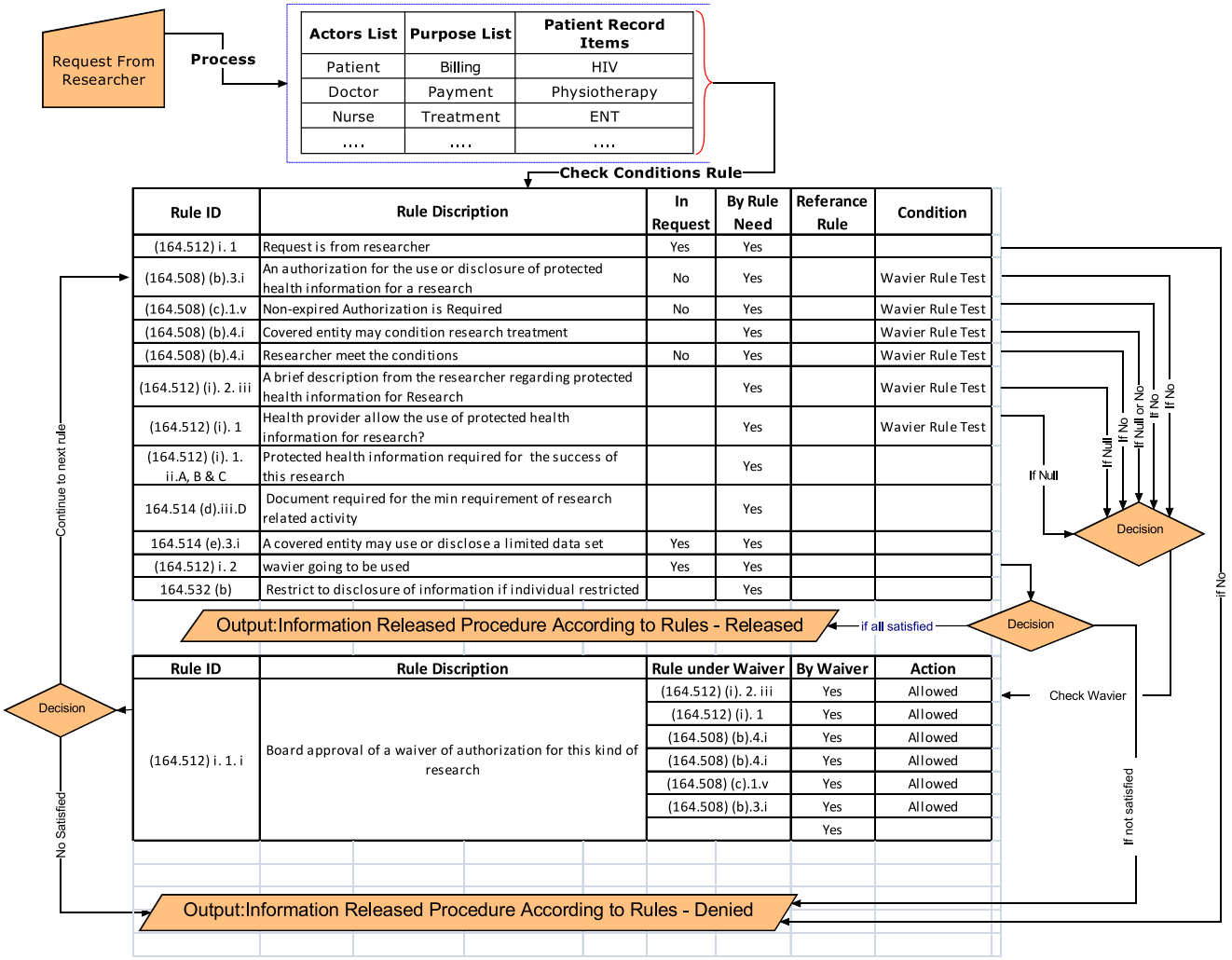

FIGURE 4 | Request processing for researcher with the SMDEE model.

TABLE 3 | A contrast between limited data and de-identifiable data.

S.No	Data attributes	De-identified data	Limited data
1.	Name, all types of addresses, cities and zip codes	Remove	Remove home,street No.
2.	Except for years, all data pertaining to dates	Remove	May included if needed
3.	Various means of communication, including cell phone, email and fax.	Remove	Remove
4.	Identification card, bank account number, medical record number etc.	Remove	Remove
5.	Particulars such as licence, health insurance, vehicle identification numbers etc.	Remove	Remove
6.	Identification via biometrics, photographs etc.	Remove	Remove
7.	Any identifying feature or numerical value	Remove	May include

components in the Rule Pattern
for all rules from $POS_{tag,f}$ **do**
  Read Rule Identifier
  Read words W_i corresponding to $R_c[i]$ for $1 \le p \le n$
  Add W_i into its relevant list L_p
  Set rule $\leftarrow R_c[rule]$
  if the length of each list L_i is 1 **then**
    Use each list L_i
    rule $\leftarrow rule + R_c[i+1]; L_i \leftarrow L_c[i+1]$
    if the length of L_2 is greater than 1 **then**
      len $\leftarrow$ length(L_2)
      Generate len copies of the rule
      Set $RuleLen = rule$
      $RuleLen = rule$
    end if
    while $1 = 1 \rightarrow len$ **do**
    rule $\leftarrow Rule + L_c[i+1]; rule \leftarrow rule + R_c[i+1]$
  end if
  while for all rules where $L_1 < L_2 > L_2[i] < R_c[2]$ **do**
    while $1 = 1 \rightarrow len$ **do**
    $Rule = Rule + L_c[i+1]; L_c[i] < R_c[1]$
    while while $1 = 1 \rightarrow len$ **do do**
      rule $\leftarrow Rule + R_c[i]; L_i < R_c[i+1] +$ `newline`
    end while
  end while
end for
end for
end while

ALGORITHM 3 | Request processing algorithm.

