Technical Report 2013-06-01
Internetworking and Media Communications Research Laboratories
Department of Computer Science, Kent State University
http://medianet.kent.edu/technicalreports.html

Kent State University

# Decision System for Evolutionary Edict: Rule Set for A HIPAA Privacy Laws

CS89098- Research

**Student:** Nahla Abid

**Advisor:** Dr. Javed I. Khan

**Date:** 05/02/2013

Technical Report 2013-06-01
Internetworking and Media Communications Research Laboratories
Department of Computer Science, Kent State University
http://medianet.kent.edu/technicalreports.html

# Decision System for Evolutionary Edict: Rule Set for HIPAA Privacy Laws

**Nahla Abid**
Department of Computer Science, Kent State University
nabid@kent.edu

**Advisor:**
Dr. Javed Khan, javed@kent.edu

## Abstract

Health Insurance Portability and Accountability Act (HIPAA) defines privacy rules of using and disclosing health data according to the government regulations and policies. To ensure HIPAA compliance of such policies, there is a need for an enforcement mechanism. However, the privacy rules defined in HIPAA has to be well-analyzed and defined. In this paper, the "Law enforcement purposes" section from HIPAA is demonstrated on varies presentations for automated verification of HIPAA compliance. The first proposed method is flowchart with an extra node to resolve ambiguity. The second equivalent presentation is written in Prolog. User request can be verified to make the disclosure decision.

## 1. Introduction

The HIPAA Privacy Rule provides federal protections for personal health information held by covered entities. The Privacy Rule permits the disclosure of personal health information needed for patient care and other important purposes such as law enforcement purposes or research demands [2].

HIPAA privacy rules are expressed in complex interdependencies with different level of abstraction [7], making them hard to understand, predict, and control [8]. Therefore, the privacy rules may be misinterpreted which may lead to unauthorized disclosure. That raises the demand to develop a mechanism for enforcing HIPAA law. To assure the correct interpretation of HIPAA privacy rules, the disclosure and use scenarios have to be well-analyzed.

Our work involves a detailed analysis of two sub-sections of HIPAA privacy rules by extracting objects and related conditions needed to make a disclosure decision for law enforcement purposes. Such analysis also involves developing the entity relationship model, drawing flowchart, and implementing decision system using Prolog. Moreover, three examples and scenarios of law enforcement purposes are demonstrated.

The organization of the paper is as the following. Section two explains some of HIPAA vocabularies that used in this paper. Section three to section six demonstrate the analysis of 164.512 (f) and (c) from HIPAA while section seven includes related works. Section eight provides the conclusion and future work.

## 2. HIPAA vocabulary [1] [2]

**Individual** means the person who is the subject of protected health information.

**Covered entity** means:

1. A health care provider: a provider of medical or a health service which includes Doctors, Clinics, Psychologists, Dentists, Chiropractors, Nursing Homes, or Pharmacies.
2. A health plan includes: Health insurance companies, HMOs, Company health plans, and Government programs that pay for health care, such as Medicare, Medicaid, and the military and veterans health care programs
3. A health care clearinghouse includes entities that process nonstandard health information they receive from another entity into a standard (i.e., standard electronic format or data content), or vice versa.

**Disclosure** means the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information.

**Protected Health information** means any information, whether oral or recorded in any form or medium, that:

1. Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
2. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

**Required by law**: it includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

## 3. Disclosure for law enforcement purposes

Two sub-sections were selected from HIPAA privacy rules to be analyzed. Because the goal of this analysis is to focus on a complete unit that stands alone, section 164.512 (f) is chosen to be examined. 164.512 (f) explains situations where a covered entity is allowed to disclose protected health information to a law enforcement official. 164.512 (f) contains six cases which are: required by law, identification purposes, victim of a crime, decedents, crime on premises, and reporting a crime in emergencies. A detailed explanation of all cases is provided later in the document. However, case (f) (6) "reporting a crime in emergencies" requires testing case 164.512(c) first. Therefore, section 164.512 (c) is included in our work.
In our analysis, we used the following terms:

**Initiator:** the disclosure could be initiated by the covered entity or as a respond to a law enforcement official request.

**Receiver:** the receivers of the protected health information are law enforcement official, or public authority including social service or protective services agency. Table 1 displays the possible disclosure initiators and receivers.

**Case:** in this study, we shall discuss seven main cases that allow a covered entity to disclose protected health information. Table 2 includes a list of all cases related to law enforcement purposes.

**Individual Notification:** in some cases, covered entity has to notify the individual about the disclosed PHI. The individuals or their relatives may be informed about the disclosure.

| **Element** | | | **Explanation** |
|---|---|---|---|
| Individual | dead | | |
| | alive | Capacity | Means that the individual is able to make a decision. |
| | | Incapacity | Means that the individual is unable to make a decision. (ex. unconscious) |
| Disclosure initiator | Covered entity | | |
| | Third party | Individual | The patient |
| | | LEO | Law Enforcement Official |
| | | Court-ordered warrant or grand jury subpoena | |
| | | Administrative request | Including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law. |
| Receiver | LEO | | |
| | Public authority | social service | |
| | | protective services agency | |

Table 1: Disclosure for Law Enforcement purposes

### 3.1. The seven cases were grouped based on the disclosure initiator:

- **Group1:** Required to be disclosed by Law.
  It is the group of cases that requires the disclosure to be made to LEO because of court-ordered warrant, grand jury subpoena, or administrative request. It also includes reporting certain type of injuries to LEO. Group 1 in flowchart reflects case 164.512 (f) (1) from HIPAA.

- **Group2:** Can be initiated by the covered entity or law enforcement official.
  PHI can be either requested by law enforcement official or reported directly by the covered entity without a request. Group 2 reflects case decedents 164.512 (f) (4), crime on promises 164.512 (f) (5), reporting crime on emergences 164.512 (f) (6), and reporting a victim of abuse, neglect, and domestic violence 164.512 (c) from HIPAA.

- **Group3**: requires law enforcement official request.
  The disclosure of PHI can be made in a response to law enforcement official's request only. Group 3 reflects case limited information for identification purposes 164.512 (f) (2), and a victim of a crime 164.512 (f) (3) from HIPAA. Table 2 presents three groups and their associated cases.

| Group# | Cases | Explanation |
|---|---|---|
| **Group1** | Required by Law | Reporting of certain types of wounds or other physical injuries [1]. |
| | Court order | Court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer [1]. |
| | Subpoena | A grand jury subpoena [1]. |
| | An administrative request | Including an administrative subpoena or summons [1]. |
| **Group2** | Decedents | Alerting law enforcement of the death of the individual if the CE has a suspicion that such death may have resulted from criminal conduct [1]. |
| | Crime on promises | A CE may disclose PHI to a LEO that the CE believes in good faith constitutes evidence of criminal conduct that occurred on the premises of the covered entity [1]. |
| | Reporting crime on emergences | A health care provider may disclose PHI if such disclosure appears necessary to alert law enforcement to: the commission and nature of a crime, the location of such crime or of the victim(s) of such crime; and the identity, description, and location of the perpetrator of such crime [1]. |
| | reporting a victim of abuse, neglect, and domestic violence | A CE may disclose PHI about an individual whom the covered entity reasonably believes to be a victim of abuse, neglect, or domestic violence to a government authority authorized by law to receive such a report [1]. |
| **Group3** | Limited information for identification purposes | A CE may disclose PHI in response to a LEO's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person [1]. |
| | A victim of a crime | A CE may disclose PHI in response to a LEO's request for such information about an individual who is or is suspected to be a victim of a crime, other than disclosures that are subject to section 164.512 (c) " Reporting a victim of abuse, neglect, or domestic violence" [1]. |

Table 2: The three groups and their associated cases

## 4. Entity Relationship Model

Entity relationship model is used to presents the relationship between objects and roles in HIPAA. Objects and classes are characterized with rectangle and actions with diamond as shown in figure1. ERM is necessary to indentify the objects that used to design flowchart and Prolog code. At this point, our entity relationship presents the disclosure for law enforcement purposes and can be expanded to cover all disclosure and using purposes allowed by HIPAA.

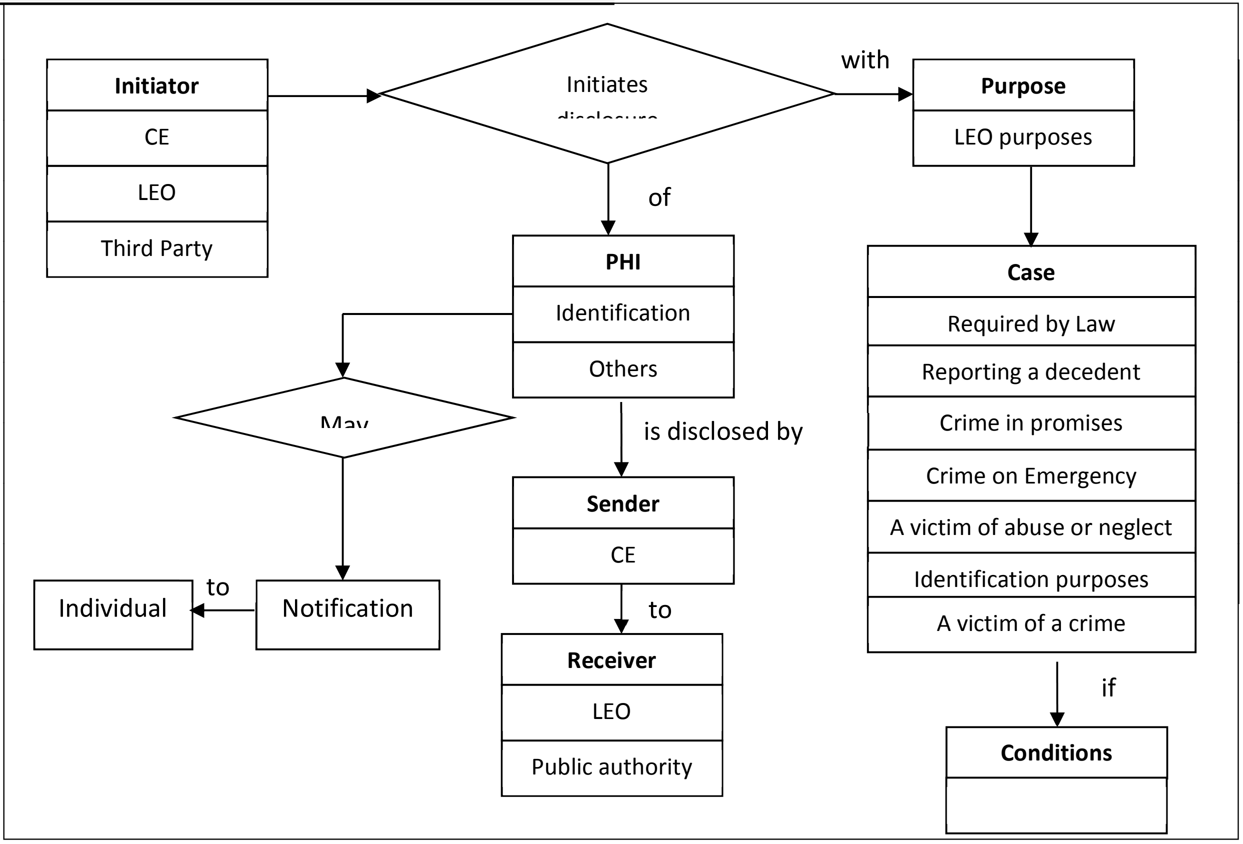


Figure 1: Entity Relationship Model

## 5. Flow Chart

The privacy rules from 164.125 in HIPAA are presented using Flowchart to help visualize and understand the process of decision making. Flowcharts are graphical representations of complex process that provides visual maps of correct behavior. The flow chart presentation allows the ordering of the law enforcement cases to assure that correct decision is extracted from the chart. For example, "a victim of abuse" case should be checked before "a victim of a crime" case because the second one is more general. "Child being abused" is also "being a victim of a crime" but both cases have different conditions to check.

