Article

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

Imran Khan [1,*], Muhammad Sher [1,†], Javed I. Khan [2,†], Syed M. Saqlain [1,†], Anwar Ghani [1,†], Husnain A. Naqvi [1,†] and Muhammad Usman Ashraf [1,†]

[1] Department of Computer Science & Software Engineering, International Islamic University, H-10 Campus, Islamabad 4400, Pakistan; m.sher@iiu.edu.pk (M.S.); syed.saqlain@iiu.edu.pk (S.M.S.); anwar.ghani@iiu.edu.pk (A.G.); husnain.naqvi@iiu.edu.pk (H.A.N.); usmanashraf@iiu.edu.pk (M.U.A.)

[2] Department of Computer Science, Kent State University, Kent, OH 44240, USA; javed@cs.kent.edu

[*] Correspondence: imran.khan@iiu.edu.pk; Tel.: +92-334-551-8805; Fax: +92-51-925-7954

[†] These authors contributed equally to this work.

Abstract: Automated formalization of legal text is a time- and effort-consuming task, but human-based validation consumes even more of both. The exchange of healthcare data in compliance with the medical privacy law requires experts with deep familiarity of its intricate provisions for verification. The article presents a medical relational model (MRM) for the extraction of logical rules from medical law, required to design a medical decision support system (MDSS) that facilitates the process of exchanging data electronically with minimum human intervention. The division of medical law into small concept classes makes it easier to formalize the legal text of medical law into logical rules. These logical rules are then used to make a precise decision in compliance with the law, after evaluating requests from different entities for different purposes in MDSS. Our methodology is to analyze the legal text and release records in compliance with the medical law. For developing countries where medical laws are not as mature as HIPAA (Health Insurance Portability and Accountability Act) in the USA, the proposed methodology can be adapted to build their MDSS based on MRM.

Keywords: HIPAA; privacy rules; logical rules; formalization; medical relational model (MRM); medical decision support system (MDSS); protected health information (PHI)

1. Introduction

Conversion to a logical rules set from a legal text document remains an important and difficult task [1] due to the complex structure of legal text documents. The legal text document consists of different sections, subsections, clauses, sub-clauses and sub-sub-clauses. Therefore, it is a complex job for a software engineer who does not understand the exact meaning of these clauses and has been given the task of building a medical decision support system (MDSS), which supports the exchange of private health information according to the medical law of that country. However, it will make it easier for a software engineer to design and build MDSS if we provide him or her a logical rules set. Informatics-assisted compliance verification with laws and regulations is however highly challenging [2,3]. Legal drafts often contain ambiguities and have incomplete contingencies. There are frequent cross-references to different subsections of the same or other sections [4]. Furthermore, there

are implied cross-reference meanings of its provisions associated with the intent of the law, possibly conflicting definitions and domain-specific terminology [5]. The implementation of laws also gets refined gradually as the various provisions are tested in contests and courts provide case-specific clarifications [6]. In addition, laws and regulations undergo updates and amendments that would require a software engineer to manage and track these changes [7].

Therefore, the first step to build MDSS is to formalize the medical law into logical rules. These logical rules can further be used for making a decision to release or the denial of certain medical records in compliance with the law, when requested by any entity of the medical system. The users of the medical system are almost the same all over the world, *i.e.*, doctors, nurses, hospitals, labs, researchers, *etc.*, but the medical laws for those entities may differ from country to country. The U.S. Department of Health and Human Services (HHS) in 1996 created the Health Insurance Portability and Accountability Act HIPAA as a means of providing a mechanism to protect broad civil rights, including the privacy of medical information [8,9]. Failing to conform to HIPAA may result in a fine of up to $25,000 per year and one to five years of imprisonment [10]. HIPAA Administrative Simplification, Regulation Text: 45 CFR (Code of Federal Regulations) Parts 160, 162 and 164 specifically regulate the disclosure of personal health information [11].

The complexity of HIPAA, combined with potentially stiff penalties for violators, has led physicians and hospitals to withhold information from those who may have a right to it [12]. A review of the implementation of the HIPAA privacy rules by the U.S. government accountability office found that healthcare providers worry "about their legal privacy responsibilities and often responded with an overly guarded approach to disclosing information than necessary to ensure compliance with the privacy rules" [13].

Several attempts have been made to convert legal text into logic rules [14,15] with a special focus on HIPAA, given its importance to healthcare. The authors of [16] attempted to generate Datalog rules corresponding to the sentences in the legal text. Their proposed mechanism combines associated rules in the form of "permitted_by" and "forbidden_by", where the latter has precedence for making a decision, and prohibition takes precedence over permission in the case of "conflicts". Similarly, the authors of [17] attempted to convert legal text into Prolog statements using several steps based on Hohfeldian concepts of defining/classifying legal rights [17,18]. Each clause and the corresponding rules are categorized into four types, such as right, obligation, permission and definition. In some similar studies [19,20], the authors proposed least fixed point (LFP) logic for assigning the particular semantic modal and signature, which specify the privacy regulations, where all legal constraints are expressed as positive and negative norms to make a decision, whereas the latter takes precedence over the former in the case of conflict. For the exchange of medical data, the authors of [21–23] proposed different approaches for the exchange of protected health information among the medical entities.

