Logical Specification of the GLBA and HIPAA Privacy Laws

Henry DeYoung, Deepak Garg, Dilsun Kaynar, Anupam Datta

April 29, 2010

CMU-CyLab-10-007

CyLab
Carnegie Mellon University
Pittsburgh, PA 15213

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **29 APR 2010**	2. REPORT TYPE	3. DATES COVERED **00-00-2010 to 00-00-2010**

4. TITLE AND SUBTITLE **Logical Specification of the GLBA and HIPAA Privacy Laws**	5a. CONTRACT NUMBER 5b. GRANT NUMBER 5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER 5e. TASK NUMBER 5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Carnegie Mellon University,CyLab,Pittsburgh,PA,15213**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S) 11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Despite the wide array of frameworks proposed for the formal specification and analysis of privacy laws, there has been comparatively little work on expressing large fragments of actual privacy laws in these frameworks. We attempt to bridge this gap by presenting what we believe to be the most complete logical formalizations of the Gramm-Leach-Bliley Act (GLBA) and the Health Insurance Portability and Accountability Act (HIPAA) to date. Specifically, we formalize xx6802 and 6803 of GLBA and xx164.502, 164.506, 164.508, 164.510 164.512, 164.514, and 164.524 of HIPAA. The remaining sections of both laws are not stated in terms of operational requirements, and therefore cannot be formalized in our model. Along the way, we also give a novel extension of an existing privacy logic with real-time features and fixed point operators; these provide the expressive power necessary to capture legal clauses found in GLBA and HIPAA involving bounded-time obligations and reuse of information.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**128**	

Abstract

Despite the wide array of frameworks proposed for the formal specification and analysis of privacy laws, there has been comparatively little work on expressing large fragments of actual privacy laws in these frameworks. We attempt to bridge this gap by presenting what we believe to be the most complete logical formalizations of the Gramm-Leach-Bliley Act (GLBA) and the Health Insurance Portability and Accountability Act (HIPAA) to date.

Specifically, we formalize §§6802 and 6803 of GLBA and §§164.502, 164.506, 164.508, 164.510, 164.512, 164.514, and 164.524 of HIPAA. The remaining sections of both laws are not stated in terms of operational requirements, and therefore cannot be formalized in our model.

Along the way, we also give a novel extension of an existing privacy logic with real-time features and fixed point operators; these provide the expressive power necessary to capture legal clauses found in GLBA and HIPAA involving bounded-time obligations and reuse of information.

This work was partially supported by the U.S. Army Research Office contract on Perpetually Available and Secure Information Systems (DAAD19-02-1-0389) to Carnegie Mellon CyLab, the NSF Science and Technology Center TRUST, the NSF CyberTrust grant "Privacy, Compliance and Information Risk in Complex Organizational Processes" and the AFOSR MURI "Collaborative Policies and Assured Information Sharing". The first author was also supported under an NSF Graduate Research Fellowship. Any opinions, findings, conclusions, or recommendations expressed in this publication are those of the authors and do not necessarily reflect the views of the U.S. Army Research Office, National Science Foundation, or the Air Force Office of Scientific Research.

Contents

Chapter 1

Introduction

With advances in communication and data processing, especially digital forms, over the last several decades, there has been an explosion in the amount and detail of information maintained by organizations about clients, patients, and other individuals. Such information is incredibly valuable to both organizations and individuals: organizations can operate more efficiently and provide higher quality services to individuals. At the same time, these benefits must be balanced against the individuals' right to privacy.

In response, democratic governments have instituted numerous laws to regulate the collection and use of personal information. Example privacy laws of the United States of America include the Gramm-Leach-Bliley Act (GLBA) [US 99] for financial privacy and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) [US 02] for privacy in the healthcare context.

Even after a cursory glance through these laws, it is apparent that the legal language is much too dense and intricate for the laws to serve as a day-to-day guide to managers of the regulated organizations. Managers (and the general public too) are instead interested in answers to concrete, practical questions, such as "Is the organizational privacy policy of Hospital X consistent with HIPAA?" and "Does GLBA permit Bank Y to disclose Bob's account information to Charlie?"

Recently, in efforts including role-based access control (RBAC) [Cra03, JSSS01, LMW02], the Extensible Access Control Markup Language (XACML) [ANP$^+$04], the Enterprise Privacy Authorization Language (EPAL) [BKBS04, BPS03], the Platform for Privacy Preferences (P3P) [RC99, BCK03, ACR99], and the Logic of Privacy and Utility (LPU) [BDMN06, BDMS07, Bar08], researchers have begun to attack the problem of formally expressing the content of both organizational privacy policies and privacy laws. The hope is that these languages and logics will permit the construction of tools that can directly answer the kinds of questions that arise in day-to-day business operations.

Despite the wide array of various privacy languages and logics, to the best of our knowledge, there has been comparatively little work on expressing *large* fragments of actual privacy laws in these frameworks[1]; instead, the encodings have been limited to small proof-of-concept examples. But this is a significant deficiency if the program of obtaining practical benefits from formal specification of privacy laws is to succeed. We must be confident that the techniques invented for the small examples scale to full privacy laws.

[1] The exceptions are work by Breaux and Antón on a classification of all HIPAA clauses [BA08], a Datalog formalization of §§164.502, 164.506, and 164.510 of HIPAA by Lam *et al.* [LMS09], and an access control-based encoding of §164.506 of HIPAA by May *et al.* [MGL06]. See Chapter 5 for more details.

This work is intended to help bridge this gap. In Chapters 3 and 4, we give what we believe is the most complete logical formalization of the privacy-relevant portions of GLBA and HIPAA to date. Specifically, we formalize §§6802 and 6803 of GLBA and §§164.502, 164.506, 164.508, 164.510, 164.512, 164.514, and 164.524 of HIPAA in a novel logic, which we call PrivacyLFP, based on the Logic of Privacy and Utility [BDMN06, BDMS07, Bar08]. As discussed in Chapter 2, only three significant modifications of LPU were needed to enable it to scale to this level of formalization.

We do not formalize the remaining sections of GLBA and HIPAA, not due to lack of time or energy, but because those sections are inherently incompatible with logical formalization for operational purposes. Typically, this is because the section is not phrased operationally. For example, §6801 of GLBA abstractly states that

> *[E]ach agency or authority [...] shall establish appropriate standards for the financial institutions [...] to insure the security and confidentiality of customer records and information,*

without providing implementation specifications for this policy. Similarly, §164.514(e)(4)(iii) of HIPAA defines non-compliance but does not regulate specific transmissions of protected health information:

> *A covered entity is not in compliance [...] if the covered entity knew of a pattern of activity or practice of the limited data set recipient that constituted a material breach or violation of the data use agreement.*

Contributions. The contributions of this work are two-fold.

First, to the best of our knowledge, we present the most complete formalization of GLBA and HIPAA in a privacy logic or language to date. These kind of large-scale case studies are crucial to justify the viability of formal specification as a means of obtaining practical benefits. While more privacy laws deserve this kind of detailed specification if we are to achieve broad applicability, we believe that our efforts represent a solid first step.

Second, we present a logic, PrivacyLFP, that significantly extends the expressive power of (the privacy fragment of) LPU. Most importantly, we give a novel synthesis of ideas from fixed point and privacy logics, showing that such a combination is both coherent and useful. A sister project on auditing and accountability [DGJ^{+}10] has demonstrated that fixed points, especially greatest ones, can be present in those analyses, as well: we are not using a construct in specification that is too exotic for operational applications.

Other extensions to LPU include 1. disclosure purposes, since many laws allow or deny disclosures based on purpose; 2. explicit real-time features, since lawmakers often impose concrete time limits, such as “within 30 days;” and 3. a distinction between acting in and belonging to a role, to express clauses that prescribe privacy actions that depend on an individual’s “citizenship” in a role.

Outline of the Report. In Chapter 2, we motivate PrivacyLFP’s extensions to (the privacy fragment of) LPU, describe the syntax and semantics of the core first-order fixed point logic, present the assumptions we make about the underlying first-order structure, and give convenient syntactic sugar for concisely representing standard temporal operators. In Chapters 3 and 4, we give our formalizations of the privacy-relevant portions of the Gramm-Leach-Bliley Act and the Health Insurance Portability and Accountability Act. In Chapter 5, we overview the related work.

Chapter 2

PrivacyLFP: A Logic of Privacy with Fixed Points

As stated, our primary goal in this work is to extend techniques developed in other privacy languages and logics so that the privacy-relevant portions of the Gramm-Leach-Bliley Act (GLBA) [US 99] and the Health Insurance Portability and Accountability Act (HIPAA) [US 02] may be completely formalized. With an eye toward eventual auditing and assigning blame based on agents' irresponsibility [DGJ$^+$10] in the manner of the Logic of Privacy and Utility (LPU) [BDMN06, BDMS07, Bar08], we choose to use LPU as a starting point.

Unfortunately, however, LPU is not sufficiently expressive to permit full formalization of GLBA and HIPAA. In particular, we require constructs for expressing purposes, real-time features, and fixed points. Therefore, we propose a new logic, PrivacyLFP, based on LPU, but with these new constructs. Just as LPU is a particular signature of ATL* [AHK02], PrivacyLFP is a particular signature of the fixed point logic LFP [Räs02, BS06].

Before describing these extensions in detail, we motivate them using three concrete examples from HIPAA and GLBA.

2.1 Background on LPU

Being based on contextual integrity model [Nis04], a philosophical framework of privacy centered around norms of transmission, LPU's fundamental concept is that of the positive and negative norms of a given privacy regulation.

Positive norms, φ^+, state that communication may occur if a condition is satisfied. For example, a positive norm might be that protected health information may be sent *if* the recipient keeps that information confidential. In this way, the positive norms capture the permitting, or "allow", clauses of the regulation. On the other hand, negative norms, φ^-, state that communication may occur only if a condition is satisfied. For example, a negative norm might be that protected health information may be sent *only if* the reciepient keeps that information confidential. In a sense, the negative norms capture the denying clauses of the regulation.

To respect the if-only if duality of positive and negative norms, LPU requires that one of the positive norms and all of the negative norms are satisfied when a disclosure occurs. Thus, to check the compliance of a trace, σ, of send actions against a privacy law in LPU, one essentially checks:

$$\sigma \models \Box \forall p_1, p_2, m.\, \mathrm{send}(p_1, p_2, m) \supset \bigvee_i \varphi_i^+ \wedge \bigwedge_i \varphi_i^-$$

where the φ_i^+s capture the permitting clauses of the law and the φ_i^-s capture the denying clauses of the law.

Also, in introducing LPU, Barth *et al.* give a syntactic characterization of positive and negative norms, which is essentially:

$$\begin{aligned} \text{positive norm } \varphi_i^+ &: \quad \theta \wedge \psi \\ \text{negative norm } \varphi_i^- &: \quad \theta \supset \psi \end{aligned}$$

where θ is a formula that constrains the roles of the sender, recipient, subject, and message contents, and ψ is a temporal constraint formalizing past and future obligations. It may be useful to adopt the slogan "positive norms as conjunction, negative norms as implication" to further appreciate the duality of the two types of norms.

2.2 Motivating Examples

2.2.1 Purposes

In addition to using the disclosure's contents, privacy laws often consider a disclosure's purpose when determining whether it should be allowed or denied. For example, §164.506(c)(1) of HIPAA states:

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

Although the word "purpose" is not found in this clause, the intent is clearly to allow disclosures which have the *purpose* of furthering treatment, payment, or health care operations. Any formalization of this clause must somehow incorporate a disclosure's purpose so that it can be checked against these three permitted classes.

Unfortunately, LPU ignores disclosure purposes. To remedy this, we will extend LPU with a new sort purp of purposes. Purposes will also be equipped with a partial order $\preceq_{\mathcal{U}}$ that models purposes' inherent subtype structure. For example, *administer-blood-test* $\preceq_{\mathcal{U}}$ *treatment* because the purpose of administering a blood test is a particular kind of treatment purpose.

Given appropriate constants and the atomic proposition $(u_1 \in_{\mathcal{U}} u_2)$, which holds when u_1 is a subpurpose of u_2, we can express §164.506(c)(1) as:

$$\begin{aligned} \varphi^+_{\texttt{164.506c1}} \triangleq\ & \mathrm{activerole}(p_1, \textit{covered-entity}) \wedge \\ & (t \in_{\mathcal{T}} \textit{phi}) \wedge \\ & ((u \in_{\mathcal{U}} \textit{treatment}(p_1)) \vee \\ & \ (u \in_{\mathcal{U}} \textit{payment}(p_1)) \vee \\ & \ (u \in_{\mathcal{U}} \textit{healthcare-operations}(p_1))) \end{aligned}$$

2.2.2 Real-Time

Being based on the temporal logic LTL [MP95], LPU is squarely in the philosophical tradition of being concerned solely with the relative order of events, and not the wall-clock time that separates them. We have found that this abstraction perfectly suits many clauses in privacy laws. Unfortunately, however, this abstraction is at odds with other clauses; legislators sometimes wish to impose specific time limits, such as “within 30 days” or “annually”.

For example, §6803(a) of GLBA states that:

> *At the time of establishing a customer relationship with a consumer and not less than annually during the continuation of such relationship, a financial institution shall provide a clear and conspicuous disclosure to such consumer [...], of such financial institution's policies and practices with respect to [disclosing nonpublic personal information].*

Clearly, we will need real-time features to be able to express this clause, since there is no notion of a calendar year in LTL (and, consequently, LPU).

For these features, we borrow ideas from Alur and Henzinger's timed propositional temporal logic (TPTL) [AH94]. Specifically, as in TPTL, we assign a wall-clock time to each state. These times must be nondecreasing with respect to the order of states in the trace. We also borrow the freeze quantifier $\downarrow x.\phi$ which binds x in ϕ to the current state's time.

Using these ideas, if given appropriate beginrole and endrole predicates, we might express §6803(a) of GLBA as:

$$\begin{aligned}
\mathbf{G}\ \forall q, r, p_1.\ & \mathrm{beginrole}(q, r) \land \\
& \quad (r = \mathit{customer}(p_1)) \supset \\
& \qquad \varphi^{-}_{\mathsf{6803a}}
\end{aligned}$$

and

$$\begin{aligned}
\varphi^{-}_{\mathsf{6803a}} \triangleq\ & (\downarrow x.\ \Diamond(\downarrow y.\ (y = x) \land \\
& \qquad\qquad \exists m''.\ \mathrm{send}(p_1, q, m'') \land \\
& \qquad\qquad\qquad \mathrm{is\text{-}annual\text{-}notice}(m'', p_1, q))) \land \\
& ((\downarrow x.\ \Diamond(\downarrow y.\ (y \le x + 365) \land \\
& \qquad\qquad ((\exists m''.\ \mathrm{send}(p_1, q, m'') \land \\
& \qquad\qquad\qquad \mathrm{is\text{-}annual\text{-}notice}(m'', p_1, q)) \lor \\
& \qquad\qquad \mathrm{endrole}(q, \mathit{customer}(p_1))))) \mathcal{W} \\
& \ \mathrm{endrole}(q, \mathit{customer}(p_1)))
\end{aligned}$$

The freeze quantifiers, specifically the fragment $\downarrow x.\ \Diamond(\downarrow y.\ (y \le x + 365) \land$, crucially ensure that, in every state, there exists a state occurring no more than 365 days later in which an annual notice is sent.

In the interest of full disclosure, we wish to admit here that our PrivacyLFP logic will not truly be a temporal logic or literally include freeze quantifiers. Instead, PrivacyLFP is the fixed point logic analogue of the first-order logic obtained by the standard translation of a modal logic to first-order logic: states and times will be characterized using a particular first-order structure. In this way, the freeze quantifier and other temporal operators are but (very) useful syntactic sugar for propositions in our first-order logic. We return to this point in Section 2.3.3.

2.2.3 Fixed Points

As overviewed in Section 2.1, to check the compliance of a trace, σ, of send actions against a privacy law, one essentially checks:

$$\sigma \models \Box \forall p_1, p_2, m.\, \mathrm{send}(p_1, p_2, m) \supset \bigvee_i \varphi_i^+ \wedge \bigwedge_i \varphi_i^-$$

Although not performed in any prior work on LPU, for narrative purposes, suppose that we define the proposition $\mathrm{maysend}(p_1, p_2, m)$ as a macro:

$$\mathrm{maysend}(p_1, p_2, m) \triangleq \bigvee_i \varphi_i^+ \wedge \bigwedge_i \varphi_i^-$$

and instead check:

$$\sigma \models \Box \forall p_1, p_2, m.\, \mathrm{send}(p_1, p_2, m) \supset \mathrm{maysend}(p_1, p_2, m)$$

At this point, we have not made any fundamental changes: the body of the macro can just be substituted in for $\mathrm{maysend}(p_1, p_2, m)$.

In many cases, it works well to follow this approach of simply taking $\mathrm{maysend}(p_1, p_2, m)$ as a macro for the conditions under which the law allows a disclosure to occur. That is, it works well until a clause refers recursively to those conditions. For example, consider §6802(c) of GLBA, which places limits on the reuse of information:

> *Except as otherwise provided in this subchapter, a nonaffiliated third party that receives from a financial institution nonpublic personal information under this section shall not, directly or through an affiliate of such receiving third party, disclose such information to any other person that is a nonaffiliated third party of both the financial institution and such receiving third party, unless such disclosure would be lawful if made directly to such other person by the financial institution.*

Roughly, we would like to express this clause as something like:

$$\begin{aligned}
\varphi^-_{\mathsf{6802c}} \triangleq \forall p'.\ & \neg\mathrm{activerole}(p_1, \mathit{affiliate}(p')) \wedge \\
& \neg\mathrm{activerole}(p_2, \mathit{affiliate}(p')) \wedge \\
& \neg\mathrm{activerole}(p_2, \mathit{affiliate}(p_1)) \wedge \\
& \diamondminus(\mathrm{send}(p', p_1, m) \wedge \\
& \quad \mathrm{activerole}(p', \mathit{institution})) \supset \\
& \quad \diamondminus \mathrm{maysend}(p', p_2, m)
\end{aligned}$$

However, if we define maysend as a macro, then this formalization would not even be syntactically well-formed. The natural idea is to generalize the definition of maysend as a macro to a fixed point definition, so that this formalization is at least syntactically well-formed. Of course, doing so requires a significant extension to LPU, since fixed point operators are not present in that logic.

(At this point, we would like to note that we are significantly overstating the obviousness of this generalization. Of course, once the positive and negative norms are factored out as a maysend macro, generalization from a macro to a fixed point is indeed a natural step; but realizing that this factoring is possible and conceptually useful was a key turning point in our work.)

The remaining question is which fixed point operator is semantically correct for this clause: should it be the least fixed point, μ, the greatest fixed point, ν, or something else altogether? Intuitively, we claim that the greatest fixed point is the correct interpretation since we do not want to impose any constraints beyond those required by the law. Stated differently, we want to allow everything that is not explicitly denied by the law.

As a result, we arrive at the following general top-level formula:

$$\begin{array}{l}\mathbf{G}\ \forall p_1, p_2, m.\, \mathrm{send}(p_1, p_2, m) \supset \\ \qquad\qquad\qquad \big(\nu \mathrm{maysend}(p_1', p_2', m').\ \bigvee_i \varphi_i^+ \wedge \bigwedge_i \varphi_i^-\big)\,(p_1, p_2, m)\end{array}$$

(Note that, for the sake of brevity, we have replaced $\sigma \models \square$ with the equivalent $\mathbf{G}$ modality, meaning "in all states".) Although it is not necessary for our motivating example, one can further generalize this formula to include a least fixed point over the φ_i^+s:

$$\begin{array}{l}\mathbf{G}\ \forall p_1, p_2, m.\, \mathrm{send}(p_1, p_2, m) \supset \\ \qquad\qquad\qquad \big(\nu \mathrm{maysend}(p_1', p_2', m').\ \big(\mu X(p_1'', p_2'', m'').\ \bigvee_i \varphi_i^+\big)(p_1', p_2', m') \wedge \\ \qquad\qquad\qquad\qquad\qquad\qquad \bigwedge_i \varphi_i^-\big)(p_1, p_2, m)\end{array}$$

This reveals an elegant duality between the positive and negative norms. For positive norms, a least fixed point is used because we want to permit no more disclosures than the law does; for negative norms, a greatest fixed point is used because we want to be no more restrictive than the law is.

2.3 PrivacyLFP Logic

Having motivated our extensions to LPU, we now turn to a formal description of our PrivacyLFP-logic. Its core is Least Fixed Point logic (LFP) [BS06, Räs02], which is a first-order logic with least and greatest fixed point operators, and is described in Section 2.3.1. In Section 2.3.2, we detail the particulars of the first-order structure that we assume for PrivacyLFP. Finally, in Section 2.3.3, we give convenient syntactic sugar for temporal operators, including the freeze quantifier.

2.3.1 Syntax and Semantics of Core Logic

Syntax

Terms t come from a collection of domains $\mathcal{D}_s$ (carrier sets), indexed by sorts s, and may mention variables x and y. Predicate symbols $P \in \mathcal{P}$ and predicate variables $X \in \mathcal{X}$ represent respectively known relations over terms and unknown relations (of known arities) over terms. Formulas, φ, ϕ, and ψ, have the following syntax.

$$\begin{array}{rcl}\varphi, \phi, \psi & ::= & P(\vec{t}) \mid X(\vec{t}) \mid \top \mid \neg\varphi \mid \varphi \wedge \psi \mid \exists x{:}s.\varphi \\ & & \mid (\mu X, \vec{x}.\ \varphi)(\vec{t}) \mid (\nu X, \vec{x}.\ \varphi)(\vec{t})\end{array}$$

As is typical, we can define falsehood $\bot$ as $\neg\top$, the disjunction $\varphi \vee \psi$ as $\neg(\neg\varphi \wedge \neg\psi)$, the implication $\varphi \supset \psi$ as $\neg\varphi \vee \psi$, and the universal quantification $\forall x{:}s.\varphi$ as $\neg\exists x{:}s.\neg\varphi$.

In other words, LFP is an extension of first-order logic with the least fixed-point operator $(\mu X(\vec{x}).\varphi)(\vec{t})$ and the greatest fixed-point operator $(\nu X(\vec{x}).\varphi)(\vec{t})$. The former defines an implicit predicate X as the least solution of the equation $X(\vec{x}) \triangleq \varphi$ and checks that the tuple of terms $\vec{t}$

satisfies the predicate (i.e., it lies in the least solution). Both X and $\vec{x}$ are bound in φ and may be tacitly α-renamed. The greatest fixed-point operator is similar, except that it defines the predicate as the *greatest* solution of the same equation. In order to ensure that the least and greatest solutions exist, any occurrences of X in φ must be under an even number of negations.

