Technical Report 2012-06-01
Internetworking and Media Communications Research Laboratories
Department of Computer Science, Kent State University
http://medianet.kent.edu/technicalreports.html

Quantitative Charting of HIPAA Section 164's Legal Universe Privacy Rules of HIPAA *(Technical Report)*

Imran Khan, Moheeb Alwarsh & Javed I. Khan

Department of Computer Science
Kent State University, Kent, Ohio 44240, USA

imran.khan@iiu.edu.pk | malwarsh@kent.edu | javed@kent.edu

Key Words—HIPAA, Privacy Rules, Formalization, Logical rules set

Abstract

A critical step is how to formalize HIPAA legal text to help machine processing. It's not a trivial task. Because of the complexity of HIPAA text structure, we propose a novel approached based on deeper modeling of HIPAA world. The technique is based on one of the first of its kind- a model of the complete conceptual space (actors/action/decision/constraints) in which the original HIPAA Privacy Acts has been defined in terms of an Entity Relation Action (ERA) model. The clauses of HIPAA legal text is then converted into a logical rule set involving only the elements from this ERA model.

1. Introduction

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 civil rights when sharing patients' medical health information and we will refer to this information as protected health information. Failing in conforming to the HIPAA Act may result in a fine up to $25,000 per year and between 1 to 5 years in prison [2, 3, 4]. HIPAA Administrative Simplification, Regulation Text: 45 CFR Parts 160, 162, and 164 [5] regulate the use and disclosure of personal health information.

HIPAA defines how a *covered entity*- which includes Health Plans, Health Care Clearinghouse, or a Health Care Provider, Hospital, etc. who can share the protected health information in under various circumstances meeting the often conflicting needs of doctors, hospitals, patients, insurers, employers, researchers, and other myriads of health and medical service providers. The law covers *protected health information* that includes all individually identifiable health information that can be transmitted or maintained in electronic or any other kind of media.

The length of law is quite extensive and delves into finance, accounting, amendment rights, and even standards and specification of service such as how the information to be handed over. The complexity of the act itself and the organization of the legal text often make it very difficult for practitioners to determine whether they are in compliance or not [6].

Particularly if we regularized the HIPAA Act it looks very difficult and complex for the inexperienced person due to several reasons. For example the law generally allows protected information to be shared between appropriate entities for the purpose of treatment. However, clause 164.508.a.2 [5], seems to contradict this by stating that "if the protected information is a psychotherapy note then a covered entity, i.e., a health plan, a health care provider or a clearinghouse, must obtain an authorization before disclosure". Thus simple reasoning based on actions allowed by one portion of the law, without accounting for prohibitions in other portions of the law, might provide inaccurate result [7].

The complexity of HIPAA, combined with potentially stiff penalties for violators, has lead physicians and medical centres to withhold information from those who may have a right to it. A review of the implementation of the HIPAA Privacy Rule by the U.S. Government Accountability Office found that health care providers were "uncertain about their legal privacy responsibilities and often responded with an overly guarded approach to disclosing information than necessary to ensure compliance with the Privacy rule [13].

Complying with laws and regulations is challenging, because legal texts contain ambiguities, cross-references to sections of the same or different legal texts, and possibly conflicting definitions and domain-specific terminology [11]. In addition, laws and regulations undergo updates and amendments, requiring software engineers to manage and track these changes [11]. Also, in legal systems implementation of the acts gets refined gradually as its various provisions are tested in contests and courts provides case specific clarifications.

Several studies proposed solutions to formalize HIPAA legal text into some form of logic rule set. In last decades, general attempts have been made to convert legal text into logic rules [14, 15]. More recently there is renewed interest to tackle HIPAA. In [7], the authors examined sections of HIPAA and investigated if Datalog like stratified first order system of logic can be instituted to verify compliance of a medical information release request messages sent by providers. In the process of interpreting the legal text they also observed extensive “conflicts” as well as “anomalies” regarding lack of regulation in HIPAA. The proposed stratified Datalog with limited use of negation technique for ensuring termination and efficiency. Their proposed mechanism combines associated rules in the form of “permitted by” and “forbidden by” where the later has precedence for making a decision. In [1], authors use production rule model to verify HIPAA compliance. They have classified rules to four types; rights, obligations, permissions and definition. The problem with this approach is its deficiencies in resolving overlapping conditions between two obligations. In [12], the authors presented the concept of positive and negative norms to take a decision.

It seems one the basic problem with all the previous approaches is the lack of a clearly defined overall context in which the HIPAA legal Act has been framed. HIPAA- defined in 1996 did not anticipate machine processing and has been defined on the assumption of a domain expert who will be familiar with the general context of the rune.