One of the common perils in such approaches is the inability to capture the deep semantic connections between various sections of the large HIPAA text. In close observation, one would notice that these first generation approaches (such as [16,17,19]) are attempts to translate the legal text, clause by clause, into corresponding logical expressions. The rules set reflects the clausal organization and syntax of the legal text. It spares comprehension of the overall HIPAA semantics, except for the part by part attempt to model the semantics of the sentences. The inference process is expected to drive from one "sentence" (presented in the form of a logical expression) to another and to find the connections between constraints defined in various parts of the act by shared predicates. In one sense, it is remarkable, without the explicit comprehension of the overall HIPAA, how much success they have achieved in making many decisions correctly. However, the resulting logical systems in such approaches seem to miss yet many higher cognitive level connections hidden in the semantics of the overarching HIPAA environment. Indeed, several cases of "conflict" cited are artifacts of missing deeper semantic/indirect cross-references. A human expert can connect the context and may not see these cases as a conflict. Indeed, to resolve the conflict artifacts, all of these approaches have to use in some form of preference/precedence meta rules extensively, though these are not part of HIPAA.

Supporting programmable legal compliance and real life actions requires a substantial understanding of the conceptual framework of medical law. For automatic verification of HIPAA privacy compliance, an understanding of the structure and interrelation of the privacy rules is needed. For example, why do we need a law to govern the release, exchange and use of information? How does one respond to a requester or entities in a medical system? What conditions are applied for accessing specific information? What kind of actions should be taken by the system in response to different events? It can be argued that every law has its reasons and purposes, and there are some conditions for these purposes. Each request has a response and action. In other words, in order to build an effective MDSS, all aspects beyond the legal text must be covered.

This paper mainly focuses on Section 164 of HIPAA, which is related to the security and privacy issues of healthcare. In the remainder of this paper, Section 2 briefly presents the methodology, the concept space of HIPAA, the tag set and the rule set formation from HIPAA. Section 3 explains the result used in the example. Section 4 is about the discussion, with a comparison of different approaches to the proposed solution using different studies. Section 5 concludes the discussion on MRM for any medical law and medical decision support system for EHR.

2. Materials and Methods

This research attempts to capture and accommodate deeper underlying semantics of the complex aspects of medical law. A medical relational model (MRM) is used, which includes the medical entities and their relationships that define the semantics of the domain, on which the Act and their provisions have been laid and structured. Based on the MRM, a systematic tag-based approach is adopted to convert the corpus of legal texts into a set of logical constraints and actions. It requires the designer to explicitly comprehend and extract the connections (with HIPAA experts) and to summarize the overall behavior as a set of independently-constructed rules. The system pre-resolves the semantic connections and, thus, generates very precise resolutions. The MRM and the rules generated, then, can provide a very transparent process in the form of decision trees to precisely resolve information requests. Besides the decisions, the resulting system can much better articulate other intents of HIPAA. It also specifies how to release particular pieces of information. If denied, what are the alternate options that generate a logically-coherent explanation to support and conform the decisions? Conforming to the original expectations of HIPAA, the entire process can be subsequently automated.

2.1. Concept Space of HIPAA

Figure 1 shows eight (8) elementary concept classes, named requester, purpose, patient record items, condition, action, fee and time, information procedure and, finally, record release. It is an internal structure of medical law, which is based on these concept classes.

Concept classes indeed have relations with each other. Some of these relations are conceptual, whereas others are compositional. However, making a relationship between tags in concept classes requires MRM to understand the semantics of these connections.

Figure 2 represents the proposed MRM that governs the connection of conceptual and compositional relations between classes. Our MRM is based on eight conceptual relations between concept classes and three compositional relations that form three classes. These classes are request flow, evaluation and release.

The first conceptual relation is between a requester (1) and purposes (5), where a requester could have different purposes for a request. Furthermore, remaining conceptual relations are explained as follows: a requester (1) requests records from a covered entity (2); the covered entity manages patient's information (3), which contains record types (4) and has an information release procedure (10); the covered entity takes an action (6) based on the conditions (7) and takes the appropriate time and fee (9) for that action.