Moreover, we proposed to add additional nodes to address ambiguity in HIPAA. An example of such a case is "Reporting crime on emergences." Based on the way that three conditions were written, HIPAA requires that the disclosure has be necessary to alert LEO to the nature of the crime, the location of such crime or victim(s), and the identity of the perpetrator. However, it seems that if such a disclosure may help to determine one of this information, it would be better to disclose. Therefore, the combined conditions need to be written in a clearer to way to be correctly interpreted.

The extra node is added before the "and" condition is checked. It shows where the conflict occurs and the right path with "or" condition is colored as shown in figure2 Part D. This mechanism not only helps to highlight the ambiguity, but also keep track of the old conditions and save the history of rules. Because the flowchart is large in size, it is divided in to six pages. The end point in one page is marked with a numbered triangle which also indicates the start point in the next page.

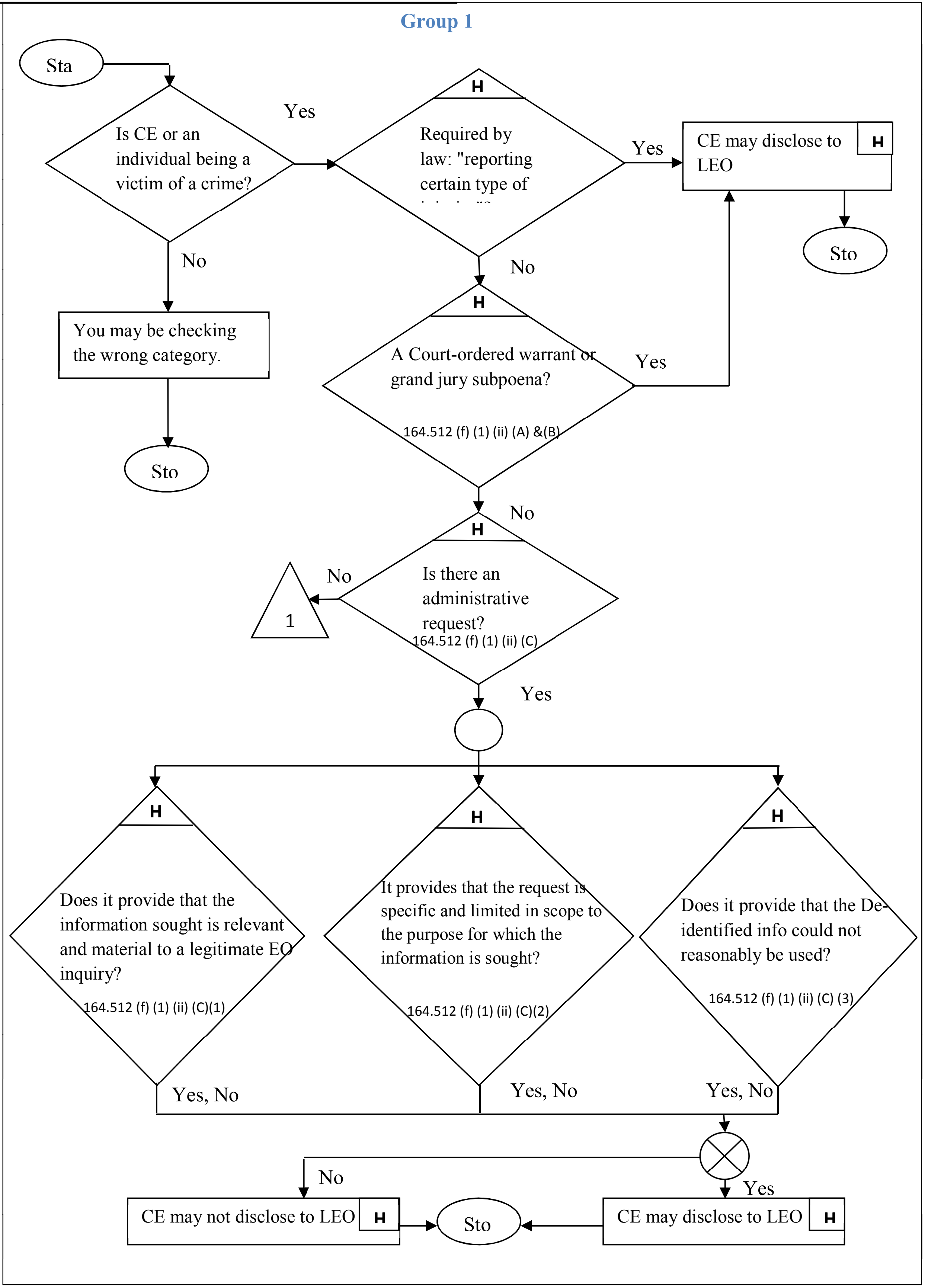

Group 1
Sta
Is CE or an individual being a victim of a crime?
Yes
No
You may be checking the wrong category.
Sto
H
Required by law: "reporting certain type of
Yes
CE may disclose to LEO
H
Sto
No
H
A Court-ordered warrant or grand jury subpoena?
164.512 (f) (1) (ii) (A) &(B)
Yes
No
H
Is there an administrative request?
164.512 (f) (1) (ii) (C)
No
1
Yes
H
Does it provide that the information sought is relevant and material to a legitimate EO inquiry?
164.512 (f) (1) (ii) (C)(1)
Yes, No
H
It provides that the request is specific and limited in scope to the purpose for which the information is sought?
164.512 (f) (1) (ii) (C)(2)
Yes, No
H
Does it provide that the De-identified info could not reasonably be used?
164.512 (f) (1) (ii) (C) (3)
Yes, No
No
CE may not disclose to LEO
H
Sto
Yes
CE may disclose to LEO
H

Figure 2: The Flow chart – Part A

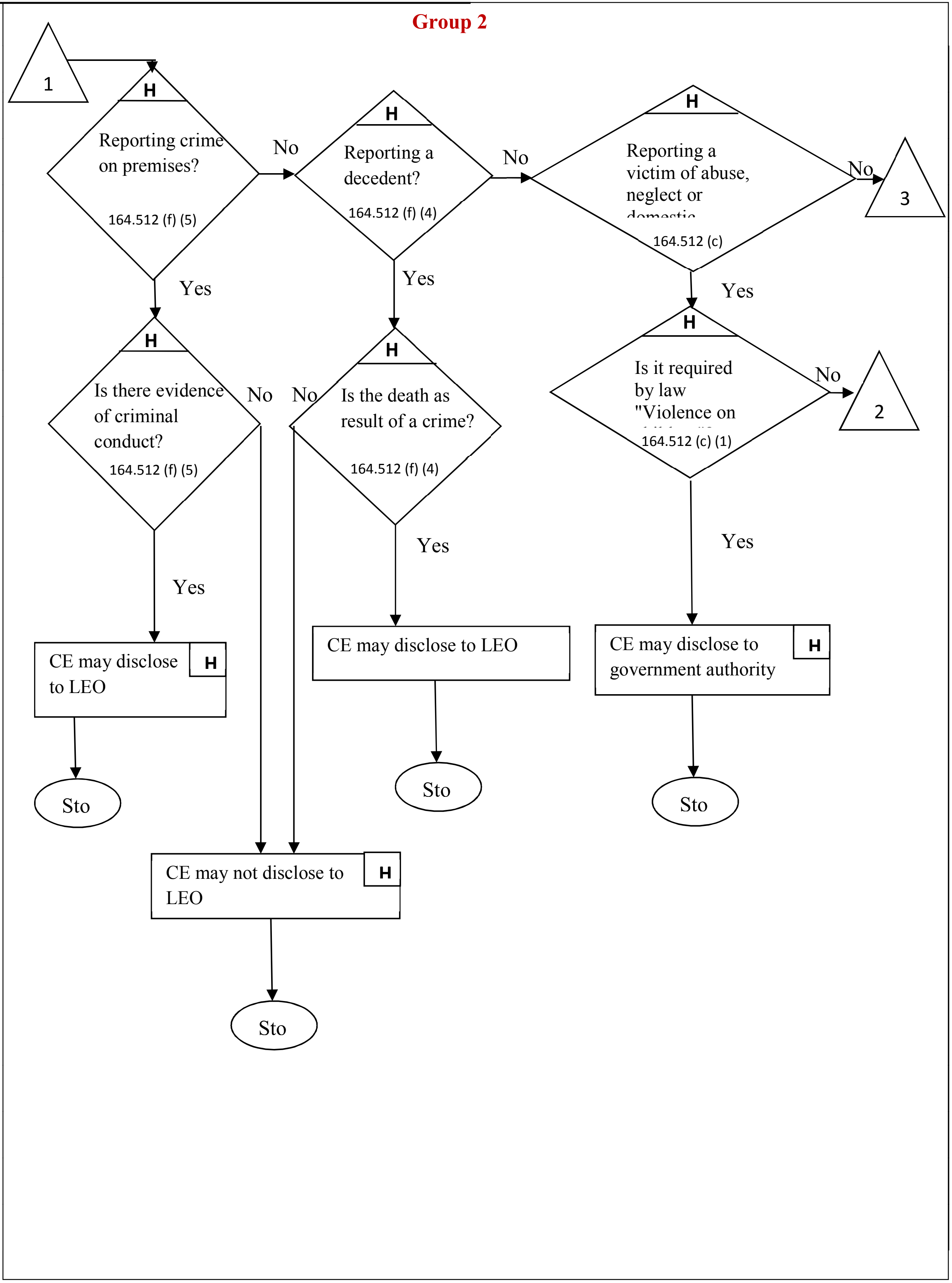

Group 2
1
H
Reporting crime on premises?
164.512 (f) (5)
No
H
Reporting a decedent?
164.512 (f) (4)
No
H
Reporting a victim of abuse, neglect or domestic
164.512 (c)
No
3
Yes
Yes
Yes
H
Is there evidence of criminal conduct?
164.512 (f) (5)
No
No
H
Is the death as result of a crime?
164.512 (f) (4)
H
Is it required by law "Violence on
164.512 (c) (1)
No
2
Yes
Yes
Yes
CE may disclose to LEO
H
CE may disclose to LEO
CE may disclose to government authority
H
Sto
Sto
Sto
CE may not disclose to LEO
H
Sto