We attempt to capture and accommodate deeper underlying semantics of the complex aspects of health information sharing, for that approach we have to start one step back. Unlike others we first construct the Entity Relationship Model (ERM) and it includes the entities (actors, and their relationships)- medical entities, records, actions, rights- etc., that defines the semantics of the domain on which the HIPAA Act and their provisions have been laid and structured. Based on the HIPPA World ERM and generated concept categories we convert the corpus of legal texts into a set of logical constraints and actions.

2. LEGAL TEXT TO LOGICAL RULE SET PROCESS

Converting legal text to logics rules set, requires a full understand of how information is processed logically. This would require a conceptual view of how privacy rules of HIPAA Act consists of different data types that need to be integrated in certain way to comply with proper implementation of these rules. To understand how rules are formed logically, pre-processing of legal text for different data types will be discussed in the following sub-sections.

We need to understand how privacy rules structured, interrelated and overlapped. For example, why do we need a law to govern the release, exchange and use of information? What is the purpose of the law? Who is responsible for implementing it? In what conditions can this law be used? What will be the action taken? How to respond to requesters? We can conclude that there are some reasons or purposes for laws and there are some conditions for these purposes. Also, for each condition there is a response and action. In other words, we need to cover all aspects of legal text of privacy rules and create Concept Classes. Each Concept Class will contain related information. Privacy rules of HIPAA Act are divided into different sections and each section contains clauses. For example, clause 164.506.C.1 of privacy rules that belong to section 164.506 stats

“*A covered entity may use or disclose protected health information for its own treatment, payment, or health care* operations”.

We could extract several pieces of information from this clause. For example, a “covered entity” is a requester of information, “treatment, payment or health care operations” are purposes for disclosing protected health information, and “its own” is a pre-condition for using or disclosing protected health information. All requesters are grouped under one Concept Class for this section, conditions and pre-conditions are also grouped in separate Concept Classes.

Based on our understanding of the privacy rules, we found 10 types of Concept Classes and some of these classes available only in certain sections. As a result, we created a generalized version to be used in all privacy rules sections. Whereas, each section of privacy rules of HIPAA act will generate 10 concept classes. Each concept class consist of legal text from different clauses. To distinguish between these clauses in each concept class, we have assigned a tag for each clause, see Table 1.

Tag	Description of Concept Classes
ReqT	**Requester Class**: This class contains tags used to identify requesters (Actor) of information role. For example researcher
PCT	**Pre-Condition Class:** all prerequisites that need to be satisfied before evaluating requests are collected under this class. For example, if authorization is available or not.
PPT	**Purpose Class**: Purposes for disclosing protected health information.
CPT	**Conditional Purpose Class:** All rules for evaluating privacy rules of HIPAA Act with PPT, PCT and ReqT will be under this class.
AT	**Decision Class:** Atomic action that is produced as a result of evaluating each request.
TT	**Time Class:** Time Required for processing a request. For example, protected health information will be released after 30 days to de-identify this information
RRT	**Record Class:** Information that will be released as a result of a request.
IPT	**Information Procedure Class:** Rule to Inform how information will be release. For example information will be released with a fee that needs to be paid.
FT	**Fee Class:** Rules that identify non-free to release protected health information.
PRI	**Patient Record Item Class:** Medical and none medical records related to patients.

Table. 1. Concept class description

3. ER Model with Concept Space of Hipaa

To make a relationship between tags in concept classes for each section, we need to create entity relationship diagram to connect these concept classes together based on how information logically flow. Each request for disclosing protected health information must conform to this diagram, see Figure 1.