Input: User Request with Request Info *URI*, Medical Rules *MR*
Output: Release or Denial of Requested Medical Data
Step 1: Initialise Medical Data $MD \leftarrow$ Null
Step 2:
Parse *URI* to extract required information:
Parsed Data To Obtain $\leftarrow$ {Requesting Entity *REI*, Requesting From Entity *RFI*, Purposes *Purpose*, Record Items *RItems*, Record Format *RFormat*}
Step 3:
Divide Parsed Data *PData* into two function groups:
  i Check_Authorisation(*REI*, *MR*) $\rightarrow$ returns 1
  ii Check_Eligibility(*RFI*, *Purpose*, *RItems*, *MR*) $\rightarrow$ returns 1
if Check_Authorisation(*REI*, *MR*) $= 0$ **then**
  Deny Request and return *MD*
end if
if Check_Eligibility(*RFI*, *Purpose*, *RItems*, *MR*) $= 0$ **then**
  Not Eligible for this request and return *MD*
end if
 if both Check_Authorisation(*REI*, *MR*) $= 1$ and Check_Eligibility(*RFI*, *Purpose*, *RItems*, *MR*) $= 1$ **then**
  Check User's Preferences from Records
  Set Preferences *PREData* $\leftarrow$ Check_Preferences (*RItems*)
  Prepare Medical Data in the required format
  Format Data *Data_Fmt*(*RFormat, PREData*) $\leftarrow MD_{ata}$
  Set $MD \leftarrow MD_{ata}$
  Return *MD*
end if

3.10 | Part-of-Speech Tagging

The first step to run SMDEE (Smart Medical Data Exchange Engine), explained in Algorithm 1, is to create a list of words using part-of-speech (POS) tagging. POS tagging means identifying whether a word is a noun, verb etc. This helps understand the meaning of each word correctly. Some words can have more than one meaning or use. For example, the word 'note' can be used as a verb (e.g., 'Please note this') or as a noun (e.g., 'He wrote a note'). So, POS tagging helps figure out the correct use of each word by looking at how it is used in a sentence. There are two ways to do POS tagging:

- Rule-based method (uses grammar rules)
- Stochastic method (uses probabilities and data)

In this paper, we used the rule-based method. We made rules to decide what tag (noun, verb, etc.) to give each word, depending on how it is used. These rules help us better understand and process medical laws according to the medical entities.

3.11 | Tagging of Unknown Words

In order to handle unfamiliar terms in medical laws, we have built our Access Level lexicon to comprehend each word's context through conversations with professionals. We put our trust in the rules to fix mistakes after assigning certain terms to the most popular POS. We use our Access Level dictionary for POS tagging to construct Algorithm 1 with NLTK.

3.12 | Results and Discussion

Various parts of the HIPAA were used to test the POS tagging technique. Sections 164.502–164.534 include 683 clauses, according to our research. We extract over 112,000 words for POS labeling. To ensure accuracy, the technology was initially tested on all HIPAA sections. After reviewing the mistakes, it was discovered that 26% of them were caused by unfamiliar terminology. To accurately understand medical law terminology, which is considered unfamiliar or ambiguous in the NLTK, a distinct Access Level dictionary is compiled. In an effort to lower the error rate, new, unfamiliar words were introduced to the Access Level vocabulary for every part. The original file and an expanded word dictionary using the Access Level Dictionary are the files the POS tagging algorithm takes as inputs. In contrast, the Tagged Data File that includes the details of every word is what is called the Output. General tagging errors achieved a best result of 2.3% and particular tagging errors of 3.6% for each section.

The XML logical rule generator (Algorithm 2) takes the Tagged Data File and Rule Template File as inputs after the POS tagging algorithm and produces the logical rules. The algorithm's output is the XML logical rules for every medical entity.

Finally, the requests are processed by the request processing algorithm. This algorithm is activated when any entity requests data from the system. Because it generates outcomes based on legislation, this algorithm is a crucial part of the SMDEE.

3.12.1 | Open Vocabulary Test

The efficacy of the tagging algorithm is evaluated with Open Vocabulary. About 26% of the words were unknown when the Access Level dictionary was not created.

Accuracy without Access Level dictionary.

Known words: 78%

Unknown words: 53%

All words: 81%

3.12.2 | Closed Vocabulary Test

The part-of-speech tagging method undergoes this test to ensure that the text to be tagged does not contain any remaining unknown terms. The tagging accuracy, expressed as a percentage, measures how well the tagging algorithm performs. When the rules template is applied to the tagged data, the resulting XML logical rules are evaluated for accuracy.

Accuracy with Access Level dictionary.

Tagging Accuracy: 88%

XML Rules Accuracy: 91%

The accuracy percentages obtained using the Open (i.e., without the Access Level dictionary) and Closed (i.e., with the Access Level dictionary) vocabulary tests are displayed in Figure 5. Figures show that it is more difficult to attain greater accuracy for data tagging and XML logical rule generation in the Open Vocabulary test, which does not employ the Access Level dictionary. However, with the Access Level dictionary, tagging performance on the closed vocabulary test improved significantly. In the first test shown in the picture, the number of terms known (the dictionary size) is smaller than in the Open Vocabulary exam. From Test 2 to Test 5, the number of words known increased, and the results improved, with Test 5 being the best.