Figure 2: The Flow chart – Part B

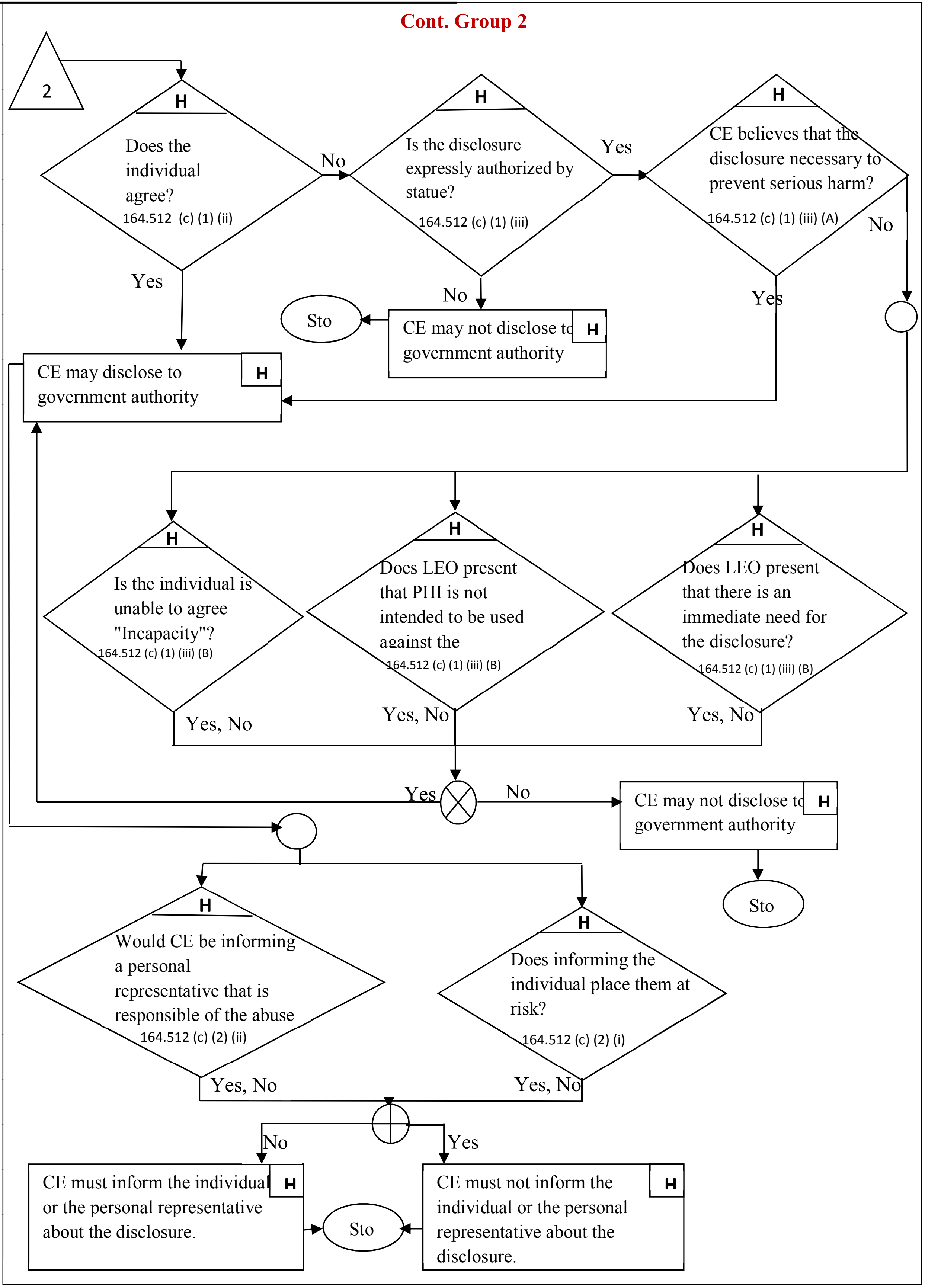

Cont. Group 2
2
H
Does the individual agree?
164.512 (c) (1) (ii)
No
Yes
H
Is the disclosure expressly authorized by statue?
164.512 (c) (1) (iii)
Yes
No
H
CE believes that the disclosure necessary to prevent serious harm?
164.512 (c) (1) (iii) (A)
No
Yes
Sto
CE may not disclose to government authority
H
CE may disclose to government authority
H
H
Is the individual is unable to agree "Incapacity"?
164.512 (c) (1) (iii) (B)
Yes, No
H
Does LEO present that PHI is not intended to be used against the
164.512 (c) (1) (iii) (B)
Yes, No
H
Does LEO present that there is an immediate need for the disclosure?
164.512 (c) (1) (iii) (B)
Yes, No
Yes
No
CE may not disclose to government authority
H
Sto
H
Would CE be informing a personal representative that is responsible of the abuse
164.512 (c) (2) (ii)
Yes, No
H
Does informing the individual place them at risk?
164.512 (c) (2) (i)
Yes, No
No
Yes
CE must inform the individual or the personal representative about the disclosure.
H
Sto
CE must not inform the individual or the personal representative about the disclosure.
H

Figure 2: The Flow chart – Part C

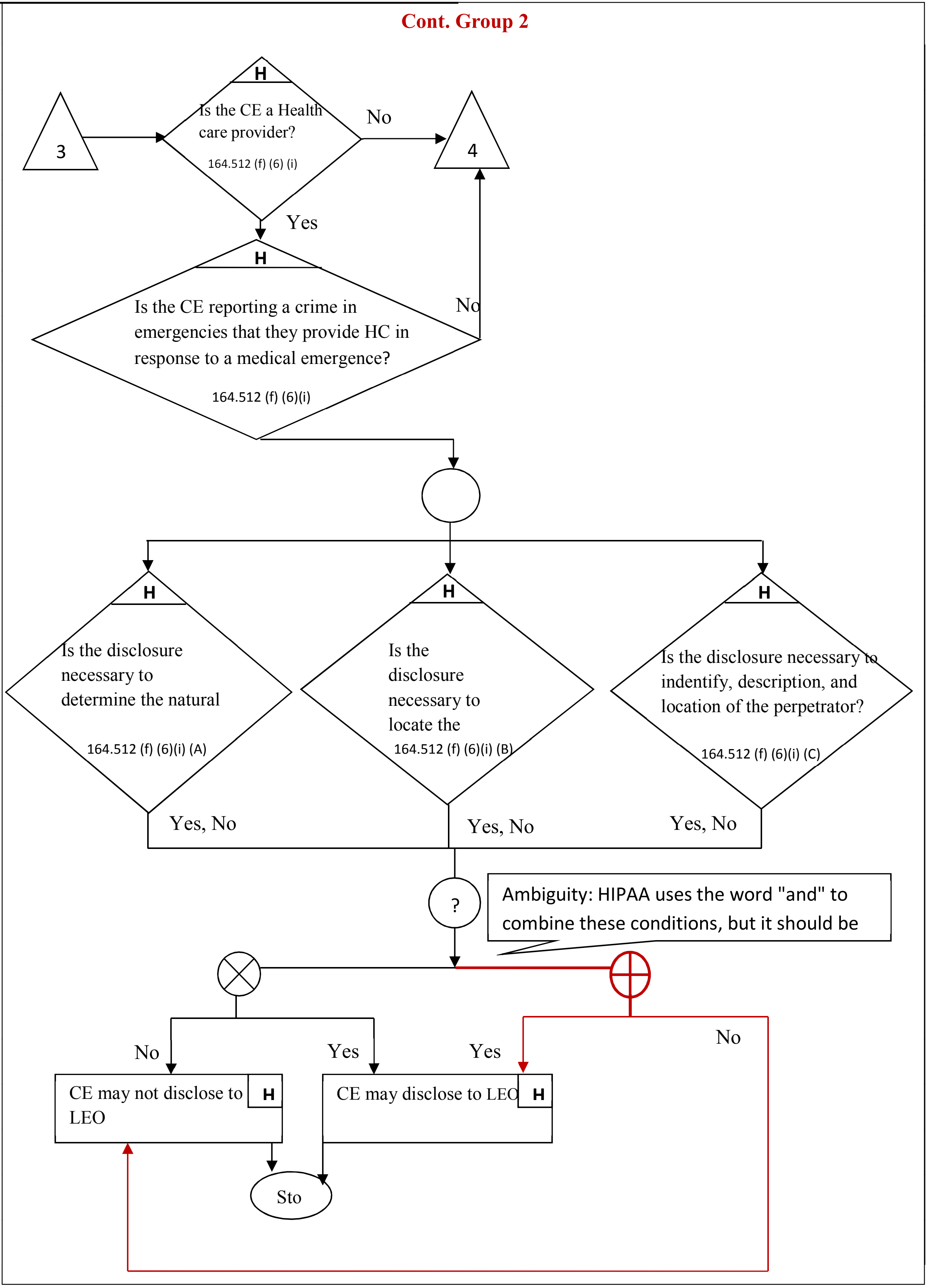

Cont. Group 2
3
H
Is the CE a Health care provider?
164.512 (f) (6) (i)
No
4
Yes
H
Is the CE reporting a crime in emergencies that they provide HC in response to a medical emergence?
164.512 (f) (6)(i)
No
H
Is the disclosure necessary to determine the natural
164.512 (f) (6)(i) (A)
H
Is the disclosure necessary to locate the
164.512 (f) (6)(i) (B)
H
Is the disclosure necessary to indentify, description, and location of the perpetrator?
164.512 (f) (6)(i) (C)
Yes, No
Yes, No
Yes, No
?
Ambiguity: HIPAA uses the word "and" to combine these conditions, but it should be
No
Yes
Yes
No
CE may not disclose to LEO
H
CE may disclose to LEO
H
Sto