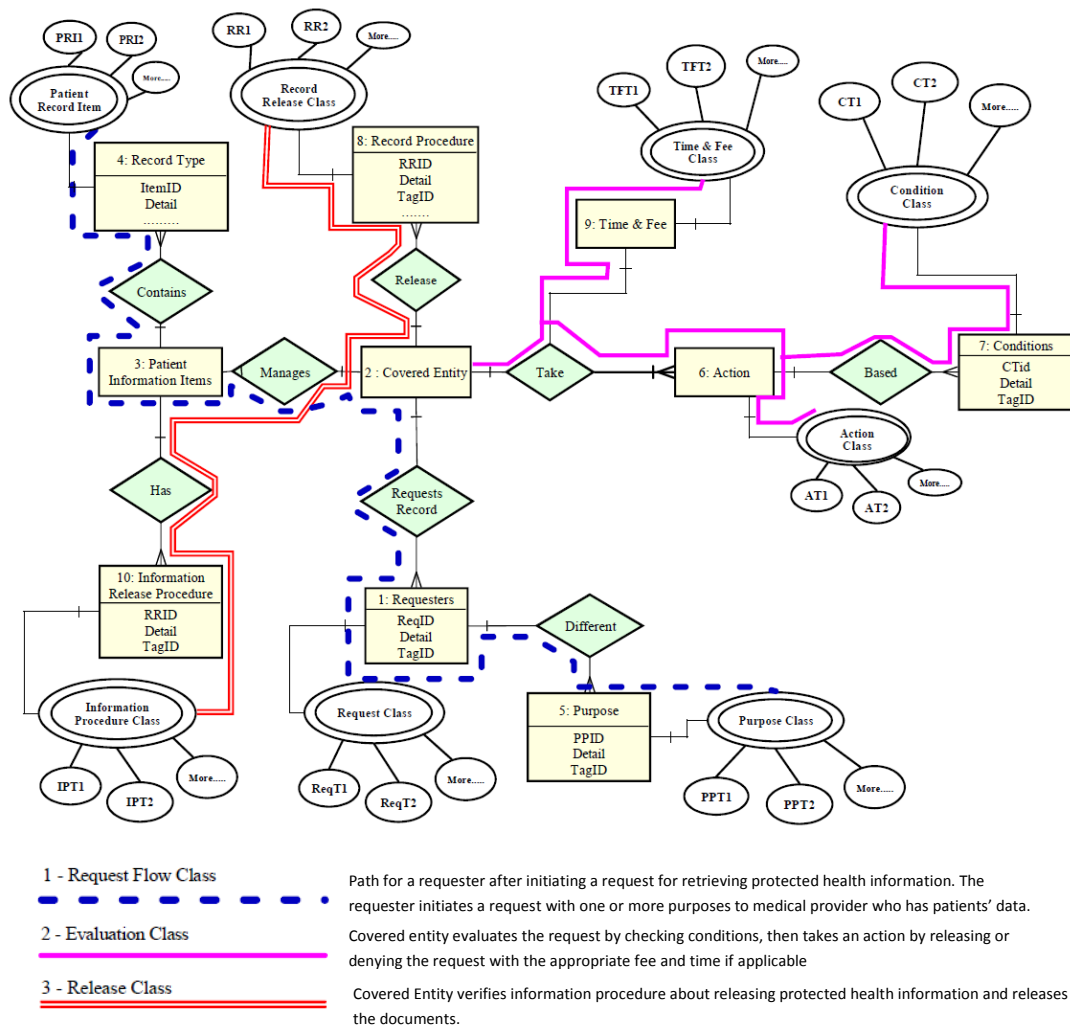| Tag	Description of Concept Classes
ReqT	**Request Class**: A designated class of the individual/entity making the release request. For example "Researcher", "Doctor", etc.
PPT	**Purpose Class**: Requires every request to have a valid purpose specifying the intended use of the requested PHI. Example purposes are "research", "amendment", "treatment","operation".etc.
PRI	**Patient Record Item Marker:** A marker attached to individual record items specifying their significance of records. Example is "Billing Information, "Psychotherapy Notes", etc.
CT	**Condition Class:** Conditions are triggered based on requester (ReqT) and submitted purposes (PPT) and patient records items (PRI). Example, if the ReqT is a researcher does he/she have an authorization for research?, If the PPT is for research, is the requester has the role of a researcher?, if the PRI requested is psychotherapy notes, is there any requirements, like specific authorization for psychotherapy, available?, etc.
AT	**Action Class:** Action that is performed on each request as a result of evaluating rules' sets. Examples "Deny", "Release", "Update", etc.
TFT	**Time & Fee Class:** Fee and Time Required for processing a request. Example, more time is required to de-identify patients information. Cost of preparing documents, postage fee, etc.
IPT	**Information Procedure Class:** Rules that specify how information will be released. Example, information will be released with a fee and time delay, Information will be de-identified before releasing it.
RRT	**Record Release Class:** Actual information that will be released as a result of a request. Example, 5 patients record are released.

Figure 1. Concept classes' description.

Figure 2. Medical relational model (MRM).

There are three compositional relation classes that are formed by several concept classes. The request flow class is composed of request (1), purpose (5) and patient record item (4) classes. The evaluation class is composed of request flow, time and fee (9), action (6) and condition (7) classes. The release class consists of record release (8), information procedure (10) and evaluation.

In Figure 2, big ovals represent our concept classes; small ovals with the concept classes represent the tags associated with each class; and rectangle shapes represent the processes that use those classes.

2.2. Tags' Set

Related clauses are grouped under any one of the concept classes and assign tags to these clauses. For example, the concept class related to requester is searched for the requester's information clauses. Then, each requester is assigned a tag (ReqT1, ReqT2, *etc.*) and added under the requester concept class. Each tag refers to a clause that contains the information related to the requester concept class. Conditions that need to be satisfied are placed under the conditions concept class, and each condition rule is assigned a (CT) tag. The time and fee class indicates the time and fee needed to release PHI, referred to as TFT. For example, the covered entity might place a preparation fee on disclosing documents. Some medical records may require human verification to make sure these records cannot be identified. This requires a processing time that might delay the release of these records. All purposes of requests, which are related to the requester, indicating the reasons for disclosing PHI are listed under the purpose concept class, and each rule is assigned a PPTtag. Action needs to be taken whether to deny or disclose PHI. We collect these actions under the actions concept class, and each action is assigned an AT tag. The information procedure concept class represents how information will be released, and the IPT tag is used in this class. The record release concept class is related to the rules that indicate what type of information will be released.