4 | SMDEE Deployment With MDB for Standardised Clinical Document

The exchange of medical data in accordance with the country's privacy regulations is the responsibility of SMDEE. It helps create and execute documents that abide by medical legislation by formalising the legal text into an automated set of rules for compliance verification. Healthcare providers, hospitals, clinics, labs, researchers, government organisations and other related entities will be able to share patient records more easily. The deployment of SMDEE with MDB for any country has two levels, that is, Regional Health Information Exchange (RHIX) and National Health Information Exchange (NHIX). In the RHIX deployment architecture, SMDEE processes requests to exchange information locally between different cities in the country. For example, an individual is not a resident of the same city where they visited a doctor, and their information is available at the hospital in their city. In NHIX, SMDEE processes requests from outside the country for individuals who have visited a hospital in another country, and the hospital needs the individual's medical history for proper medication. Figure 6 shows the deployment architecture in RHIX and NHIX.

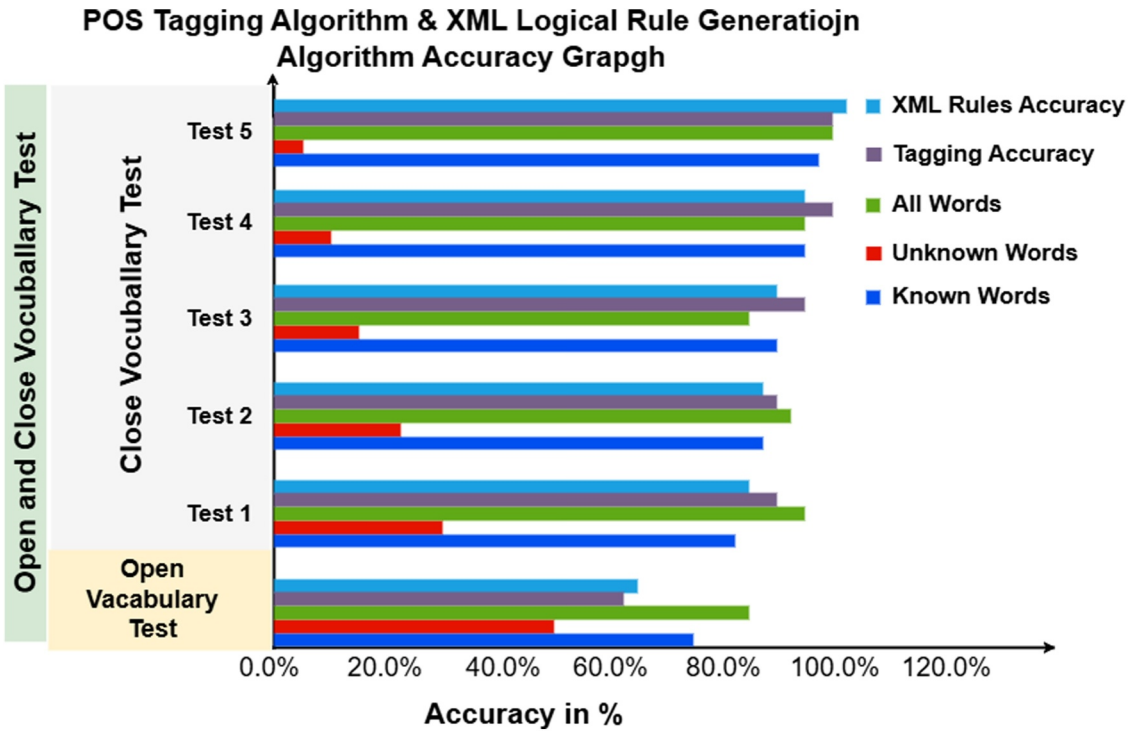

FIGURE 5 | Open and close vocabulary test for Algorithms 1 and 2.

4.1 | SMDEE Patients Information Extraction From MDB

In this research, we have proposed the FHIR standard for medical data exchange. After processing the privacy rules for releasing information, SMDEE processes patient data, extracts useful information and then shares it with other medical entities. In Algorithm 4, take the patient information in the standard HL7 (FHIR) format, and then SMDEE reads and processes data for further operations. Algorithm 5 extracts the information from the MDB and then feeds it to SMDEE to exchange information related to patient insurance. The output of the algorithms is shown in Figure 7.

ALGORITHM 4 | Algorithm for patient information.

Input: Patient complete information
Output: Patient record
1: Upload CSV file
2: **if** File name ends with 'CSV' **then**

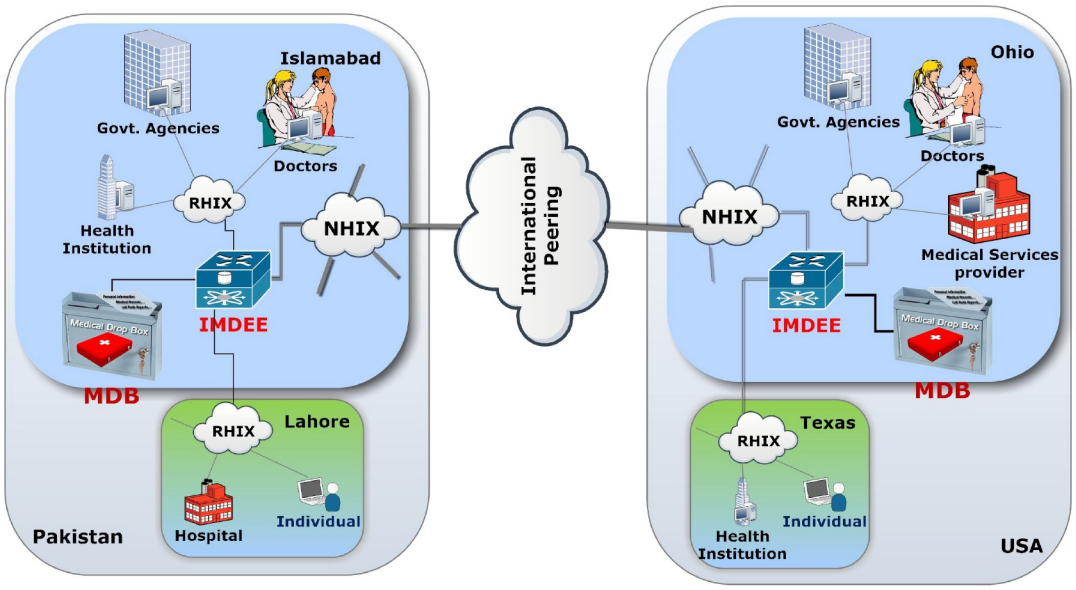

FIGURE 6 | SMDEE deployment architecture in RHIX and NHIX.