Figure 2: The Flow chart – Part D

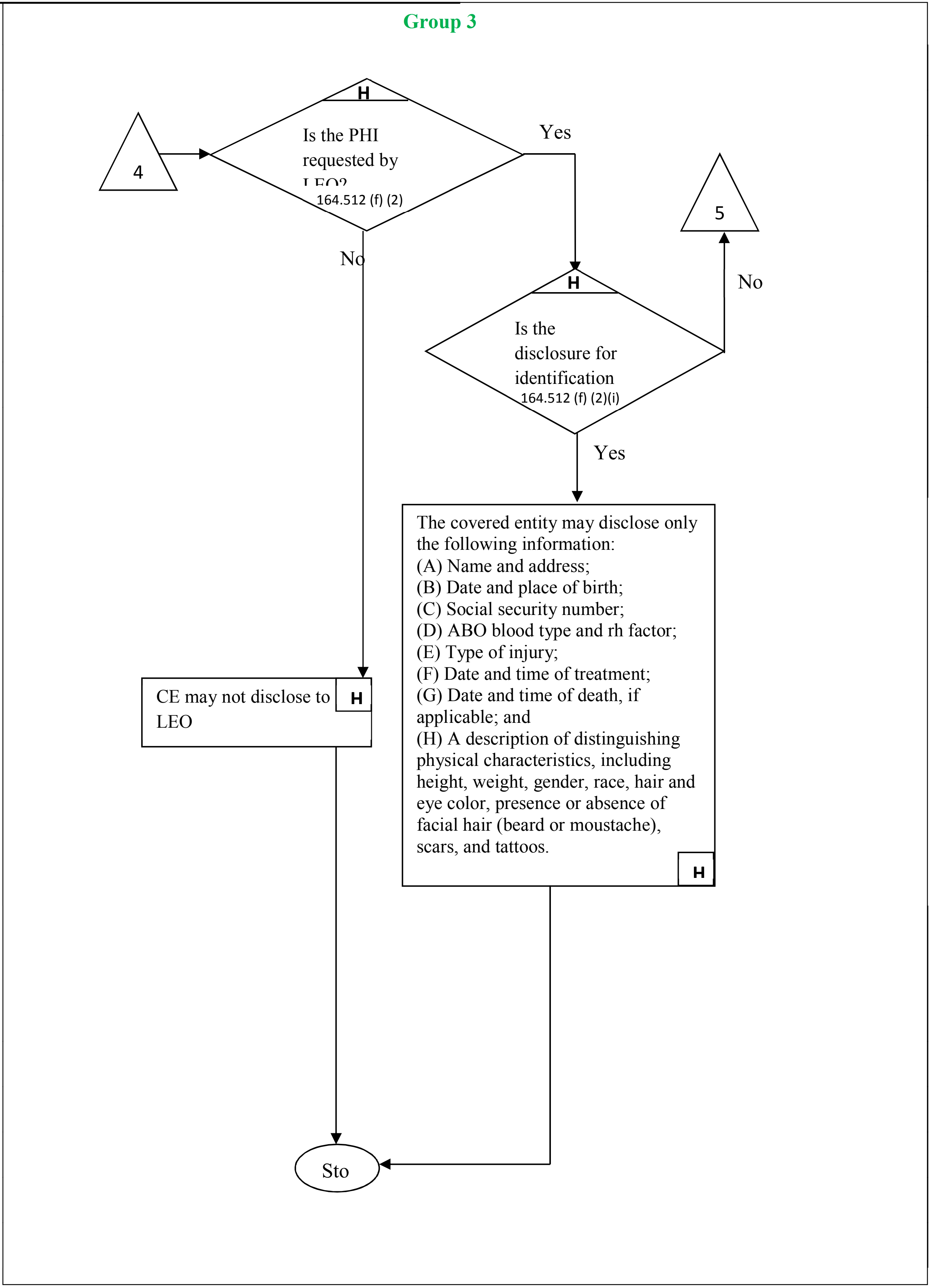

Group 3
4
H
Is the PHI requested by LEO?
164.512 (f) (2)
Yes
No
5
H
Is the disclosure for identification
164.512 (f) (2)(i)
No
Yes
The covered entity may disclose only the following information:
(A) Name and address;
(B) Date and place of birth;
(C) Social security number;
(D) ABO blood type and rh factor;
(E) Type of injury;
(F) Date and time of treatment;
(G) Date and time of death, if applicable; and
(H) A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.
H
CE may not disclose to LEO
H
Sto

Figure 2: The Flow chart – Part E

## Cont. Group 3

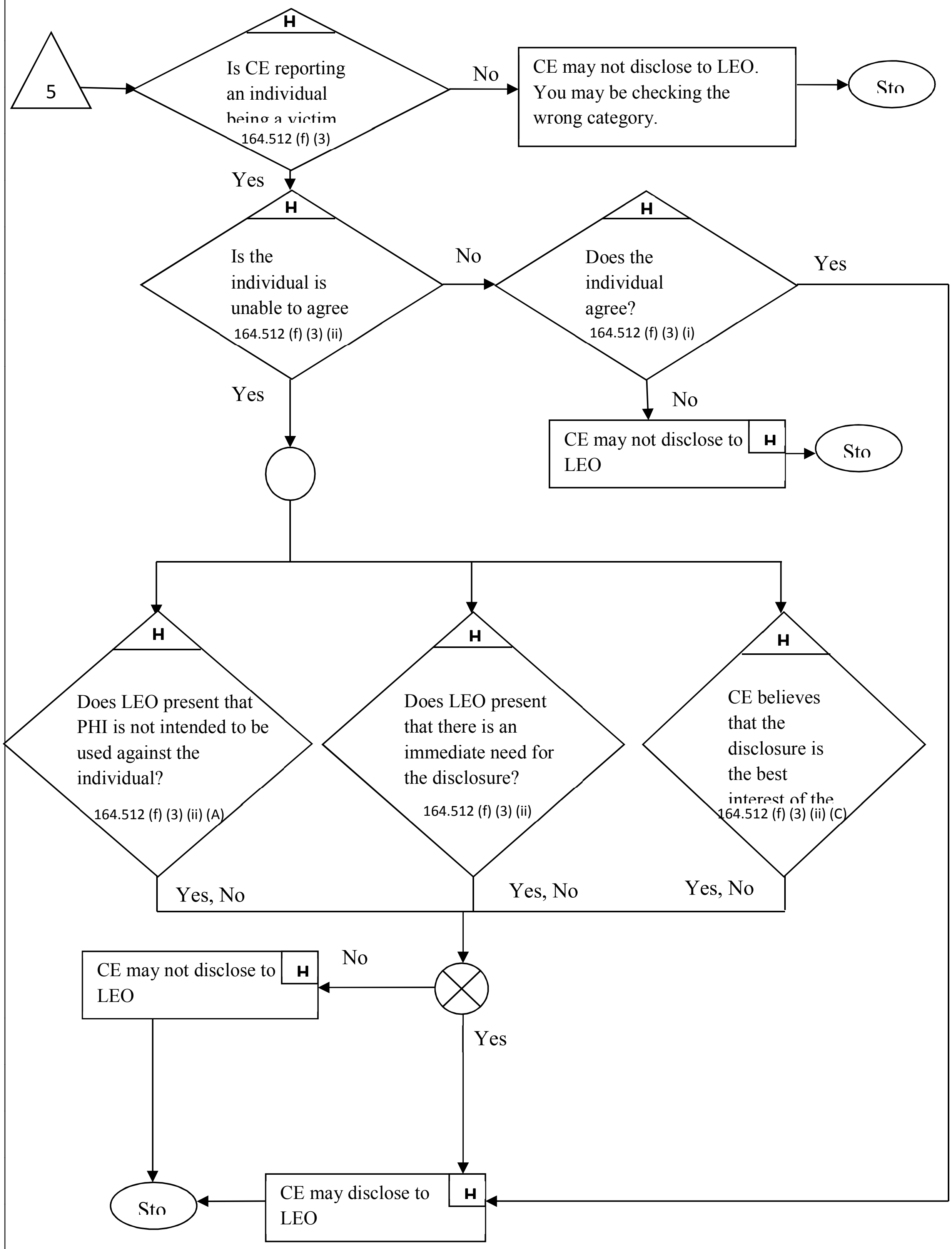
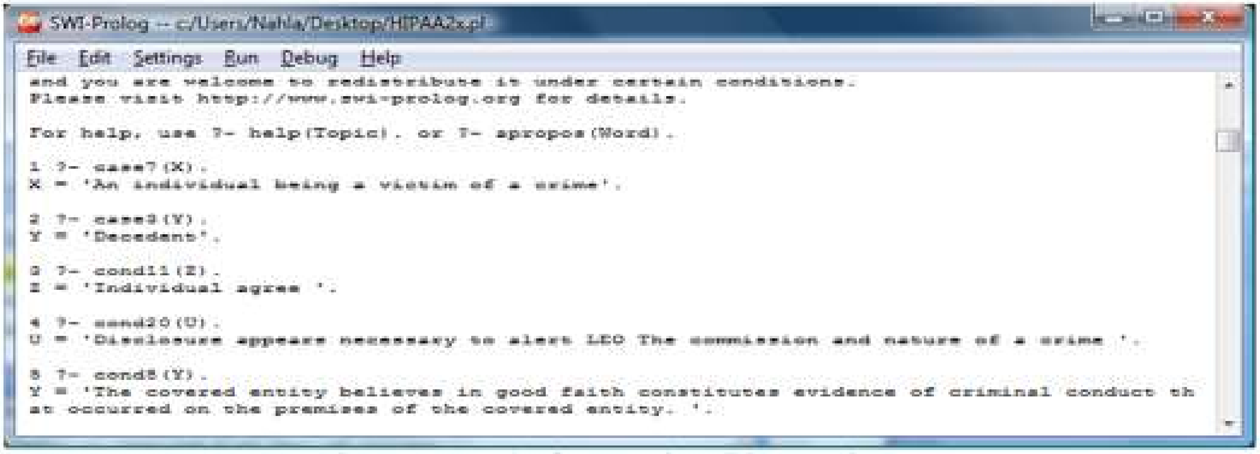

5
H
Is CE reporting an individual being a victim
164.512 (f) (3)
No
CE may not disclose to LEO. You may be checking the wrong category.
Sto
Yes
H
Is the individual is unable to agree
164.512 (f) (3) (ii)
No
H
Does the individual agree?
164.512 (f) (3) (i)
Yes
Yes
No
CE may not disclose to LEO
H
Sto
H
Does LEO present that PHI is not intended to be used against the individual?
164.512 (f) (3) (ii) (A)
H
Does LEO present that there is an immediate need for the disclosure?
164.512 (f) (3) (ii)
H
CE believes that the disclosure is the best interest of the
164.512 (f) (3) (ii) (C)
Yes, No
Yes, No
Yes, No
CE may not disclose to LEO
H
No
Yes
Sto
CE may disclose to LEO
H

Figure 2: The Flow chart – Part F

## 6. Rules in Prolog

As the flowchart increases in size, it becomes more difficult to manage and maintain. Therefore, we used Prolog is a logic programming language that allows to write and express rules in a manageable manner. There are only three basic constructs in Prolog: facts, rules, and queries. A collection of facts and rules is called a knowledge base or a database. After writing a set of rules and facts, users can ask query (or question) about them. For simplicity, all cases has been numbered from case1 to case 7 and all conditions has been labeled between cond1 to cond25 as shown in table 3 and 4.