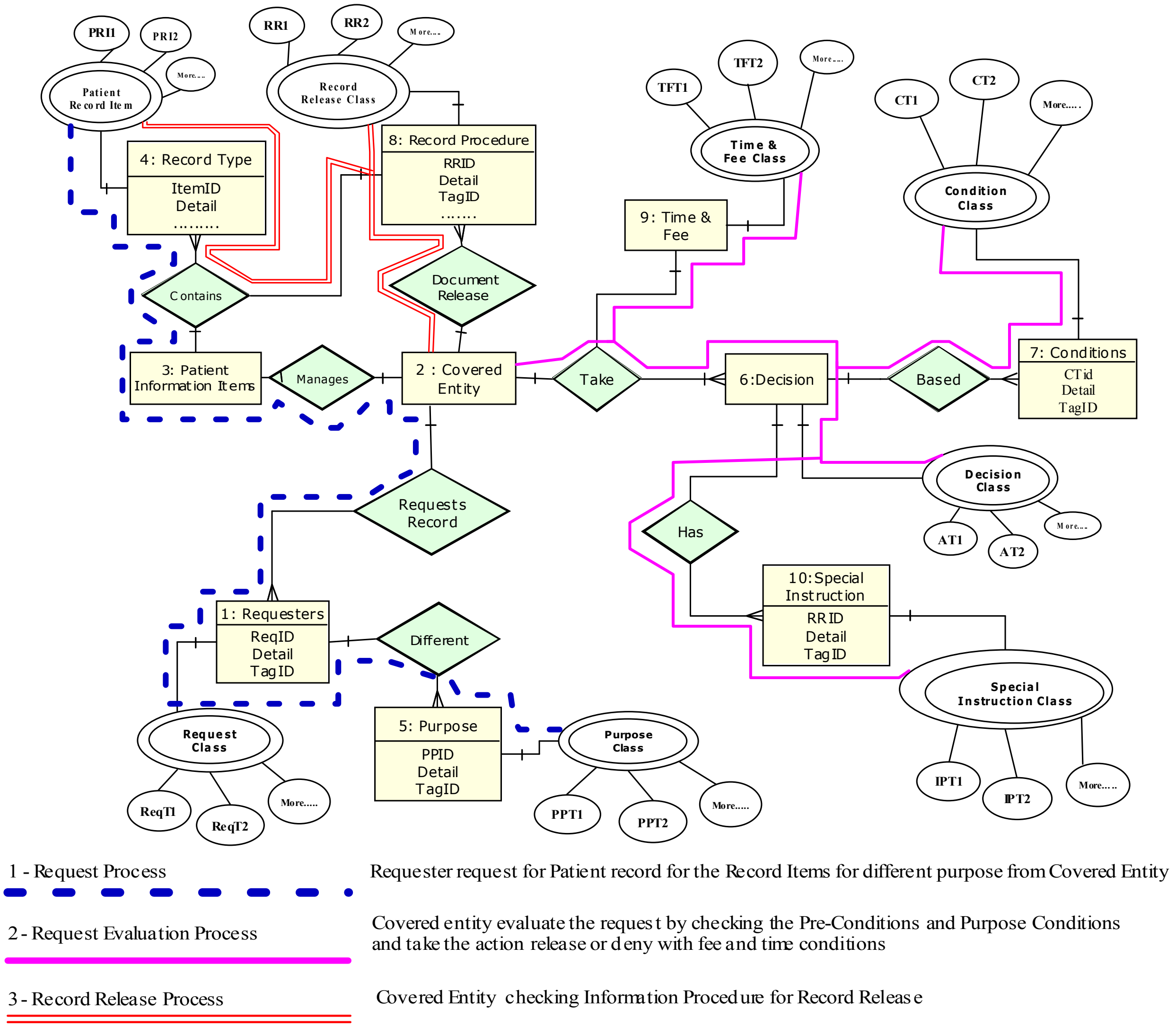
By analysing HIPAA privacy rules [5], we classified the workflow of disclosing PHI into 8 elementary concept classes named (Requestor, Purpose, Patient Record Item (like HIV, psychotherapy notes, etc.), Condition, Action, Information Procedure, Record Release, Time & Fee class). For example, clause 164.506.c.1 (1) states that;

"A covered entity may use or disclose protected health information for its own treatment, payment, or health care operations".

This clause has a requester of PHI which is a covered entity, purposes for disclosing PHI (treatment, payment or health care operations) and condition (disclose only if the PHI is used by the covered entity). In this example we could extract three types of information; requester, purpose, condition. We assign an id or tag to each requester, purpose, condition and add them to the concept classes.

Making a relation between these concepts classes requires some sort of associations. We created three functional processes (FP) on which the privacy rules of HIPAA is scoped. "Request Flow FP" consists of request (1), purpose (5) and patient record item (4) classes. The second FP is "Evaluation" and it composed of "Request Flow FP", time & fee (9), decision (6), condition (7) classes and special instructions (10). Finally, "Release FP" consists of record release class (8), "Evaluation FP" and patient record item. To understand the relation between these classes, we created and ER diagram that explains how a request is handled in HIPAA world, see Figure 1.

Example, if a researcher wants to disclose protected health information, he/she would first initiate a request (1) to a covered entity (2). The request must at least contain requester information (1), required PRI (4) and the purpose of the request (5). Covered entity (2) will take a decision (6) based on the provided information against HIPAA conditions (7) and assign special instruction (10) for each decision. Generated decision will be associated with special instructions for how information will be released (10) and what will be released (8) which will be applied on released PRI (4).



1 - Request Process — Requester request for Patient record for the Record Items for different purpose from Covered Entity

2 - Request Evaluation Process — Covered entity evaluate the request by checking the Pre-Conditions and Purpose Conditions and take the action release or deny with fee and time conditions

3 - Record Release Process — Covered Entity checking Information Procedure for Record Release

Figure.1. Entity Relation Diagram for HIPAA Privacy Rules

The figure 2 shows flow of information in the usual healthcare system. Patient medical records could be used for various purposes, not only for the diagnosis and treatment facility, that can be used for the efficiency and improvement within the healthcare system, for making the public related policies, to conduct survey and research for the advancement in medical science [18]. Patient's records also be shared between the payers of patient, such as Insurance companies, Medicaid or Medicare for the justifications of payment related services that done by the physicians. Healthcare providers may also use the records to manage their operations, for the service quality. Health care providers share information with the regional health information organization. Medical related information also used by the government for the public health management, medical research, hospital certification, for the social and welfare system management. Actors in HIPAA are involved in this flow of information.