Semantics

The semantics of LFP are based on those of first-order logic, with provision for the fixed-point operators. Let $\mathcal{D}_s$ be a collection of algebras, indexed by sorts, matching the signature of the terms and predicates of the logic. Let $[\![\, t \,]\!]^\theta$ denote the interpretation of term t under substitution θ for its variables and some implicit interpretation of function symbols which respects their sorts. Let $[\![\, \vec{t} \,]\!]^\theta$ is its component-wise lifting to tuples. Let $\mathcal{I}$ denote a map from $\mathcal{P} \cup \mathcal{X}$ to relations of respective arities over the domains for the corresponding sorts of arguments. The semantics of a formula φ are captured by the relation $\theta; \mathcal{I} \models \varphi$, defined by induction on φ using standard rules as follows:

$$\begin{array}{lll}
\theta;\mathcal{I} \models P(\vec{t}) & \text{iff} & [\![\vec{t}]\!]^\theta \in \mathcal{I}(P) \\
\theta;\mathcal{I} \models X(\vec{t}) & \text{iff} & [\![\vec{t}]\!]^\theta \in \mathcal{I}(X) \\
\theta;\mathcal{I} \models \top & & \text{always} \\
\theta;\mathcal{I} \models \neg\varphi & \text{iff} & \text{not } \theta;\mathcal{I} \models \varphi \\
\theta;\mathcal{I} \models \varphi \wedge \psi & \text{iff} & \theta;\mathcal{I} \models \varphi \text{ and } \theta;\mathcal{I} \models \psi \\
\theta;\mathcal{I} \models \exists x{:}s.\varphi & \text{iff} & \theta[x \mapsto d];\mathcal{I} \models \varphi \text{ for some } d \in \mathcal{D}_s \\
\theta;\mathcal{I} \models (\mu X, \vec{x}.\ \varphi)(\vec{t}) & \text{iff} & [\![\vec{t}]\!]^\theta \in \mu F^{X,\vec{x}}_{\mathcal{I},\theta}(\varphi) \\
\theta;\mathcal{I} \models (\nu X, \vec{x}.\ \varphi)(\vec{t}) & \text{iff} & [\![\vec{t}]\!]^\theta \in \nu F^{X,\vec{x}}_{\mathcal{I},\theta}(\varphi)
\end{array}$$

In the last two clauses, $F^{X,\vec{x}}_{\mathcal{I},\theta}(\varphi) : 2^{\prod_{x \in \vec{x}} \mathcal{D}_{\Gamma(x)}} \to 2^{\prod_{x \in \vec{x}} \mathcal{D}_{\Gamma(x)}}$ is the function that maps a set S of tuples, each with $|\vec{x}|$ components, to $\{\vec{d} \mid \theta[\vec{x} \mapsto \vec{d}];\mathcal{I}[X \mapsto S] \models \varphi\}$, assuming that Γ is a sort assignment for $\vec{x}$. This is a monotone map because of the constraint that every occurrence of X in φ be under an even number of negations. So, its greatest and least fixed points, $\nu F^{X,\vec{x}}_{\mathcal{I},\theta}(\varphi)$ and $\mu F^{X,\vec{x}}_{\mathcal{I},\theta}(\varphi)$, in the lattice $2^{\prod_{x \in \vec{x}} \mathcal{D}_{\Gamma(x)}}$ exist by the Knaster-Tarski theorem [Tar55].

2.3.2 First-Order Structure

At this point, we have a generic first-order logic with least and greatest fixed point operators. However, it cannot currently support privacy applications since the first-order structure is left wholly unspecified. In response, we now provide details of the first-order structure that we assume for PrivacyLFP.

Much of this development closely follows that of LPU [BDMN06, BDMS07, Bar08]; readers familiar with that work may choose to skim this section, but should note the addition of purposes and actions for beginning and ending roles.

Data Model

Principals. We assume a sort prin of principals with an associated carrier set $\mathcal{P}$.

Raw Data and Attributes. To model the raw data over which privacy laws impose flow restrictions, we introduce a sort data and an associated carrier set $\mathcal{D}$. Intuitively, the raw data is unstructured and may even be free text. For this reason, we do not introduce constructors for or operators on sort data. We should note that our notion of raw data corresponds to that of messages in LPU; we reserve the term *message* for our extensible data type built on top of raw data (see below), which is not found in LPU.

By itself, raw data is wholly unsuitable for our purpose: privacy laws do not describe regulations on information flow at the level of bytes or even strings. Instead, they assume various more abstract, structured classes of data, such as "protected health information" and "psychotherapy notes", and regulate according to the classification.

To model these classes of data, we follow LPU's lead and introduce *attributes* which have sort attr and denote members of the carrier set $\mathcal{T}$. As in LPU, relationships between attributes are characterized by a set $\mathcal{C}$ of *computation rules* which dictate when the value of a principal's attribute can be inferred from other information. Thus, a rule is $(T, t) \in \mathcal{C}$, meaning that, for any principal, the value of attribute t can be inferred from the values of the attributes in T (where $T \subseteq \mathcal{T}$ and $t \in \mathcal{T}$).[1] As an example rule, we have $(\{\mathit{street}, \mathit{city}, \mathit{state}\}, \mathit{postal\text{-}code}) \in \mathcal{C}$ because one can infer the postal code from combined knowledge of the street, city, and state. We internalize this notion of computation rules as the proposition $t_1 \in_{\mathcal{T}} t_2$:

$$\theta; \mathcal{I} \models t_1 \in_{\mathcal{T}} t_2 \quad \text{iff} \quad (\{[\![t_2]\!]^\theta\}, [\![t_1]\!]^\theta) \in \mathcal{C}$$

To relate raw data to its attribute classification, we introduce a semantic function data_contents that maps raw data to its abstract contents, a subset of $\mathcal{P} \times \mathcal{T}$. Due to the vast complexity of deciding how raw data should be classified, we cannot give an explicit definition for this function; instead, we rely on an oracle for its implementation. However, to capture both the immediate contents of the data and any indirect information that can be inferred from the immediate contents, we require that the oracle's response is closed with respect to the computation rules:

$$\mathrm{cl}_{\mathcal{C}} \circ \text{data\_contents} = \text{data\_contents}$$

where $\mathrm{cl}_{\mathcal{C}}$ is the closure operator on subsets of $\mathcal{P} \times \mathcal{T}$ with respect to the computation rules in $\mathcal{C}$.

As an example, $(\mathrm{Bob}^{\mathcal{P}}, \mathit{blood\text{-}test}^{\mathcal{T}}(\mathit{11/18/09})) \in \text{data\_contents}(d)$ if and only if the raw data d contains, either directly or indirectly, the results of Bob's blood tests from November 18, 2009.

Purposes. As argued in Section 2.2.1, we require that our logic has some way to express disclosure purposes. To do so, we introduce a sort purp of purposes with carrier set $\mathcal{U}$. Note that parameterized purposes, such as $\mathit{treatment}(p)$ (treatment performed by p), are intentionally allowed.

The carrier set $\mathcal{U}$ is equipped with a partial order $\preceq_{\mathcal{U}}$ that models purposes' structure. If $u_1 \preceq_{\mathcal{U}} u_2$, then we say that u_1 is a specific form of the u_2 purpose. For example, $\mathit{administer\text{-}blood\text{-}test}^{\mathcal{U}} \preceq_{\mathcal{U}} \mathit{treatment}^{\mathcal{U}}$ because administering a blood test is a particular type of treatment purpose.

We internalize this partial order as the proposition $u_1 \in_{\mathcal{U}} u_2$:

$$\theta; \mathcal{I} \models u_1 \in_{\mathcal{U}} u_2 \quad \text{iff} \quad [\![u_1]\!]^\theta \preceq_{\mathcal{U}} [\![u_2]\!]^\theta$$

[1] One might consider generalizing computation rules to include the subject for each attribute, i.e., $(K, (p, t)) \in \mathcal{C}$ where $K \subseteq \mathcal{P} \times \mathcal{T}$ and $(p, t) \in \mathcal{P} \times \mathcal{T}$. However, we leave this generalization to future work since it becomes unclear how to enforce rules that might hold for some principals but might not hold for others.

Messages. By omitting message constructors and including only a contents observer, LPU's data model effectively assumes that all messages are morally lists of subject-attribute pairs. This assumption works well in some cases, but ignores the fact that a privacy law may circumscribe behavior on other message forms. For example, HIPAA gives patients the right to request access to their protected health information, and requires that covered entities respond to such requests (either by granting or denying access). To make a request for access, the patient sends a message listing the information attributes that she would like to access.

One could possibly shoehorn requests for access into LPU's subject-attribute message format using a special "request-for-access" attribute that is itself parameterized by the requested attribute. However, this introduces the problem of who the subject of a "request-for-access" attribute should be, and is somewhat ad hoc.

Therefore, we significantly generalize the data model of LPU by using an *extensible* algebraic data type msg of messages, having carrier set $\mathcal{M}$. To recover the expressiveness of LPU's subject-attribute message format (with the disclosure's purpose added), we include the info message constructor:

$$\mathrm{info} : \mathsf{data} \times \mathsf{purp} \to \mathsf{msg}$$

Thus, a message $\mathrm{info}(d, u)$ carries the raw data d disclosed for purpose u.

Because the message data type is extensible, we can add application-specific message forms as necessary. For example, to cleanly express requests for access in a formalization of HIPAA, we may add a req_for_access message constructor:

$$\mathrm{req\_for\_access} : \mathsf{prin} \times \mathsf{attr} \to \mathsf{msg}$$

To relate a message to the personal information it contains, we include the function msg_contents function, which lifts the data_contents function to messages. As a general principle, msg_contents should be closed under the computation rules in $\mathcal{C}$, that is:

$$\mathrm{cl}_{\mathcal{C}} \circ \mathrm{msg\_contents} = \mathrm{msg\_contents}$$

Since we include the $\mathrm{info}^{\mathcal{M}}$ message constructor by default, we specify its clause of msg_contents as:

$$\mathrm{msg\_contents}(\mathrm{info}^{\mathcal{M}}(d, u)) = \mathrm{data\_contents}(d)$$

Note that closure of the contents of $\mathrm{info}^{\mathcal{M}}$ is inherited from data_contents.

If we included a $\mathrm{req\_for\_access}^{\mathcal{M}}$ message constructor, then, because a request carries no data (its subject-attribute pair acts as a *name* for the requested data), we would define

$$\mathrm{msg\_contents}(\mathrm{req\_for\_access}^{\mathcal{M}}(q, t)) = \{\}$$

Using the msg_contents function, we can give the semantics for a proposition $\mathrm{contains}(m, (q, t))$:

$$\theta; \mathcal{I} \models \mathrm{contains}(m, (q, t)) \quad \text{iff} \quad (\llbracket q \rrbracket^{\theta}, \llbracket t \rrbracket^{\theta}) \in \mathrm{msg\_contents}(\llbracket m \rrbracket^{\theta})$$

Encoding a Trace in the First-Order Structure

In LPU, the evolving system is modeled as a trace σ: an infinite sequence of states $\sigma = s_0 s_1 s_2 \cdots$. Each LPU state is a tuple $s_i = (\kappa_i, \rho_i, a_i)$ of a knowledge map κ_i, role map ρ_i, and an action a_i. The action a_i constrains the shape of the next state, s_{i+1} according to a predefined relation: $s_i \xrightarrow{a_i} s_{i+1}$.

We will use a similar notion of trace. To associate with a state the knowledge held by principals, the roles to which principals belong, the roles in which principals are active, the set of concurrent actions presently occurring, its time, and the interpretation of predicates, we have functions κ, ρ^B, ρ^A, a, and ι, respectively. States s will then be tuples $(\kappa(s), \rho^B(s), \rho^A(s), a(s), \tau(s), \iota(s))$. We now turn to describing these components of states in detail.

Interpretation of Predicates. So that we may refer to states within formula, we introduce a new sort state and associated carrier set $\mathcal{S}$. States from $\mathcal{S}$ are ordered according to the total order $<_{\mathsf{st}}$ (and its natural weakening $\leq_{\mathsf{st}}$). In this way, we may think of states as being natural numbers. This approach to interpreting formulas against traces by making state explicit in formulas is inspired by work on hybrid modal logics [Bla00, CMS06, Bd03].

To interpret formulas of LFP over traces, we restrict ourselves to a fragment of the logic in which the first argument of every atomic formula is the state in which the formula is to be interpreted, so each atomic formula has the form $P(s, \vec{t})$ or $X(s, \vec{t})$. Given a trace σ, we define the interpretation $\mathcal{I}_\sigma$ so that $(s, \vec{d}) \in \mathcal{I}_\sigma(P)$ if and only if $\vec{d} \in \iota(s)(P)$. Moreover, we define $\theta; \sigma \models \varphi$ to mean the satisfaction $\theta; \mathcal{I}_\sigma \models \varphi$ as defined in Section 2.3.1.

Knowledge and the Send Action. We track the knowledge of each principal in state s using a knowledge map $\kappa(s)$ from $\mathcal{P}$ to a subset of $\mathcal{P} \times \mathcal{T}$. (In other words, $\kappa(s) : \mathcal{P} \to 2^{\mathcal{P} \times \mathcal{T}}$.) Thus, if $(q, t) \in \kappa(s)(p)$, then we say that, in state s, principal p knows the value of attribute t for subject q.

Provided that he knows the contents of the message, a principal p_1 can send a message m to another principal p_2. Upon receiving the message, the recipient updates his knowledge state to reflect the contents he just learned and any facts he can compute from them. Sending a message should not affect the roles held by the various principals in the system.

This intuition gives us properties which must be satisfied by the first-order structure for Send actions:

- For all $\mathsf{Send}(p_1, p_2, m) \in a(s)$, we require $\mathrm{msg\_contents}(m) \subseteq \kappa(s)(p_1)$.
- Let $\mathrm{msgs}(p_2)$ be defined as $\{m \mid \mathsf{Send}(p_1, p_2, m) \in a(s) \text{ for some } p_2\}$.
  Then, we require $\kappa(s+1)(p_2) = \mathrm{cl}_{\mathcal{C}}(\kappa(s)(p_2) \cup \bigcup_{m \in \mathrm{msgs}(p_2)} \mathrm{msg\_contents}(m))$.

So that we can access the Send actions in the logical formulas, we include a $\mathrm{send}(s, p_1, p_2, m)$ proposition, meaning that message m is sent from p_1 to p_2 in state s:

$$\theta; \mathcal{I}_\sigma \models \mathrm{send}(s, p_1, p_2, m) \quad \text{iff} \quad \mathsf{Send}([\![p_1]\!]^\theta, [\![p_2]\!]^\theta, [\![m]\!]^\theta) \in a(s)$$

Roles and the $\mathsf{BeginRole}$ and $\mathsf{EndRole}$ Actions. Principals hold roles that enable or restrict their behavior. For example, if Bob is a doctor, he may (or at least should) be able to disclose or receive different information than if he were an insurance representative. To express roles, we follow LPU and introduce a sort role of roles and the corresponding carrier set $\mathcal{R}$.

As in LPU, roles are equipped with a partial order $\preceq_{\mathcal{R}}$ that expresses *role specialization*. That is, if $r_1 \preceq_{\mathcal{R}} r_2$ holds, we say that r_1 is a specialization of role r_2. For example, we would expect $\mathit{psychiatrist}^{\mathcal{R}} \preceq_{\mathcal{R}} \mathit{doctor}^{\mathcal{R}}$ since a psychiatrist is a special type of doctor.

We extend LPU's treatment of roles in two ways. First, we allow general parameterized roles; only a very limited and ad hoc form was present in LPU. For example, we can now cleanly express the "doctor-of-p" role as $\mathit{doctor}(p)$, for each p.

Second, and more significantly, we introduce a distinction between the set of roles to which a principal *belongs* and the role in which he currently *acts*. Although a principal may change the roles to which he belongs, belonging to a role is generally a longer term property than being active in a role. For example, a doctor who is also a member of an oversight board would belong to both the *doctor* and *oversight-board-member* roles, but would freely alternate his active role between the two from state to state depending on his duties in that state.

By having an explicit notion of belonging to, and not just acting in, a role, we will be able to formalize legal clauses that require certain privacy-related behavior when a client or patient *belongs to* some role. For example, §6803(a) of GLBA requires that financial institutions annually provide customers with a privacy notice. If we only had a notion of transiently acting in a customer role, this clause would be difficult, if not impossible, to correctly express in our logic.

The roles, in state s, to which principals belong and in which they are active are tracked using distinct role maps $\rho^B(s)$ and $\rho^A(s)$, respectively. Because a principal may belong to multiple roles at once but may be active in at most one role, $\rho^B(s)$ is a total function from $\mathcal{P}$ to subsets of $\mathcal{R}$, whereas $\rho^A(s)$ is a partial function from $\mathcal{P}$ to $\mathcal{R}$.

A principal can freely and silently change his active role from state to state, but it must always be a role to which he belongs: we require that

$$\text{If defined, } \rho^A(s)(p) \in \rho^B(s)(p), \text{ for all states } s \in \mathcal{S} \text{ and all } p \in \mathcal{P}.$$

To capture active roles in the logical formulae, we include a proposition $\mathrm{activerole}(s, p, r)$, meaning that, in state s, principal p is active in role r:

$$\theta; \mathcal{I}_\sigma \models \mathrm{activerole}(s, p, r) \quad \text{iff} \quad [\![\, r \,]\!]^\theta = \rho^A(s)([\![\, p \,]\!]^\theta)$$

To change the set of roles he belongs to, a principal must use the following $\mathsf{BeginRole}$ and $\mathsf{EndRole}$ actions[2]. When starting to belong to a new role, a principal must also start belonging to all generalizations of that role. (If Bob starts belonging to the psychiatrist role, he must also start belonging to the more general role of doctor.) Moreover, no principals gain knowledge when one starts belonging to a new role. Dually, when a principal finishes belonging to a role, he must also finish belonging to all specializations of that role. (If Bob finishes belonging to the doctor role, he must no longer hold the specialized psychiatrist role.) Again, no principals learn knowledge when one finishes belonging to a role. In addition, to avoid race conditions, a principal should not simultaneously begin and end belonging to a role.

This intuition yields the following properties required of our first-order structure:

- Let $\mathrm{roles}^+(p) = \{r \mid \mathsf{BeginRole}(p, r) \in a(s)\}$ and $\mathrm{roles}^-(p) = \{r \mid \mathsf{EndRole}(p, r) \in a(s)\}$. Then, we require:
  - $\rho^B(s+1)(p) = \Big(\rho^B(s)(p) \cup \bigcup_{r \in \mathrm{roles}(p)} \mathrm{succ}_{\preceq_\mathcal{R}}(r)\Big) \setminus \bigcup_{r \in \mathrm{roles}^-(p)} \mathrm{pred}_{\preceq_\mathcal{R}}(r)$, and
  - $\mathrm{succ}_{\preceq_\mathcal{R}}(r_1) \cap \mathrm{pred}_{\preceq_\mathcal{R}}(r_2) = \emptyset$ for all $r_1 \in \mathrm{roles}^+(p)$ and $r_2 \in \mathrm{roles}^-(p)$

  where $\mathrm{succ}_{\preceq_\mathcal{R}}(r) = \{r' \in \mathcal{R} \mid r \preceq_\mathcal{R} r'\}$ and $\mathrm{pred}_{\preceq_\mathcal{R}}(r) = \{r' \in \mathcal{R} \mid r' \preceq_\mathcal{R} r\}$.

To include in the logical formulae the roles to which a principal belongs, we include a proposition $\mathrm{belongstorole}(s, p, r)$:

$$\theta; \mathcal{I}_\sigma \models \mathrm{belongstorole}(s, p, r) \quad \text{iff} \quad [\![\, r \,]\!]^\theta \in \rho^B(s)([\![\, p \,]\!]^\theta)$$

[2] Perhaps $\mathsf{StartBelongingToRole}$ and $\mathsf{FinishBelongingToRole}$ would have been more precise names, but they are much too verbose.

It will also be useful to have a method for referencing the beginning and ending events for a principal's role. This is found especially in §6803 of GLBA (see Chapter 3). For this purpose, we include $\mathrm{beginrole}(s, p, r)$ and $\mathrm{endrole}(s, p, r)$ propositions:

$$\begin{array}{lll} \theta; \mathcal{I}_\sigma \models \mathrm{beginrole}(s,p,r) & \text{iff} & \mathsf{BeginRole}([\![\, p \,]\!]^\theta, [\![\, r \,]\!]^\theta) \in a(s) \\ \theta; \mathcal{I}_\sigma \models \mathrm{endrole}(s,p,r) & \text{iff} & \mathsf{EndRole}([\![\, p \,]\!]^\theta, [\![\, r \,]\!]^\theta) \in a(s) \end{array}$$

Times

As described in Section 2.2.2, we wish to express real-time properties similar to that of Alur and Henzinger's TPTL [AH94]. Consequently, $\tau(s)$ is the time at which state s occurs.

We introduce a sort time and the first-order function symbol time of arity 1 so that $\mathrm{time}(s)$ is interpreted as $\tau(s)$. Moreover, propositions $<$ and the natural weakening to $\leq$, interpreted as a total order on times, are included. Similarly to TPTL, we require that the times assigned to states observe a monotonicity property: for all states s and s' such that $s <_{\mathsf{st}} s'$, we must have $\mathrm{time}(s) < \mathrm{time}(s')$.

2.3.3 Syntactic Sugar

At this point, we can express temporal notions on the basis of the particulars of our first-order structure. For example, to say that, in all states in the future of state s, principal p is active in the role of an institution, we could write:

$$\forall i{:}\mathsf{state}.\, (s \leq_{\mathsf{st}} i) \supset \mathrm{activerole}(i, p, \mathit{institution})$$

Although the needed expressive power is there, the syntax for accessing it is somewhat cumbersome. To alleviate this additional burden, we choose to introduce convenient syntactic sugar.

We will express this syntactic sugar in the form $(\phi)^{@s} \triangleq \varphi$, meaning that, if the current state is s, then ϕ is simply syntactic sugar for φ. Since φ may itself contain propositions annotated with ${}^{@s'}$, this definition takes the flavor of a translation. This definition follows the Kripke semantics of the standard LTL operators [MP95], interpreting the meta-language quantifiers, etc. as the corresponding first-order constructs.

$$\begin{array}{rcl} (P(\vec{t}))^{@s} & \triangleq & P(s, \vec{t}) \\ (X(\vec{t}))^{@s} & \triangleq & X(s, \vec{t}) \\ \\ (\top)^{@s} & \triangleq & \top \\ (\phi \wedge \psi)^{@s} & \triangleq & \phi^{@s} \wedge \psi^{@s} \\ (\neg\phi)^{@s} & \triangleq & \neg\phi^{@s} \\ (\exists x{:}\tau.\, \phi)^{@s} & \triangleq & \exists x{:}\tau.\, \phi^{@s} \\ \\ ((\mu X(\vec{x}).\ \phi)(\vec{t}))^{@s} & \triangleq & (\mu X(y, \vec{x}).\ \phi^{@y})(s, \vec{t}) \\ ((\nu X(\vec{x}).\ \phi)(\vec{t}))^{@s} & \triangleq & (\nu X(y, \vec{x}).\ \phi^{@y})(s, \vec{t}) \end{array}$$

$$
\begin{aligned}
(\mathbf{G}\ \phi)^{@s} &\triangleq \forall s'.\, \phi^{@s'} \\
(\Diamond \phi)^{@s} &\triangleq \exists s'.\, (s \leq_{\mathsf{st}} s') \land \phi^{@s'} \\
(\Box \phi)^{@s} &\triangleq \forall s'.\, (s \leq_{\mathsf{st}} s') \land \phi^{@s'} \\
(\diamondminus \phi)^{@s} &\triangleq \exists s'.\, (s' \leq_{\mathsf{st}} s) \land \phi^{@s'} \\
(\boxminus \phi)^{@s} &\triangleq \forall s'.\, (s' \leq_{\mathsf{st}} s) \land \phi^{@s'} \\
(\phi\, \mathcal{U}\, \psi)^{@s} &\triangleq \exists j{:}\mathsf{state}.\, (s \leq_{\mathsf{st}} j) \land \psi^{@j} \land \\
&\qquad\qquad\qquad (\forall i{:}\mathsf{state}.\, (s \leq_{\mathsf{st}} i) \land (i <_{\mathsf{st}} j) \supset \phi^{@i}) \\
(\phi\, \mathcal{S}\, \psi)^{@s} &\triangleq \exists j{:}\mathsf{state}.\, (j \leq_{\mathsf{st}} s) \land \psi^{@j} \land \\
&\qquad\qquad\qquad (\forall i{:}\mathsf{state}.\, (j <_{\mathsf{st}} i) \land (i \leq_{\mathsf{st}} s) \supset \phi^{@i}) \\
(\bigcirc \phi)^{@s} &\triangleq \phi^{@(s+1)} \\
(\downarrow x.\, \phi)^{@s} &\triangleq ([\mathrm{time}(s)/x]\phi)^{@s}
\end{aligned}
$$

We can then obtain the remaining standard connectives by the usual duality-based definitions.

$$
\begin{aligned}
(\bot)^{@s} &\triangleq (\neg\top)^{@s} \\
(\phi \lor \psi)^{@s} &\triangleq (\neg(\neg\phi \land \neg\psi))^{@s} \\
(\phi \supset \psi)^{@s} &\triangleq (\neg\phi \lor \psi)^{@s} \\
(\forall x{:}\tau.\, \phi)^{@s} &\triangleq (\neg\exists x{:}\tau.\, \neg\phi)^{@s} \\
\\
(\phi\, \mathcal{W}\, \psi)^{@s} &\triangleq ((\phi\, \mathcal{U}\, \psi) \lor \Box\phi)^{@s}
\end{aligned}
$$

We claim that all of these abbreviations are semantically justified, given an expected semantics for a first-order version of the modal μ-calculus [BS06]. However, because the underlying first-order logic with least and greatest fixed point operators is the smallest necessary core, we do not pursue the second semantics needed to make this claim precise.