For example, the psychotherapy notes (RRT) tag is used to distinguish among rules in its class. All record items in each section need to be evaluated for dependencies. For example, psychotherapy notes cannot be disclosed without an authorization from the individual, as stated in clause 164.508.a.2 of HIPAA. This indicates that a condition needs to be satisfied for this type of record item. We mark all patient's record items that have dependencies and put them in one PRI class.

2.3. Rule Set Formation from HIPAA

For illustration in this article, we focus only on the HIPAA edicts specific to the use of PHI by the researchers. HIPAA clauses in Sections 164.508, 164.512, 164.514 and 164.532, respectively, cover the portion of this usage. There are multiple ways of organizing the logical rule expressions. In this system, logical rules are organized based on possible combinations of the requester (ReqT), purpose (PPT) and patient record item types (PRI). Each rule also has associated condition tags (CT). Each logical rule then specifies a unique decision action (AT) and special instruction (IPT) on release process format choices (RRT); time and fee restrictions (TFT) are applied when applicable.

The resolution process reads those as: If (Requester = "Researcher" & Purpose = "Purpose Tags" & Items = "Patient Record Items"; then check conditions (Pre-Condition = "Pre-Conditions Tags" & ReqT Condition = "Requester Tags" & Purpose Condition = "Conditional Purpose Tags") then (Action = "Action Tags" & Record Release = "Record Release Tags" & Information Procedure = "Information Procedure Tags" & Time Taken = "Time Tags" & Fee = "Fee Tags"). As a result, extracted information from all HIPAA sections will be distributed among 8 concept classes, and decision will be based on combinations of tags from these concept classes. Note: the fee class and time class might not be available in all privacy rules sections of HIPAA.

A three-step approach is undertaken in this article to address the challenge of HIPAA. In Figure 3, the first part of the modeling process consists of parsing the HIPAA text to identify the compositional and functional model of the HIPAA regimen in terms of components and core processes. This involves identification and classification of the key concepts in terms of entities, actors, actions and conditions, including factors that build the conditions and action modifiers described in various parts of HIPAA.

Once these concepts are extracted, they are further organized into classes, types and their relations in the second step. Thirdly, the core processes involving these entities (functional relationship between the entities) are also ascribed. This process leads to an MRM model.
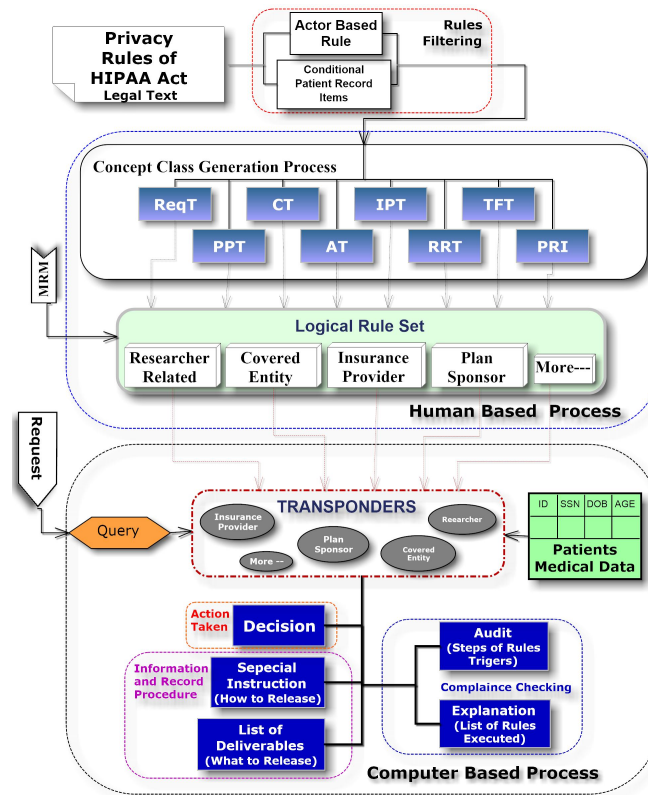

Figure 3. World rule model using MRM for a decision support system.