Users of our prolog program post a query about the corresponding case or condition using the queries. For example, a query that asks about the content of cond10 will be written as "cond10(X)." where X is the variable name. Note that variables are expressed using any word that start with capital letter. X, Value, and Number_id are all variables. Figure 3 shows an example of cases and conditions queries.  The complete list of facts is attached in the appendix in the end of the document.


SWI-Prolog -- c:/Users/Nahla/Desktop/HIPAA2x.pl
File Edit Settings Run Debug Help

```
and you are welcome to redistribute it under certain conditions.
Please visit http://www.swi-prolog.org for details.

For help, use ?- help(Topic). or ?- apropos(Word).

1 ?- case7(X).
X = 'An individual being a victim of a crime'.

2 ?- case3(Y).
Y = 'Decedent'.

3 ?- cond11(Z).
Z = 'Individual agree '.

4 ?- cond20(U).
U = 'Disclosure appears necessary to alert LEO The commission and nature of a crime '.

5 ?- cond5(Y).
Y = 'The covered entity believes in good faith constitutes evidence of criminal conduct th
at occurred on the premises of the covered entity. '.
```

Figure 3: Example of cases and conditions queries.

There are 16 facts that represent the rules of disclosing information for law enforcement purposes. The set of facts are shown in figure 4. All facts have the same predicate named disclose. The 16 facts reflect the cases where the covered entities are allowed to disclose to law enforcement official or public authority. The number of facts varies between cases. Case1 have four facts which reflect the different circumstances that a CE can disclose if case1 applied. Case2, 3 and 5 has only one fact. Case4 has four facts while case5 has three facts. Finally, case7 has two facts.

### 6.1. Predicates main clauses

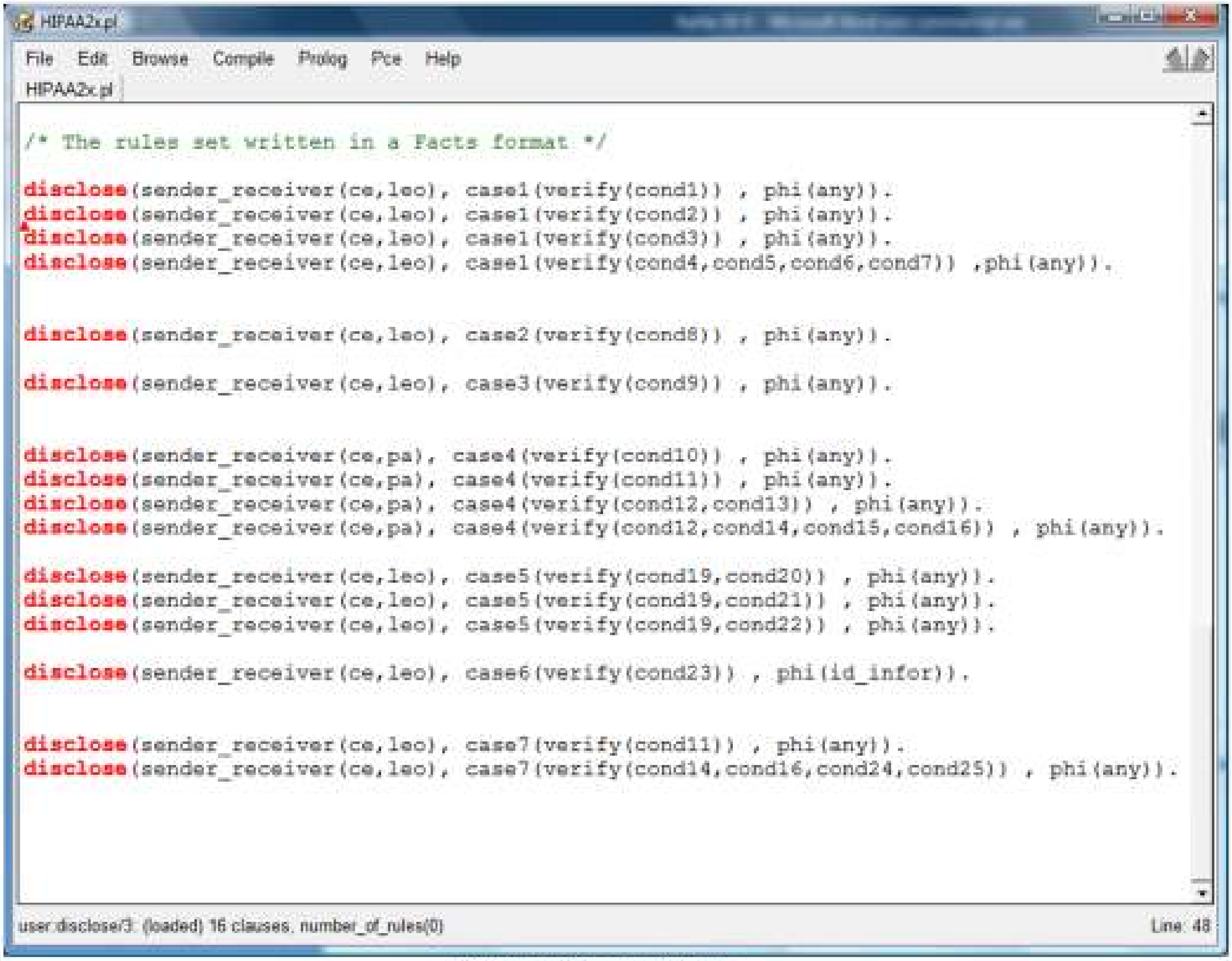
- The first part is the sender and receiver writhen as "sender_receiver(X,Y)", where X is the sender role and Y is the receiver role.

- The second part of predicates is the case number and conditions writhen as case1(verify(cond1)). The previous example means that case1 requires cond1 to be applied  in order to disclose PHI. Note that "verify" can have as many conditions as needed. For example, case4(verify(cond12,cond13)) means that to disclose under case4, cond12 and cond13 have to be applied.

- The last part of predicates is the limit of information being disclosed and written as PHI(Y), where Y is the type of information that can be disclosed. PHI(id_infor) means that only identification information is allowed to be disclosed.

| Case # | Full text | Receiver | Notes |
|---|---|---|---|
| Case1 | Required by Law [512 (f) (1) ] | Law enforcement official | |
| Case2 | Crime on premises [512 (f) (5) ] | Law enforcement official | |
| Case3 | Decedent [512 (f) (4) ] | Law enforcement official | |
| Case4 | Disclosures about victims of abuse, neglect or domestic violence [512 (c) ] | Government authority including (social service or protective services agency) | |
| Case5 | Reporting crime in emergencies [512 (f) (6) ] | Law enforcement official | From Health care provider |
| Case6 | the purpose of identifying or locating a suspect, fugitive, material witness, or missing person [512 (f)(2) ] | Law enforcement official | Disclose certain type of information |
| Case7 | An individual being a victim of a crime [512 (f) (3) ] | Law enforcement official | |

Table3: A list of the seven cases under law enforcement purposes



```
/* The rules set written in a Facts format */

disclose(sender_receiver(ce,leo), case1(verify(cond1)) , phi(any)).
disclose(sender_receiver(ce,leo), case1(verify(cond2)) , phi(any)).
disclose(sender_receiver(ce,leo), case1(verify(cond3)) , phi(any)).
disclose(sender_receiver(ce,leo), case1(verify(cond4,cond5,cond6,cond7)) ,phi(any)).


disclose(sender_receiver(ce,leo), case2(verify(cond8)) , phi(any)).

disclose(sender_receiver(ce,leo), case3(verify(cond9)) , phi(any)).


disclose(sender_receiver(ce,pa), case4(verify(cond10)) , phi(any)).
disclose(sender_receiver(ce,pa), case4(verify(cond11)) , phi(any)).
disclose(sender_receiver(ce,pa), case4(verify(cond12,cond13)) , phi(any)).
disclose(sender_receiver(ce,pa), case4(verify(cond12,cond14,cond15,cond16)) , phi(any)).

disclose(sender_receiver(ce,leo), case5(verify(cond19,cond20)) , phi(any)).
disclose(sender_receiver(ce,leo), case5(verify(cond19,cond21)) , phi(any)).
disclose(sender_receiver(ce,leo), case5(verify(cond19,cond22)) , phi(any)).

disclose(sender_receiver(ce,leo), case6(verify(cond23)) , phi(id_infor)).


disclose(sender_receiver(ce,leo), case7(verify(cond11)) , phi(any)).
disclose(sender_receiver(ce,leo), case7(verify(cond14,cond16,cond24,cond25)) , phi(any)).
```

```
user:disclose/3: (loaded) 16 clauses, number_of_rules(0)                Line: 48
```

Figure 4: The set of facts

Users can post queries about any information they wish to know. The complete facts should be written and the part that needed is replaced with a variable. Section 6.2 demonstrates three query examples of three different cases.