Input: (Patient Insurance Information) Xml file sample

1. Upload XML File
2. If file name ends with "XML"
3. Var file path = Get XML uploaded path ()
4. Var xmltext = Read XML File (file path)
5. **foreach** tag in xmltext **do**
6. **If** tag.name == period start **then**
7. Store patient insurance start date in variable
8. **endif**
9. **If** tag.name == period end **then**
10. Store patient insurance end date in variable
11. **endif**
12. **If** tag.name == network display **then**
13. Store patient insurance network in variable
14. **endif**
15. **If** tag.name == identifier system **then**
16. Store patient hospital name in variable
17. **endif**
18. **endloop**
19. **foreach** data in patient data **do**
20. Feed data to exchange engine
21. **endloop**

(a) Algorithm for Insurance Information

```
<?xml version="1.0" encoding="UTF-8"?><OrganizationAffiliation xmlns="http://hl7.org/fhir">
    <id value="example"/>
    <text>
    </text>
    <identifier>
    </identifier>
    <active value="true"/>
    <period>
    </period>
    <organization>
        <reference value="Organization/hl7pay"/>
    </organization>
    <participatingOrganization>
    </participatingOrganization>
    <network>
    </network>

    <!--  General Practice Provider for the first 3 months of 2012  -->
    <code>
    </code>
    <specialty>
    </specialty>
    <location>
    </location>
    <healthcareService>
        <reference value="HealthcareService/example"/>
    </healthcareService>
    <telecom>
    </telecom>
    <endpoint>
    <!--  Endpoint that handles the v2 messaging for the network  -->
    <reference value="Endpoint/example"/>
  </endpoint>
</OrganizationAffiliation>
```

(b) Insurance Information generated for exchangeable format

FIGURE 7 | Example of insurance information generation.

```
    Var file path ← Get CSV uploaded path ()
    Var CSV text ← Read CSV file (file path)
end if
while Readline = True do
     patient data ← line
     if Patient data = personal data then
          Store patient's data in a variable
          Apply dictionary rule on patient data
     end if
     if patient data = insurance then
          Store patient insurance data in a variable
          Apply dictionary rule on patient data
     end if
     if patient data = medication data then
          Store patient medication data in a variable
          Apply dictionary rule on patient medication data
     end if
end while
```

TABLE 4 | Nomenclature data mapping dictionary.

S.No	Normal data	Pointing data
1	Firstname	Naming_firstname
2	Middlename	Naming_middle
3	Lastname	Naming_lastname
4	First_name	Naming_firstname
5	Middle_name	Naming_middle
6	Last_name	Naming_lastname
7	Sr_name	Naming_firstname
8	Given_name	Naming_middle
9	Family_name	Naming_lastname

ALGORITHM 5 | Algorithm for insurance information.

```
Input: Patient complete information
Output: Patient insurance information generation
Upload XML File
if File name ends with 'XML' then then
     Var file path ← Get XML uploaded path()
     Var xmltext ← Read XML File (file path)
end if
for all tags in xmltext do
     if tag.name = period start then
          Store patient insurance start date in variable
     end if
     if tag.name = period end then
          Store patient insurance end date in variable
     end if
     if tag.name = Network display then
          Store patient insurance network in variable
     end if
     if tag.name = identifier system then
          Store patient hospital name in variable
     end if
end for
for all data in patient data do
     feed data to the exchange engine
end for
```

Multiple algorithms are designed for SMDEE to generate standard exchangeable medical data, for example, data related to patient medication, previous history, research-related data and many more. A request for medical data exchange can be generated from different regions of the medical industry, and different nomenclatures are used, so we additionally developed the data mapping dictionary inside the SMDEE, ensuring that nomenclature rules are intact. When a request is generated for patient data from SMDEE, it will use the nomenclature data mapping dictionary, making the patient data standardised by

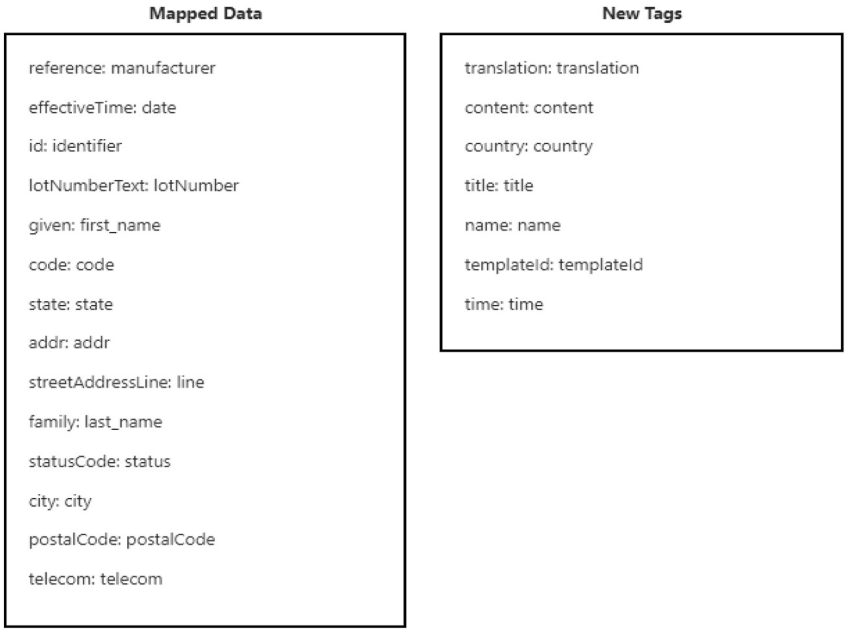

FIGURE 8 | Data mapping example in CDA to FHIR.

implementing the data mapping dictionary rules. The concept of a data mapping dictionary is shown in Table 4.