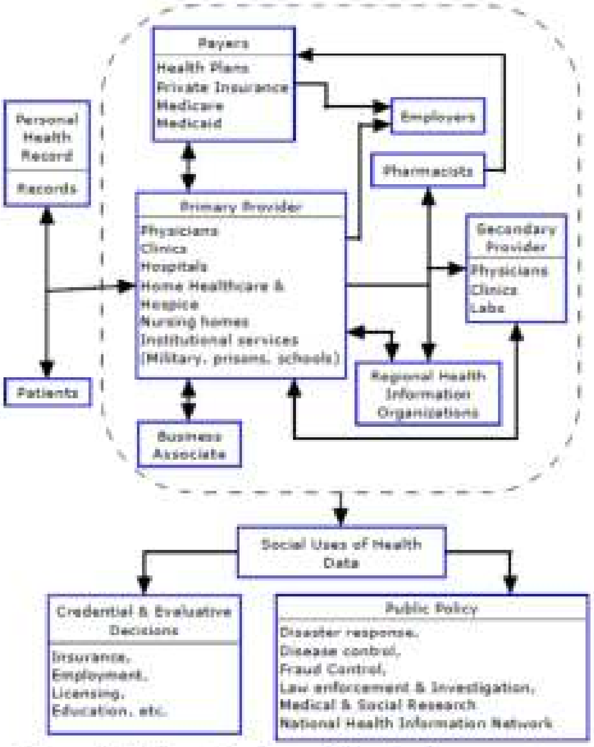


Figure.2. Information flow in the healthcare system

4. Actors/Requester in HIPAA

There are number of actors in HIPAA that participate in different kind of activities, each actor have a distinct role and purpose according to the regulations of HIPAA. These actors play a specific role in HIPAA as they are connected directly and indirectly. If we see this world we find that there are different kind of laws, so why we need these laws? To answer this question we can say that all the participants in that specific law have to do their work in some kind of purpose under some kind of conditions. These participates are may be the organizations or individual. So if we see in the depth of HIPAA rules we find that there are different kinds of actors involve for who the HIPAA rules are made. Like Hospital, Health Plan Provider, Insurance Company, Patients, Doctors, Nurses, Law Enforcement Agencies and many more. If we see the HIPAA rules all are related to these actors having to do their work with some purposes and conditions, these actors are communicating with each other according to some conditions for some purpose.

The definition of Actors/Stakeholders can be observed from HIPAA in 160.103, 164.500 and 164.501. The role related to these Actors can be observed from HIPAA in 164.502 to 164.532. Each box in figure.3 represents an

Actor or Stakeholder and arrows point from sub-classes to super-classes. The color boxes show that actors appeared in the subject and target properties of rules but did not appear in the definitions. For particular Actor/Stakeholder, to determine what legal requirements are applied in a specified situation to evaluate rules that apply for the classifications of that stakeholder. For example, a "Group Health Plan" have to consider rules that directly apply to their stakeholder class and rules, the domain which defines a stakeholder hierarchy that includes the covered entity (CE), the health plan (HP), the group health plan (GHP) and the healthcare provider (HCP). As shown in figure 3.a, 3.b and 3.c. The figure .3.a, b, c shows the maximum no. of actors that are involve in HIPAA. The rules related to these actors are present in different part of sections of HIPAA and all the actors are connected with each other directly or indirectly.