| Cond# | Full text | Cond Label |
|---|---|---|
| Cond1 | Reporting a certain type of injury [512 (f) (1) (i)] | injury |
| Cond2 | Court order [512 (f) (1) (ii) (A)] | Court order |
| Cond3 | Grand jury subpoena [512 (f) (1) (ii) (B)] | Grand jury subpoena |
| Cond4 | Administrative request [512 (f) (1) (ii) (C)] | Admin request |
| Cond5 | The request provides that the information sought is relevant and material to a legitimate EO inquiry. [512 (f) (1) (ii) (C) (1)] | Admin_cond1 |
| Cond6 | The request provides that the request is specific and limited in scope to the purpose for which the information is sought [512 (f) (1) (ii) (C) (2)] | Admin_cond2 |
| Cond7 | The request provides that the de-identified information could not reasonably be used. [512 (f) (1) (ii) (C) (3)] | Admin_cond3 |
| Cond8 | The covered entity believes in good faith constitutes evidence of criminal conduct that occurred on the premises of the covered entity. [512 (f) (5)] | Evidence of criminal |
| Cond9 | The purpose of alerting law enforcement of the death of the individual is that the covered entity has a suspicion that such death may have resulted from criminal conduct [512 (f) (4)] | criminal conduct |
| Cond10 | Child abuse or neglect [ 512 (b) (1) (ii) ] | Violence on Child |
| Cond11 | Individual agree [512 (c) (ii) ] [512 (f) (3) (i) ] | agreement |
| Cond12 | The disclosure is expressly authorized by statute or regulation [512 (c) ] | statute |
| Cond13 | CE, in the exercise of professional judgment, believes the disclosure is necessary to prevent serious harm to the individual or other potential victims [512 (c) (iii) (A) ] | necessity |
| Cond14 | the individual is unable to agree because of incapacity [512 (c) (iii) (B)] or other emergency circumstance [512 (f) (3) (ii)] | incapacity |
| Cond15 | A law enforcement or other public official authorized to receive the report represents that the protected health information for which disclosure is sought is not intended to be used against the individual [512 (c) (iii) (B)]. | Indemnity |
| Cond16 | An immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure [512 (c) (iii) (B)] and [512 (f) (3) (ii) (B) ] | immediacy |
| Cond17 | CE believes informing the individual would place the individual at risk of serious harm. [512 (c) (2) (i)]. | Informing1 |
| Cond18 | CE would be informing a personal representative, and the covered entity reasonably believes the personal representative is responsible for the abuse, neglect, or other injury, and that informing such person would not be in the best interests of the individual [512 (c) (2) (ii)]. | Informing2 |
| Cond19 | The CE is a health care provider [512 (f) (6)] | HCP |
| Cond20 | Disclosure appears necessary to alert LEO The commission and nature of a crime [512 (f) (6) (i) (A)] | Nature of a crime |
| Cond21 | Disclosure appears necessary to alert law enforcement to (B) The location of such crime or of the victim(s) of such crime [512 (f) (6) (i) (B)] | Venue |
| Cond22 | Disclosure appears necessary to alert law enforcement to (C) The identity, description, and location of the perpetrator of such crime [512 (f) (6) (i) (C)] | Perpetrator |
| Cond23 | PHI is requested by LEO [512 (f) (2)] and [512 (f) (3)] | Request |
| Cond24 | The law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the victim has occurred and such information is not intended to be used against the victim. [512 (f) (3) (ii) (A)] | Investigation for other victims and Indemnity |
| Cond25 | The disclosure is in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment [512 (f) (3) (ii) (C)] | interest |

Table 4: List of the 25 conditions and their label

### 6.2. Three query examples

**Example1:** A hospital receives a case where a child being a victim of abuse.
**Questions:**

- To whom, the CE sends the report?
- The limit of the information included in the report.

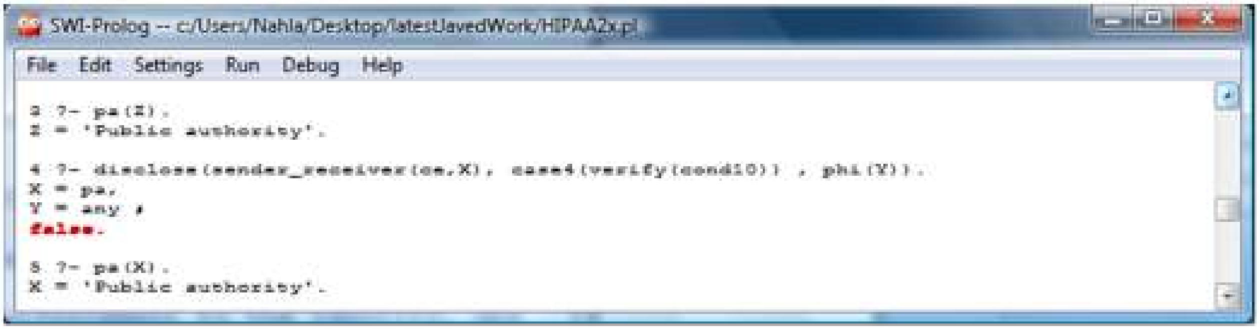
**Query:**

From the previous explanation, we can identify what information is available and add it to the query as shown in table 5. In this example, "abuse" is case4, and "child is a victim" indicates that there is violence on child and thus cond10. The receiver and the limit of information are requested; therefore, they are replaced with variables in the query.

| | |
|---|---|
| **Available Information** | Abuse -> case4<br>Violence on child -> cond10 |
| **The Query** | disclose(sender_receiver(ce,X), case4(verify(cond10)) , phi(Y)). |

Table5: The available information and the query of example 1

Figure5 shows the system response after posing the query. X=pa, means that the CE can disclose to a public authority. If the user needs further explanation about the result, they can ask query such as "pa" by posting pa(Variable_name).


SWI-Prolog -- c:/Users/Nahla/Desktop/latestJavedWork/HIPAA2x.pl
File Edit Settings Run Debug Help

```
3 ?- pa(Z).
Z = 'Public authority'.

4 ?- disclose(sender_receiver(ce,X), case4(verify(cond10)) , phi(Y)).
X = pa,
Y = any ;
false.

5 ?- pa(X).
X = 'Public authority'.
```

Figure5: The system response for the first example

**Example2:** LEO requests identification information about a missing person from a covered entity.
**Questions:**

- What is the limit of the information that CE can disclose?

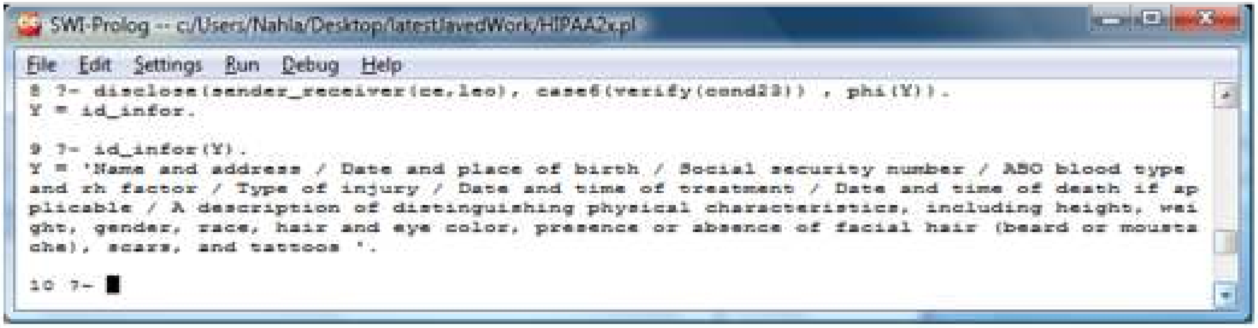
**Query:**

From the previous explanation, we can identify what information is available and add it to the query as shown in table6. The limit of information is requested; therefore, it will be replaced with a variable in the query as shown in table6.

| | |
|---|---|
| **Available Information** | Missing person -> case6<br>LEO request -> cond23 |
| **The Query** | disclose(sender_receiver(ce,leo), case6(verify(cond23)) , phi(Y)). |

Table6: The available information and the query of example 2

Figure6 shows the system response after posing the query. Y=id_infor, means that the CE can disclose identification information only. If the user needs further explanation about the result, they can ask query such as "id_infor" by posting id_infor(Variable_name).


SWI-Prolog -- c:/Users/Nahla/Desktop/latestJavedWork/HIPAA2x.pl
File Edit Settings Run Debug Help

```
8 ?- disclose(sender_receiver(ce,leo), case6(verify(cond23)) , phi(Y)).
Y = id_infor.

9 ?- id_infor(Y).
Y = 'Name and address / Date and place of birth / Social security number / ABO blood type
and rh factor / Type of injury / Date and time of treatment / Date and time of death if ap
plicable / A description of distinguishing physical characteristics, including height, wei
ght, gender, race, hair and eye color, presence or absence of facial hair (beard or mousta
che), scars, and tattoos '.

10 ?- █
```

Figure6: The system response for the second example

**Example3:** A CE is a health care provider. It provides medical emergency to an individual who is a victim of a crime.

**Questions:**

- Under what circumstances I have to disclose to LEO?
- What the limit of the information that CE can disclose.

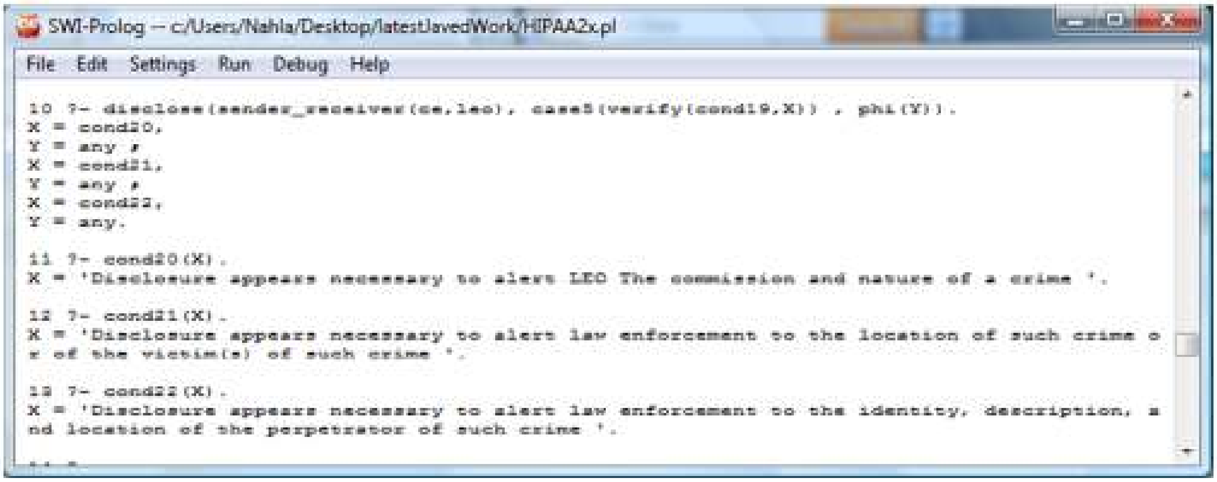
**Query:**

From the previous explanation, we can identify what information as shown in table7.

| | |
|---|---|
| **Available Information** | Victim of a crime -> case5<br>HCP -> cond19 |
| **The Query** | disclose(sender_receiver(ce,leo), case5(verify(cond19,X)) , phi(Y)). |

Table7: The available information and the query of example 3

Figure7 shows the system response after posing the query. In this case there are three possible values of X which means that if one of these conditions applies, the covered entity can disclose PHI to LEO. If the user needs further explanation about the result, they can ask query such as "cond22" by posting cond22(Variable_name). This example demonstrate the ambiguity case that resolved by our flowchart.