5 | Conversion of Patient Information From CDA to FHIR

If the medical data is not presented in FHIR to SMDEE and the medical entity uses the basic HL7 (CDA) standard, SMDEE first converts the document to FHIR. This is achieved by mapping, searching and adding tags where information loss is possible and no data can be interpreted in FHIR. When patient data (CDA) are seeded, it is mapped to FHIR, and new tags are added as necessary to capture the full meaning and information in the FHIR format. The concept of data mapping for CDA to FHIR is shown in Figure 8.

5.1 | Document Conversion From CDA to FHIR Algorithm

To prevent the loss of information from converting a document from CDA to FHIR, the standardisation of data between CDA and FHIR is achieved by creating two dictionaries. A static dictionary consists of predefined, or already existing, data, also called mapped data that are common between CDA and FHIR. In contrast, the second dictionary consists of new tags used to add to unmapped data, preventing the loss of information and handling null flavours.

All Laboratory Studies

Provider: George F Carson, MD
Patient: Sample H Patient **Providers Pt ID:** 6910828 **Sex:** Male
Birthdate: 24 Sep 1932
Attachment Control Number: XA728302

Hematology Tests + Cell Counts

Result name	Result Value	Normal Range	Abnormal flag	date/time
hematocrit	45	39-49		10/2/1995 6.38 PM
erythrocytes count	4.94 10*6/mm3	4.30-5.90		10/2/1995 6.38 PM
mean corpuscular volume	91 f1	90-98		10/2/1995 6.38 PM
platelets count	233 10*3/mm3	150-450		10/2/1995 6.38 PM
leukocytes count	25 10*3/mm3	3.2-9.8		10/2/1995 6.38 PM
neutrophils/100 leukocytes	83.1%	37.0-80.0	H	10/2/1995 6.38 PM
basophils/100 leukocytes	10.1%	10.0-50.0	H	10/2/1995 6.38 PM
monoophils/100 leukocytes	6.3 %	0.0-12.0		10/2/1995 6.38 PM
eosophils/100 leukocytes	0.3 %	0.0-7.0		10/2/1995 6.38 PM
basophils/100 leukocytes	0.2 %	0.0-2.0		10/2/1995 6.38 PM
neutrophils count	20.8 10*3/mm3	2.0-7.0	H	10/2/1995 6.38 PM
lymphocytes count	2.5 10*3/mm3	0.6-3.5		10/2/1995 6.38 PM
monocytes count	1.6 10*3/mm3	0.0-0.9	H	10/2/1995 6.38 PM
eosinphilis count	0.08 10*3/mm3	0.00-0.70		10/2/1995 6.38 PM
basophils count	0.04 10*3/mm3	0.00-0.20		10/2/1995 6.38 PM

(a) Sample of Lab Report in CDA Format

Test	Units	Value	Reference Range
Haemoglobin	g/L	176	135 -180
Red Cell Count	x10*12/L	5.9	4.2 - 6.0
Haematocrit		0.55+	0.38 - 0.52
Mean Cell Volume	f L	99+	80 - 98
Mean Cell haemoglobin	p g	36+	27 - 35
Platelet Count	x10*9/L	444	150 - 450
White Cell Count	x10*9/L	4.6	4.0 - 11.0
Neutrophils	%	20	
Neutrophils	x10*9/L	0.9	2.0 - 7.5
Lymphocytes	%	20	
Lymphocytes	x10*9/L	0.9	1.1 - 4.0
Monocytes	%	20	
Monocytes	x10*9/L	0.9	0.2 - 1.0
Eosinophils	%	20	
Eosinophils	x10*9/L	0.92++	0.004 - 0.40
Basophils	%	20	
Basophils	x10*9/L	0.92++	<0.21

(b) Sample of Lab Report in FHIR Format

Provider: George F Carson, MD Issued: 1995-10-25 Effective: 1995-10-02
Patient: Sample patient Provider Pt ID: 6910828 BirthDate: 1932-09-24
Attachment Control Number: XA728302 Category: All Laboratory Studies

Test	Value	Reference Range	Abnormal flag
hematocrit	45	39-49	
erthrocytes count	4.94 10*6/mm3	4.30-5.90	
mean corpuscular volume	91 f1	90-98	
platelets count	233 10*3/mm3	150-450	
leukocytes count	25 10*3/mm3	3.2-9.8	
neutrophils/100 leukocytes	83.1%	37.0-80.0	H
basophils/100 leukocytes	10.1%	10.0-50.0	H
monoophils/100 leukocytes	6.3 %	0.0-12.0	
eosophils/100 leukocytes	0.3 %	0.0-7.0	
hematocrit	0.2 %	0.0-2.0	
hematocrit	20.8 10*3/mm3	2.0-7.0	H
hematocrit	2.5 10*3/mm3	0.6-3.5	
hematocrit	1.6 10*3/mm3	0.0-0.9	H
hematocrit	0.08 10*3/mm3	0.00-0.70	
hematocrit	0.04 10*3/mm3	0.00-0.20	

(c) Proposed algorithm Converted Lab Report from CDA to FHIR

FIGURE 9 | CDA to FHIR lab report example.