2.4. HIPAA Rules' Filtration through the World Rule Model

We proposed partial formalization of legal text into logical rules in the first part of WRM. Instead of formalizing the comprehensive text of privacy rules, only rules that are related to a certain discipline will be formalized. Logical rules from different sections of HIPAA are extracted using Algorithm 1, and the flow of the algorithm is shown in Figure 4.
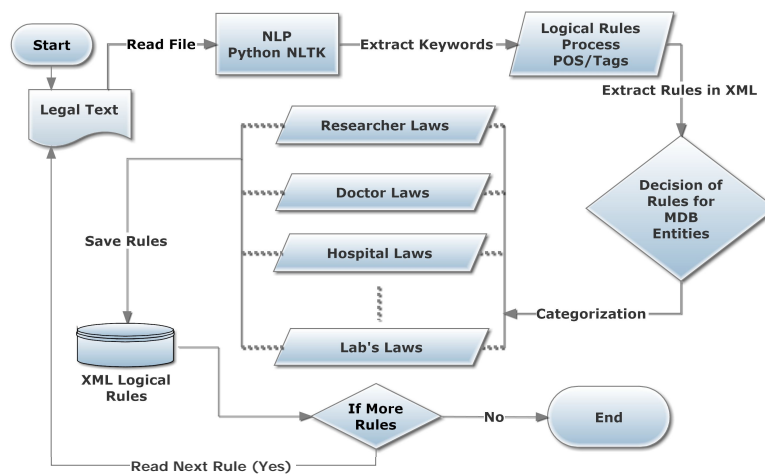

Figure 4. XML rule-filtering algorithm model.

Tag rules are complied with for each medical entity, as shown in Figure 5 for the researcher. After that, tag rules are compiled into XML-based logical rules for each entity with Algorithm 1. A sample of XML logical rules generated through the algorithm from HIPAA is shown below.

```
<rules>
 <rule ruleid="164.512.b">
  <Request>access</Request>
  <Requester>patient</Requester>
  <Entity>hospital</Entity>
  <AccessLevel>permission</AccessLevel>
  <Condition>hospital_Law_3</Condition>
          <CrossReference>164.508.a.1</CrossReference>
 </rule>
</rules>
```

Data: **Input:** Rule Pattern File R_{PF}, POST Data File POS_{tagF}
Result: XML-Based Logical Rules
Step 1 Read R_{PF} to Extract R_p (Rule Pattern);
Read R_p and Placed in a List Rcl;
Step 2 Create Lists L_m where $2 \leq m \leq n$ n is the No. of Components in the Rule Pattern;
forall the *Ruleid from POS_{tagF}* **do**
 Read Ruleid R_i;
 Read Words W_i Corresponding to $Rcl[p]$ $1 \leq p \leq n$;
 Add it into its Relevantlist Lp;
 $rule = < Ruleid > R_i < Ruleid >$;
 if *length of each list L_i is 1* **then**
  use each list L_i ;
  $rule = rule+ < Rcl[i+1] > L_i[1] < Rcl[i+1] >$;
 end
 else
  if *Length of $L_2 > 1$* **then**
   $len = length(L_2)$;
   Generate lenmany copies of Rule ;
   $Rule_1 = rule$;
   $Rule_2 = rule$;
   $\cdots$;
   $\cdots$;
   $Rule_{len} = rule$;
  end
  while $t = 1 \rightarrow len$ **do**
   $Rule_t = Rule_t+ < Rcl[2] > L_2[t] < Rcl[2] >$
  end

  forall the *$Rule_t$ where $1 \leq t \leq len$* **do**
   forall the *List L_i where $i > 2$* **do**
    while $s = 1 \rightarrow Length(L_i)$ **do**
     $Rule_t = Rule_t+ < Rcl[i] > L_i[s] < Rcl[i] > + $ newline;
    end
   end
  end
 end
end
Output: XML Logical Rules Generated

Algorithm 1: The XML logical rule generation algorithm.

The second part of the modeling process is the derivation of the actual constraints expressed in the Act. The constraints can be of a logical, temporal or functional type. In this step, the logical constraints, conditions and exemptions of the information release process as expressed in HIPAA are derived. Each rule or clause in these concept classes is identified (in terms of tag) and is connected together based on how a request of disclosing PHI is processed in the privacy rules of HIPAA. Different

sections of the privacy rules may consist of related information, which needs to be considered in this process. At the end, the HIPAA requirements are compiled together as a set of logical rules.

Generated Rules for Researcher From All Sections					
Requestor	**Purpose**	**PRI**	**Conditions**	**Action**	**Information Release Procedure**
Researcher	PPT1	Any PRI	" CT1 ^ CT2 ^ CT3 ^ CT4 " & " ~**CT5** (**CT6** ^ **CT7**) ^ ~CT8 (CT9 ^ CT10 ^ CT11) ^ **CT12**	AT4	" RRT1 || RRT2 " & "~IPT1 ^ IPT2 ^ IPT3
Researcher	PPT1	Any PRI	" ! (CT1 ^ CT2 ^ CT3 ^ CT4) " & " **CT5** (**CT6** ^ **CT7**) ^ ~CT8 (CT9 ^ CT10 ^ CT11) ^ **CT12**	AT4	" RRT1 || RRT2 " & "~IPT1 ^ IPT2 ^ IPT3
Researcher	PPT1	Any PRI	"! CT1 ^ CT2 ^ CT3 ^ CT4 " & " ! **CT5** (**CT6** ^ **CT7**) ^ ~ CT8 (CT9 ^ CT10 ^ CT11) ^ **CT12**	AT1	
Researcher	PPT1	Any PRI	" !CT1 ^ CT2 ^ CT3 ^ CT4 " & " **CT5** (!**CT6** ^ **CT7**) ^ ~ CT8 (CT9 ^ CT10 ^ CT11) ^ **CT12**	AT1	
Researcher	PPT1	Any PRI	" !CT1 ^ CT2 ^ CT3 ^ CT4 " & " **CT5** (**CT6** ^ **CT7**) ^ ~ CT8 (CT9 ^ CT10 ^ CT11) ^ ! **CT12**	AT1	
!Researcher	PPT1	Any PRI		AT1	
Researcher	!PPT1	Any PRI		AT1	
!Researcher	!PPT1	Any PRI		AT1	

Figure 5. Generated rules for researcher.