SWI-Prolog -- c:/Users/Nahla/Desktop/latestJavedWork/HIPAA2x.pl
File Edit Settings Run Debug Help

```
10 ?- disclose(sender_receiver(ce,leo), case5(verify(cond19,X)) , phi(Y)).
X = cond20,
Y = any ;
X = cond21,
Y = any ;
X = cond22,
Y = any.

11 ?- cond20(X).
X = 'Disclosure appears necessary to alert LEO The commission and nature of a crime '.

12 ?- cond21(X).
X = 'Disclosure appears necessary to alert law enforcement to the location of such crime o
r of the victim(s) of such crime '.

13 ?- cond22(X).
X = 'Disclosure appears necessary to alert law enforcement to the identity, description, a
nd location of the perpetrator of such crime '.
```

Figure7: The system response for the third example

## 7. Related Work

Several access control methods has been proposed [4] [5] [6] [7]. In the Privacy-aware role based Access control models in [4] privacy policy enforcement and access control enforcement are combined into one access control model. The idea is that purposes, condition and obligations are assigned to the role, when assigning the action on the object.

The other approach of access control uses the purpose as based access control [5]. Their work focuses on the notion of purposes which are designed in a hierarchy. In [3], the proposed framework combines the notion of purpose and role. Moreover, their access decision is based on purpose compliancy and HIPAA privacy rules.

In [6] [7], the proposed approach is a method of extracting policy and rules in a systematic way. Their methodology extracts and prioritizes rights and obligations from regulations [6]. However, due to un-involvement of the human analysis and the complexity of policy rules, the ambiguity of these rules would not be handled correctly. A fragment of first logic is considered in [8]. Based on the policies they collected, their approach is likely to be sufficiently expressive for many applications. For typical polices, they could efficiently determines if actions are permitted or prohibited.

Similar to [8], our approach aims to precisely define the privacy rules. However, our method targets the privacy rules in HIPAA. We also adopted the combination of purpose and role [8] in the process of decision making. The notion of cases is added in our approach. In other word, the purpose in our paper is "law enforcement purpose" and that includes seven different cases or scenarios each of which has their own conditions. Moreover, unlike previous approaches, we have resolved ambiguity by adding the extra node to the flow chart that determines the ambiguity location and define the new path.

## 8. Conclusion and Future work

In the USA, the Health Insurance Portability and Accountability Act (HIPAA) provides the privacy rules in regards to the use and disclosure of health information. However, this information maybe incorrectly interpreted that would lead to unauthorized disclosure. In this paper, section 164.512 (f) and (c) were chosen from HIPAA to be examined. Our analysis includes drawing a flow chart that helps the process of decision making. To handle ambiguity in privacy rules, an extra node is added to the flowchart. Moreover, flowchart assists users to choose the right cases by checking some cases before others.

In addition, Prolog, logic programming, is used to develop a query system that has the knowledge base of privacy rules in a precise way with a unique meaning. Users of our system, can ask queries about conditions involved in each case, the limit of information, and to whom to disclose. However, since the user has to follow the exact query format, a friendlier interface is more desirable.

Later phases of this paper will be to build more friendly interface that display what need to be checked first. Additionally, the ambiguity was removed from Prolog set of rules but a mechanism to handle it is still needed. The potential application would not only handle user query but also provides high level services such as a patient reminder of their appointment. Moreover, the time life line of a condition or rules can be added to determine when such a rule is changed and keep track of any updates.

## 9. References

[1] HIPAA Administrative Simplification, 2006

[2] " Understanding Health Information Privacy," http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html

[3] A. AL Faresi, D. Wijesekera, and K. Moidu, "A Comprehensive Privacy-aware Authorization Framework Founded on HIPAA Privacy Rules," IHI'10, Arlington, Virginia, pp. 637-646, 2010

[4] Q. Ni, A. Trombetta, E. Bertino, and J. Lobo, "Privacy aware role based access control," In SACMAT '07: Proceedings of the 12th ACM symposium on Access control models and technologies. New York, NY, USA: ACM Press, 2007

[5] N. Yang, H. Barringer, and N. Zhang, "A purpose-based access control model," In IAS'07, Manchester, UK, pp. 143-148, 2007

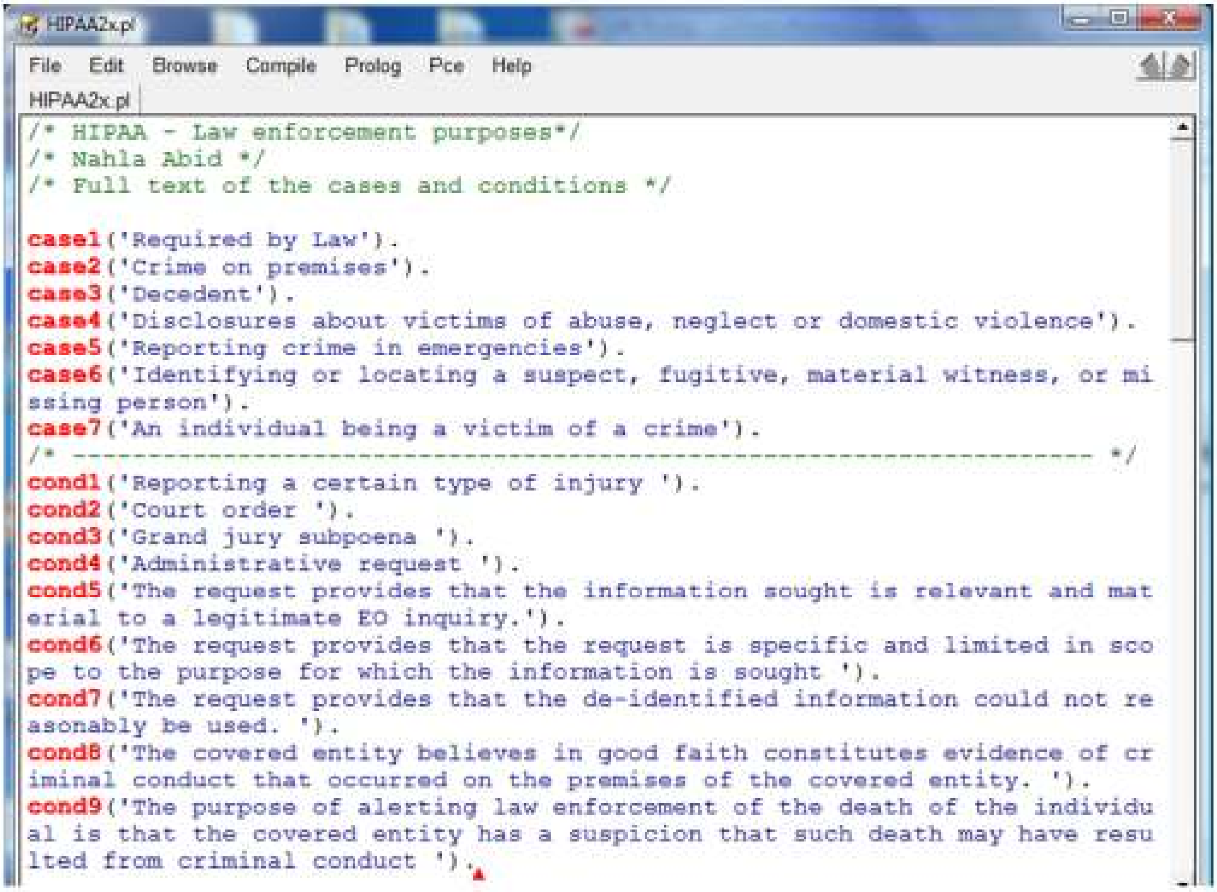
[6] Travis D. Breaux, Matthew W. Vail, and Annie I. Anton, "Towards regulatory compliance: Extracting rights and obligations to align requirements with regulations," In RE'06: Proceedings of the 14th IEEE International Requirements Engineering Conference (RE'0 6), Washington, DC, USA: IEEE, pp. 49– 58, 2006

[7] Seok-Won Lee, Robin Gandhi, Divya Muthurajan, Deepak Yavagal, and Gail-Joon Ahn, "Building problem domain ontology from security requirements in regulatory documents," In SESS'06 , Shanghai, China, ACM, May 2006

[8] Joseph Y. Halpern and Vicky Weissman, "Using First-order logic to reason about policies," In Proceedings of the Computer Security Foundations Workshop (CSFW'03), Los Alamitos, CA, USA: IEEE, 2003