When the input is provided as an XML CDA file, the algorithm successfully parses the data. After data parsing, the data are mapped between CDA and FHIR elements. Once mapping is done, the data are divided into mapped and unmapped data. A diagnostic report of CDA in Figure 9 has been converted to FHIR by using the proposed algorithms, which saves the loss of data by adding a skipped column of CDA, that is, abnormal flag to FHIR, and standardising some terms, that is, the normal range as the reference range.

6 | Conclusion

The demand for medical data interchange among different countries is developing at a very rapid pace. Hospital visits while traveling abroad are likely necessary for many people who travel. If this is the case, the doctors can only provide adequate care to the visiting patient after reviewing their medical records. For this to be possible, there must be an international exchange of clinical data [16, 58]. When it comes to the transfer of sensitive information, healthcare records rank high. Still, imagine a standard medical application and the Intelligent Medical Data Exchange Engine (SMDEE) running in each country. Assuming that is so, local privacy laws will not be violated when handling the requested medical data. The medical drop box (MDB) was also developed as part of the SMDEE; it provides users easy, 24/7 access to their medical records. We developed an HL7-compliant, portable clinical document for medical records that may be shared across several healthcare organisations. When fully operational, the SMDEE and MDB will facilitate the secure and rapid transfer of patient records by applicable national and international privacy regulations.

Developing nations without a medical law system as developed as the United States' HIPAA have motivated this study to create a medical law engine to process medical-legal material. One example of how our work is efficient is the HIPAA privacy guidelines, which were established through our studies. The regulations imposed by HIPAA do not restrict the usage of MDB. It is still feasible from every angle about the individual's privacy concerns, as outlined in the local medical regulations of the individual's nation, and it can be exchanged.

6.1 | Future Work

Our research currently focuses on sharing medical data between different healthcare entities. We are working with the idea that all users in the medical network are already verified (authenticated) and the network is secure for sending data. In the future, we plan to use a blockchain-based network to make the sharing of medical data even more secure. At this stage, we are only working with medical laws written in English. But in the future, we plan to support multiple languages, so the system can exchange data in any language, using standard formats and medical terms. We also plan to add AI and large language models (LLMs) to help understand both requests and medical laws better. These AI tools will learn from the data and help the system process requests faster and smarter in this worldwide medical network.

Funding

The research work of M. Faheem is fully supported by the University of Vaasa and VTT Technical Research Centre of Finland.

Conflicts of Interest

The authors declare no conflicts of interest.

Data Availability Statement

The data will be available upon request to the corresponding author.

Code Availability

The code will be available upon request to the corresponding author.

References

1. J. M. Marchibroda, "Health Information Exchange Policy and Evaluation," *Journal of Biomedical Informatics* 40, no. 6 (2007): S11–S16, https://doi.org/10.1016/j.jbi.2007.08.008.

2. H. Administrative, HIPAA Administrative 45 CFR, Parts 160, 162 and 164. Department of Health and Human Services, Office for Civil Rights, (2009), http://www.hhs.gov.

3. J. C. Maxwell and A. I. Anton, "Developing Production Rule Models to Aid in Acquiring Requirements From Legal Texts," *IEEE* (2009): 101–110, https://doi.org/10.1109/re.2009.21.

4. P. E. Lam, J. C. Mitchell, and S. Sundaram, *A Formalization of HIPAA for a Medical Messaging System* (Springer, 2009), 73–85.

5. H. DeYoung, D. Garg, L. Jia, D. Kaynar, and A. Datta, "Experiences in the Logical Specification of the HIPAA and GLBA Privacy Laws," in *ACM*, (2010), 73–82.

6. J. C. Maro, R. Platt, J. H. Holmes, et al., "Design of a National Distributed Health Data Network," *Annals of Internal Medicine* 151, no. 5 (2009): 341–344, https://doi.org/10.7326/0003-4819-151-5-200909010-00139.

7. T. Takemura, K. Araki, K. Arita, et al., "Development of Fundamental Infrastructure for Nationwide EHR in Japan," *Journal of Medical Systems* 36, no. 4 (2012): 2213–2218, https://doi.org/10.1007/s10916-011-9688-z.

8. M. S. Qazi and M. Ali, "Pakistan's Health Management Information System: Health Managers' Perspectives," *Journal of the Pakistan Medical Association* 59, no. 1 (2009): 10–14.

9. H. People, "Conclusion and Future Directions: CDC Health Disparities and Inequalities Report United States, 2013," *CDC Health Disparities and Inequalities Report United States* 62, no. 3 (2013): 184.

10. K. Sebelius, US Department of Health and Human Services Strategic Plan; Fiscal Years 2010–2015 (Online Publication, 2012).

11. S. Albagmi, "The Effectiveness of EMR Implementation Regarding Reducing Documentation Errors and Waiting Time for Patients in Outpatient Clinics: A Systematic Review," *F1000Research* 10, no. 514 (2021): 514, https://doi.org/10.12688/f1000research.45039.2.

12. P. Anthonysamy and A. Rashid, "Software Engineering for Privacy in-the-large," *2015 IEEE/ACM 37th IEEE International Conference on Software Engineering*, no. 2 (2015), 947–948, https://doi.org/10.1109/icse.2015.300.

13. D. M. West and A. Friedman, *Health Information Exchanges and Megachange* (Governance Studies at Brookings, 2012).

14. J. R. Vest, "Health Information Exchange: National and International Approaches," *Advances in Health Care Management* 12 (2012): 3–24, https://doi.org/10.1108/s1474-8231(2012)0000012005.