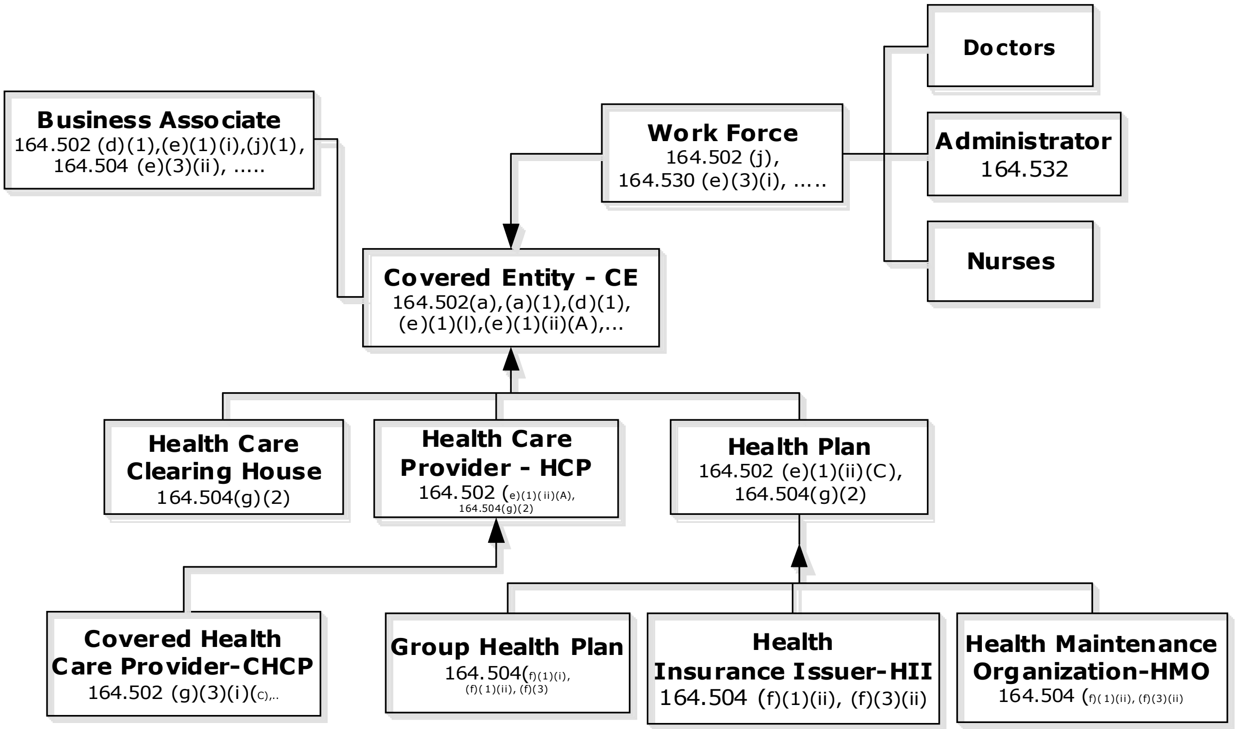

Doctors
Business Associate
164.502 (d)(1),(e)(1)(i),(j)(1),
164.504 (e)(3)(ii), ...
Work Force
164.502 (j),
164.530 (e)(3)(i), ...
Administrator
164.532
Nurses
Covered Entity - CE
164.502(a),(a)(1),(d)(1),
(e)(1)(l),(e)(1)(ii)(A),...
Health Care Clearing House
164.504(g)(2)
Health Care Provider - HCP
164.502 (e)(1)(ii)(A),
164.504(g)(2)
Health Plan
164.502 (e)(1)(ii)(C),
164.504(g)(2)
Covered Health Care Provider-CHCP
164.502 (g)(3)(i)(c),..
Group Health Plan
164.504(f)(1)(i),
(f)(1)(ii), (f)(3)
Health Insurance Issuer-HII
164.504 (f)(1)(ii), (f)(3)(ii)
Health Maintenance Organization-HMO
164.504 (f)(1)(ii), (f)(3)(ii)