2.4 Conclusion

In this chapter, we have presented PrivacyLFP, a particular signature of first-order logic with fixed point operators, as an extension of the privacy fragment of LPU. We motivated the key extensions through the use of concrete examples from GLBA and HIPAA. Although PrivacyLFP does not include temporal operators as primitive connectives, we gave a set of convenient abbreviations for them in terms of constructs provided by the first-order structure.

With this logic in hand, we are now prepared to tackle the formalization of GLBA and HIPAA.

Chapter 3

Gramm-Leach-Bliley Act

In this chapter, we present a complete formalization of the privacy component of the Gramm-Leach-Bliley Act (GLBA) [US 99], namely §§6802 and 6803. We begin with a top-level formula and then proceed clause-by-clause through the law.

3.1 Top-Level Formula

We need a means of combining the (positive and) negative norms we will obtain from a clause-by-clause consideration of GLBA. As in LPU, this is done by a top-level formula; it is the top-level formula that is checked when verifying that a trace of actions complies with the privacy law. The top-level formula that we propose for GLBA is:

$$
\begin{aligned}
&\mathbf{G}\ ((\forall p'_1, p'_2{:}\mathsf{prin}.\ \forall m'{:}\mathsf{msg}.\\
&\qquad \mathrm{hlsend}(p'_1, p'_2, m') \supset\\
&\qquad\quad (\nu \mathrm{maysend}(p_1, p_2, m).\ \forall d{:}\mathsf{data}.\ \forall u{:}\mathsf{purp}.\ \forall q{:}\mathsf{prin}.\ \forall t{:}\mathsf{attr}.\\
&\qquad\qquad\qquad\qquad\qquad\qquad (m = \mathrm{info}(d, u)) \wedge \mathrm{contains}(m, q, t) \supset\\
&\qquad\qquad\qquad\qquad\qquad\qquad\quad \varphi^{-}_{\mathsf{6802ae}} \wedge \varphi^{-}_{\mathsf{6802be}} \wedge\\
&\qquad\qquad\qquad\qquad\qquad\qquad\quad \varphi^{-}_{\mathsf{6802c}} \wedge \varphi^{-}_{\mathsf{6802d}}\\
&\qquad\quad)(p'_1, p'_2, m')) \wedge\\
&\quad (\forall q, p{:}\mathsf{prin}.\ \forall r{:}\mathsf{role}.\\
&\qquad \mathrm{beginrole}(q, r) \wedge (r = \mathit{customer}(p)) \supset\\
&\qquad\quad \varphi^{-}_{\mathsf{6803a}} \vee \varphi^{+}_{\mathsf{6803d1}}))
\end{aligned}
$$

where hlsend is a macro defining an abstraction over the physical recipient of the message, as described in the discussion of §6809(9). Note the use of the greatest fixed point operator, as motivated in Section 2.2.3; this is a novel feature of our work.

Also, note that GLBA places obligations on the action of beginning to hold a role, so these obligations live outside the greatest fixed point for send actions.

3.2 §6802 Obligations with respect to disclosures of personal information

6802(a) Notice Requirements

> *Except as otherwise provided in this subtitle, a financial institution may not, directly or through any affiliate, disclose to a nonaffiliated third party any nonpublic personal information, unless such financial institution provides or has provided to the consumer a notice that complies with section 6803 of this title.*

$$
\begin{aligned}
\varphi^{-}_{\mathtt{6802a}} \triangleq\ & \text{activerole}(p_1, \mathit{institution}) \land \\
& \neg\text{activerole}(p_2, \mathit{affiliate}(p_1)) \land \\
& \text{belongstorole}(q, \mathit{consumer}(p_1)) \land \\
& (t \in_{\mathcal{T}} \mathit{npi}) \supset \\
& \quad \diamondminus(\exists m''.\ \text{hlsend}(p_1, q, m'') \land \\
& \qquad\qquad \text{is-notice-of-disclosure}(m'', p_1, p_2, (q, t), u)) \lor \\
& \quad \Diamond(\exists m''.\ \text{hlsend}(p_1, q, m'') \land \\
& \qquad\qquad \text{is-notice-of-disclosure}(m'', p_1, p_2, (q, t), u))
\end{aligned}
$$

6802(b) Opt Out

As we will see, 6802(b) contains a negative norm and an exception. Therefore, we define:

$$\varphi^{-}_{\mathtt{6802b}} \triangleq \varphi^{-}_{\mathtt{6802b1}} \lor \varphi^{+}_{\mathtt{6802b2}}$$

6802(b)(1) In General

> *A financial institution may not disclose nonpublic personal information to a nonaffiliated third party unless—*
>
> *(A) such financial institution clearly and conspicuously discloses to the consumer, in writing or in electronic form or other form permitted by the regulations prescribed under section 6804 of this title, that such information may be disclosed to such third party;*
>
> *(B) the consumer is given the opportunity, before the time that such information is initially disclosed, to direct that such information not be disclosed to such third party; and*
>
> *(C) the consumer is given an explanation of how the consumer can exercise that nondisclosure option.*

At first glance, it appeared to us that 6802(a) and 6802(b)(1)(A) impose the same requirement. However, we now interpret 6802(a) as requiring notices regarding disclosures that have taken or will *actually* take place, whereas 6802(b)(1) requires notice of the kinds of disclosures an institution may *potentially* make. Assuming that c is a constant representing the minimum length of the consumer's opportunity for opt-out, we can capture this clause as:

$$
\begin{aligned}
\varphi^{-}_{\mathtt{6802b1}} \triangleq {\downarrow}x.\ & \text{activerole}(p_1, \mathit{institution}) \land \\
& \neg\text{activerole}(p_2, \mathit{affiliate}(p_1)) \land
\end{aligned}
$$

$$
\begin{array}{l}
\text{belongstorole}(q, \mathit{consumer}(p_1)) \wedge \\
(t \in_{\mathcal{T}} \mathit{npi}) \supset \\
\quad (\neg \exists m'''.\ \text{hlsend}(q, p_1, m''') \wedge \\
\qquad\qquad \text{is-opt-out}(m''', p_1, p_2, (q, t), u))\ \mathcal{S} \\
\quad (\downarrow y.\ (x \geq y + c) \wedge \\
\qquad \exists m''.\ \text{hlsend}(p_1, q, m'') \wedge \\
\qquad\qquad \text{is-notice-of-potential-disclosure}(m'', p_1, p_2, (q, t), u))
\end{array}
$$

6802(b)(2) Exception

> *This subsection shall not prevent a financial institution from providing nonpublic personal information to a nonaffiliated third party to perform services for or functions on behalf of the financial institution, including marketing of the financial institution's own products or services, or financial products or services offered pursuant to joint agreements between two or more financial institutions that comply with the requirements imposed by the regulations prescribed under section 6804 of this title, if the financial institution fully discloses the providing of such information and enters into a contractual agreement with the third party that requires the third party to maintain the confidentiality of such information.*

$$
\begin{array}{ll}
\varphi^{+}_{\mathsf{6802b2}} \triangleq & \text{activerole}(p_1, \mathit{institution}) \wedge \\
& \neg\text{activerole}(p_2, \mathit{affiliate}(p_1)) \wedge \\
& \text{belongstorole}(q, \mathit{consumer}(p_1)) \wedge \\
& (t \in_{\mathcal{T}} \mathit{npi}) \wedge \\
& (u \in_{\mathcal{U}} \mathit{perform\text{-}services}) \wedge \\
& \diamondminus(\exists m''.\ \text{hlsend}(p_1, q, m'') \wedge \\
& \qquad\qquad \text{is-notice-of-potential-disclosure}(m'', p_1, p_2, (q, t), u)) \wedge \\
& \text{exists-confidentiality-agreement}(p_1, p_2, t)
\end{array}
$$

6802(c) Limits on Reuse of Information

> *Except as otherwise provided in this subchapter, a nonaffiliated third party that receives from a financial institution nonpublic personal information under this section shall not, directly or through an affiliate of such receiving third party, disclose such information to any other person that is a nonaffiliated third party of both the financial institution and such receiving third party, unless such disclosure would be lawful if made directly to such other person by the financial institution.*

This clause was the key to motivating the introduction of greatest fixed points into PrivacyLFP, as seen in Section 2.2.3. We critically need to be able to refer to maysend(p', p_2, m'') to model the requirement that information may not be reused "unless such disclosure would be lawful if made directly to such other person by the financial institution." We need some way to characterize GLBA's reflection on its own definition of lawful disclosures; fixed points fit the bill.

$$
\begin{array}{ll}
\varphi^{-}_{\mathsf{6802c}} \triangleq \forall p', m''. & \neg\text{activerole}(p_1, \mathit{affiliate}(p')) \wedge \\
& (\neg\text{activerole}(p_2, \mathit{affiliate}(p')) \wedge \\
& \ \neg\text{activerole}(p_2, \mathit{affiliate}(p_1))) \wedge
\end{array}
$$

$$\begin{aligned}
&(t \in_{\mathcal{T}} \mathit{npi}) \wedge \\
&\diamondminus(\mathrm{hlsend}(p', p_1, m'') \wedge \\
&\quad \mathrm{contains}(m'', q, t) \wedge \\
&\quad \mathrm{activerole}(p', \mathit{institution}) \wedge \\
&\quad \neg\mathrm{activerole}(p_1, \mathit{affiliate}(p')) \wedge \\
&\quad \mathrm{belongstorole}(q, \mathit{consumer}(p'))) \supset \\
&\quad \diamondminus\mathrm{maysend}(p', p_2, m'')
\end{aligned}$$

6802(d) Limitations on the Sharing of Account Number Information for Marketing Purposes

> *A financial institution shall not disclose, other than to a consumer reporting agency, an account number or similar form of access number or access code for a credit card account, deposit account, or transaction account of a consumer to any nonaffiliated third party for use in telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer.*

This captures the fact that if an institution p_1 ever sends an account number, or similar form of access number or code, to a nonaffiliated third party p_2 which uses the number for marketing purposes, then p_2 must be a consumer reporting agency. This is a subtly different notion from preventing the institution's disclosure from being marketing related, and critically depends on the use of temporal future modalities.

$$\begin{aligned}
\varphi^{-}_{\mathtt{6802d}} \triangleq\ & \mathrm{activerole}(p_1, \mathit{institution}) \wedge \\
& \neg\mathrm{activerole}(p_2, \mathit{affiliate}(p_1)) \wedge \\
& \mathrm{belongstorole}(q, \mathit{consumer}(p_1)) \wedge \\
& (t \in_{\mathcal{T}} \mathit{account\text{-}number}) \wedge \\
& \Diamond(\exists p', m'', d', u', t'.\ \mathrm{hlsend}(p_2, p', m'') \wedge \\
& \qquad\qquad\qquad\qquad (m'' = \mathrm{info}(d', u')) \wedge \\
& \qquad\qquad\qquad\qquad \mathrm{contains}(m'', q, t') \wedge \\
& \qquad\qquad\qquad\qquad (t' \in_{\mathcal{T}} t) \wedge \\
& \qquad\qquad\qquad\qquad (u' \in_{\mathcal{U}} \mathit{marketing})) \supset \\
& \quad \mathrm{activerole}(p_2, \mathit{consumer\text{-}reporting\text{-}agency})
\end{aligned}$$

6802(e) General Exceptions

> *Subsections (a) and (b) of this section shall not prohibit the disclosure of nonpublic personal information—*

Therefore, we create versions of 6802(a) and (b) which carry the exceptions listed here:

$$\begin{aligned}
\varphi^{-}_{\mathtt{6802ae}} \triangleq\ & \varphi^{-}_{\mathtt{6802a}} \vee \\
& \varphi^{+}_{\mathtt{6802e1}} \vee \varphi^{+}_{\mathtt{6802e2}} \vee \\
& \varphi^{+}_{\mathtt{6802e3}} \vee \varphi^{+}_{\mathtt{6802e4}} \vee \\
& \varphi^{+}_{\mathtt{6802e5}} \vee \varphi^{+}_{\mathtt{6802e6}} \vee \\
& \varphi^{+}_{\mathtt{6802e7}} \vee \varphi^{+}_{\mathtt{6802e8}}
\end{aligned}$$

and

$$\begin{aligned}\varphi^{-}_{\mathtt{6802be}} \triangleq{} & \varphi^{-}_{\mathtt{6802b}} \lor \\ & \varphi^{+}_{\mathtt{6802e1}} \lor \varphi^{+}_{\mathtt{6802e2}} \lor \\ & \varphi^{+}_{\mathtt{6802e3}} \lor \varphi^{+}_{\mathtt{6802e4}} \lor \\ & \varphi^{+}_{\mathtt{6802e5}} \lor \varphi^{+}_{\mathtt{6802e6}} \lor \\ & \varphi^{+}_{\mathtt{6802e7}} \lor \varphi^{+}_{\mathtt{6802e8}}\end{aligned}$$

6802(e)(1)

> *as necessary to effect, administer, or enforce a transaction requested or authorized by the consumer, or in connection with—*
>
> *(A) servicing or processing a financial product or service requested or authorized by the consumer;*
>
> *(B) maintaining or servicing the consumer's account with the financial institution, or with another entity as part of a private label credit card program or other extension of credit on behalf of such entity; or*
>
> *(C) a proposed or actual securitization, secondary market sale (including sales of servicing rights), or similar transaction related to a transaction of the consumer;*

We have the following positive norm for this exception. Given GLBA's lack of further specification of "extension of credit on behalf of", we choose to implement this feature with a new predicate, extends-credit-on-behalf, whose semantics are given by an oracle.

$$\begin{aligned}\varphi^{+}_{\mathtt{6802e1}} \triangleq{} & (u \in_{\mathcal{U}} \mathit{process\text{-}consumer\text{-}authorized\text{-}service}(q)) \lor \\ & ((\exists p'.\ (p' = p_1) \lor \\ & \qquad \text{extends-credit-on-behalf}(p_1, p')) \land \\ & \ (u \in_{\mathcal{U}} \mathit{maintain\text{-}consumer\text{-}account}(q, p'))) \lor \\ & (u \in_{\mathcal{U}} \mathit{securitization\text{-}sale\text{-}etc}(q))\end{aligned}$$

6802(e)(2)

> *with the consent or at the direction of the consumer;*

Again, we rely on an oracle to give semantics to the new is-consent-for-disclosure:

$$\begin{aligned}\varphi^{+}_{\mathtt{6802e2}} \triangleq \exists m''.\ & \diamondminus \text{hlsend}(q, p_1, m'') \land \\ & \text{is-consent-for-disclosure}(m'', p_1, p_2, (q, t), u)\end{aligned}$$

6802(e)(3)

> *(A) to protect the confidentiality or security of the financial institution's records pertaining to the consumer, the service or product, or the transaction therein;*
>
> *(B) to protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability;*
>
> *(C) for required institutional risk control, or for resolving customer disputes or inquiries;*
>
> *(D) to persons holding a legal or beneficial interest relating to the consumer; or*

(E) to persons acting in a fiduciary or representative capacity on behalf of the consumer;

$$\begin{aligned}\varphi^{+}_{\mathsf{6802e3}} \triangleq\ & (u \in_{\mathcal{U}} \textit{protect-records-security}(q)) \vee \\ & (u \in_{\mathcal{U}} \textit{fraud-prevention}) \vee \\ & ((u \in_{\mathcal{U}} \textit{required-risk-control}) \vee \\ & \ (u \in_{\mathcal{U}} \textit{resolve-customer-dispute}(q))) \vee \\ & \text{activerole}(p_2, \textit{beneficial-interest}(q)) \vee \\ & \text{activerole}(p_2, \textit{financial-representative}(q))\end{aligned}$$

6802(e)(4)

to provide information to insurance rate advisory organizations, guaranty funds or agencies, applicable rating agencies of the financial institution, persons assessing the institution's compliance with industry standards, and the institution's attorneys, accountants, and auditors;

$$\begin{aligned}\varphi^{+}_{\mathsf{6802e4}} \triangleq\ & \text{activerole}(p_2, \textit{insurance-rate-advisory-org}) \vee \\ & \text{activerole}(p_2, \textit{guaranty-agency}) \vee \\ & \text{activerole}(p_2, \textit{rating-agency}(p_1)) \vee \\ & \text{activerole}(p_2, \textit{compliance-assessor}(p_1)) \vee \\ & (\text{activerole}(p_2, \textit{attorney}(p_1)) \vee \\ & \ \text{activerole}(p_2, \textit{accountant}(p_1)) \vee \\ & \ \text{activerole}(p_2, \textit{auditor}(p_1)))\end{aligned}$$

6802(e)(5)

to the extent specifically permitted or required under other provisions of law and in accordance with the Right to Financial Privacy Act of 1978 [12 U.S.C. 3401 et seq.], to law enforcement agencies (including a Federal functional regulator, the Secretary of the Treasury with respect to subchapter II of chapter 53 of title 31, and chapter 2 of title I of Public Law 91–508 (12 U.S.C. 1951–1959), a State insurance authority, or the Federal Trade Commission), self-regulatory organizations, or for an investigation on a matter related to public safety;

$$\begin{aligned}\varphi^{+}_{\mathsf{6802e5}} \triangleq\ & (\text{specifically-permitted-or-required-by-law}(p_1, p_2, (q, t), u) \vee \\ & \ \text{in-accordance-with-Right-to-Financial-Privacy-Act-of-1978}(p_1, p_2, (q, t), u)) \vee \\ & \text{activerole}(p_2, \textit{law-enforcement-agency}) \vee \\ & \text{activerole}(p_2, \textit{self-regulatory-org}) \vee \\ & (u \in_{\mathcal{U}} \textit{public-safety-investigation})\end{aligned}$$

To simplify our formalization of GLBA, we assume that an oracle provides semantics for the new predicate in-accordance-with-Right-to-Financial-Privacy-Act-of-1978; a formalization of that law would eliminate the need for this oracle, but we choose not to do so. On the other hand, we use an oracle to give semantics for the permitted-required-by-law out of necessity: we cannot possibly give formalizations of all laws or a semantics for all possible judicial interpretations of those laws.

6802(e)(6)

> *(A) to a consumer reporting agency in accordance with the Fair Credit Reporting Act [15 U.S.C. 1681 et seq.], or*
>
> *(B) from a consumer report reported by a consumer reporting agency;*

$$\begin{aligned}
\varphi^{+}_{\mathsf{6802e6}} \triangleq\ & (\text{activerole}(p_2, \textit{consumer-reporting-agency}) \wedge \\
& \ \text{in-accordance-with-Fair-Credit-Reporting-Act}(p_1, p_2, (q,t), u)) \vee \\
& \diamondminus(\exists p', m''.\ \text{activerole}(p', \textit{consumer-reporting-agency}) \wedge \\
& \qquad\qquad\quad \text{hlsend}(p', p_1, m'') \wedge \\
& \qquad\qquad\quad \text{is-consumer-report}(m'') \wedge \\
& \qquad\qquad\quad \text{contains}(m'', q, t))
\end{aligned}$$

Oracles are assumed for the is-consumer-report and in-accordance-with-Fair-Credit-Reporting-Act.

6802(e)(7)

> *in connection with a proposed or actual sale, merger, transfer, or exchange of all or a portion of a business or operating unit if the disclosure of nonpublic personal information concerns solely consumers of such business or unit; or*

$$\begin{aligned}
\varphi^{+}_{\mathsf{6802e7}} \triangleq \exists p', p''.\ & \text{belongstorole}(p'', \textit{subunit}(p')) \wedge \\
& ((u \in_{\mathcal{U}} \textit{sale}(p'')) \vee \\
& \ (u \in_{\mathcal{U}} \textit{merger}(p'')) \vee \\
& \ (u \in_{\mathcal{U}} \textit{transfer}(p'')) \vee \\
& \ (u \in_{\mathcal{U}} \textit{exchange}(p''))) \wedge \\
& \text{belongstorole}(q, \textit{consumer}(p''))
\end{aligned}$$

6802(e)(8)

> *to comply with Federal, State, or local laws, rules, and other applicable legal requirements; to comply with a properly authorized civil, criminal, or regulatory investigation or subpoena or summons by Federal, State, or local authorities; or to respond to judicial process or government regulatory authorities having jurisdiction over the financial institution for examination, compliance, or other purposes as authorized by law.*

$$\begin{aligned}
\varphi^{+}_{\mathsf{6802e8}} \triangleq\ & (u \in_{\mathcal{U}} \textit{compliance-with-legal-requirements}) \vee \\
& ((u \in_{\mathcal{U}} \textit{compliance-with-investigation}) \vee \\
& \ (u \in_{\mathcal{U}} \textit{compliance-with-summons})) \vee \\
& (\diamondminus(\exists m''.\ \text{hlsend}(p_2, p_1, m'') \wedge \\
& \qquad\qquad \text{is-response-to}(m, m'')) \wedge \\
& \ (\text{activerole}(p_2, \textit{judicial-process}) \vee \\
& \ \ \text{activerole}(p_2, \textit{government-regulatory-authority}(p_1))) \wedge \\
& \ (u \in_{\mathcal{U}} \textit{authorized-by-law}(p_2)))
\end{aligned}$$

Note that we capture purposes for which the judicial process or regulatory authority, p_2, is authorized by law by structuring those purposes so that they are subpurposes of $\textit{authorized-by-law}(p_2)$.