15. H. C. Huang, W. C. Fang, and W. H. Lai, "Secure Medical Information Exchange With Reversible Data Hiding," in *IEEE*, (2012), 1424–1427.

16. Z. Ts, J. Chu, K. Araki, and H. Yoshihara, "Design and Development of an International Clinical Data Exchange System: The International Layer Function of the Dolphin Project," *Journal of the American Medical Informatics Association* 18, no. 5 (2014): 683–689, https://doi.org/10.1136/amiajnl-2011-000111.

17. J. D. Young, "Commitment Analysis to Operationalize Software Requirements From Privacy Policies," *Requirements Engineering* 16, no. 1 (2011): 33–46, https://doi.org/10.1007/s00766-010-0108-6.

18. J. Liu, C. Wang, and S. Liu, "Utility of ChatGPT in Clinical Practice," *Journal of Medical Internet Research* 25 (2023): e48568, https://doi.org/10.2196/48568.

19. A. Čartolovni, A. Tomičić, and E. L. Mosler, "Ethical, Legal, and Social Considerations of AI-Based Medical Decision-Support Tools: A Scoping Review," *International Journal of Medical Informatics* 161 (2022): 104738, https://doi.org/10.1016/j.ijmedinf.2022.104738.

20. J. M. Balkin, "The Hohfeldian Approach to Law and Semiotics," *University of Miami Law Review* 44 (1990): 1119.

21. J. C. Maxwell and A. I. Anton, "A Refined Production Rule Model for Aiding in Regulatory Compliance," *tech. rep.* North Carolina State University. Dept. of Computer Science (2010).

22. M. Hashmi, "A Methodology for Extracting Legal Norms From Regulatory Documents," in *IEEE*, (2015), 41–50.

23. A. O Neill, "An Action Framework for Compliance and Governance," *Clinical Governance: An International Journal* 19, no. 4 (2014): 342–359, https://doi.org/10.1108/cgij-07-2014-0022.

24. T. Alshugran and J. Dichter, "Toward a Privacy Preserving HIPAA-Compliant Access Control Model for Web Services," in *IEEE*, (2014), 163–167.

25. T. Alshugran and J. Dichter, "Extracting and Modeling the Privacy Requirements From HIPAA for Healthcare Applications," in *IEEE* (Long Island, 2014), 1–5.

26. T. Alshugran, J. Dichter, and M. Faezipour, "Formally Expressing HIPAA Privacy Policies for Web Services," in *IEEE* (2015), 295–299.

27. T. Benson and G. Grieve, *Standards Development Organizations* (Springer, 2021), 427–442.

28. A. J. Moy, J. M. Schwartz, R. Chen, et al., "Measurement of Clinical Documentation Burden Among Physicians and Nurses Using Electronic Health Records: A Scoping Review," *Journal of the American Medical Informatics Association* 28, no. 5 (2021): 998–1008, https://doi.org/10.1093/jamia/ocaa325.

29. T. K. Colicchio and J. J. Cimino, "Clinicians Reasoning as Reflected in Electronic Clinical Note-Entry and Reading/Retrieval: A Systematic Review and Qualitative Synthesis," *Journal of the American Medical Informatics Association* 26, no. 2 (2019): 172–184, https://doi.org/10.1093/jamia/ocy155.

30. E. Joukes, A. Abu-Hanna, R. Cornet, and N. F. Keizer, "Time Spent on Dedicated Patient Care and Documentation Tasks Before and After the Introduction of a Structured and Standardized Electronic Health Record," *Applied Clinical Informatics* 9, no. 1 (2018): 046–053, https://doi.org/10.1055/s-0037-1615747.

31. B. G. Arndt, J. W. Beasley, M. D. Watkinson, et al., "Tethered to the EHR: Primary Care Physician Workload Assessment Using EHR Event Log Data and Time-Motion Observations," *Annals of Family Medicine* 15, no. 5 (2017): 419–426, https://doi.org/10.1370/afm.2121.

32. P. Mishra, J. C. Kiang, and R. W. Grant, "Association of Medical Scribes in Primary Care With Physician Workflow and Patient Experience," *JAMA Internal Medicine* 178, no. 11 (2018): 1467–1472, https://doi.org/10.1001/jamainternmed.2018.3956.

33. R. H. Dolin, L. Alschuler, S. Boyer, et al., "HL7 Clinical Document Architecture, Release 2," *Journal of the American Medical Informatics Association* 13, no. 1 (2006): 30–39, https://doi.org/10.1197/jamia.m1888.

34. J. M. Ferranti, R. C. Musser, K. Kawamoto, and W. E. Hammond, "The Clinical Document Architecture and the Continuity of Care Record," *Journal of the American Medical Informatics Association* 13, no. 3 (2006): 245–252, https://doi.org/10.1197/jamia.m1963.

35. E. W. Huang, T. L. Tseng, M. L. Chang, M. L. Pan, and D. M. Liou, "Generating Standardized Clinical Documents for Medical Information Exchanges," *IT professional* 12, no. 2 (2010): 26–32, https://doi.org/10.1109/mitp.2010.56.

36. P. Poba-Nzaou, S. Uwizeyemungu, M. Dakouo, A. Tchibozo, and B. Mboup, "Patterns of Health Information Exchange Strategies Underlying Health Information Technologies Capabilities Building," *Health Systems* 11, no. 3 (2021): 1–21, https://doi.org/10.1080/20476965.2021.1952113.

37. P. Taber, C. Radloff, G. Del Fiol, C. Staes, and K. Kawamoto, "New Standards for Clinical Decision Support: A Survey of the State of Implementation," *Yearbook of medical informatics* 30, no. 1 (2021): 159–171, https://doi.org/10.1055/s-0041-1726502.