Fig. 3.a Hierarchy in Actors of HIPAA

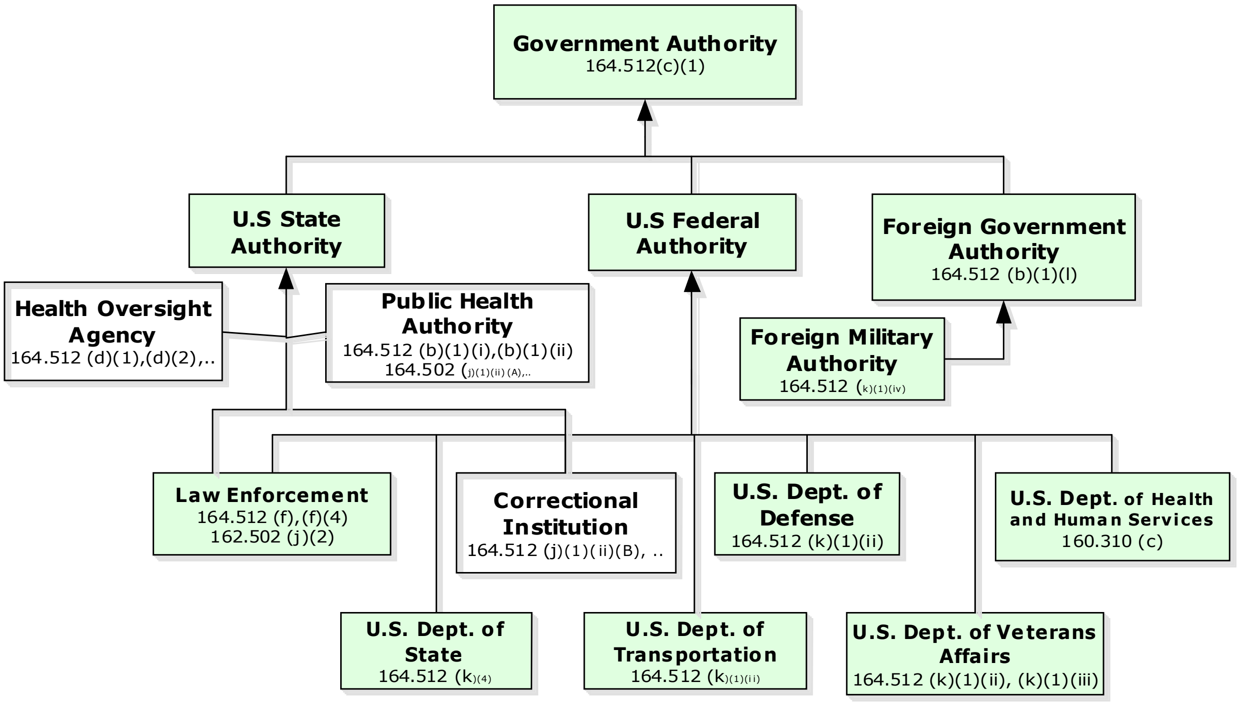


Fig. 3.b Hierarchy in Actors of HIPAA

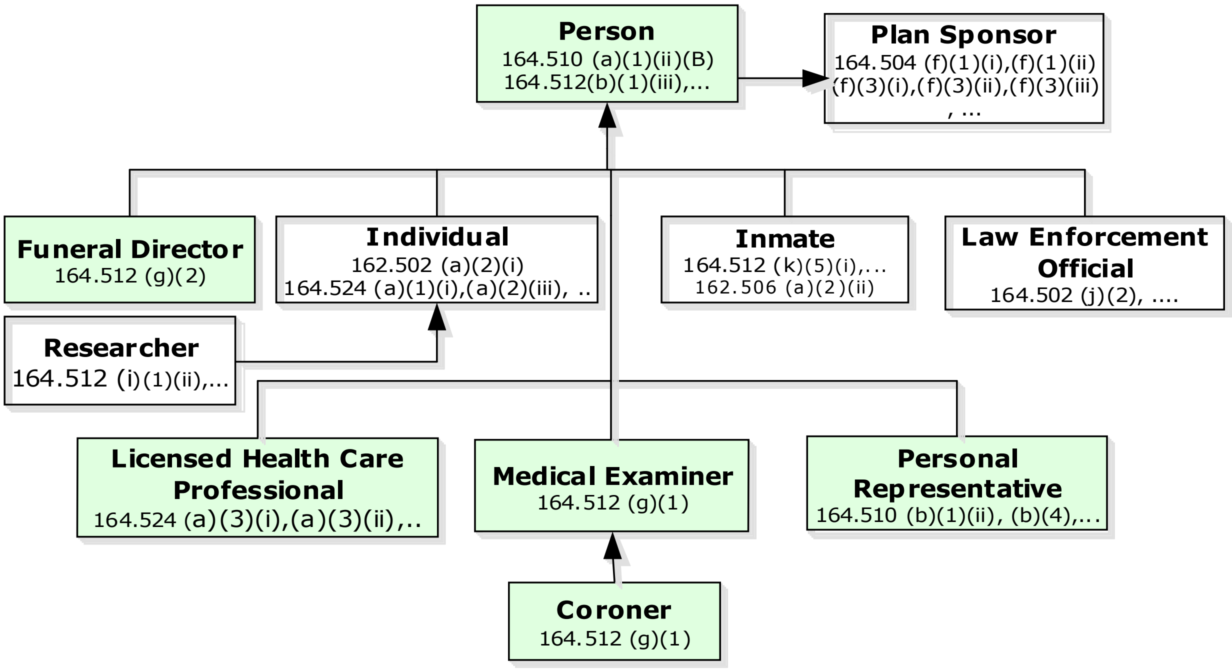


Fig. 3.c Hierarchy in Actors of HIPAA

These actors/requesters are communicating with each other on some conditions for some purpose. If one actor wants to request for some kind of information from other, after checking the purpose and conditions that actor will take an action and send the response as output to another actor who sends the request. The high level flow of information according to HIPAA rules for actor is show in figure.4.