3.3 §6803 Disclosure of institution privacy policy

6803(a) Disclosure Required

> *At the time of establishing a customer relationship with a consumer and not less than annually during the continuation of such relationship, a financial institution shall provide a clear and conspicuous disclosure to such consumer, in writing or in electronic form or other form permitted by the regulations prescribed under section 6804 of this title, of such financial institution's policies and practices with respect to—*
>
> *(1) disclosing nonpublic personal information to affiliates and nonaffiliated third parties, consistent with section 6802 of this title, including the categories of information that may be disclosed;*
>
> *(2) disclosing nonpublic personal information of persons who have ceased to be customers of the financial institution; and*
>
> *(3) protecting the nonpublic personal information of consumers.*

To capture this requirement, we want to enforce continuing annual notices for each principal that begins a customer role with the financial institution. To do so, we use:

$$\begin{aligned}
\mathbf{G}\ \forall q, r, p_1.\ & \mathrm{beginrole}(q, r) \wedge \\
& \quad (r = \mathit{customer}(p_1)) \supset \\
& \qquad \varphi^-_{\mathtt{6803a}} \vee \varphi^+_{\mathtt{6803d1}}
\end{aligned}$$

where $\varphi^+_{\mathtt{6803d1}}$ is defined below and

$$\begin{aligned}
\varphi^-_{\mathtt{6803a}} \triangleq\ & (\exists m''.\ \mathrm{hlsend}(p_1, q, m'') \wedge \\
& \qquad \text{is-annual-notice}(m'', p_1, q)) \wedge \\
& \quad ((\downarrow x.\ \Diamond(\downarrow y.\ (y \leq x + 365) \wedge \\
& \qquad\qquad ((\exists m''.\ \mathrm{hlsend}(p_1, q, m'') \wedge \\
& \qquad\qquad\qquad \text{is-annual-notice}(m'', p_1, q)) \vee \\
& \qquad\qquad \mathrm{endrole}(q, \mathit{customer}(p_1))))) \ \mathcal{W} \\
& \quad \mathrm{endrole}(q, \mathit{customer}(p_1)))
\end{aligned}$$

Note the use of the weak until operator $\mathcal{W}$. The weak version is necessary because it is possible (in theory) that a customer relationship never ends.

This clause was a primary motivating factor in our decision to distinguish active roles from the roles to which a principal belongs. If we had only a notion of active role, it would be difficult to speak about a continuing customer relationship.

6803(b) Regulations

> *Disclosures required by subsection (a) shall be made in accordance with the regulations prescribed under section 6804 of this title.*

§6804 talks about individual regulations enacted by various oversight bureaus. If we were to model all of these individual regulations, then more would need to be done here. However, since we choose not to model those regulations, this clause is automatically satisfied.

6803(c) Information to be Included

The disclosure required by subsection (a) shall include—

(1) the policies and practices of the institution with respect to disclosing nonpublic personal information to nonaffiliated third parties, other than agents of the institution, consistent with section 6802 of this title, and including—

  (A) the categories of persons to whom the information is or may be disclosed, other than the persons to whom the information may be provided pursuant to section 6802(e) of this title; and

  (B) the policies and practices of the institution with respect to disclosing of nonpublic personal information of persons who have ceased to be customers of the financial institution;

(2) the categories of nonpublic personal information that are collected by the financial institution;

(3) the policies that the institution maintains to protect the confidentiality and security of nonpublic personal information in accordance with section 6801 of this title; and

(4) the disclosures required, if any, under section 1681a(d)(2)(A)(iii) of this title.

This clause defines what it means for a message to be an annual notice, notice of disclosure, or notice of potential disclosure.

For example, although we have previously assumed is-annual-notice to be a predicate, this clause allows us to define it as a macro:

$$\begin{aligned}\text{is-annual-notice}(m'', p_1, q) \triangleq\ & \text{contains}(m'', p_1, \textit{npi-policies-and-practices}) \wedge \\ & \text{contains}(m'', p_1, \textit{npi-categories-collected}) \wedge \\ & \text{contains}(m'', p_1, \textit{npi-security-policies}) \wedge \\ & \text{contains}(m'', p_1, \textit{npi-disclosures-to-affiliates})\end{aligned}$$

Similarly, we may define is-notice-of-potential-disclosure and is-notice-of-disclosure as macros. To do so, we invent types of attributes that describe a potential or actual disclosure:

$$\begin{aligned}&\text{is-notice-of-potential-disclosure}(m'', p_1, p_2, (q, t), u) \triangleq \\ &\quad \text{contains}(m'', p_1, \textit{will-possibly-disclose}(p_1, p_2, (q, t), u))\end{aligned}$$

and

$$\begin{aligned}&\text{is-notice-of-disclosure}(m'', p_1, p_2, (q, t), u) \triangleq \\ &\quad \text{contains}(m'', p_1, \textit{has-or-will-disclose}(p_1, p_2, (q, t), u))\end{aligned}$$

6803(d) Exemption for Certified Public Accountants

6803(d)(1) In General

The disclosure requirements of subsection (a) do not apply to any person, to the extent that the person is—

(A) a certified public accountant;

(B) certified or licensed for such purpose by a State; and

> *(C) subject to any provision of law, rule, or regulation issued by a legislative or regulatory body of the State, including rules of professional conduct or ethics, that prohibits disclosure of nonpublic personal information without the knowing and expressed consent of the consumer.*

$$\begin{aligned}\varphi^{+}_{\texttt{6803d1}} \triangleq \exists S.\ & \mathrm{belongstorole}(S, \mathit{State}) \land \\ & \mathrm{activerole}(p_1, \mathit{certified\text{-}public\text{-}accountant}(S)) \land \\ & \text{subject-to-ethical-disclosure-provision}(p_1, S)\end{aligned}$$

Again, we assume that the semantics of the subject-to-ethical-disclosure-provision predicate are given by an oracle.

6803(d)(2) Limitation

> *Nothing in this subsection shall be construed to exempt or otherwise exclude any financial institution that is affiliated or becomes affiliated with a certified public accountant described in paragraph (1) from any provision of this section.*

We ensure this condition by requiring that our model satisfies the following constraint in every state:

$$\begin{aligned}\neg(&\mathrm{belongstorole}(p, \mathit{institution}) \land \\ &\mathrm{belongstorole}(p, \mathit{affiliate}(p)))\end{aligned}$$

3.4 §6809 Definitions

6809(5) Nonaffiliated Third Party

> *The term 'nonaffiliated third party' means any entity that is not an affiliate of, or related by common ownership or affiliated by corporate control with, the financial institution, but does not include a joint employee of such institution.*

This condition is ensured by our general approach. A joint employee can be active in at most one of his employers' roles; being active in the *institution* role does not force him to simultaneously act in the nonaffiliate role.

6809(9) Consumer

> *The term 'consumer' means an individual who obtains, from a financial institution, financial products or services which are to be used primarily for personal, family, or household purposes, and also means the legal representative of such an individual.*

In effect, this clause is stating that anywhere "consumer" was stated in the law, the individual's legal representative is a suitable substitute. For example, the institution may choose to send disclosure notices to a consumer's legal representative, rather than sending them directly to the consumer. To handle this, we introduce a high-level send macro that abstracts away from the low-level, physical send action provided by our model: a high-level send to p_2 is either a low-level send to p_2 or a low-level send to p_2's legal representative.

$$\begin{aligned}\text{hlsend}(p_1, p_2, m) \triangleq\ & \text{send}(p_1, p_2, m) \\ & \vee (\exists p_1'.\ \text{send}(p_1', p_2, m) \wedge \\ & \qquad \text{activerole}(p_1', \textit{legal-representative}(p_1)) \wedge \\ & \qquad \exists p'.\ \text{belongstorole}(p_1, \textit{consumer}(p')) \wedge \\ & \qquad\quad \text{belongstorole}(p', \textit{institution})) \\ & \vee (\exists p_2'.\ \text{send}(p_1, p_2', m) \wedge \\ & \qquad \text{activerole}(p_2', \textit{legal-representative}(p_2)) \wedge \\ & \qquad \exists p'.\ \text{belongstorole}(p_2, \textit{consumer}(p')) \wedge \\ & \qquad\quad \text{belongstorole}(p', \textit{institution}))\end{aligned}$$

All uses of send in the norms would then be replaced by hlsend (as we have done consistently so far).

6809(11) Customer Relationship

> *The term 'time of establishing a customer relationship' shall be defined by the regulations prescribed under section 6804 of this title, and shall, in the case of a financial institution engaged in extending credit directly to consumers to finance purchases of goods or services, mean the time of establishing the credit relationship with the consumer.*

Hence, we require that the underlying model's role structure satisfies

$$\textit{customer}(p_1) \preceq_{\mathcal{R}} \textit{consumer}(p_1)$$

for all financial institutions p_1.

Chapter 4

Health Insurance Portability and Accountability Act

In this chapter, we give our formalization of §§164.502, 164.506, 164.508, 164.510, 164.512, 164.514, and 164.524 of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) [US 02]. In addition, for the clauses also formalized by Lam *et al.* in Datalog (i.e., §§164.502, 164.506, and 164.510) [LMS09, Sta], we give a comparison of our method with their formulation. In this comparison, Datalog code snippets are shown in `monospace` font.

4.1 Top-Level Formula

As in our formalization of GLBA, we require a top-level formula that combines the individual positive and negative norms. It is this formula that is checked when verifying compliance of a trace σ with the law. For HIPAA, we propose the top-level formula:

$$\begin{array}{l}
\mathbf{G}\ \forall p_1, p_2{:}\mathsf{prin}.\ \forall m{:}\mathsf{msg}.\\
\qquad \mathrm{send}(p_1, p_2, m) \supset\\
\qquad\quad (\forall d{:}\mathsf{data}.\ \forall u{:}\mathsf{purp}.\ \forall q{:}\mathsf{prin}.\ \forall t{:}\mathsf{attr}.\\
\qquad\qquad (m = \mathrm{info}(d, u)) \wedge \mathrm{contains}(m, q, t) \supset\\
\qquad\qquad\quad \bigvee_i \varphi_i^{+} \wedge \bigwedge_i \varphi_i^{-}\ ) \wedge\\
\qquad\quad (\forall t{:}\mathsf{attr}.\\
\qquad\qquad (m = \mathrm{req\_for\_access}(p_1, t)) \supset\\
\qquad\qquad\quad \varphi^{-}_{\mathtt{164.524b2i}'} \vee \varphi^{-}_{\mathtt{164.524b2ii}'})
\end{array}$$

Note that HIPAA does not contain clauses that require fixed points, and so we have no greatest fixed point operator $\nu \mathrm{maysend}(p_1, p_2, m)$. as we did in the top-level formula for GLBA.

4.2 §164.502 Uses and disclosures of protected health information: General rules

```
permitted_by_164_502(A):-
  permitted_by_164_502_a(A);
  permitted_by_164_502_b(A);    %must satisfy
  permitted_by_164_502_c(A);
  permitted_by_164_502_d(A);
  permitted_by_164_502_e(A);    %must satisfy
  permitted_by_164_502_f(A);
  permitted_by_164_502_g(A);
  permitted_by_164_502_h(A);
  permitted_by_164_502_i(A);
  permitted_by_164_502_j(A).
```

We have no norm that corresponds to this Datalog clause. This is because we choose to flatten the permission structure, and so any positive norms that arise from §164.502 will be directly inserted into our top-level formula when they appear.

164.502(a)

> *A covered entity may not use or disclose protected health information, except as permitted or required by this subpart or by subpart C of part 160 of this subchapter.*

```
permitted_by_164_502_a(A) :-
  is_from_coveredEntity(A),
  is_phi(A),
  (permitted_by_160_C(A);
   permitted_by_164_502_a_1(A);
   required_by_164_502_a_2(A)).
```

Again, we have no corresponding norm because the norms implied by §164.502(a)(1) and (2) will be included when we reach those sections.

164.502(a)(1)

> *A covered entity is permitted to use or disclose protected health information as follows:*

```
permitted_by_164_502_a_1(A) :-
  permitted_by_164_502_a_1_i(A);
  permitted_by_164_502_a_1_ii(A);
  permitted_by_164_502_a_1_iii(A);
  permitted_by_164_502_a_1_iv(A);
  permitted_by_164_502_a_1_v(A);
  permitted_by_164_502_a_1_vi(A).
```

Again, in our approach, we have no corresponding norm.

164.502(a)(1)(i)

> *To the individual;*

```
permitted_by_164_502_a_1_i(A) :-
  (is_to_concernedIndividual(A);
   is_from_concernedIndividual(A)),
  writeln('HIPAA rule 164_502_a_1_i;').
```

We include the positive norm:

$$\begin{aligned}\varphi^{+}_{\texttt{164.502a1i}} \triangleq\ & \text{activerole}(p_1, \textit{covered-entity}) \wedge \\ & (p_2 \approx q) \wedge \\ & (t \in_{\mathcal{T}} \textit{phi})\end{aligned}$$

where

$$(p_2 \approx q) \triangleq \text{activerole}(p_2, \textit{personal-representative}(q)) \vee (p_2 = q)$$

Unlike Lam *et al.*'s Datalog formulation, we do not believe that this HIPAA clause allows the individual to send messages. This is a reasonable property to expect, but is captured elsewhere.

164.502(a)(1)(ii)

> *For treatment, payment, or health care operations, as permitted by and in compliance with §164.506;*

```
permitted_by_164_502_a_1_ii(A) :-
  is_for_eitherPurpose(A),
  permitted_by_164_506(A),
  writeln('HIPAA rule 164_502_a_1_ii;').
```

Again, we have no corresponding norm. §164.506 will insert positive norms directly into the top-level formula.

164.502(a)(1)(iii)

> *Incident to a use or disclosure otherwise permitted or required by this subpart, provided that the covered entity has complied with the applicable requirements of §164.502(b), §164.514(d), and §164.530(c) with respect to such otherwise permitted or required use or disclosure;*

```
permitted_by_164_502_a_1_iii(A) :-
  is_for_incidentToUse(A),
  permitted_by_164_502_b(A),
  permitted_by_164_514_d(A),
  permitted_by_164_530_c(A),
  writeln('HIPAA rule 164_502_a_1_iii;').
```

$$\varphi^{+}_{\texttt{164.502a1iii}} \triangleq \text{incident-to-use-disclosure}(p_1, p_2, (q, t), u)$$

164.502(a)(1)(iv)

> *Pursuant to and in compliance with a valid authorization under §164.508;*

```
permitted_by_164_502_a_1_iv(A) :-
  require_authorization_by_164_508(A),
  writeln(’HIPAA rule 164_502_a_1_iv;’).
```

To allow disclosures that have valid authorizations, we include the positive norm:

$$\begin{aligned}\varphi^{+}_{\texttt{164.502a1iv}} \triangleq\ & \text{activerole}(p_1, \textit{covered-entity}) \wedge \\ & (t \in_{\mathcal{T}} \textit{phi}) \wedge \\ & \text{obtained-authorization-164.508}(p_1, p_2, (q, t), u)\end{aligned}$$

The constraints on the process of obtaining an individual’s authorization are imposed directly in §164.508.

164.502(a)(1)(v)

> *Pursuant to an agreement under, or as otherwise permitted by, §164.510; and*

```
permitted_by_164_502_a_1_v(A) :-
  permitted_by_164_510(A),
  writeln(’HIPAA rule 164_502_a_1_v;’).
```

Again, we have no directly corresponding norm. §164.510 will insert the relevant norms into the top-level formula.

164.502(a)(1)(vi)

> *As permitted by and in compliance with this section, §164.512, or §164.514(e), (f), or (g).*

```
permitted_by_164_502_a_1_vi(A) :-
  permitted_by_164_512(A);
  permitted_by_164_514_e(A);
  permitted_by_164_514_f(A);
  permitted_by_164_514_g(A).
```

Again, we have no corresponding norm.

164.502(a)(2)

> *A covered entity is required to disclose protected health information:*

```
%required by!!
required_by_164_502_a_2(A) :-
  required_by_164_502_a_2_i(A);
  required_by_164_502_a_2_ii(A).
```

Again, we have no corresponding norm.

164.502(a)(2)(i)

> *To an individual, when requested under, and required by §164.524 or §164.528; and*

```
required_by_164_502_a_2_i(A) :-
  is_to_concernedIndividual(A),
  is_replyTo_request(A),
  (required_by_164_524(A);
   required_by_164_528(A)),
  writeln('HIPAA rule 164_502_a_2_i;').
```

We have no directly corresponding norm. Instead, a "requirement" splits into two pieces: a positive norm that permits the required flow and a negative norm that obligates the covered entity to ensure that the required flow actually occurs. For this HIPAA clause, the positive fragment is already present via §164.502(a)(1)(i), since that section allows protected health information to be sent to the individual. The negative fragment will come from §164.524.

164.502(a)(2)(ii)

> *When required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the covered entity's compliance with this subpart.*

```
required_by_164_502_a_2_ii(A) :-
  is_to_secretary(A),
  is_for_investigation(A),
  permitted_by_160_C(A),
  writeln('HIPAA rule 164_502_a_2_ii;').
```

The positive fragment of this clause is captured by:

$$\begin{aligned}\varphi^{+}_{\texttt{164.502a2ii}} \triangleq\ & \mathrm{activerole}(p_1, \textit{covered-entity}) \wedge \\ & \mathrm{activerole}(p_2, \textit{Secretary}) \wedge \\ & (t \in_{\mathcal{T}} \textit{phi}) \wedge \\ & (u \in_{\mathcal{U}} \textit{compliance-investigation}(p_1))\end{aligned}$$

We do not have a negative norm here: the relevant negative fragment of this requirement will come from §160.310.

164.502(b)

```
permitted_by_164_502_b(A) :-
  permitted_by_164_502_b_1(A);
  excluded_164_502_b_2(A).
```

We introduce $\varphi^{-}_{\texttt{164.502b}}$ as the negative norm from (b)(1) with positive exceptions drawn from (b)(2):

$$\begin{aligned}\varphi^{-}_{\texttt{164.502b}} \triangleq (&\varphi^{-}_{\texttt{164.502b1}} \vee \\ &\varphi^{+}_{\texttt{164.502b2i}} \vee \varphi^{+}_{\texttt{164.502b2ii}} \vee \\ &\varphi^{+}_{\texttt{164.502b2iii}} \vee \varphi^{+}_{\texttt{164.502b2iv}} \vee \\ &\varphi^{+}_{\texttt{164.502b2v}} \vee \varphi^{+}_{\texttt{164.502b2vi}})\end{aligned}$$

This is essentially the same as what is done by Lam *et al.*.

164.502(b)(1)

> *When using or disclosing protected health information or when requesting protected health information from another covered entity, a covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.*

```
permitted_by_164_502_b_1(A) :-
  is_from_coveredEntity(A),
  is_to_coveredEntity(A),
  is_belief_from_minimum(A),
  writeln('HIPAA rule 164_502_b_1;').
```

$$\begin{aligned}\varphi^-_{\texttt{164.502b1}} \triangleq\ & \text{activerole}(p_1, \textit{covered-entity}) \wedge \\ & (t \in_{\mathcal{T}} \textit{phi}) \supset \\ & \quad \text{believes-minimum-necessary-for-purpose}(p_1, p_2, (q,t), u)\end{aligned}$$

The predicate believes-minimum-necessary-for-purpose is given semantics via an oracle.

164.502(b)(2)

> *This requirement does not apply to:*

```
excluded_164_502_b_2(A) :-
  excluded_164_502_b_2_i(A);
  excluded_164_502_b_2_ii(A);
  excluded_164_502_b_2_iii(A);
  excluded_164_502_b_2_iv(A);
  excluded_164_502_b_2_v(A);
  excluded_164_502_b_2_vi(A).
```

We have no corresponding norm since these exceptions were applied to the previous negative norm as part of $\varphi^-_{\texttt{164.502b}}$.

164.502(b)(2)(i)

> *Disclosures to or requests by a health care provider for treatment;*

```
excluded_164_502_b_2_i(A) :-
  is_for_treatment(A),
  is_to_healthCareProvider(A),
  writeln('HIPAA rule 164_502_b_2_i;').
```

We formalize this using our notion of purpose:

$$\begin{aligned}\varphi^+_{\texttt{164.502b2i}} \triangleq\ & \text{activerole}(p_2, \textit{provider}) \wedge \\ & (u \in_{\mathcal{U}} \textit{treatment})\end{aligned}$$

164.502(b)(2)(ii)

> *Uses or disclosures made to the individual, as permitted under paragraph (a)(1)(i) of this section or as required by paragraph (a)(2)(i) of this section;*

```
excluded_164_502_b_2_ii(A) :-
  (permitted_by_164_502_a_1_i(A);
   required_by_164_502_a_2_i(A)),
  writeln('HIPAA rule 164_502_b_2_ii;').
```

We have:

$\varphi^{+}_{\texttt{164.502b2ii}} \triangleq \varphi^{+}_{\texttt{164.502a1i}}$

Note that, because a requirement splits into positive and negative fragments, disclosures required by paragraph (a)(2)(i) are permitted by positive norms. It so happens that for (a)(2)(i) the positive piece is $\varphi^{+}_{\texttt{164.502a1i}}$, since that norm permits protected health information to be sent to the individual.

164.502(b)(2)(iii)

> *Uses or disclosures made pursuant to an authorization under §164.508;*

```
excluded_164_502_b_2_iii(A) :-
  is_for_obtainingAuthorization(A),
  writeln('HIPAA rule 164_502_b_2_iii;').
```

We have:

$\varphi^{+}_{\texttt{164.502b2iii}} \triangleq \varphi^{+}_{\texttt{164.502a1iv}}$

Note that paragraph (a)(1)(iv) defines when a disclosure is made pursuant to an authorization under §164.508.

164.502(b)(2)(iv)

> *Disclosures made to the Secretary in accordance with subpart C of part 160 of this subchapter;*

```
excluded_164_502_b_2_iv(A) :-
  is_to_secretary(A),
  permitted_by_160_C(A),
  writeln('HIPAA rule 164_502_b_2_iv;').
```

We have:

$\varphi^{+}_{\texttt{164.502b2iv}} \triangleq \varphi^{+}_{\texttt{164.502a2ii}}$

Note that paragraph (a)(2)(ii) defines when a disclosure is made to the Secretary for compliance with investigations.

164.502(b)(2)(v)

> *Uses or disclosures that are required by law, as described by §164.512(a); and*

```
excluded_164_502_b_2_v(A) :-
  required_by_164_512_a(A),
  writeln('HIPAA rule 164_502_b_2_v;').
```

We have the norm:

$\varphi^{+}_{\texttt{164.502b2v}} \triangleq \bigvee_{i \in \texttt{164.512a}} \varphi^{+}_{i}$

164.502(b)(2)(vi)

> *Uses or disclosures that are required for compliance with applicable requirements of this subchapter.*

```
%Need to add all required types. Found only this.
excluded_164_502_b_2_vi(A) :-
  required_by_164_502_a_2(A),
  writeln('HIPAA rule 164_502_b_2_vi;').
```

Because it appears that this HIPAA clause overlaps with paragraphs (b)(2)(ii), (iv), and (v), we have no norm for this paragraph.

164.502(c)

> *A covered entity that has agreed to a restriction pursuant to §164.522(a)(1) may not use or disclose the protected health information covered by the restriction in violation of such restriction, except as otherwise provided in §164.522(a).*

```
permitted_by_164_502_c(A) :-
% must also check whether restriction exists for a particular case
  is_from_coveredEntity(A),
  is_phi(A),
  (permitted_by_164_522_a_1(A);
   permitted_by_164_522_a(A)),
  writeln('HIPAA rule 164_502_c;').
```

Again, we have no corresponding norms here; they will come from §164.522(a).