38. E. Karaarslan and E. Konacaklı, *Decentralized Solutions for Data Collection and Privacy in Healthcare*, Vol. 167–190 (De Gruyter, 2021).

39. S. Biswas, K. Sharif, F. Li, A. K. Bairagi, Z. Latif, and S. P. Mohanty, "Globechain: An Interoperable Blockchain for Global Sharing of Healthcare Data–A COVID-19 Perspective," *IEEE Consumer Electronics Magazine* 10, no. 5 (2021): 64–69, https://doi.org/10.1109/MCE.2021.3074688.

40. A. A. Abdellatif, L. Samara, A. Mohamed, et al., "MEdge-Chain: Leveraging Edge Computing and Blockchain for Efficient Medical Data Exchange," *IEEE Internet of Things Journal* (2021): 1, https://doi.org/10.1109/JIOT.2021.3052910.

41. C. Dhasaratha, M. K. Hasan, S. Islam, et al., "Data Privacy Model Using Blockchain Reinforcement Federated Learning Approach for Scalable Internet of Medical Things," *CAAI Transactions on Intelligence Technology* (2024): cit2.12287, https://doi.org/10.1049/cit2.12287.

42. V. Thakkar, V. Shah, and A. Khang, *Electronic Health Records Security and Privacy Enhancement Using Blockchain Technology* (CRC Press, 2023), 1–13.

43. I. Masood, A. Daud, Y. Wang, A. Banjar, and R. Alharbey, "A Blockchain-Based System for Patient Data Privacy and Security," *Multimedia Tools and Applications* 83, no. 21 (2024): 60443–60467, https://doi.org/10.1007/s11042-023-17941-y.

44. R. K. Saripalle, "Fast Health Interoperability Resources (FHIR): Current Status in the Healthcare System," *International Journal of E-Health and Medical Communications* 10, no. 1 (2019): 76–93, https://doi.org/10.4018/ijehmc.2019010105.

45. S. Maxhelaku and A. Kika, "Improving Interoperability in Healthcare Using HL7 FHIR," in *International Institute of Social and Economic Sciences* (2019), 35–42.

46. T. Takeda, D. Zhang, S. Wada, et al., *The Acquisition of Structured Clinical Data From a Document-Based Electronic Medical Record System* (IOS Press, 2019), 1600–1601.

47. A. Almalawi, A. I. Khan, F. Alsolami, Y. B. Abushark, and A. S. Alfakeeh, "Managing Security of Healthcare Data for a Modern Healthcare System," *Sensors* 23, no. 7 (2023): 3612, https://doi.org/10.3390/s23073612.

48. Z. Wu, H. Wang, J. Wan, L. Zhang, and J. Huang, "An Inner Product Predicate-Based Medical Data-Sharing and Privacy Protection System," *IEEE Access* 12 (2024): 68680–68696, https://doi.org/10.1109/access.2024.3400611.

49. H. Rafik, A. Ettaoufik, and A. Maizate, "Securing Medical Data Exchange: A Decentralized Approach Based on the e-IPGPChain Framework," *International Journal of Safety & Security Engineering* 14, no. 3 (2024): 815–829, https://doi.org/10.18280/ijsse.140314.

50. M. Xie, Z. Zhang, H. Hong, G. Zhang, and Y. Qin, "Secure Medical Data Sharing Featuring Traceable Data Usage and Automatic Audit Mechanism," *IEEE Internet of Things Journal* 12, no. 13 (2025): 25587–25600, https://doi.org/10.1109/jiot.2025.3559926.

51. S. Arefin and N. T. Zannat, "Securing AI in Global Health Research: A Framework for Cross-Border Data Collaboration," *Clinical Medicine And Health Research Journal* 5, no. 2 (2025): 1187–1193, https://doi.org/10.18535/cmhrj.v5i02.457.

52. T. K. Alhasan, "Managing Legal Risks in Health Information Exchanges: A Comprehensive Approach to Privacy, Consent, and Liability," *Journal of Healthcare Risk Management* 44, no. 4 (2025): 12–24, https://doi.org/10.1002/jhrm.70002.

53. I. Khan, M. Alwarsh, and J. I. Khan, "A Comprehension Approach for Formalizing Privacy Rules of HIPAA for Decision Support," *IEEE*, (2013), 390–395.

54. I. Khan, M. Sher, J. I. Khan, et al., "Conversion of Legal Text to a Logical Rules Set From Medical Law Using the Medical Relational Model and the World Rule Model for a Medical Decision Support System," *Informatics* 3, no. 1 (2016): 2, https://doi.org/10.3390/informatics3010002.

55. I. Khan, M. Sher, S. Aslam, et al., "MEDICAL DROP BOX (MDB)," *Professional Medical Journal* 23, no. 4 (2016): 489–498, https://doi.org/10.29309/tpmj/2016.23.04.1538.

56. I. Khan, M. Sher, J. I. Khan, S. M. Saqlain, A. Ghani, and M. U. Ashraf, "Clinical Document Construction Using HL7 With Medical Drop Box for Exchange of Electronic Health Records Under Country Medical Law," *International Journal of Computer Science and Information Security* 14, no. 10 (2016): 559–576.

57. I. Khan, M. Sher, S. M. Saqlain, et al., "Role-Based Efficient Information Extraction Using Rule-Based Decision Tree," *International Journal of Advanced and Applied Sciences* 4, no. 1 (2017): 74–83, https://doi.org/10.21833/ijaas.2017.01.011.

58. L. Lenert, D. Sundwall, and M. E. Lenert, "Shifts in the Architecture of the Nationwide Health Information Network," *Journal of the American Medical Informatics Association* 19, no. 4 (2012): 498–502, https://doi.org/10.1136/amiajnl-2011-000442.