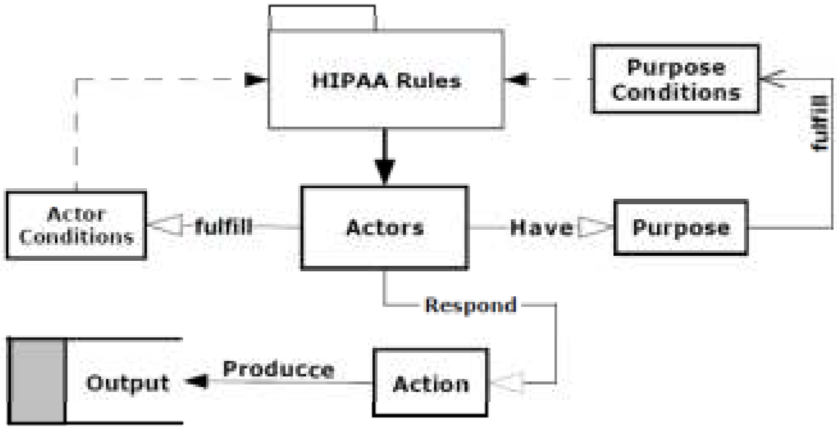


Figure. 4. Actor's rules information flow

The rules that defined in HIPAA are explained the actors responsibilities, purpose, condition and actions. All the rules are placed in different sections of HIPAA, if we want to find the rules related to one actor, we have to check all the sections of HIPAA. For example there are many rules in on section of HIPAA that are referring to other section of HIPAA for the same actor then it's easy to relate that rule with that particular actor. But there are some rules that are not referred by the rule but these rules are important and they are in different section for that particular actor.

The purpose for which data me be required for action is very important, because these purposes have ever more issues which are very important for the information security [8, 9, 16]. Usually the Role Based Access Control System [17], actors/stakeholders are allowed or denied to get the information which is related their job function that they perform is call as roll. These rolls are basically assigned to the Users/Actors where purposes are related to the data that is used for kind of transaction. For example if and Actor wants to access the data must have to imply data purpose (data used for what) so purposes are as the constraint with actors subject and the targeted objective.

HIPAA complexity increases very much as there are many types of purposes for the data, and these purposes are constrained with the Actors request. For each purpose it has to classify that the specific actor is eligible for that purpose or not. The example of purposes in HIPAA is as *Treatment, Payment, Health care operations, Health care fraud, Abuse detection, Compliance, Billing, Access and Amendment* etc. All these purposes are related to different Actors. For normal request in HIPAA according to Figure 1 have to fallow the different steps for the response.

Step 1: Check from the list of Actor/Requester who is requesting. i.e. **ReqT**

Step 2: Check what are the purposes of the Actor from the list of Purposes. i.e. **PPT**

Step 3: Check for the requested Patient Record Item (PRI) from the list of PRI. i.e. **PRI**

After step 3 for further processing we need to process the request according to given information, first of all verify that the requester is eligible of that purpose for which data is requested, then for that purpose the requested PRI are need or not, then to verify between Actor and PRI are accessible. To verify any of PRI conditional and the actor is fulfilling that condition. For processing we have the no. of comparison required. i.e. ***ReqT * PPT * PRI***

Step 4: Check from the list of Conditions that are applied on actors who is requesting. i.e. **CT** so the complexity increases as i.e. ***ReqT * PPT * PRI * CT***

Step 5: Check what the possible action is taken according to fee and time constraint for that Purposes.

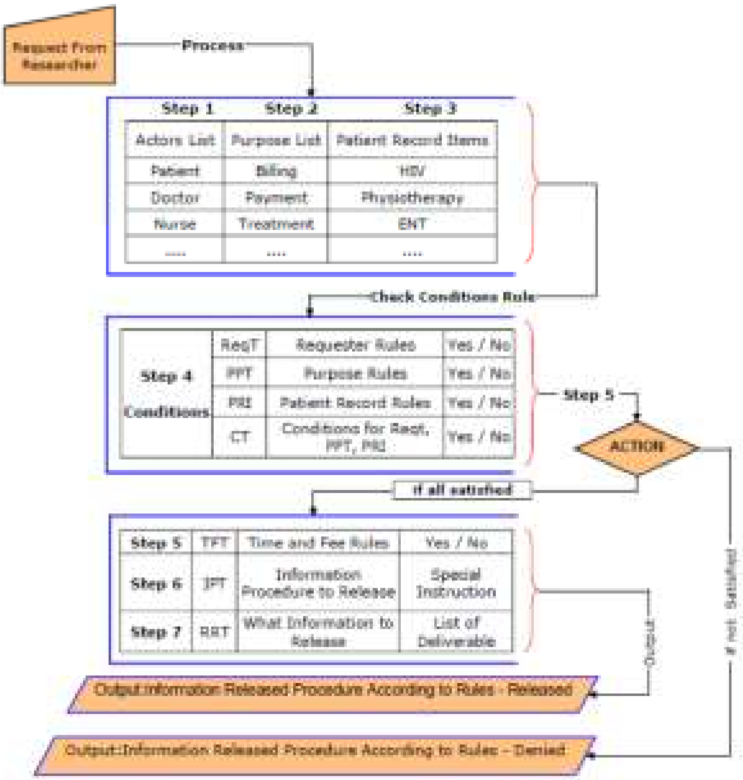
i.e. **AT * TFT**

so ***ReqT * PPT * PRI * CT + (AT * TFT)***

Step 6: Check for the Special Instruction how to Release the record from the list of Information Procedure. i.e. **IPT**

Step 7: Check for the Record Release what to Release from the list of Record Release Procedure. i.e. **RRT.** Finally the complexity of comparison for generating the response can presented as below in equation and flow chart in figure.5.