164.502(d)

```
permitted_by_164_502_d(A) :-
  permitted_by_164_502_d_1(A);
  permitted_by_164_502_d_2(A).
```

164.502(d)(1)

> *A covered entity may use protected health information to create information that is not individually identifiable health information or disclose protected health information only to a business associate for such purpose, whether or not the de-identified information is to be used by the covered entity.*

```
permitted_by_164_502_d_1(A) :-
%use part is not so clear, just modelled the disclosure part.
  is_phi(A),
  is_from_coveredEntity(A),
  is_to_businessAssociateOf(A),
  is_for_createDeidentifiedInfo(A),
  writeln('HIPAA rule 164_502_d_1;').
```

We have the positive norm:

$$\begin{aligned}\varphi^{+}_{\texttt{164.502d1}} \triangleq\ & \text{activerole}(p_1, \textit{covered-entity}) \wedge \\ & \text{activerole}(p_2, \textit{business-associate}(p_1)) \wedge \\ & (t \in_{\mathcal{T}} \textit{phi}) \wedge \\ & (u \in_{\mathcal{U}} \textit{create-deidentified-info})\end{aligned}$$

Note that we again rely on purposes to capture the crucial component of this HIPAA clause.

164.502(d)(2)

> *Health information that meets the standard and implementation specifications for de-identification under §164.514(a) and (b) is considered not to be individually identifiable health information, i.e., de-identified. The requirements of this subpart do not apply to information that has been de-identified in accordance with the applicable requirements of §164.514, provided that:*

```
permitted_by_164_502_d_2(A) :-
  permitted_by_164_514(A),
  (excluded_by_164_502_d_2_i(A);
   permitted_by_164_502_d_2_ii(A)),
  writeln('HIPAA rule 164_502_b_2;').
```

In our system, de-identified information will be classified as $(t \in_{\mathcal{T}} \textit{dii})$. Since we ensure that this class is distinct from *phi*, we have no norm here. All other norms that we have in HIPAA will include the constraint that the attribute t is from the class *phi*. Therefore, de-identified information will be able to "escape" those norms and be sent.

164.502(d)(2)(i)

> *Disclosure of a code or other means of record identification designed to enable coded or otherwise de-identified information to be re-identified constitutes disclosure of protected health information; and*

```
excluded_by_164_502_d_2_i(A) :-
%verify that the message does not have identifiable
%attributes for join like primary keys
  fail.
```

We include the following constraint:

$$\begin{aligned}&(t \in_{\mathcal{T}} \mathit{dii}) \Rightarrow \\ &\quad \neg\exists m'.\, \text{contains}(m', (q, \mathit{identification\text{-}code})) \wedge \\ &\qquad\quad \Diamond\!\!\!\!-\,\text{send}(p_1, p_2, m')\end{aligned}$$

where $\phi \Rightarrow \psi$ means that, in all states, ϕ must imply ψ.

164.502(d)(2)(ii)

> *If de-identified information is re-identified, a covered entity may use or disclose such re-identified information only as permitted or required by this subpart.*

```
permitted_by_164_502_d_2_ii(A) :-
% verify that the de-indentified information is not re-identified
  fail.
```

Since we only classify $(t \in_{\mathcal{T}} \mathit{dii})$ when t has not been re-identified, we do not need to do anything here. Once t is re-identified, it will be classified as $(t \in_{\mathcal{T}} \mathit{phi})$ and will be appropriately treated by the other norms.

164.502(e)

```
permitted_by_164_502_e(A) :-
  excluded_164_502_e_1_ii(A);
  permitted_by_164_502_e_1_i(A).
  %not sure what this means. non-compliance of BA.
  %permitted_164_502_e_1_iii(A).
  %surely cant implement this written notice thing.
  %permitted_164_502_e_2(A).
```

We have a positive norm with negative restrictions, forming a positive norm:

$$\begin{aligned}\varphi^{+}_{\texttt{164.502e}} \triangleq (&\varphi^{+}_{\texttt{164.502e1i}} \wedge \\ &\varphi^{-}_{\texttt{164.502e1iiA}} \wedge \varphi^{-}_{\texttt{164.502e1iiB}} \wedge \varphi^{-}_{\texttt{164.502e1iiC}})\end{aligned}$$

164.502(e)(1)

164.502(e)(1)(i)

> *A covered entity may disclose protected health information to a business associate and may allow a business associate to create or receive protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information.*

```
%See if the message is allowed to be received by any of the covered entities
%of this business associate or if the covered entity is disclosing protected
%health to a business associate. An entity is a business associate of some
%covered entity if that covered entity receives assurance that the BA will
%appropriately safeguard the info and act on behalf of the covered entity.

permitted_by_164_502_e_1_i(A) :-
  is_phi(A),
  ( (is_from_coveredEntity(A),
     is_to_businessAssociateOf(A),
     is_belief_to_lawfulBusinessAssociate(A, X));
    (is_to_coveredEntity(A),
     is_from_businessAssociateOf(A),
     is_belief_from_lawfulBusinessAssociate(A, X))
  ),
  (is_for_createProtectedHealthInfo(A);
   is_for_receiveProtectedHealthInfo(A)),
  writeln('HIPAA rule 164_502_e_1_i;').
```

We have the norm:

$$\begin{aligned}\varphi^{+}_{\texttt{164.502e1i}} \triangleq\ & \text{activerole}(p_1, \textit{covered-entity}) \land \\ & \text{activerole}(p_2, \textit{business-associate}(p_1)) \land \\ & (t \in_{\mathcal{T}} \textit{phi}) \land \\ & \text{satisfactory-assurances-will-safeguard-info}(p_1, p_2, (q, t), u)\end{aligned}$$

where the newly introduced predicate satisfactory-assurances-will-safeguard-info is defined as a macro in §164.502(e)(2).

164.502(e)(1)(ii)

This standard does not apply:

```
excluded_164_502_e_1_ii(A):-
  excluded_164_502_e_1_ii_a(A);
  excluded_164_502_e_1_ii_b(A);
  excluded_164_502_e_1_ii_c(A).
```

We have no corresponding norm, as these exceptions were captured in §164.502(e).

164.502(e)(1)(ii)(A)

With respect to disclosures by a covered entity to a health care provider concerning the treatment of the individual;

```
excluded_164_502_e_1_ii_a(A) :-
  is_about_individual(A),
  is_to_healthCareProvider(A),
  is_for_treatment(A),
  is_from_coveredEntity(A),
  writeln('HIPAA rule 164_502_e_1_ii_a;').
```

We have the exception:

$$
\begin{aligned}
\varphi^{-}_{\texttt{164.502e1iiA}} \triangleq \neg(&\text{activerole}(p_1, \textit{covered-entity}) \land \\
&\text{activerole}(p_2, \textit{provider}(q)) \land \\
&(u \in_{\mathcal{U}} \textit{treatment}))
\end{aligned}
$$

164.502(e)(1)(ii)(B)

> *With respect to disclosures by a group health plan or a health insurance issuer or HMO with respect to a group health plan to the plan sponsor, to the extent that the requirements of 164.504(f) apply and are met; or*

```
excluded_164_502_e_1_ii_b(A) :-
  %to plan sponsor
  (is_from_healthInsuranceIssuer(A);
   is_from_groupHealthPlan(A)),
  permitted_by_164_504_f(A),
  writeln('HIPAA rule 164_502_e_1_ii_b;').
% "with respect to a group health plan" could be
% represented by storing group health plan in type or purpose?
```

We have the exception:

$$
\begin{aligned}
\varphi^{-}_{\texttt{164.502e1iiB}} \triangleq \neg((&\exists p_1'.\ \text{activerole}(p_1', \textit{group-health-plan}) \land \\
&\quad((p_1 = p_1') \lor \\
&\quad\ \text{activerole}(p_1, \textit{health-insurance-issuer}(p_1')) \lor \\
&\quad\ \text{activerole}(p_1, \textit{HMO}(p_1'))) \land \\
&\quad\text{activerole}(p_2, \textit{sponsor}(p_1'))) \land \\
&\varphi^{+}_{\texttt{164.504f}})
\end{aligned}
$$

To capture "to the extent that the requirements of §164.504(f) apply and are met," we include $\varphi^{+}_{\texttt{164.504f}}$.

164.502(e)(1)(ii)(C)

> *With respect to uses or disclosures by a health plan that is a government program providing public benefits, if eligibility for, or enrollment in, the health plan is determined by an agency other than the agency administering the health plan, or if the protected health information used to determine enrollment or eligibility in the health plan is collected by an agency other than the agency administering the health plan, and such activity is authorized by law, with respect to the collection and sharing of individually identifiable health information for the performance of such functions by the health plan and the agency other than the agency administering the health plan.*

```
%enrollment information is collected by the government agency.
%(incomplete) lot of insurance stuff
excluded_164_502_e_1_ii_c(A) :-
  is_from_governmentAgencyHealthPlan(A),
  writeln('HIPAA rule 164_502_e_1_ii_c;').
```

We have the exception:

$$
\begin{aligned}
\varphi^{-}_{\texttt{164.502e1iiC}} \triangleq \neg(&\text{activerole}(p_1, \mathit{agency}) \land \\
&\text{activerole}(p_2, \mathit{government\text{-}health\text{-}plan}) \land \\
&((\neg(p_2 = p_1) \land \\
&\quad \text{determines-eligibility-enrollment}(p_1, p_2)) \lor \\
&\ \neg\text{eligibility-enrollment-info-collected-by}(p_2)) \land \\
&(u \in_{\mathcal{U}} \mathit{determine\text{-}eligibility\text{-}enrollment}))
\end{aligned}
$$

164.502(e)(1)(iii)

> *A covered entity that violates the satisfactory assurances it provided as a business associate of another covered entity will be in noncompliance with the standards, implementation specifications, and requirements of this paragraph and §164.504(e).*

Because this paragraph appears to be simply a statement of intent, we have no norm here.

164.502(e)(2)

> *A covered entity must document the satisfactory assurances required by paragraph (e)(1) of this section through a written contract or other written agreement or arrangement with the business associate that meets the applicable requirements of §164.504(e).*

We capture this paragraph using a macro satisfactory-assurances-will-safeguard-info:

$$
\begin{aligned}
&\text{satisfactory-assurances-will-safeguard-info}(p_1, p_2, (q, t), u) \triangleq \\
&\quad \exists m'.\ \Diamond\text{send}(p_1, p_2, m') \land \\
&\qquad\quad \text{is-contract-164.504e}(m', p_1, p_2, (q, t), u)
\end{aligned}
$$

164.502(f)

> *A covered entity must comply with the requirements of this subpart with respect to the protected health information of a deceased individual.*

```
permitted_by_164_502_f(A) :-
%comply to subpart if individual dead
% so basically dont care dead or alive.
  fail.
```

Similarly to the Datalog formalization of Lam *et al.*, there will be no norms that rely on whether or not an individual is deceased. Therefore, living and deceased individuals will be treated uniformly, and there is no need for an explicit norm here.

164.502(g)

```
permitted_by_164_502_g(A) :-
  permitted_by_164_502_g_1(A);
  permitted_by_164_502_g_2(A);
  permitted_by_164_502_g_3(A);
  permitted_by_164_502_g_4(A);
  permitted_by_164_502_g_5(A).
```

Again, we have no corresponding norm since the relevant norms will be directly included when they appear.

164.502(g)(1)

> *As specified in this paragraph, a covered entity must, except as provided in paragraphs (g)(3) and (g)(5) of this section, treat a personal representative as the individual for purposes of this subchapter.*

```
permitted_by_164_502_g_1(A) :-
%treat personal representative as individual except by g-3 ang g-5.
  fail,
  writeln('HIPAA rule 164_502_g_1;').
```

164.502(g)(2)

> *If under applicable law a person has authority to act on behalf of an individual who is an adult or an emancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation.*

```
permitted_by_164_502_g_2(A) :-
% should treat adult or emancipated minor in making decision as individual,
% relavant to such personal representatives.
  is_about_adult(A),
  msg_about(A, X),
  personal_representative(X, Y),
  (msg_to(A, Y);
   msg_from(A, Y)),
  writeln('HIPAA rule 164_502_g_2;').
```

Unlike Lam *et al.*, we do not choose to base this clause around disclosure. Instead, the clause speaks about when a covered entity should treat a principal as a personal representative. In our view, this is most clearly captured as a constraint on when a principal may act in the role of a personal representative:

$$
\begin{array}{l}
\text{has-authority-to-act-on-behalf-healthcare}(p, q) \land \\
(\text{belongstorole}(q, \textit{adult}) \lor \\
\ \text{belongstorole}(q, \textit{emancipated-minor})) \Rightarrow \\
\quad \text{activerole}(p, \textit{personal-representative}(q))
\end{array}
$$

The connective ⇒ requires that the underlying implication hold in all states. It effectively functions as a constraint on our model. Also, the semantics of has-authority-to-act-on-behalf-healthcare are given by an oracle.

164.502(g)(3)

```
permitted_by_164_502_g_3(A) :-
%Assuming there are no applicable provisions or other applicable state laws,
%should be allowed if 3i and 164.524 allow it, and denied if they deny.
%Else (when neither are applicable) the decision is made by licensed health
%professional.
  permitted_by_164_502_g_3_i(A);
  permitted_by_164_502_g_3_ii(A).
```

Again, we have no corresponding norm; refer to the following paragraphs.

164.502(g)(3)(i)

> *If under applicable law a parent, guardian, or other person acting in loco parentis has authority to act on behalf of an individual who is an unemancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation, except that such person may not be a personal representative of an unemancipated minor, and the minor has the authority to act as an individual, with respect to protected health information pertaining to a health care service, if:*
>
> *(A) The minor consents to such health care service; no other consent to such health care service is required by law, regardless of whether the consent of another person has also been obtained; and the minor has not requested that such person be treated as the personal representative;*
>
> *(B) The minor may lawfully obtain such health care service without the consent of a parent, guardian, or other person acting in loco parentis, and the minor, a court, or another person authorized by law consents to such health care service; or*
>
> *(C) A parent, guardian, or other person acting in loco parentis assents to an agreement of confidentiality between a covered health care provider and the minor with respect to such health care service.*

```
is_guardian(X, Y) :-
  parent(X, Y);
  guardian(X, Y);
  loco_parentis(X, Y).

permitted_by_164_502_g_3_i(A) :-
% relavant to such personal representatives.
% about health care services
  is_about_minor(A),
  msg_about(A, X),
  (msg_to(A, Y);
   msg_from(A,Y)),
  is_guardian(X, Y),
  \+ (permitted_by_164_502_g_3_i_A(A),
      permitted_by_164_502_g_3_i_B(A),
      permitted_by_164_502_g_3_i_C(A)),
  writeln('HIPAA rule 164_502_g_3_i;').
%rule requires you to remove a parents role
% as a personal representative globally in the shh file.
% this can be done if the child requests such or parent agrees

permitted_by_164_502_g_3_i_A(A) :-
  fail.

permitted_by_164_502_g_3_i_B(A) :-
  fail.

permitted_by_164_502_g_3_i_C(A) :-
  fail.
```

Again, it is our opinion that it is incorrect to treat this HIPAA clause as being based around disclosures. We consider it to be a constraint on the conditions under which a principal may act as a personal representative:

$$
\begin{aligned}
&(\text{activerole}(p, \textit{parent}(q)) \vee \\
&\ \text{activerole}(p, \textit{guardian}(q)) \vee \\
&\ \text{activerole}(p, \textit{in-loco-parentis}(q))) \wedge \\
&\text{belongstorole}(q, \textit{unemancipated-minor}) \wedge \\
&\text{has-authority-to-act-on-behalf-healthcare}(p, q) \Rightarrow \\
&\quad \text{activerole}(p, \textit{personal-representative}(q))
\end{aligned}
$$

164.502(g)(3)(ii)

> *Notwithstanding the provisions of paragraph (g)(3)(i) of this section:*

```
permitted_by_164_502_g_3_ii(A) :-
  permitted_by_164_502_g_3_ii_A(A);
  permitted_by_164_502_g_3_ii_B(A);
  permitted_by_164_502_g_3_ii_C(A).
```

Again, we have no corresponding norm.

164.502(g)(3)(ii)(A)

> *If, and to the extent, permitted or required by an applicable provision of State or other law, including applicable case law, a covered entity may disclose, or provide access*

in accordance with §164.524 to, protected health information about an unemancipated minor to a parent, guardian, or other person acting in loco parentis;

```
permitted_by_164_502_g_3_ii_A(A) :-
% covered entity may send to guardian based on applicable law
  fail,
  writeln('HIPAA rule 164_502_g_3_ii_A;').
%add if permitted by any othe sepcified by laws
```

$$
\begin{aligned}
\varphi^{+}_{\mathtt{164.502g3iiA}} \triangleq\ & \text{activerole}(p_1, \textit{covered-entity}) \land \\
& (\text{activerole}(p_2, \textit{parent}(q)) \lor \\
& \ \text{activerole}(p_2, \textit{guardian}(q)) \lor \\
& \ \text{activerole}(p_2, \textit{in-loco-parentis}(q))) \land \\
& (t \in_{\mathcal{T}} \textit{phi}) \land \\
& \text{permitted-by-other-law}(p_1, p_2, (q, t), u)
\end{aligned}
$$

164.502(g)(3)(ii)(B)

If, and to the extent, prohibited by an applicable provision of State or other law, including applicable case law, a covered entity may not disclose, or provide access in accordance with §164.524 to, protected health information about an unemancipated minor to a parent, guardian, or other person acting in loco parentis; and

```
permitted_by_164_502_g_3_ii_B(A) :-
% covered entity may NOT send to guardian based on applicable law
  fail,
  writeln('HIPAA rule 164_502_g_3_ii_B;').
```

$$
\begin{aligned}
\varphi^{-}_{\mathtt{164.502g3iiB}} \triangleq \neg(& \text{activerole}(p_1, \textit{covered-entity}) \land \\
& (\text{activerole}(p_2, \textit{parent}(q)) \lor \\
& \ \text{activerole}(p_2, \textit{guardian}(q)) \lor \\
& \ \text{activerole}(p_2, \textit{in-loco-parentis}(q))) \land \\
& (t \in_{\mathcal{T}} \textit{phi}) \land \\
& \text{prohibited-by-other-law}(p_1, p_2, (q, t), u))
\end{aligned}
$$

164.502(g)(3)(ii)(C)

Where the parent, guardian, or other person acting in loco parentis, is not the personal representative under paragraphs (g)(3)(i)(A), (B), or (C) of this section and where there is no applicable access provision under State or other law, including case law, a covered entity may provide or deny access under §164.524 to a parent, guardian, or other person acting in loco parentis, if such action is consistent with State or other applicable law, provided that such decision must be made by a licensed health care professional, in the exercise of professional judgment.

```
permitted_by_164_502_g_3_ii_C(A) :-
% will add one more rule representing personal representative in add. to guardian
%if personal rep ties are broken, then
% licensed medical practioner may send based on professional judgement
  fail,
  writeln('HIPAA rule 164_502_g_3_ii_C;').
```

We have no corresponding norm here. This will be handled by the allow and deny rules in §164.524.

164.502(g)(4)

> *If under applicable law an executor, administrator, or other person has authority to act on behalf of a deceased individual or of the individual's estate, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation.*

```
permitted_by_164_502_g_4(A) :-
  is_about_deceasedIndividual(A),
  msg_about(A, X),
  personal_representative(X, Y),
  (msg_to(A, Y);
   msg_from(A, Y)),
  writeln('HIPAA rule 164_502_g_4;').
```

Again, we treat this clause as specifying a constraint on when a principal may be considered a personal representative, rather than a disclosure-based clause:

$$
\begin{array}{l}
(\text{activerole}(p, \mathit{executor}) \lor \\
\ \text{activerole}(p, \mathit{administrator}) \lor \\
\ \top) \land \\
\text{belongstorole}(q, \mathit{deceased}) \land \\
\text{has-authority-to-act-on-behalf-healthcare}(p, q) \Rightarrow \\
\quad \text{activerole}(p, \mathit{personal\text{-}representative}(q))
\end{array}
$$

164.502(g)(5)

> *Notwithstanding a State law or any requirement of this paragraph to the contrary, a covered entity may elect not to treat a person as the personal representative of an individual if:*
>
> *(i) The covered entity has a reasonable belief that:*
>
> *(A) The individual has been or may be subjected to domestic violence, abuse, or neglect by such person; or*
>
> *(B) Treating such person as the personal representative could endanger the individual; and*

(ii) *The covered entity, in the exercise of professional judgment, decides that it is not in the best interest of the individual to treat the person as the individual's personal representative.*

```
permitted_by_164_502_g_5(A) :-
  permitted_by_164_502_g_5_i(A);
  permitted_by_164_502_g_5_ii(A).

permitted_by_164_502_g_5_i(A) :-
  msg_about(A, X),
  msg_to(A, Y),
  %is_belief_dangerousRepresentative(X, Y).
  fail,
  writeln('HIPAA rule 164_502_g_5_i;').

permitted_by_164_502_g_5_ii(A) :-
  %is_belief_notBestInterestOfIndividual(X, Y).
  fail,
  writeln('HIPAA rule 164_502_g_5_ii;').
```

We have the constraint:

$$\begin{array}{l}\text{believes-has-been-or-may-be-subject-of-abuse-from}(q, p) \land \\ \text{believes-treating-as-personal-representative-dangerous}(p, q) \land \\ \text{professional-judgment-treating-as-personal-representative-not-best-interest}(p, q) \Rightarrow \\ \quad \text{activerole}(p, \textit{personal-representative}(q))\end{array}$$

The predicates in this formalization rely on oracles for their semantics.

At this point, we have seen all of the clauses from paragraph §164.502(g), and have given their formalizations as constraints on when a principal may act as a personal representative. Our interpretation is that §164.502(g) operates under a kind of closed-world assumption: these are sufficient and necessary conditions for a principal to act as a personal representative. Therefore, we replace the earlier constraints with one large constraint that is an equivalence. Since it is an equivalence, we can now treat it as a macro definition:

$$\begin{array}{l}\text{activerole}(p, \textit{personal-representative}(q)) \triangleq \\ \qquad (((\text{belongstorole}(q, \textit{adult}) \lor \\ \qquad\quad \text{belongstorole}(q, \textit{emancipated-minor})) \land \\ \qquad\quad \text{has-authority-to-act-on-behalf-for-healthcare}(p, q)) \lor \\ \qquad ((\text{activerole}(p, \textit{parent}) \lor \\ \qquad\quad \text{activerole}(p, \textit{guardian}) \lor \\ \qquad\quad \text{activerole}(p, \textit{in-loco-parentis})) \land \\ \qquad\quad \text{belongstorole}(q, \textit{unemancipated-minor}) \land \\ \qquad\quad \text{has-authority-to-act-on-behalf-for-healthcare}(p, q)) \lor \\ \qquad ((\text{activerole}(p, \textit{executor}) \lor \\ \qquad\quad \text{activerole}(p, \textit{administrator}) \lor\end{array}$$

$$\begin{array}{l}
\quad\quad \top) \land \\
\quad\quad \text{belongstorole}(q, \textit{deceased}) \land \\
\quad\quad \text{has-authority-to-act-on-behalf-for-healthcare}(p, q))) \land \\
\quad \neg((\text{believes-victim-of-abuse-by}(q, p) \lor \\
\quad\quad\quad \text{believes-treating-as-personal-representative-is-dangerous}(p, q)) \land \\
\quad\quad \text{professional-judgment-treating-as-personal-representative-not-in-best-interest}(p, q))
\end{array}$$

Unfortunately, there does not appear to be a cleaner way of combining the individual sufficient constraints from the subparagraphs of §164.502(g) in a way that they are also necessary.