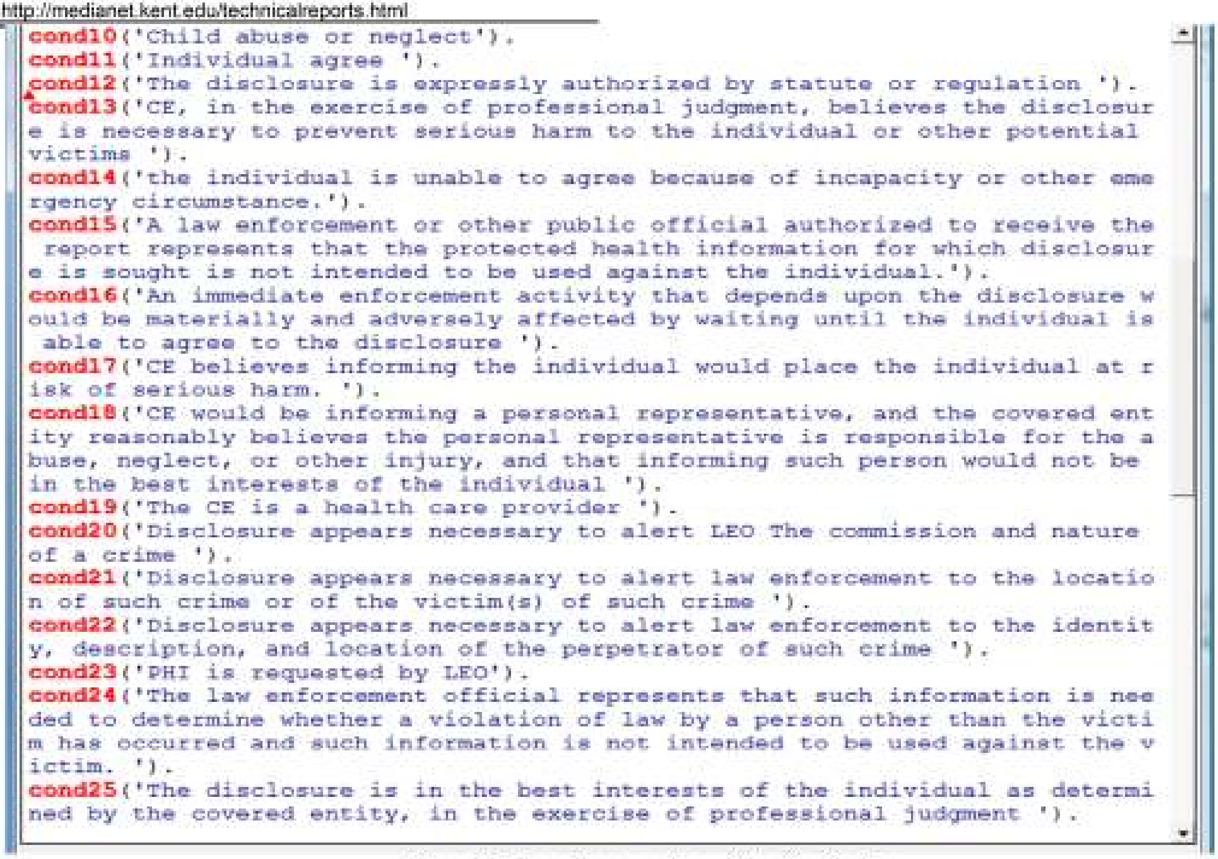
[9] Nicholas Hebb, Flowchart Symbols Defined, http://www.breezetree.com/article-excel-flowchart-shapes.htm, 2013

## 10. Appendix



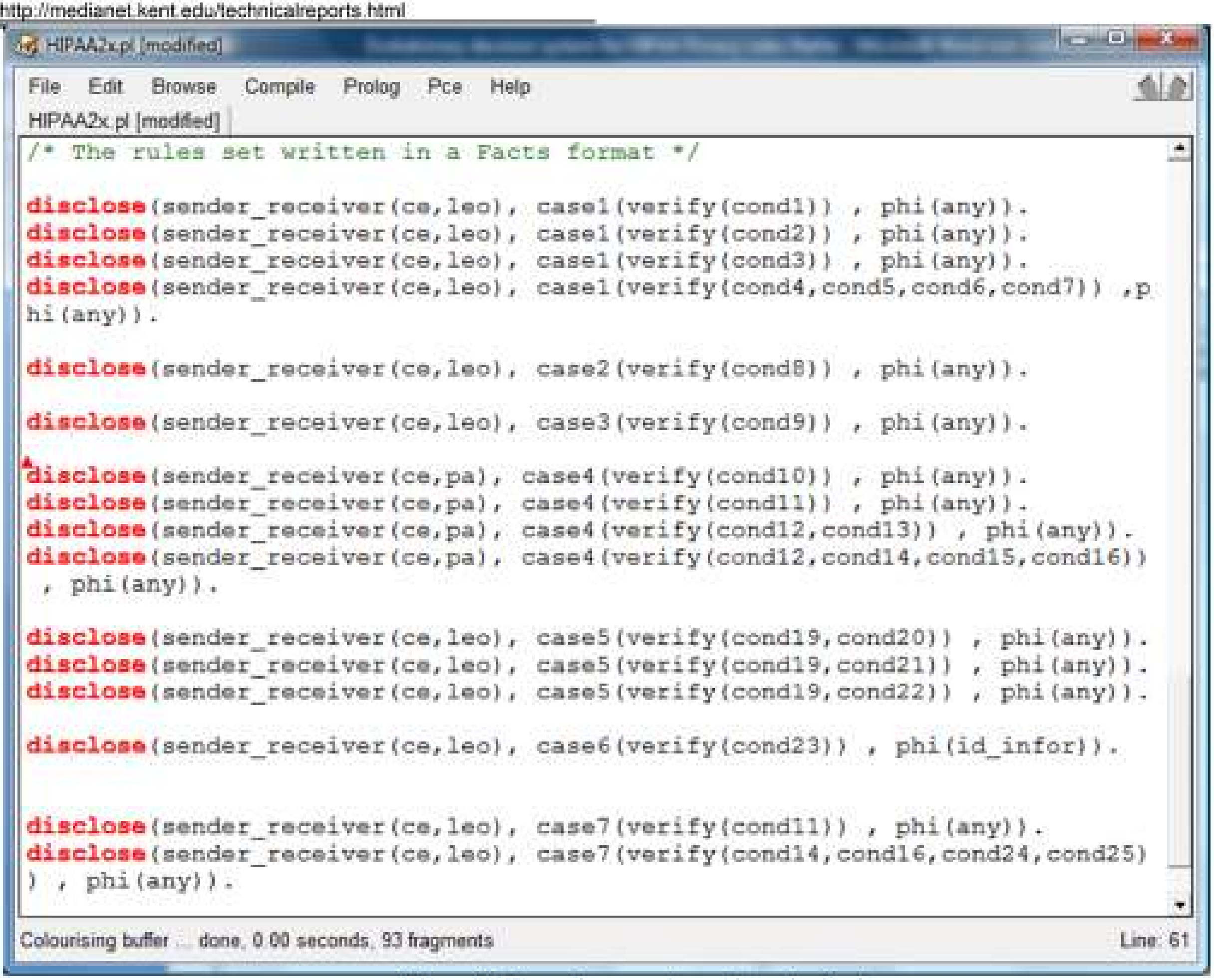
```
/* HIPAA - Law enforcement purposes*/
/* Nahla Abid */
/* Full text of the cases and conditions */

case1('Required by Law').
case2('Crime on premises').
case3('Decedent').
case4('Disclosures about victims of abuse, neglect or domestic violence').
case5('Reporting crime in emergencies').
case6('Identifying or locating a suspect, fugitive, material witness, or missing person').
case7('An individual being a victim of a crime').
/* -------------------------------------------------------------------- */
cond1('Reporting a certain type of injury ').
cond2('Court order ').
cond3('Grand jury subpoena ').
cond4('Administrative request ').
cond5('The request provides that the information sought is relevant and material to a legitimate EO inquiry.').
cond6('The request provides that the request is specific and limited in scope to the purpose for which the information is sought ').
cond7('The request provides that the de-identified information could not reasonably be used. ').
cond8('The covered entity believes in good faith constitutes evidence of criminal conduct that occurred on the premises of the covered entity. ').
cond9('The purpose of alerting law enforcement of the death of the individual is that the covered entity has a suspicion that such death may have resulted from criminal conduct ').
```



```
cond10('Child abuse or neglect').
cond11('Individual agree ').
cond12('The disclosure is expressly authorized by statute or regulation ').
cond13('CE, in the exercise of professional judgment, believes the disclosur
e is necessary to prevent serious harm to the individual or other potential
victims ').
cond14('the individual is unable to agree because of incapacity or other eme
rgency circumstance.').
cond15('A law enforcement or other public official authorized to receive the
 report represents that the protected health information for which disclosur
e is sought is not intended to be used against the individual.').
cond16('An immediate enforcement activity that depends upon the disclosure w
ould be materially and adversely affected by waiting until the individual is
 able to agree to the disclosure ').
cond17('CE believes informing the individual would place the individual at r
isk of serious harm. ').
cond18('CE would be informing a personal representative, and the covered ent
ity reasonably believes the personal representative is responsible for the a
buse, neglect, or other injury, and that informing such person would not be
in the best interests of the individual ').
cond19('The CE is a health care provider ').
cond20('Disclosure appears necessary to alert LEO The commission and nature
of a crime ').
cond21('Disclosure appears necessary to alert law enforcement to the locatio
n of such crime or of the victim(s) of such crime ').
cond22('Disclosure appears necessary to alert law enforcement to the identit
y, description, and location of the perpetrator of such crime ').
cond23('PHI is requested by LEO').
cond24('The law enforcement official represents that such information is nee
ded to determine whether a violation of law by a person other than the victi
m has occurred and such information is not intended to be used against the v
ictim. ').
cond25('The disclosure is in the best interests of the individual as determi
ned by the covered entity, in the exercise of professional judgment ').
```

Figure8: The privacy rules written in Prolog



```
/* The rules set written in a Facts format */

disclose(sender_receiver(ce,leo), case1(verify(cond1)) , phi(any)).
disclose(sender_receiver(ce,leo), case1(verify(cond2)) , phi(any)).
disclose(sender_receiver(ce,leo), case1(verify(cond3)) , phi(any)).
disclose(sender_receiver(ce,leo), case1(verify(cond4,cond5,cond6,cond7)) ,p
hi(any)).

disclose(sender_receiver(ce,leo), case2(verify(cond8)) , phi(any)).

disclose(sender_receiver(ce,leo), case3(verify(cond9)) , phi(any)).

disclose(sender_receiver(ce,pa), case4(verify(cond10)) , phi(any)).
disclose(sender_receiver(ce,pa), case4(verify(cond11)) , phi(any)).
disclose(sender_receiver(ce,pa), case4(verify(cond12,cond13)) , phi(any)).
disclose(sender_receiver(ce,pa), case4(verify(cond12,cond14,cond15,cond16))
 , phi(any)).

disclose(sender_receiver(ce,leo), case5(verify(cond19,cond20)) , phi(any)).
disclose(sender_receiver(ce,leo), case5(verify(cond19,cond21)) , phi(any)).
disclose(sender_receiver(ce,leo), case5(verify(cond19,cond22)) , phi(any)).

disclose(sender_receiver(ce,leo), case6(verify(cond23)) , phi(id_infor)).


disclose(sender_receiver(ce,leo), case7(verify(cond11)) , phi(any)).
disclose(sender_receiver(ce,leo), case7(verify(cond14,cond16,cond24,cond25)
) , phi(any)).
```

Colourising buffer ... done, 0.00 seconds, 93 fragments

Line: 61

Figure9: The privacy rules written in Prolog