In the final part, requests for various administrative actions are processed. An administrative request originates from the requester. It includes, but is not limited to, identity, purpose, specifications of information requested and a set of associated credentials (such as authorization, waiver, *etc.*). The transponder (decision work flow specific to a particular type of administrative request) generates the "decision" or "conformance verification" as per HIPAA.

The transponder acts as the mediator between the administrative requests on one side and the medical databases with HIPAA tagging on the other side. The transponder runs the resolution process as per the specification in the HIPAA rule set. The transponder can also generate four other items, namely: (i) a list of deliverables; (ii) special instructions specifying format choices (raw record, summary, *etc.*), special processing (like de-identification required), fee and time constraints, *etc.*, as specified in HIPAA; upon request, the system can also provide (iii) an explanation identifying rules triggered and (iv) an audit specifying who, when and what has been requested, created, released, *etc.*. This paper focuses only on the first item "generation of decision".

3. Results

3.1. Rule Set for the Researcher from HIPAA

For example, if the requester is a researcher role (ReqT1) with a research purpose (PPT1), a request to disclose patient record item (PRI) is initiated. He/she must have a non-expired authorization, and if there are restrictions from the covered entity, the requester must satisfy these restrictions "CT1 $\wedge$ CT2 $\wedge$ CT3 $\wedge$ CT4". If a waiver is provided "CT5 (CT6 $\wedge$ CT7)", then the minimum requirements of the waiver (CT7) must be satisfied, and a brief description about the research "CT6" needs to be provided. If the researcher intends to do the research on decedent information "CT8", then he/she must present a representation "CT9" indicating that the use or disclosure of this information is only for research. In addition, the requester must agree to provide the covered entity with the documentation of descendent "CT10" death if requested by the covered entity. Nevertheless, providing a representation indicating the necessity of this type of PHI for the research "CT11" is a must. For any type of research, the covered entity must obtain consents "CT12" from the researcher. Consents must conform such that the disclosure is sought solely to review PHI as necessary to prepare a research protocol or for similar purposes that are preparatory for the research "CT13". The researcher must not remove PHI from the covered entity "CT14" and provide a representation indicating the necessity of this information for the

research "CT15". Figure 5 shows all of the rules that are generated for the researcher. The tags' details are explained in [24].

Symbols used in Figure 5 are explained as follows: "∧" means "and within a rule"; "&" means "and between rules"; "∥" is used as "or"; "!" for "not"; "∼" means "may".

3.2. Query and Result

In this section, an example is presented to provide a practical explanation of how a request is processed with the proposed world rule model approach using MRM in a decision support system.

Researcher Example

The researcher requests in natural language "A researcher wants to disclose psychotherapy notes for patients who were registered after the year 2013. The researcher has authorization to access PHI for research purposes. The PHI is requested to be received via email".

Query in SQL Format: select Patient_Data from Patients records where PRI == Psychotherapy and Date > 2013 and Requester == Researcher and Purpose == Research group by Requester && Purpose having Waiver rule == None && Authorization == Patients_Authorization

In this example, when the query (Figure 6) is processed on Patients' Record (Figure 7), Rule Number 1 from Figure 5 will be triggered because the researcher has an authorization. In addition, regarding the list of instructions and deliverables for releasing information, the will be released by email based on RR2. Figure 8 is the actual output. Note that personal information is presented in this table, because the researcher has authorization from the patients to disclose PHI.

Requester Role:	Researcher	**ID:**	5678
Authorized By:	Yes - Research	**Waiver Rule:**	No
Purpose 1:	Research	**Single Record Items:**	Psychotherapy
Purpose 2:	None	**Multi Record Items:**	None
Multi Purpose:	None		
Date From: day/month/year	1/1/2014	**Date To:** day/month/year	12/12/2014
Record Format:	Default		

Figure 6. Researcher query form.

ID	Name	PRI	Date day/month/year	Patient IPT = research	Covered Entity IPT = research	Conditional PRI Status
1	Abaad	PRI1	05/02/2014	Deny	Deny	
2	Maria	PRI1	04/10/2014	Disclose	Deny	
3	Raja	PRI5	13/10/2014		Disclose	Authorized
4	Tena	PRI1	03/06/2014	Disclose	Disclose	
5	Nelo	PRI5	15/08/2014		Disclose	Authorized
6	Lala	PRI2	02/12/2014	Disclose	Deny	
7	Mao	PRI1	01/09/2014	Deny	Disclose	
8	Tina	PRI5	22/02/2014		Deny	Unauthorized

Figure 7. Patients' records.

ID	Name	PRI	Date day/month/year
3	Raja	PRI5	13/10/2014
5	Nelo	PRI5	15/08/2014

Figure 8. Output result of the query.