164.502(h)

> *A covered health care provider or health plan must comply with the applicable requirements of §164.522(b) in communicating protected health information.*

```
permitted_by_164_502_h(A) :-
  (is_from_healthCareProvider(A);
   is_from_healthPlan(A)),
  is_phi(A),
  permitted_by_164_522_b(A),
  writeln('HIPAA rule 164_502_h;').
```

We have no norms for §164.502(h); the requirements will be satisfied on the basis of norms from §164.522(b).

164.502(i)

> *A covered entity that is required by §164.520 to have a notice may not use or disclose protected health information in a manner inconsistent with such notice. A covered entity that is required by §164.520(b)(1)(iii) to include a specific statement in its notice if it intends to engage in an activity listed in §164.520(b)(1)(iii)(A)–(C), may not use or disclose protected health information for such activities, unless the required statement is included in the notice.*

```
permitted_by_164_502_i(A) :-
  debug('160._502_i: not implemeted disclosure with notice;').
```

Again, we have no corresponding norm since the relevant norms will be introduced by section §164.520.

164.502(j)

```
permitted_by_164_502_j(A) :-
  permitted_by_164_502_j_1(A);
  permitted_by_164_502_j_2(A).
```

We have no directly corresponding norm. The positive norms from (j)(1) and (2) will be inserted at the top level.

164.502(j)(1)

> *A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce or a business associate discloses protected health information, provided that:*
>
> *(i) The workforce member or business associate believes in good faith that the covered entity has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the covered entity potentially endangers one or more patients, workers, or the public; and*
>
> *(ii) The disclosure is to:*
>
> *(A) A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the covered entity or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the covered entity; or*
>
> *(B) An attorney retained by or on behalf of the workforce member or business associate for the purpose of determining the legal options of the workforce member or business associate with regard to the conduct described in paragraph (j)(1)(i) of this section.*

```
permitted_by_164_502_j_1(A) :-
  (is_from_employeeOf(A, Y);
   is_from_businessAssociateOf(A, Y)),
  permitted_by_164_502_j_1_i(A, Y),
  permitted_by_164_502_j_1_ii(A, Y).

permitted_by_164_502_j_1_i(A, Y) :-
%basically this belief includes "they believe in good faith
% that the covered Entity has engaged in conduct
% that is unlawful or otherwise violates professional
% or clinical standards, or that the care,
% services or conditions provided by covered entity
% potentially endangers one or more patients,
% workers or the public"
  is_belief_from_unlawfulCoveredEntity(A, Y),
  writeln('HIPAA rule 164_502_j_1_i;').

permitted_by_164_502_j_1_ii(A, Y) :-
  permitted_by_164_502_j_1_ii_A(A, Y);
  permitted_by_164_502_j_1_ii_B(A, Y).

permitted_by_164_502_j_1_ii_A(A, Y) :-
  is_to_healthOversightAgency(A);
  (is_to_publicHealthAuthority(A),
   is_for_investigation(A));
  (is_to_healthCareAccreditationOrganization(A),
   is_for_standardsFailureMisconduct(A, Y)),
  writeln('HIPAA rule 164_502_j_1_ii_A;').

permitted_by_164_502_j_1_ii_B(A, Y) :-
  is_to_legalAttorney(A),
  is_for_determiningLegalOptions(A),
  %is_belief_from_unlawfulCoveredEntity(A, Y),
  writeln('HIPAA rule 164_502_j_1_ii_B;').
```

We have:

$$\begin{aligned}
\varphi^{+}_{\texttt{164.502j1}} \triangleq \exists p_1'.\ & \text{belongstorole}(p_1', \textit{covered-entity}) \land \\
& (\text{activerole}(p_1, \textit{workforce-member}(p_1')) \lor \\
& \ \text{activerole}(p_1, \textit{business-associate}(p_1'))) \land \\
& \text{believes-unlawful-unethical-or-dangerous}(p_1, p_1') \land \\
& (((\text{activerole}(p_2, \textit{oversight-agency}) \lor \\
& \quad \text{activerole}(p_2, \textit{public-health-authority})) \land \\
& \quad \text{authorized-by-law-to-investigate-allegations}(p_2, (p_1, p_1'))) \lor \\
& \ (\text{activerole}(p_2, \textit{healthcare-accreditation-organization}) \land \\
& \ \ (u \in_{\mathcal{U}} \textit{report-unethical-conduct-allegations}(p_1, p_1'))) \lor \\
& \ (\text{activerole}(p_2, \textit{attorney}(p_1)) \land \\
& \ \ (u \in_{\mathcal{U}} \textit{determine-legal-options}(p_1, p_1')))) \land \\
& (t \in_{\mathcal{T}} \textit{phi})
\end{aligned}$$

164.502(j)(2)

> *A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce who is the victim of a criminal act discloses protected health information to a law enforcement official, provided that:*
>
> *(i) The protected health information disclosed is about the suspected perpetrator of the criminal act; and*
>
> *(ii) The protected health information disclosed is limited to the information listed in §164.512(f)(2)(i).*

```
permitted_by_164_502_j_2(A) :-
  is_from_employeeOf(A, Y),
  is_belief_from_employeeVictimOfCriminalAct(A, Y),
  is_to_lawEnforcementOfficer(A),
  is_phi(A),
  permitted_by_164_502_j_2_i(A),
  permitted_by_164_502_j_2_ii(A),
  writeln('HIPAA rule 164_502_j_2;').

permitted_by_164_502_j_2_i(A) :-
  is_about_suspectedCrimePerpetrator(A).
```

```
permitted_by_164_502_j_2_ii(A) :-
  permitted_by_164_512_f_2_i(A).
```

We have the following positive norm, where *info-164.512f2i* is an attribute that contains all possible attributes specified in §164.512(f)(2)(i):

$$\begin{aligned}\varphi^{+}_{\texttt{164.502j2}} \triangleq \exists c.\ (&\exists p_1'.\ \text{belongstorole}(p_1', \textit{covered-entity}) \land \\ &\quad\ \text{belongstorole}(p_1, \textit{workforce-member}(p_1'))) \land \\ &\text{activerole}(p_1, \textit{victim-of-crime}(c)) \land \\ &\text{activerole}(p_2, \textit{law-enforcement-official}) \land \\ &\text{belongstorole}(q, \textit{suspected-perpetrator}(c)) \land \\ &(t \in_{\mathcal{T}} \textit{info-164.512f2i})\end{aligned}$$

4.3 §164.506 Uses and disclosures to carry out treatment, payment, or health care operations.

```
%%Uses and disclosures to carry out treatment, payment or health care operations.
permitted_by_164_506(A) :-
  permitted_by_164_506_a(A);
  permitted_by_164_506_b(A);
  permitted_by_164_506_c(A).
```

We have no corresponding norm. Instead, all norms from §164.506 are installed as top-level positive norms.

164.506(a)

> *Except with respect to uses or disclosures that require an authorization under sections 164.508(a)(2) and (3), a covered entity may use or disclose protected health information for treatment, payment, or health care operations as set forth in paragraph (c) of this section, provided that such use or disclosure is consistent with other applicable requirements of this subpart.*

```
permitted_by_164_506_a(A) :-
%Standard permitted uses and disclosures
  \+ require_authorization_by_164_508(A),
  is_from_coveredEntity(A),
  is_for_eitherPurpose(A),
  permitted_by_164_506_c(A),
  writeln(’HIPAA rule 164_506_a;’).
```

We have no directly corresponding norms. The relevant positive norms will be extracted from paragraph (c). The exception for disclosures that require an authorization will be handled by the existence of negative norms for authorization. Similarly, other applicable requirements refer to other negative norms.

164.506(b)

164.506(b)(1)

> *A covered entity may obtain consent of the individual to use or disclose protected health information to carry out treatment, payment, or health care operations.*

```
permitted_by_164_506_b(A) :-
% This consent is only sufficient if authorization is not
% required or there is no other condition before the diclosure
% that needs to be met.
  is_for_eitherPurpose(A),
  is_consentedby_about(A).
```

We have the following positive norm, where we make crucial use of the purposes *treatment*, *payment*, and *healthcare-operations*:

$$
\begin{aligned}
\varphi^{+}_{\texttt{164.506b1}} \triangleq\ & \text{activerole}(p_1, \textit{covered-entity}) \land \\
& \text{obtained-consent-164.506b}(p_1, p_2, (q, t), u) \land \\
& (t \in_{\mathcal{T}} \textit{phi}) \land \\
& ((u \in_{\mathcal{U}} \textit{treatment}) \lor \\
& \ (u \in_{\mathcal{U}} \textit{payment}) \lor \\
& \ (u \in_{\mathcal{U}} \textit{healthcare-operations}))
\end{aligned}
$$

Note that HIPAA does not explicitly give a description of how a covered entity obtains an individual's consent under paragraph §164.506(b). Therefore, the obtained-consent-164.506b predicate relies on an oracle to provide its semantics.

164.506(b)(2)

> *Consent, under paragraph (b) of this section, shall not be effective to permit a use or disclosure of protected health information when an authorization, under §164.508, is required or when another condition must be met for such use or disclosure to be permissible under this subpart.*

There is no Datalog clause in Lam *et al.*'s formalization for this paragraph.

We also have no directly corresponding norm. Instead, the use of different predicates for consent and authorization and the fact that authorization is handled by negative norms ensure that the distinction between consent and authorization is preserved.

164.506(c)

```
permitted_by_164_506_c(A) :-
%Implementation Specification
  permitted_by_164_506_c_1(A);
  permitted_by_164_506_c_2(A);
  permitted_by_164_506_c_3(A);
  permitted_by_164_506_c_4(A);
  permitted_by_164_506_c_5(A).
```

We have no corresponding norm. Instead, the norms from the following subparagraphs are installed as positive norms at the top-level.

164.506(c)(1)

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

```
permitted_by_164_506_c_1(A) :-
  is_for_eitherPurpose(A),
  is_phi(A),
  is_msg_to_within(A).
```

We have the positive norm:

$$\begin{aligned}\varphi^{+}_{\texttt{164.506c1}} \triangleq\ & \text{activerole}(p_1, \textit{covered-entity}) \wedge \\ & (t \in_{\mathcal{T}} \textit{phi}) \wedge \\ & ((u \in_{\mathcal{U}} \textit{treatment}(p_1)) \vee \\ & \ (u \in_{\mathcal{U}} \textit{payment}(p_1)) \vee \\ & \ (u \in_{\mathcal{U}} \textit{healthcare-operations}(p_1)))\end{aligned}$$

where the purposes are now parameterized by p_1, indicating that the purpose is the covered entity's own treatment, payment, or health care operations.

This norm brings up a interesting point of difference with the Datalog formalization of Lam *et al.*. The Datalog implementation requires that the disclosure is made within the covered entity's organization, whereas our formalization makes the weaker requirement that the purpose is that of the covered entity. It is unclear to us which of these interpretations is correct. The stronger requirement could be formalized in our framework as:

$$\begin{aligned}& \text{activerole}(p_1, \textit{covered-entity}) \wedge \\ & \text{activerole}(p_2, \textit{organization-member}(p_1)) \wedge \\ & (t \in_{\mathcal{T}} \textit{phi}) \wedge \\ & ((u \in_{\mathcal{U}} \textit{treatment}) \vee \\ & \ (u \in_{\mathcal{U}} \textit{payment}) \vee \\ & \ (u \in_{\mathcal{U}} \textit{healthcare-operations}))\end{aligned}$$

164.506(c)(2)

> *A covered entity may disclose protected health information for treatment activities of a health care provider.*

```
permitted_by_164_506_c_2(A) :-
  is_for_treatment(A),
  is_phi(A),
  is_to_healthCareProvider(A).
```

We interpret this paragraph as implicitly requiring that the provider is a provider of the subject q (so that providers cannot learn information about strangers) and that the specified provider is actually the recipient. Therefore, we render this clause as:

$$\begin{aligned}\varphi^{+}_{\texttt{164.506c2}} \triangleq\ & \text{activerole}(p_1, \textit{covered-entity}) \land \\ & \text{activerole}(p_2, \textit{provider}(q)) \land \\ & (t \in_{\mathcal{T}} \textit{phi}) \land \\ & (u \in_{\mathcal{U}} \textit{treatment}(p_2))\end{aligned}$$

164.506(c)(3)

> *A covered entity may disclose protected health information to another covered entity or a health care provider for the payment activities of the entity that receives the information.*

```
permitted_by_164_506_c_3(A) :-
  is_for_payment(A),
  is_phi(A),
  (is_to_healthCareProvider(A);
   is_to_coveredEntity(A)).
```

We interpret this clause as implicitly requiring that the provider be a provider of the subject q. Therefore, we have the norm:

$$\begin{aligned}\varphi^{+}_{\texttt{164.506c3}} \triangleq\ & \text{activerole}(p_1, \textit{covered-entity}) \land \\ & (\text{activerole}(p_2, \textit{covered-entity}) \lor \\ & \ \text{activerole}(p_2, \textit{provider}(q))) \land \\ & (t \in_{\mathcal{T}} \textit{phi}) \land \\ & (u \in_{\mathcal{U}} \textit{payment}(p_2))\end{aligned}$$

164.506(c)(4)

> *A covered entity may disclose protected health information to another covered entity for health care operations activities of the entity that receives the information, if each entity either has or had a relationship with the individual who is the subject of the protected health information being requested, the protected health information pertains to such relationship, and the disclosure is:*
>
> *(i) For a purpose listed in paragraph (1) or (2) of the definition of health care operations; or*
>
> *(ii) For the purpose of health care fraud and abuse detection or compliance.*

```
permitted_by_164_506_c_4(A) :-
  %writeln('HIPAA rule 164.506.c.4: How to ensure that its a
  %diff covered entitiy? information pertains to that relation'),
  is_from_coveredEntity(A),
  is_to_coveredEntity(A),
  is_for_healthCareOperations(A),
  %pertains_to(A),
  is_belief_from_about_pertainingToRelationship(A),
  is_msg_about_to_inRelation(A).
  %satisfy_164_506_c_4(A).
```

```
satisfy_164_506_c_4(A) :-
%%Purpose has to be health care operations along with the ones below.
%%Currently not working as you need a list of purposes. Right now it's
%%just one purpose.
  permitted_by_164_506_c_4_i(A);
  permitted_by_164_506_c_4_ii(A).

permitted_by_164_506_c_4_i(A) :-
  debug('164.506.c.4.i: Could not figure out this para;'),
  is_for_definitionOfHealthCareOperations(A).

permitted_by_164_506_c_4_ii(A) :-
  is_for_healthCareFraudAbuseDetection(A);
  is_for_compliance(A).
```

We have the norm:

$$\begin{aligned}
\varphi^{+}_{\texttt{164.506c4}} \triangleq\ & \text{activerole}(p_1, \textit{covered-entity}) \land \\
& \text{activerole}(p_2, \textit{covered-entity}) \land \\
& (t \in_{\mathcal{T}} \textit{phi}) \land \\
& (\exists r_1{:}\mathsf{rel}.\ \diamondminus \text{inrelationship}(p_1, r_1, q) \land \\
& \qquad\qquad \text{pertains-to}(t, r_1)) \land \\
& (\exists r_2{:}\mathsf{rel}.\ \diamondminus \text{inrelationship}(p_2, r_2, q) \land \\
& \qquad\qquad \text{pertains-to}(t, r_2)) \land \\
& ((u \in_{\mathcal{U}} \textit{healthcare-operations-paras-1-2}(p_2)) \lor \\
& \ (u \in_{\mathcal{U}} \textit{healthcare-fraud-abuse-detection}) \lor \\
& \ (u \in_{\mathcal{U}} \textit{healthcare-fraud-abuse-compliance}))
\end{aligned}$$

We introduce a new sort rel for abstract relationships and a predicate inrelationship to judge when a relationship holds. Although this is very similar to our notion of parameterized roles, technically, it is not quite the same. This clause requires us to existentially quantify over a relationship. This cannot be done if parameterized roles are taken as the notion of relationship, since that would mean quantifying over function symbols. The need to add a distinct notion of relationship is somewhat disappointing.

164.506(c)(5)

> *A covered entity that participates in an organized health care arrangement may disclose protected health information about an individual to another covered entity that participates in the organized health care arrangement for any health care operations activities of the organized health care arrangement.*

```
% Create organizations for each organization and have global rules that
% link each member to the organization. Then just confirm that from and to
% are part of same organization and the purpose is the organization's
%purpose
```

```
permitted_by_164_506_c_5(A) :-
  debug('164.506_c_5: Not Implemented yet;').
```

We have the norm:

$$\begin{aligned}
\varphi^{+}_{\texttt{164.506c5}} \triangleq \exists p.\ & \mathrm{belongstorole}(p, \mathit{organized\text{-}healthcare\text{-}arrangement}) \land \\
& \mathrm{activerole}(p_1, \mathit{covered\text{-}entity}) \land \\
& \mathrm{activerole}(p_1, \mathit{participant}(p)) \land \\
& \mathrm{activerole}(p_2, \mathit{covered\text{-}entity}) \land \\
& \mathrm{activerole}(p_2, \mathit{participant}(p)) \land \\
& (t \in_{\mathcal{T}} \mathit{phi}) \land \\
& (u \in_{\mathcal{U}} \mathit{healthcare\text{-}operations}(p))
\end{aligned}$$

4.4 §164.508 Uses and disclosures for which an authorization is required.

Lam *et al.*'s Datalog formalization does not cover §164.508:

```
%% Uses and disclosures for which authorization is required.
  %should check if all valid authorizations have been obtained
require_authorization_by_164_508(A) :-
  debug('164.508: TBD no authorizations required, returns true;').
```

164.508(a)

164.508(a)(1)

> *Except as otherwise permitted or required by this subchapter, a covered entity may not use or disclose protected health information without an authorization that is valid under this section. When a covered entity obtains or receives a valid authorization for its use or disclosure of protected health information, such use or disclosure must be consistent with such authorization.*

We have no norms for §164.508(a)(1), since we interpret this paragraph as a statement of intent, rather than a statement of implementation specification.

164.508(a)(2)

> *Notwithstanding any provision of this subpart, other than the transition provisions in §164.532, a covered entity must obtain an authorization for any use or disclosure of psychotherapy notes, except:*
>
> *(i) To carry out the following treatment, payment, or health care operations:*
>
> *(A) Use by the originator of the psychotherapy notes for treatment;*
>
> *(B) Use or disclosure by the covered entity for its own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling; or*

(C) *Use or disclosure by the covered entity to defend itself in a legal action or other proceeding brought by the individual; and*

(ii) *A use or disclosure that is required by §164.502(a)(2)(ii) or permitted by §164.512(a); §164.512(d) with respect to the oversight of the originator of the psychotherapy notes; §164.512(g)(1); or §164.512(j)(1)(i).*

The core of this paragraph is given by the following negative norm:

$$\begin{aligned}\varphi^-_{\texttt{164.508a2}} \triangleq\ & \text{activerole}(p_1, \textit{covered-entity}) \wedge \\ & (t \in_{\mathcal{T}} \textit{psychotherapy-notes}) \supset \\ & \quad \text{obtained-authorization-164.508}(p_1, p_2, (q,t), u)\end{aligned}$$

This negative norm is then given several exceptions, resulting in the new negative norm:

$$\begin{aligned}\varphi^-_{\texttt{164.508a2}'} \triangleq\ & \varphi^-_{\texttt{164.508a2}} \vee \\ & (\varphi^+_{\texttt{164.508a2iB}} \vee \\ & \ \varphi^+_{\texttt{164.508a2iC}}) \vee \\ & \varphi^+_{\texttt{164.508a2ii}}\end{aligned}$$

These positive exception norms are given by the following. First, note that §164.508(a)(2)(i)(A) applies only to uses of the psychotherapy notes, not disclosures. Since we handle only disclosures in our formalization, we ignore this exception.

Second, we have an exception for §164.508(a)(2)(i)(B):

$$\begin{aligned}\varphi^+_{\texttt{164.508a2iB}} \triangleq\ & \text{activerole}(p_1, \textit{covered-entity}) \wedge \\ & (u \in_{\mathcal{U}} \textit{counseling-training-programs}(p_1))\end{aligned}$$

Note that the purpose *counseling-training-programs*(p_1) is parameterized by p_1 to ensure that the programs are run by the covered entity that obtained the authorization.

Third, we have an exception for §164.508(a)(2)(i)(C):

$$\begin{aligned}\varphi^+_{\texttt{164.508a2iC}} \triangleq\ & \text{activerole}(p_1, \textit{covered-entity}) \wedge \\ & (u \in_{\mathcal{U}} \textit{defense-in-legal-proceeding}(p_1, q))\end{aligned}$$

Again, we parameterize the purpose to ensure that the proceeding is being brought against p_1 by q.

Finally, §164.508(a)(2)(ii):

$$\begin{aligned}\varphi^+_{\texttt{164.508a2ii}} \triangleq\ & \varphi^+_{\texttt{164.502a2ii}} \vee \\ & (\textstyle\bigvee_{i \in \texttt{164.512a}} \varphi^+_i) \vee \\ & (\textstyle\bigvee_{i \in \texttt{164.512d}} \varphi^+_i) \vee \\ & \varphi^+_{\texttt{164.512g1}} \vee \\ & \varphi^+_{\texttt{164.512j1i}}\end{aligned}$$

164.508(a)(3)

164.508(a)(3)(i)

> *Notwithstanding any provision of this subpart, other than the transition provisions in §164.532, a covered entity must obtain an authorization for any use or disclosure of protected health information for marketing, except if the communication is in the form of:*
>
> *(A) A face-to-face communication made by a covered entity to an individual; or*
> *(B) A promotional gift of nominal value provided by the covered entity.*

In a manner similar to that of the previous paragraph on psychotherapy notes, we handle the core of this paragraph with a negative norm.

$$\begin{aligned}\varphi^{-}_{\texttt{164.508a3i}} \triangleq\ & \text{activerole}(p_1, \textit{covered-entity}) \land \\ & (t \in_{\mathcal{T}} \textit{phi}) \land \\ & (u \in_{\mathcal{U}} \textit{marketing}) \supset \\ & \quad \text{obtained-authorization-164.508}(p_1, p_2, (q,t), u)\end{aligned}$$

This negative norm has several exceptions:

$$\begin{aligned}\varphi^{-}_{\texttt{164.508a3i}'} \triangleq\ & \varphi^{-}_{\texttt{164.508a3i}} \lor \\ & \varphi^{+}_{\texttt{164.508a3iA}} \lor \\ & \varphi^{+}_{\texttt{164.508a3iB}}\end{aligned}$$

These exceptions are given by the following positive norms. First, §164.508(a)(3)(i)(A):

$$\begin{aligned}\varphi^{+}_{\texttt{164.508a3iA}} \triangleq\ & \text{activerole}(p_1, \textit{covered-entity}) \land \\ & (p_2 \approx q) \land \\ & \text{face-to-face}(p_1, p_2, (q,t), u)\end{aligned}$$

Here we use a new predicate, face-to-face, to ensure that the disclosure is a face-to-face communication. The semantics of this predicate are given by an oracle.