(ReqT * PPT * PRI * CT + (AT * TFT)) * IPT * RRT


Request From Researcher
Process
Check Conditions Rule
Step 5
ACTION
if all satisfied
Output
if not Satisfied
Output:information Released Procedure According to Rules - Released
Output:Information Released Procedure According to Rules – Denied

Step 1	Step 2	Step 3
Actors List	Purpose List	Patient Record Items
Patient	Billing	HIV
Doctor	Payment	Physiotherapy
Nurse	Treatment	ENT
.....	....	....

Step 4 Conditions	ReqT	Requester Rules	Yes / No
	PPT	Purpose Rules	Yes / No
	PRI	Patient Record Rules	Yes / No
	CT	Conditions for Reqt, PPT, PRI	Yes / No

Step 5	TFT	Time and Fee Rules	Yes / No
Step 6	IPT	Information Procedure to Release	Special Instruction
Step 7	RRT	What Information to Release	List of Deliverable

Figure.5. Request flow for verification with HIPAA rules

5. References

[1] Maxwell, J.C., Annie I. Anton, "Developing Production Rule Models to Aid in Acquiring Requirements from Legal Texts", Proc. of the 17th Intl. IEEE Requirements Engineering Conf., Atlanta, 2009, pp. 101-110

[2] As Office for Civil Rights (2003) Summary of the HIPAA privacy rules.http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf

[3] https://www.privacyrights.org/fs/fs8a-hipaa.htm

[4] http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html

[5] "HIPAA Administrative Simplification 45 CFR Parts 160, 162, and 164", U.S. Department of Health and Human Services, Office for Civil Rights, 2006 http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/adminsimpregtext.pdf

[6] Roberta B. Ness. A year is a terrible thing to waste: early experience with HIPAA. Annals of Epidemiology, 15(2):85-86, 2005.

[7] Peifung E. Lam, John C. Mitchell & Sharada Sundaram, "A Formalization of HIPAA for a Medical Messaging System". Stanford University, Stanford, CA. Lecture Notes in Computer Science, 2009, Volume 5695/2009, 73-85, http://www.springerlink.com/content/e6281457716k0128/

[8] P. Ashley, S. Hada, G. Karjoth, and M. Schunter. E-p3p privacy policies and privacy authorization. In Proc. ACM Workshop on Privacy Electronic Society, pages 103–109, Alexandria, Virginia, 2002. ACM Press.

[9] P. Ashley, C. Powers, and M. Schunter. From privacy promises to privacy management: A new approach for enforcing privacy throughout the enterprise. In Proc. New Security Paradigms Workshop, pages 43–50, Virginia Beach, Virginia, 2002. ACM Press.

[10] T.D. Breaux, Annie.I. Antón, "Analyzing Regulatory Rules for Privacy and Security Requirements", IEEE Trans. on Software Engineering, 34(1), Jan.-Feb. 2008, pp. 5-20.

[11] P.N. Otto, Annie I. Antón, "Addressing Legal Requirements in Requirements Engineering", Proc. of the 15th IEEE International Requirements Engineering Conference, New Delhi, 2007, pp. 5-14.

[12] H.DeYoung, D. Garg, L. Jia, D. K. Kaynar, and A. Datta. Experiences in the logical specification of the HIPAA and GLBA privacy laws. In WPES, pages 73–82, 2010.

[13] Wilson J (2006). "Health Insurance Portability and Accountability Act Privacy rule causes ongoing concerns among clinicians and researchers". Ann Intern Med 145 (4): 313–6. PMID 16908928.

[14] D. M. Sherman. A prolog model of the income tax act of Canada. In ICAIL '87: Proceedings of the 1st international conference on Articial intelligence and law, pages 127{136, 1987.

[15] Marc A. Borrelli. Prolog and the law: using expert systems to perform legal analysis in the United Kingdom. Softw. Law J., 3(4):687, 715, 1990.

[16] J-W. Byon, E. Bertino, and N. Li. Purpose-based access control of complex data for privacy protection. In 10th ACM Symposium on Access Control Models and Technologies, pages 102–110, Stockholm, Sweden, 2005. ACM Press.

[17] R.S. Sandhu, E.J. Coyne, H.L. Feinstein, and C.E. Youman. Role-based access control models. IEEE Computer, 29(2):38–47, 1996.

[18] Hodge, J.G. (2003) —Health Information Privacy and Public Health, Journal of Law, Medicine & Ethics, vol.31, no.4, pp 663-671