4. Discussion

We compare our methodology to three other methods [16,17,19] using the previous example from Section 3. There are a few exceptions, like 164.508(a) (2), which indicates that a covered entity is obligated to obtain authorization for using or disclosing psychotherapy notes, except in certain conditions. In [16,17,19], a researcher without authorization (164.508.b.3.i) would not be able to obtain PHI or psychotherapy notes due to "forbidden_by" and the negative norm; even if the covered entity provided a waiver (164.512.i.1.i) for the researcher to disclose PHI for research purposes. This is due to the conflict between the "forbidden_by", "permitted_by", negative norm and positive norms to resolve an overlapping problem between clauses. In all of the above methods, the denying clause is treated as a "forbidden_by" or negative norm that does not satisfy the "only if" condition. On the one hand, information should be permitted if at least one rule of the "ifs" positive norms satisfies a condition. On the other hand, the information should be permitted if all of the rules in the "only if" negative norms are satisfied. We can conclude that if there is a negative norm, then information will not be released. More precedence is given to the negative norm as compared to the positive norm, because if any one of the negative norms is not satisfied, then it is treated as a denial of releasing information, even if there are some positive norms allowing the disclosure of PHI.

Remember, the discussed example is about a researcher who does not have an authorization, but has a waiver, meaning that there is a negative norm because the research must have an authorization to disclose PHI. As a result, the researcher will not be able to disclose PHI, because one of the negative norms has not been satisfied. Nevertheless, a waiver has precedence over authorization, and the researcher should be able to access PHI. Moreover, nothing in [16,17,19] has been discussed regarding how the output will be generated and what will be the format of the output. Individuals and medical providers preferences were not considered in [16,17,19]. Cross-referencing of clauses in different sections has been handled manually. Table 1 shows the comparison results with other approaches.

Table 1. HIPAA comparison of results with other approaches.

	Considered Items in the Study	A	B	C	D
1	Clauses are linked within the same section	Y	Y	Y	Y
2	Direct cross-references are considered	Y	Y	Y	Y
3	Indicates applied rule as a result of a query	Y	Y	Y	Y
4	Provides the type of action taken as a result of a query	Y	N	Y	Y
5	What information will be released is considered	Y	N	Y	Y
6	Study covers all of the privacy sections of HIPAA	Y	N	N	Y
7	How information will be released is considered	Y	N	N	N
8	Medical relational model for HIPAA	Y	N	N	N
9	Unreferenced information between sections is covered	Y	N	N	N

A: Medical Relational Model; B: 1st Approach [16]; C: 2nd Approach [17]; D: 3rd Approach [19].

5. Conclusions

A methodology to formalize legal text required to build and design MDSS to facilitate the process of exchanging data electronically with the lowest human intervention has been presented. Precise rule generation and information release are what distinguish this work from others. Complex information has been divided into small manageable pieces (tags) to ease the integration process based

on information flow from the requester, information owner and the laws that govern the exchange of the information. For the world rule model (WRM), which required understanding the entire process of splitting complex information and generating the output, pre-processing of the legal text would generate a searchable table that assists in making a more precise decision in disclosing or denying the release of information. We found that missing important factors that might produce less precise decisions is caused by direct formalization of legal text without understanding the big picture. Following our model in formalizing legal text will prevent such an approach and assure producing a more precise decision. There is no formal model in this domain to compare or test result globally, but we have compared our methodology to the related work that has been done on HIPAA, which is shown in Table 1. HIPAA privacy rules are just an example for our experiment.

6. Future Work

In future, our team will work to mature the MDSS application for the Pakistan medical law. In Pakistan, the medical law is not mature, and their is no MDSS available for the medical industry. Dealing with patients and medical service providers' preferences is one important subject, but considering what is released and how it is released is not less important. This will help to exchange the medical information with other medical entities just in one click, keeping in view the patient's privacy for the MDSS, as it will release information in compliance with the law.

Author Contributions: I.K. were involved in drafting the manuscript and made substantial contributions to the conception and design of MRM and WRM for the medical decision support system. M.S. was also involved in drafting the manuscript and revising it critically for important intellectual content. J.I.K. provided his constant guidance on different matters, especially reviewing articles, or the acquisition of data, or the analysis and interpretation of data from HIPAA. H.A.N. worked on understanding the HIPAA rules for the decision support system, to verify the results. A.G. helped in designing and analyzing the algorithm for both the given and proposed approaches to extract information using MRM. M.U.A. helped in the writing of the manuscript and the final revision of the article for grammatical mistakes. S.M.S. reviewed different articles critically, not only for algorithm analysis, but also for the quality of the writing.

Conflicts of Interest: There have been no involvements that might raise the question of bias in the work reported or in the conclusions, implications or opinions stated. The authors declare that they have no conflict of interest.