Second, we have an exception for §164.508(a)(3)(i)(B):

$$\begin{aligned}\varphi^{+}_{\texttt{164.508a3iB}} \triangleq\ & \text{activerole}(p_1, \textit{covered-entity}) \land \\ & \text{promotional-gift-of-nominal-value}(p_1, p_2, (q,t), u)\end{aligned}$$

Again, we rely on an oracle to provide semantics for the new promotional-gift-of-nominal-value predicate.

164.508(a)(3)(ii)

> *If the marketing involves direct or indirect remuneration to the covered entity from a third party, the authorization must state that such remuneration is involved.*

We have the following constraint, which is captured as a macro:

$$\begin{aligned}& \text{is-valid-authorization-164.508a3ii}(m', p_1, p_2, (q,t), u) \triangleq \\ & \quad (u \in_{\mathcal{U}} \textit{marketing}) \land \\ & \quad (\text{involves-remuneration}(p_1, p_2, (q,t), u) \supset \\ & \qquad \text{states-remuneration-involvement}(m', p_1, p_2, (q,t), u))\end{aligned}$$

This macro captures a validity condition on authorizations, and is of a different flavor than the previous parts of this paragraph, §164.508(a)(3).

164.508(b)

At this point, we formalize what it means to obtain an authorization. Although not explicitly stated in the law, it seems reasonable to include the following macro as the means of obtaining an authorization:

$$\begin{aligned}
&\text{obtained-authorization-164.508}(p_1, p_2, (q, t), u) \triangleq \\
&\quad \exists m'.\ \diamondminus \text{send}(q, p_1, m') \land \\
&\qquad \text{is-valid-authorization}(m', p_1, p_2, (q, t), u)
\end{aligned}$$

Based on paragraphs §164.508(b)(1) and (2), an authorization is valid if it is valid under §164.508(b)(1) and not defective under §164.508(b)(2):

$$\begin{aligned}
&\text{is-valid-authorization}(m', p_1, p_2, (q, t), u) \triangleq \\
&\quad \text{is-valid-authorization-164.508b1}(m', p_1, p_2, (q, t), u) \land \\
&\quad \neg\text{is-defective-authorization-164.508b2}(m', p_1, p_2, (q, t), u)
\end{aligned}$$

Unfortunately, this has the distinct disadvantage of not adhering to the structure of the legal text. However, there does not appear to be a clean solution that also adheres to the structure of the text.

164.508(b)(1)

> *(i) A valid authorization is a document that meets the requirements in paragraphs (a)(3)(ii), (c)(1), and (c)(2) of this section, as applicable.*
>
> *(ii) A valid authorization may contain elements or information in addition to the elements required by this section, provided that such additional elements or information are not inconsistent with the elements required by this section.*

$$\begin{aligned}
&\text{is-valid-authorization-164.508b1}(m', p_1, p_2, (q, t), u) \triangleq \\
&\quad \text{is-valid-authorization-164.508a3ii}(m', p_1, p_2, (q, t), u) \land \\
&\quad \text{is-valid-authorization-164.508c1}(m', p_1, p_2, (q, t), u) \land \\
&\quad \text{is-valid-authorization-164.508c2}(m', p_1, p_2, (q, t), u) \land \\
&\quad \text{is-valid-authorization-164.508c3}(m', p_1, p_2, (q, t), u) \land \\
&\quad \neg\text{inconsistent-authorization}(m', p_1, p_2, (q, t), u)
\end{aligned}$$

Although it is not mentioned in this paragraph, we have chosen to include the additional constraint that a valid authorization must meet the requirement in paragraph (c)(3). Without this addition, paragraph (c)(3) appears to be an orphan. This is probably just an oversight on the part of the HIPAA authors.

164.508(b)(2)

> *An authorization is not valid, if the document submitted has any of the following defects:*
>
> *(i) The expiration date has passed or the expiration event is known by the covered entity to have occurred;*
>
> *(ii) The authorization has not been filled out completely, with respect to an element described by paragraph (c) of this section, if applicable;*

(iii) The authorization is known by the covered entity to have been revoked;

(iv) The authorization violates paragraph (b)(3) or (4) of this section, if applicable;

(v) Any material information in the authorization is known by the covered entity to be false.

is-defective-authorization-164.508b2$(m', p_1, p_2, (q, t), u) \triangleq$
expiration-event-passed$(m', p_1, p_2, (q, t), u) \lor$
is-incompletely-filled-out-authorization$(m', p_1, p_2, (q, t), u) \lor$
authorization-has-been-revoked$(m', p_1, p_2, (q, t), u) \lor$
violates-164.508b3$(m', p_1, p_2, (q, t), u) \lor$
violates-164.508b4$(m', p_1, p_2, (q, t), u) \lor$
contains-information-known-to-be-false(m', p_1)

Note that the new predicates expiration-event-passed, is-incompletely-filled-out-authorization, and contains-information-known-to-be-false are given semantics via oracles. This is because the exact form of authorization messages are not specified in HIPAA. The remaining pieces of this macro are themselves macros defined below.

164.508(b)(3)

An authorization for use or disclosure of protected health information may not be combined with any other document to create a compound authorization, except as follows:

(i) An authorization for the use or disclosure of protected health information for a research study may be combined with any other type of written permission for the same research study, including another authorization for the use or disclosure of protected health information for such research or a consent to participate in such research;

(ii) An authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes;

(iii) An authorization under this section, other than an authorization for a use or disclosure of psychotherapy notes, may be combined with any other such authorization under this section, except when a covered entity has conditioned the provision of treatment, payment, enrollment in the health plan, or eligibility for benefits under paragraph (b)(4) of this section on the provision of one of the authorizations.

violates-164.508b3$(m', p_1, p_2, (q, t), u) \triangleq$
is-compound-authorization$(m', p_1, p_2, (q, t), u) \supset$
is-compound-research-authorization$(m', p_1, p_2, (q, t), u) \lor$
is-compound-psychotherapy-authorization$(m', p_1, p_2, (q, t), u) \lor$
$\neg$provision-of-healthcare-conditioned-on$(m', p_1, p_2, (q, t), u)$

164.508(b)(4)

A covered entity may not condition the provision to an individual of treatment, payment, enrollment in the health plan, or eligibility for benefits on the provision of an authorization, except:

(i) A covered health care provider may condition the provision of research- related treatment on provision of an authorization for the use or disclosure of protected health information for such research under this section;

(ii) A health plan may condition enrollment in the health plan or eligibility for benefits on provision of an authorization requested by the health plan prior to an individual's enrollment in the health plan, if:

(A) The authorization sought is for the health plan's eligibility or enrollment determinations relating to the individual or for its underwriting or risk rating determinations; and

(B) The authorization is not for a use or disclosure of psychotherapy notes under paragraph (a)(2) of this section; and

(iii) A covered entity may condition the provision of health care that is solely for the purpose of creating protected health information for disclosure to a third party on provision of an authorization for the disclosure of the protected health information to such third party.

We have the constraint:

$$
\begin{aligned}
&\text{provision-of-healthcare-conditioned-on}(m', p_1, p_2, (q, t), u) \Rightarrow\\
&\quad \text{is-for-research}(m', p_1, p_2, (q, t), u) \lor\\
&\quad (\text{is-for-healthplan-enrollment}(m', p_1, p_2, (q, t), u) \land\\
&\quad\quad \neg\text{is-psychotherapy-authorization}(m', p_1, p_2, (q, t), u)) \lor\\
&\quad \text{is-for-creation-solely-for-disclosure}(m', p_1, p_2, (q, t), u)
\end{aligned}
$$

164.508(b)(5)

An individual may revoke an authorization provided under this section at any time, provided that the revocation is in writing, except to the extent that:

(i) The covered entity has taken action in reliance thereon; or

(ii) If the authorization was obtained as a condition of obtaining insurance coverage, other law provides the insurer with the right to contest a claim under the policy or the policy itself.

We have the macro:

$$
\begin{aligned}
&\text{authorization-has-been-revoked}(m', p_1, p_2, (q, t), u) \triangleq\\
&\qquad \exists m''.\ \diamondminus\text{send}(q, p_1, m'') \land\\
&\qquad\qquad \text{is-revocation}(m'', m', p_1, p_2, (q, t), u)
\end{aligned}
$$

Note that HIPAA does not define what counts as a revocation message, and so we rely on an oracle for the is-revocation predicate.

Also, note that the first exception regarding action taken "in reliance thereon" is handled by the fact that validity of an authorization (and therefore absence of a revocation) is checked at the moment of disclosure. Any disclosure made under an authorization that is later revoked will be valid at the time of disclosure, since the authorization is not yet revoked.

The second exception is handled by other law, and so is not directly a part of our HIPAA formalization.

164.508(b)(6)

> *A covered entity must document and retain any signed authorization under this section as required by §164.530(j).*

The model used in our formalization currently supports only disclosures; we have no mechanism to track the physical records held by the various entities.

164.508(c)

164.508(c)(1)

> *A valid authorization under this section must contain at least the following elements:*
>
> *(i) A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion.*
>
> *(ii) The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure.*
>
> *(iii) The name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure.*
>
> *(iv) A description of each purpose of the requested use or disclosure. The statement "at the request of the individual" is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose.*
>
> *(v) An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. The statement "end of the research study," "none," or similar language is sufficient if the authorization is for a use or disclosure of protected health information for research, including for the creation and maintenance of a research database or research repository.*
>
> *(vi) Signature of the individual and date. If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must also be provided.*

$$
\begin{array}{l}
\text{is-valid-authorization-164.508c1}(m', p_1, p_2, (q,t), u) \triangleq \\
\quad \text{contains-description-allowed-information}(m', (q,t)) \wedge \\
\quad \text{contains-description-allowed-senders}(m', p_1) \wedge \\
\quad \text{contains-description-allowed-recipients}(m', p_2) \wedge \\
\quad \text{contains-description-allowed-purpose}(m', u) \wedge \\
\quad \text{contains-expiration-date-or-event}(m') \wedge \\
\quad (\text{contains-signature}(m', q) \vee \\
\quad\; (\exists p_q.\ \text{belongstorole}(p_q, \textit{personal-representative}(q)) \wedge \\
\quad\quad\quad \text{contains-signature}(m', p_q) \wedge \\
\quad\quad\quad \text{contains-description-representation-authority}(m', p_q)))
\end{array}
$$

Note that we must use new contains-... predicates, which are given semantics via oracles since HIPAA does not specify a concrete format for authorization messages. Our built-in contains predicate does not work here because the pieces of information in which we are interested are not associated with particular principals.

164.508(c)(2)

> *In addition to the core elements, the authorization must contain statements adequate to place the individual on notice of all of the following:*
>
> *(i) The individual's right to revoke the authorization in writing, and either:*
>
> *(A) The exceptions to the right to revoke and a description of how the individual may revoke the authorization; or*
>
> *(B) To the extent that the information in paragraph (c)(2)(i)(A) of this section is included in the notice required by §164.520, a reference to the covered entity's notice.*
>
> *(ii) The ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization, by stating either:*
>
> *(A) The covered entity may not condition treatment, payment, enrollment or eligibility for benefits on whether the individual signs the authorization when the prohibition on conditioning of authorizations in paragraph (b)(4) of this section applies; or*
>
> *(B) The consequences to the individual of a refusal to sign the authorization when, in accordance with paragraph (b)(4) of this section, the covered entity can condition treatment, enrollment in the health plan, or eligibility for benefits on failure to obtain such authorization.*
>
> *(iii) The potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient and no longer be protected by this subpart.*

$$\begin{aligned}&\text{is-valid-authorization-164.508c2}(m', p_1, p_2, (q,t), u) \triangleq\\ &\quad \text{contains-description-right-to-revoke}(m') \wedge\\ &\quad ((\text{contains-description-exceptions-right-to-revoke}(m') \wedge\\ &\quad\quad \text{contains-description-revocation-procedure}(m')) \vee\\ &\quad\ \ \text{contains-reference-to-164.520notice}(m')) \wedge\\ &\quad \text{contains-description-conditioning-treatment-etc}(m') \wedge\\ &\quad \text{contains-description-redisclosure-potential}(m')\end{aligned}$$

164.508(c)(3)

> *The authorization must be written in plain language.*

$$\begin{aligned}&\text{is-valid-authorization-164.508c3}(m', p_1, p_2, (q,t), u) \triangleq\\ &\quad \text{in-plain-language}(m', p_1, p_2, (q,t), u)\end{aligned}$$

Again, the new predicate in-plain-language relies on an oracle for its semantics.

164.508(c)(4)

> *If a covered entity seeks an authorization from an individual for a use or disclosure of protected health information, the covered entity must provide the individual with a copy of the signed authorization.*

This paragraph does not quite fit with our model. In our model, an individual sends the covered entity a signed authorization. Since the authorization comes from the individual, the individual can make his own copy.

4.5 §164.510 Uses and disclosures requiring an opportunity for the individual to agree or object.

> *A covered entity may use or disclose protected health information, provided that the individual is informed in advance of the use or disclosure and has the opportunity to agree to or prohibit or restrict the use or disclosure, in accordance with the applicable requirements of this section. The covered entity may orally inform the individual of and obtain the individual's oral agreement or objection to a use or disclosure permitted by this section.*

```
permitted_by_164_510(A):-
  is_phi(A),
  (permitted_by_164_510_a(A);
   permitted_by_164_510_b(A)).
```

As usual, we have no directly corresponding norms. Instead, the norms are taken from paragraphs (a) and (b).

164.510(a)

```
permitted_by_164_510_a(A) :-
  permitted_by_164_510_a_1(A),
  (permitted_by_164_510_a_2(A);
   excluded_by_164_510_a_3(A)).
```

Due to the nested exceptions, we follow the strategy of Lam *et al.*'s Datalog formalization and introduce a macro for the combination of the individual components:

$$\varphi^{+}_{\texttt{164.510a}} \triangleq \varphi^{+}_{\texttt{164.510a1ii}} \wedge (\varphi^{-}_{\texttt{164.510a2}} \vee (\varphi^{+}_{\texttt{164.510a3i}} \wedge \varphi^{-}_{\texttt{164.510a3ii}}))$$

164.510(a)(1)

> *Except when an objection is expressed in accordance with paragraphs (a)(2) or (3) of this section, a covered health care provider may:*

164.510(a)(1)(i)

> *Use the following protected health information to maintain a directory of individuals in its facility:*
>
> *(A) The individual's name;*
> *(B) The individual's location in the covered health care provider's facility;*
> *(C) The individual's condition described in general terms that does not communicate specific medical information about the individual; and*

> *(D) The individual's religious affiliation; and*

Lam *et al.*'s formalization has no corresponding clauses. Because our model does not currently support uses of protected information, we, too, do not have any corresponding norms.

164.510(a)(1)(ii)

> *Disclose for directory purposes such information:*
>
> *(A) To members of the clergy; or*
>
> *(B) Except for religious affiliation, to other persons who ask for the individual by name.*

```
permitted_by_164_510_a_1(A):-
  (is_for_directory_purp(A),
   is_nam_loc_or_condition(A),
   %need to implement "asked by name"
   fail);
  (is_to_clergy(A),
   (is_type_relig(A);
    is_nam_loc_or_condition(A)),
   writeln('HIPAA rule 164_510_a_1')).
```

The Datalog formalization of Lam *et al.* does not appear to include, here or elsewhere, the possibility for objection to this disclosure.

We have the positive norm:

$$\begin{aligned}
\varphi^{+}_{\texttt{164.510a1ii}} \triangleq\ & \text{activerole}(p_1, \textit{covered-entity}) \wedge \\
& (\text{activerole}(p_2, \textit{clergy}) \vee \\
& \ (\neg(t \in_{\mathcal{T}} \textit{religious-affiliation}) \wedge \\
& \quad \exists m'.\ \diamondminus \text{send}(p_2, p_1, m') \wedge \\
& \qquad\qquad \text{is-directory-request-by-name}(m', p_2, p_1, (q, t), u))) \wedge \\
& (t \in_{\mathcal{T}} \textit{directory-information}) \wedge \\
& (u \in_{\mathcal{U}} \textit{directory})
\end{aligned}$$

Note that we do not incorporate the "Except when an objection is expressed" phrase here. Instead, we choose to locate this exception in $\varphi^{-}_{\texttt{164.510a2}}$ in order to link it to the corresponding opportunity to object.

164.510(a)(2)

> *A covered health care provider must inform an individual of the protected health information that it may include in a directory and the persons to whom it may disclose such information (including disclosures to clergy of information regarding religious affiliation) and provide the individual with the opportunity to restrict or prohibit some or all of the uses or disclosures permitted by paragraph (a)(1) of this section.*

```
permitted_by_164_510_a_2(A):-
  is_about_was_given_consent_opp(A),
  writeln('HIPAA rule 164_510_a_2').
```

We have the negative norm that no objection has been received since the opportunity to object was provided:

$$\begin{aligned}\varphi^-_{\texttt{164.510a2}} \triangleq\ & (\neg\exists m''.\ \text{send}(q, p_1, m'') \wedge \\ &\qquad\qquad \text{is-directory-objection-164.510a}(m'', p_1, p_2, (q,t), u)) \\ & \mathcal{S} \\ & (\exists m'.\ \text{send}(p_1, q, m') \wedge \\ &\qquad \text{is-opportunity-to-object-164.510a}(m', p_1, p_2, (q,t), u))\end{aligned}$$

This is most cleanly expressed using the "since" temporal operator, $\mathcal{S}$.

164.510(a)(3)

164.510(a)(3)(i)

> *If the opportunity to object to uses or disclosures required by paragraph (a)(2) of this section cannot practicably be provided because of the individual's incapacity or an emergency treatment circumstance, a covered health care provider may use or disclose some or all of the protected health information permitted by paragraph (a)(1) of this section for the facility's directory, if such disclosure is:*
>
> *(A) Consistent with a prior expressed preference of the individual, if any, that is known to the covered health care provider; and*
>
> *(B) In the individual's best interest as determined by the covered health care provider, in the exercise of professional judgment.*

```
excluded_by_164_510_a_3:-
  (is_about_incapac(A);
   is_about_emerg(A)),
  fail,
  % not sure how to implement is consistent with past,
  is_belief_best_interest(A),
  writeln('HIPAA rule 164_510_a3').
```

We have the positive norm:

$$\begin{aligned}\varphi^+_{\texttt{164.510a3i}} \triangleq\ & \neg\text{practicable-to-provide-opportunity-to-object-164.510a}(p_1, p_2, (q,t), u) \wedge \\ & \text{consistent-with-prior-preference}(p_1, p_2, (q,t), u) \wedge \\ & \text{believes-in-best-interest-164.510a3iB}(p_1, p_2, (q,t), u)\end{aligned}$$

where practicable-to-provide-opportunity-to-object-164.510a is defined as the macro:

$$\begin{aligned}&\text{practicable-to-provide-opportunity-to-object-164.510a}(p_1, p_2, (q,t), u) \triangleq \\ &\qquad \neg\text{belongstorole}(q, \textit{incapacitated}) \wedge \\ &\qquad \neg\text{belongstorole}(q, \textit{emergency-treatment})\end{aligned}$$

Because this positive norm is joined by disjunction with $\varphi^-_{\texttt{164.510a2}}$ in $\varphi^+_{\texttt{164.510a}}$, this has the effect of allowing the opportunity to object to be skipped if it is not practicable to provide that opportunity.

164.510(a)(3)(ii)

> *The covered health care provider must inform the individual and provide an opportunity to object to uses or disclosures for directory purposes as required by paragraph (a)(2) of this section when it becomes practicable to do so.*

There is no corresponding Datalog clause in Lam *et al.*'s formalization, likely because Datalog has no means of speaking about future events and their obligations.

We use the following negative exception:

$$\begin{aligned}\varphi^{-}_{\texttt{164.510a3ii}} \triangleq\ & (\neg\text{practicable-to-provide-opportunity-to-object-164.510a}(p_1, p_2, (q, t), u)) \\ & \mathcal{W} \\ & (\exists m'.\ \text{send}(p_1, q, m') \wedge \\ & \qquad \text{is-opportunity-to-object-164.510a}(m', p_1, p_2, (q, t), u))\end{aligned}$$

In other words, an opportunity to object can be sent in the current state or a future state, provided that in no intervening state is it practicable to provide an opportunity to object.

This norm has the drawback of repeating text from $\varphi^{-}_{\texttt{164.510a2}}$, but it does not seem possible to avoid doing so.

164.510(b)

164.510(b)(1)

164.510(b)(1)(i)

> *A covered entity may, in accordance with paragraphs (b)(2) or (3) of this section, disclose to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual, the protected health information directly relevant to such person's involvement with the individual's care or payment related to the individual's health care.*

```
permitted_by_164_510_b_1_i(A):-
  is_phi(A),
  is_from_coveredEntity(A),
  (is_to_relative(A);
   is_to_closeFriend(A);
   is_to_personIdentified(A)),
  is_relevant_to_payment_or_care_involvement(A),
  writeln('HIPAA rule 164_510_b_1_i').
```

We have the positive norm:

$$\begin{aligned}\varphi^{+}_{\texttt{164.510b1i}} \triangleq\ & \text{activerole}(p_1, \textit{covered-entity}) \wedge \\ & (\text{activerole}(p_2, \textit{family-member}(q)) \vee \\ & \ \text{activerole}(p_2, \textit{relative}(q)) \vee \\ & \ \text{activerole}(p_2, \textit{close-personal-friend}(q)) \vee \\ & \ \text{activerole}(p_2, \textit{identified-164.510b}(q))) \wedge \\ & (t \in_{\mathcal{T}} \textit{phi}) \wedge \\ & \text{relevant-to-involvement}(t, p_2, q)\end{aligned}$$

Because HIPAA does not describe the process under which an individual may identify a person to which protected health information may be sent, we abstractly represent this relationship using a role *identified-164.510b*(q). The process of naming this person would constrain the principals that may hold this role.

164.510(b)(1)(ii)

> *A covered entity may use or disclose protected health information to notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death. Any such use or disclosure of protected health information for such notification purposes must be in accordance with paragraphs (b)(2), (3), or (4) of this section, as applicable.*

```
permitted_by_164_510_b_1_ii(A):-
  is_phi(A),
  is_from_coveredEntity(A),
  (is_for_notification_fam_personalrep_respons_of_location(A);
   is_for_notification_fam_personalrep_respons_of_gencond(A);
   is_for_notification_fam_personalrep_respons_of_death(A)),
  writeln('HIPAA rule 164_510_b_1_ii;').
```

We have the positive norm:

$$\begin{aligned}\varphi^{+}_{\texttt{164.510b1ii}} \triangleq\ & \text{activerole}(p_1, \textit{covered-entity}) \land \\ & (((\text{activerole}(p_2, \textit{family-member}(q)) \lor \\ & \quad \text{activerole}(p_2, \textit{personal-representative}(q)) \lor \\ & \quad \text{activerole}(p_2, \textit{responsible-for-care-of}(q))) \land \\ & \ (t \in_{\mathcal{T}} \textit{location-condition-death}) \land \\ & \ (u \in_{\mathcal{U}} \textit{notification-164.510b})) \lor \\ & ((t \in_{\mathcal{T}} \textit{phi}) \land \\ & \ (u \in_{\mathcal{U}} \textit{assist-notification-164.510b})))\end{aligned}$$

164.510(b)(2)

> *If the individual is present for, or otherwise available prior to, a use or disclosure permitted by paragraph (b)(1) of this section and has the capacity to make health care decisions, the covered entity may use or disclose the protected health information if it:*
>
> *(i) Obtains the individual's agreement;*
>
> *(ii) Provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection; or*
>
> *(iii) Reasonably infers from the circumstances, based the exercise of professional judgment, that the individual does not object to the disclosure.*

```
%not sure how to implement these yet:
%is_about_present,is_about_avail_for_consent,is_about_in_capac_to_make_dec
%currently they fail
```

```
permitted_by_164_510_b_2(A):-
  ((not(is_about_present(A));
    not(is_about_avail_for_consent(A))),
   not(is_about_in_capac_to_make_dec(A)));
  ((is_about_present(A);
    is_about_avail_for_consent(A)),
   (is_about_in_capac_to_make_dec(A)),
   (is_consentedby_about(A);
    is_about_was_given_consent_opp(A);
    is_belief_can_be_inferred_indiv_wouldnt_object(A))),
  writeln('HIPAA rule 164_510_b_2').
```

Lam *et al.* seem to be using negation as a means of simulating classical implication.