References

1. O'Neill, A. An action framework for compliance and governance. *Clin. Gov. Int. J.* **2014**, *19*, 342–359.
2. Breaux, T.D.; Anton, A.I. Analyzing regulatory rules for privacy and security requirements. *IEEE Trans. Softw. Eng.* **2008**, *34*, 5–20.
3. Breaux, T.D. Legal Requirements Acquisition for the Specification of Legally Compliant Information Systems; Ph.D. Thesis, North Carolina State University, Raleigh, NC, USA, 2009.
4. Maxwell, J.C.; Anton, A.I.; Swire, P.; Riaz, M.; McCraw, C.M. A legal cross-references taxonomy for reasoning about compliance requirements. *Requir. Eng.* **2012**, *17*, 99–115.
5. Otto, P.N.; Antón, A.I. Addressing legal requirements in requirements engineering. In Proceedings of the 15th IEEE International Conference on Requirements Engineering, RE '07, Delhi, India, 15–19 October 2007; pp. 5–14.
6. Massey, A.K.; Otto, P.N.; Hayward, L.J.; Antón, A.I. Evaluating existing security and privacy requirements for legal compliance. *Requir. Eng.* **2010**, *15*, 119–137.
7. Maxwell, J.C.; Antón, A.I. The production rule framework: Developing a canonical set of software requirements for compliance with law. In Proceedings of the 1st ACM International Health Informatics Symposium, Arlington, VA, USA, 11–12 November 2010; pp. 629–636.
8. Alshugran, T.; Dichter, J.; Rusu, A. Extending XACML to express and enforce laws and regulations privacy policies. In Proceedings of the 2015 IEEE Long Island Systems, Applications and Technology Conference (LISAT), Farmingdale, NY, USA, 1 May 2015; pp. 1–5.
9. Hodge, J.G. Health information privacy and public health. *J. Law Med. Ethics* **2003**, *31*, 663–671.

10. Medical Privacy, U.S. Department of Health and Human Services. *National Standards to Protect the Privacy of Personal Health Information*; Office for Civil Rights: Washington, DC, USA, 2000. Available online: http://www.hhs.gov/ocr/hipaa/finalreg.html (accessed on 12 August 2014).

11. HIPAA Administrative. *45 CFR, Parts 160, 162 and 164*; Department of Health and Human Services, Office for Civil Rights: Washington, DC, USA, 2009. Available online: http://www.hhs.gov (accessed on 13 August 2014).

12. Breaux, T.D.; Vail, M.W.; Anton, A.I. Towards regulatory compliance: Extracting rights and obligations to align requirements with regulations. In Proceedings of the 14th IEEE International Conference Requirements Engineering, Minneapolis/St. Paul, MN, USA, 11–15 September 2006; pp. 49–58.

13. Wilson, J.F. Health Insurance Portability and Accountability Act Privacy rule causes ongoing concerns among clinicians and researchers. *Ann. Intern. Med.* **2006**, *145*, 313–316.

14. Sherman, D.M. A Prolog model of the income tax act of Canada. In Proceedings of the 1st International Conference on Artificial Intelligence and Law, New York, NY, USA, 1 December 1987; pp. 127–136.

15. Borrelli, M.A. Prolog and the Law: Using Expert Systems to Perform Legal Analysis in the UK. *Softw. Law J.* **1989**, *3*, 687–715.

16. Lam, P.E.; Mitchell, J.C.; Sundaram, S. *A Formalization of HIPAA for a Medical Messaging System*; Springer: Berlin, Heidelberg, Germany, 2009.

17. Maxwell, J.C.; Anton, A.I. Developing production rule models to aid in acquiring requirements from legal texts. In Proceedings of the 17th IEEE International Requirements Engineering Conference, RE '09, Atlanta, GA, USA, 31 August–4 September 2009; pp. 101–110.

18. Maxwell, J.C.; Anton, A.I. *A Refined Production Rule Model for Aiding in Regulatory Compliance*; North Carolina State University: Raleigh, NC, USA, 2010.

19. DeYoung, H.; Garg, D.; Jia, L.; Kaynar, D.; Datta, A. Experiences in the logical specification of the HIPAA and GLBA privacy laws. In Proceedings of the 9th Annual ACM Workshop on Privacy in the Electronic Society, Chicago, IL, USA, 4–8 October 2010; pp. 73–82.

20. Garg, D.; DeYoung, H.; Kaynar, D.; Datta, A. *Logical Specification of the GLBA and HIPAA Privacy Laws*; Carnegie-Mellon University: Pittsburgh, PA, USA, 2010.

21. Li, J.S.; Zhou, T.S.; Chu, J.; Araki, K.; Yoshihara, H. Design and development of an international clinical data exchange system: The international layer function of the Dolphin Project. *J. Am. Med. Inform. Assoc.* **2011**, *18*, 683–689.

22. Takemura, T.; Araki, K.; Arita, K.; Suzuki, T.; Okamoto, K.; Kume, N.; Kuroda, T.; Takada, A.; Yoshihara, H. Development of fundamental infrastructure for nationwide EHR in Japan. *J. Med. Syst.* **2012**, *36*, 2213–2218.

23. Tello-Leal, E.; Chiotti, O.; Villarreal, P.D. Process-oriented integration and coordination of healthcare services across organizational boundaries. *J. Med. Syst.* **2012**, *36*, 3713–3724.

24. Khan, I.; Alwarsh, M.; Khan, J.I. A comprehension approach for formalizing privacy rules of HIPAA for decision support. In Proceedings of the 12th International Conference on Machine Learning and Applications (ICMLA), Miami, FL, USA, 4–7 December 2013; Volume 2, pp. 390–395.