We have the negative norm:

$$\begin{aligned}\varphi^{-}_{\texttt{164.510b2}} \triangleq\ & \diamondminus(\text{available}(p_1, q) \wedge \\ & \quad \text{has-capacity-to-make-healthcare-decisions}(q)) \supset \\ & \text{has-obtained-agreement-164.510b2}(p_1, p_2, (q, t), u) \vee \\ & \text{has-provided-opportunity-no-objection-164.510b2}(p_1, p_2, (q, t), u) \vee \\ & \text{professional-judgment-individual-does-not-object}(p_1, p_2, (q, t), u)\end{aligned}$$

Although HIPAA does not explicitly define what it means to obtain the individual's agreement or provide an opportunity to object, it seems reasonable to implement these as the following macros:

$$\begin{aligned}& \text{has-obtained-agreement-164.510b2}(p_1, p_2, (q, t), u) \triangleq \\ & \quad \exists m'.\ \diamondminus\text{send}(q, p_1, m') \wedge \\ & \qquad \text{is-agreement-164.510b2}(m', p_1, p_2, (q, t), u)\end{aligned}$$

and

$$\begin{aligned}& \text{has-provided-opportunity-no-objection-164.510b2}(p_1, p_2, (q, t), u) \triangleq \\ & \quad (\neg\exists m''.\ \text{send}(q, p_1, m'') \wedge \\ & \qquad \text{is-objection-164.510b2}(m'', p_1, p_2, (q, t), u))\ \mathcal{S} \\ & \quad (\exists m'.\ \text{send}(p_1, q, m') \wedge \\ & \qquad \text{is-opportunity-to-object-164.510b2}(m', p_1, p_2, (q, t), u))\end{aligned}$$

The predicate professional-judgment-individual-does-not-object is given semantics via an oracle.

164.510(b)(3)

> *If the individual is not present, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, the covered entity may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual and, if so, disclose only the protected health information that is directly relevant to the person's involvement with the individual's health care. A covered entity may use professional judgment and its experience with common practice to make reasonable inferences of the*

> *individual's best interest in allowing a person to act on behalf of the individual to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of protected health information.*

```
permitted_by_164_510_b_3(A):-
  (is_about_present(A),
   (not(is_about_incapac(A)),
    not(is_about_emerg(A))));
  (is_belief_best_interest(A),
   (is_relevant_to_payment_or_health_involvement(A);
    is_msg_type(A,pres_medsupp_xray_etc))),
  writeln('HIPAA rule 164_510_b_3').
```

Again, it seems that Lam *et al.* use negation to simulate classical implication.

We have the following negative norm:

$$\begin{aligned}\varphi^-_{\texttt{164.510b3}} \triangleq \neg\diamondsuit(&\text{available}(p_1, q) \land \\ &\quad \text{has-capacity-to-make-healthcare-decisions}(q)) \supset \\ &\text{professional-judgment-is-in-best-interest-of-164.510b3}(p_1, p_2, (q, t), u) \land \\ &\text{relevant-to-involvement}(t, p_2, q)\end{aligned}$$

The new predicates introduced here all rely on oracles for their semantics.

164.510(b)(4)

> *A covered entity may use or disclose protected health information to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the uses or disclosures permitted by paragraph (b)(1)(ii) of this section. The requirements in paragraphs (b)(2) and (3) of this section apply to such uses and disclosure to the extent that the covered entity, in the exercise of professional judgment, determines that the requirements do not interfere with the ability to respond to the emergency circumstances.*

```
permitted_by_164_510_b_4(A):-
  permitted_by_164_510_b_1_ii(A),
  (is_to_privateEntity(A);
   is_to_publicEntity(A)),
  (is_to_authorizedByLaw_to_assist_disasterRelief(A);
   is_to_authorizedByCharter_to_assist_disasterRelief(A)),
  ((permitted_by_164_510_b_2(A),
    permitted_by_164_510_b_3(A));
   is_belief_not_disclosing_would_interfere_with_emergResponse(A)),
  writeln('HIPAA rule 164_510_b_4').
```

We have the positive norm:

$$\begin{aligned}\varphi^+_{\texttt{164.510b4}} \triangleq\ &\text{activerole}(p_1, \textit{covered-entity}) \land \\ &\text{activerole}(p_2, \textit{authorized-by-law-or-charter-to-assist-in-disaster-relief}) \land \\ &(t \in_{\mathcal{T}} \textit{phi}) \land \\ &(u \in_{\mathcal{U}} \textit{coordinate-disclosure-under-164.510b1ii})\end{aligned}$$

The final positive norm would be restricted according to the negative norms from paragraphs (b)(2) and (3):

$$\begin{aligned}
&\varphi^{+}_{\texttt{164.510b4}'} \triangleq \\
&\quad \varphi^{+}_{\texttt{164.510b4}} \land \\
&\quad (\neg\text{prof-judgment-reqs-do-not-interfere-with-emerg-response}(p_1, p_2, (q,t), u) \lor \\
&\quad\; (\varphi^{-}_{\texttt{164.510b2}} \land \\
&\quad\;\; \varphi^{-}_{\texttt{164.510b3}}))
\end{aligned}$$

4.6 §164.512 Uses and disclosures for which an authorization or opportunity to agree or object is not required.

> *A covered entity may use or disclose protected health information without the written authorization of the individual, as described in §164.508, or the opportunity for the individual to agree or object as described in §164.510, in the situations covered by this section, subject to the applicable requirements of this section. When the covered entity is required by this section to inform the individual of, or when the individual may agree to, a use or disclosure permitted by this section, the covered entity's information and the individual's agreement may be given orally.*

The Datalog formalization of Lam *et al.* does not cover §164.512:

```
permitted_by_164_512(A) :-
  debug('164.512: not implemented: uses and disclosure where authorization
         not required;').
```

Since §164.502(a)(1)(vi) explicitly permits disclosures under this section, there is no need to add any norms at this point; they will come from the following paragraphs.

164.512(a)

164.512(a)(1)

> *A covered entity may use or disclose protected health information to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law.*

$$\begin{aligned}
\varphi^{+}_{\texttt{164.512a1}} \triangleq\; &\text{activerole}(p_1, \textit{covered-entity}) \land \\
&(t \in_{\mathcal{T}} \textit{phi}) \land \\
&\text{is-required-by-law}(p_1, p_2, (q,t), u)
\end{aligned}$$

The phrase "is limited to the relevant requirements of such law" is captured by the fact that we examine one piece of information at a time. Since we choose not to formalize all relevant laws, we rely on an oracle to provide semantics for the is-required-by-law predicate.

164.512(a)(2)

> *A covered entity must meet the requirements described in paragraph (c), (e), or (f) of this section for uses or disclosures required by law.*

To ensure that the requirements from paragraphs (c), (e), and (f) are satisfied, we join the negative norms from those paragraphs with $\varphi^{+}_{\texttt{164.512a1}}$ to form a new positive norm:

$$\begin{aligned}\varphi^{+}_{\texttt{164.512a2}} \triangleq\ & \varphi^{+}_{\texttt{164.512a1}} \wedge \\ & \textstyle\bigwedge_{i \in \texttt{164.512c}} \varphi^{-}_{i} \wedge \\ & \textstyle\bigwedge_{i \in \texttt{164.512e}} \varphi^{-}_{i} \wedge \\ & \textstyle\bigwedge_{i \in \texttt{164.512f}} \varphi^{-}_{i}\end{aligned}$$

164.512(b)

164.512(b)(1)

> *A covered entity may disclose protected health information for the public health activities and purposes described in this paragraph to:*

164.512(b)(1)(i)

> *A public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions; or, at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority;*

$$\begin{aligned}\varphi^{+}_{\texttt{164.512b1i}} \triangleq\ & \text{activerole}(p_1, \textit{covered-entity}) \wedge \\ & (\exists p_2'.\ \text{activerole}(p_2', \textit{public-health-authority}) \wedge \\ & \qquad \text{activerole}(p_2', \textit{authorized-by-law-for-purpose}(u)) \\ & \qquad ((p_2 = p_2') \vee \\ & \qquad\ (\text{activerole}(p_2, \textit{foreign-government-agency}) \wedge \\ & \qquad\quad \text{directed-disclosure}(p_2', p_1, p_2, (q,t), m')))) \wedge \\ & (t \in_{\mathcal{T}} \textit{phi}) \wedge \\ & ((u \in_{\mathcal{U}} \textit{disease-prevention-or-control}) \vee \\ & \ (u \in_{\mathcal{U}} \textit{public-health-surveillance}) \vee \\ & \ (u \in_{\mathcal{U}} \textit{public-health-investigation}) \vee \\ & \ (u \in_{\mathcal{U}} \textit{public-health-intervention}))\end{aligned}$$

164.512(b)(1)(ii)

> *A public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect;*

$$\begin{aligned}\varphi^{+}_{\texttt{164.512b1ii}} \triangleq\ & \text{activerole}(p_1, \textit{covered-entity}) \wedge \\ & (\text{activerole}(p_2, \textit{public-health-authority}) \vee\end{aligned}$$

$$\begin{aligned}
&\text{activerole}(p_2, \textit{government-authority})) \land \\
&\text{belongstorole}(p_2, \textit{authorized-by-law-for-purpose}(u)) \land \\
&(t \in_{\mathcal{T}} \textit{phi}) \land \\
&(u \in_{\mathcal{U}} \textit{reports-of-child-abuse})
\end{aligned}$$

164.512(b)(1)(iii)

> *A person subject to the jurisdiction of the Food and Drug Administration (FDA) with respect to an FDA-regulated product or activity for which that person has responsibility, for the purpose of activities related to the quality, safety or effectiveness of such FDA-regulated product or activity. Such purposes include:*
>
> *(A) To collect or report adverse events (or similar activities with respect to food or dietary supplements), product defects or problems (including problems with the use or labeling of a product), or biological product deviations;*
> *(B) To track FDA-regulated products;*
> *(C) To enable product recalls, repairs, or replacement, or lookback (including locating and notifying individuals who have received products that have been recalled, withdrawn, or are the subject of lookback); or*
> *(D) To conduct post marketing surveillance;*

$$\begin{aligned}
\varphi^{+}_{\texttt{164.512b1iii}} \triangleq\ &\text{activerole}(p_1, \textit{covered-entity}) \land \\
&\exists p{:}\mathsf{prod}.\ \text{is-FDA-regulated}(p) \land \\
&\qquad \text{activerole}(p_2, \textit{responsible-for-product}(p)) \land \\
&\qquad (t \in_{\mathcal{T}} \textit{phi}) \land \\
&\qquad (u \in_{\mathcal{U}} \textit{quality-safety-effectiveness-activities}(p))
\end{aligned}$$

Note that we use existential quantification over a new sort, prod, to link the recipient to the same product mentioned in the purpose.

164.512(b)(1)(iv)

> *A person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, if the covered entity or public health authority is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation; or*

Somewhat surprisingly, the protected health information that may be disclosed is left wholly unconstrained in this paragraph. We believe that the purpose of public health information and principle of minimum necessary disclosure will appropriately limit the protected health information that may be disclosed.

$$\begin{aligned}
\varphi^{+}_{\texttt{164.512b1iv}} \triangleq\ &\text{activerole}(p_1, \textit{covered-entity}) \land \\
&\text{belongstorole}(p_2, \textit{risk-of-contracting-or-spreading-disease}) \land \\
&(t \in_{\mathcal{T}} \textit{phi}) \land \\
&(u \in_{\mathcal{U}} \textit{notify-for-public-health-intervention})
\end{aligned}$$

164.512(b)(1)(v)

> *An employer, about an individual who is a member of the workforce of the employer, if:*
>
> *(A) The covered entity is a covered health care provider who is a member of the workforce of such employer or who provides health care to the individual at the request of the employer:*
>
> > *(1) To conduct an evaluation relating to medical surveillance of the workplace; or*
> >
> > *(2) To evaluate whether the individual has a work-related illness or injury;*
>
> *(B) The protected health information that is disclosed consists of findings concerning a work-related illness or injury or a workplace-related medical surveillance;*
>
> *(C) The employer needs such findings in order to comply with its obligations, under 29 CFR parts 1904 through 1928, 30 CFR parts 50 through 90, or under state law having a similar purpose, to record such illness or injury or to carry out responsibilities for workplace medical surveillance; and*
>
> *(D) The covered health care provider provides written notice to the individual that protected health information relating to the medical surveillance of the workplace and work-related illnesses and injuries is disclosed to the employer:*
>
> > *(1) By giving a copy of the notice to the individual at the time the health care is provided; or*
> >
> > *(2) If the health care is provided on the work site of the employer, by posting the notice in a prominent place at the location where the health care is provided.*

We have the positive norm:

$$
\begin{aligned}
\varphi^{+}_{\texttt{164.512b1v}} \triangleq\ & (\text{activerole}(p_1, \mathit{provider}) \land \\
& \ (\text{belongstorole}(p_1, \mathit{workforce\text{-}member}(p_2)) \lor \\
& \ \text{belongstorole}(p_1, \mathit{provides\text{-}medical\text{-}surveillance}(p_2)) \lor \\
& \ \text{belongstorole}(p_1, \mathit{provides\text{-}injury\text{-}evaluation}(p_2))) \land \\
& \text{activerole}(p_2, \mathit{employer}) \land \\
& \text{belongstorole}(q, \mathit{workforce\text{-}member}(p_2)) \land \\
& (((t \in_{\mathcal{T}} \mathit{workplace\text{-}injury\text{-}findings}) \land \\
& \quad (u \in_{\mathcal{U}} \mathit{obligation\text{-}to\text{-}record\text{-}workplace\text{-}injury})) \lor \\
& \ ((t \in_{\mathcal{T}} \mathit{medical\text{-}surveillance\text{-}findings}) \land \\
& \quad (u \in_{\mathcal{U}} \mathit{obligation\text{-}to\text{-}perform\text{-}medical\text{-}surveillance}))) \land \\
& \exists m'.\ \diamondminus \text{send}(p_1, q, m') \land \\
& \qquad \text{is-notice-of-workplace-disclosure}(m')
\end{aligned}
$$

Note that we have tied the attribute class *workplace-injury-findings* to the corresponding purpose *obligation-to-record-workplace-injury*. Similarly, the information type *medical-surveillance-findings* and purpose *obligation-to-perform-medical-surveillance* are tied together. Although this is not made explicit in the text, we believe that it is reasonable to assume that this was the intended meaning.

Due to our abstract send-based model, we cannot capture the distinction between giving a copy of the notice and posting the notice in a prominent public place. Therefore, we do not include paragraph (D)(2).

164.512(b)(2)

> *If the covered entity also is a public health authority, the covered entity is permitted to use protected health information in all cases in which it is permitted to disclose such information for public health activities under paragraph (b)(1) of this section.*

Because our model cannot express usage-based norms, we cannot handle this paragraph. However, given a model that supports usage-based norms, we expect that it would be straightforward to copy the norms from paragraph (b)(1) and make only slight modifications.

164.512(c)

We combine the following norms from this paragraph to form a new positive norm:

$$\begin{aligned}\varphi^{+}_{\texttt{164.512c}} \triangleq\ & \varphi^{+}_{\texttt{164.512c1}} \wedge \\ & (\varphi^{-}_{\texttt{164.512c2}} \vee \varphi^{+}_{\texttt{164.512c2i}} \vee \varphi^{+}_{\texttt{164.512c2ii}})\end{aligned}$$

Note that this construction contains a local negative norm with its own exceptions.

164.512(c)(1)

> *Except for reports of child abuse or neglect permitted by paragraph (b)(1)(ii) of this section, a covered entity may disclose protected health information about an individual whom the covered entity reasonably believes to be a victim of abuse, neglect, or domestic violence to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect, or domestic violence:*
>
> *(i) To the extent the disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of such law;*
>
> *(ii) If the individual agrees to the disclosure; or*
>
> *(iii) To the extent the disclosure is expressly authorized by statute or regulation and:*
>
> > *(A) The covered entity, in the exercise of professional judgment, believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or*
> >
> > *(B) If the individual is unable to agree because of incapacity, 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 and that 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.*

$$\begin{aligned}\varphi^{+}_{\texttt{164.512c1}} =\ & \text{activerole}(p_1, \textit{covered-entity}) \wedge \\ & \text{belongstorole}(p_2, \textit{government-authority}) \wedge \\ & \text{activerole}(p_2, \textit{authorized-by-law-for-purpose}(u)) \wedge \\ & \text{believes-victim-of-abuse}(p_1, q) \wedge \\ & (t \in_{\mathcal{T}} \textit{phi}) \wedge \\ & (u \in_{\mathcal{U}} \textit{reports-of-abuse}) \wedge \\ & (\text{is-required-by-law}(p_1, p_2, (q,t), u) \vee\end{aligned}$$

$$
\begin{array}{l}
\text{individual-has-agreed}(p_1, p_2, (q, t), u) \vee \\
(\text{authorized-by-statute-regulation}(p_1, p_2, (q, t), u) \wedge \\
\;(\text{believes-disclosure-necessary-to-prevent-harm}(p_1, p_2, (q, t), u) \vee \\
\;\;(\text{belongstorole}(q, \textit{incapacitated}) \wedge \\
\;\;\;\exists p_3.\ \text{belongstorole}(p_3, \textit{public-official}) \wedge \\
\qquad\quad \text{activerole}(p_3, \textit{authorized-for-purpose}(u)) \wedge \\
\qquad\quad \text{assurance-disclosure-not-used-against-individual}(p_3, p_1, p_2, (q, t), u) \wedge \\
\qquad\quad \text{believes-waiting-for-agreement-would-hinder-enforcement}(p_3, p_1, p_2, (q, t), u)))))
\end{array}
$$

Because there is no implementation specification for an individual's agreement, we factor this out as a new predicate, individual-has-agreed. Also, because the negative norm $\varphi^-_{\texttt{164.512c2}}$ applies *locally* to $\varphi^+_{\texttt{164.512c1}}$ (and not to $\varphi^+_{\texttt{164.512b1ii}}$), no additional work is necessary to capture the phrase "except for reports of child abuse or neglect permitted by paragraph (b)(1)(ii) of this section."

164.512(c)(2)

> *A covered entity that makes a disclosure permitted by paragraph (c)(1) of this section must promptly inform the individual that such a report has been or will be made, except if:*

We have the following negative norm. Although no definition of "promptly" is provided by the law, if we are given a promptness constant, c_{prompt}, we write:

$$
\begin{array}{l}
\varphi^-_{\texttt{164.512c2}} \triangleq {\downarrow} x. \exists m'.\ (\diamondminus \text{send}(p_1, q, m') \vee \\
\qquad\qquad\qquad\qquad \Diamond({\downarrow} y.\ (y \leq x + c_{prompt}) \wedge \\
\qquad\qquad\qquad\qquad\qquad\qquad \text{send}(p_1, q, m'))) \wedge \\
\qquad\qquad\qquad\quad \text{is-notice-of-report}(m', p_1, p_2, (q, t), u)
\end{array}
$$

164.512(c)(2)(i)

> *The covered entity, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm; or*

We have the positive norm:

$$\varphi^+_{\texttt{164.512c2i}} \triangleq \text{believes-notice-would-risk-individual}(p_1, p_2, (q, t), u)$$

Again, we rely on an oracle for the semantics of believes-notice-would-risk-individual.

164.512(c)(2)(ii)

> *The covered entity 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 as determined by the covered entity, in the exercise of professional judgment.*

It is not clear to us how to represent the necessity modality present in the phrase "[If] the covered entity *would be* informing a personal representative". We could consider adding a new modality to the logic, but it seems likely to impose more technical complications than the benefit we would gain. However, even if we considered adding a new modality, we would be breaking the abstraction of whether a message goes to an individual or the personal representative.

164.512(d)

164.512(d)(1)

> *A covered entity may disclose protected health information to a health oversight agency for oversight activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions; or other activities necessary for appropriate oversight of:*
>
> *(i) The health care system;*
> *(ii) Government benefit programs for which health information is relevant to beneficiary eligibility;*
> *(iii) Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or*
> *(iv) Entities subject to civil rights laws for which health information is necessary for determining compliance.*

We have the positive norm:

$$\begin{aligned}\varphi^{+}_{\texttt{164.512d1}} \triangleq\ & \text{activerole}(p_1, \textit{covered-entity}) \wedge \\ & \text{belongstorole}(p_2, \textit{health-oversight-agency}) \wedge \\ & \text{activerole}(p_2, \textit{authorized-by-law}(u)) \wedge \\ & (t \in_{\mathcal{T}} \textit{phi}) \wedge \\ & \exists p_3.\ (u \in_{\mathcal{U}} \textit{oversight}(p_3)) \wedge \\ & \qquad (\text{activerole}(p_3, \textit{health-care-system}) \vee \\ & \qquad\ \text{activerole}(p_3, \textit{government-benefit-programs-health-eligibility}) \vee \\ & \qquad\ \text{activerole}(p_3, \textit{government-regulated-entity-health-compliance}) \vee \\ & \qquad\ \text{activerole}(p_3, \textit{subject-to-civil-rights-health-compliance}))\end{aligned}$$

Note the use of the *authorized-by-law*(u) role, which is parameterized by the purpose u and captures the principals that are authorized by law for purpose u.

Also, paragraph (i) is unclear to us: The term "health care system" seems too generic of a term to be useful in practice. Nevertheless, we choose to formalize it using a role *health-care-system*.

164.512(d)(2)

> *For the purpose of the disclosures permitted by paragraph (d)(1) of this section, a health oversight activity does not include an investigation or other activity in which the individual is the subject of the investigation or activity and such investigation or other activity does not arise out of and is not directly related to:*
>
> *(i) The receipt of health care;*
> *(ii) A claim for public benefits related to health; or*
> *(iii) Qualification for, or receipt of, public benefits or services when a patient's health is integral to the claim for public benefits or services.*

We would like to express this paragraph as:

$$\begin{aligned}
&(u \in_{\mathcal{U}} \mathit{oversight}(q)) \supset\\
&\quad \text{related-to-receipt-health-care}(u) \lor\\
&\quad \text{related-to-public-health-benefits}(u) \lor\\
&\quad \text{related-to-public-benefits-qualification-depends-on-health}(u)
\end{aligned}$$

However, this cannot be expressed as an isolated constraint because q must refer to the individual. We resolve this problem by merging this paragraph into the norm from (d)(1):

$$\begin{aligned}
\varphi^{+}_{\texttt{164.512d1}'} \triangleq\ & \text{activerole}(p_1, \mathit{covered\text{-}entity}) \land\\
& \text{belongstorole}(p_2, \mathit{health\text{-}oversight\text{-}agency}) \land\\
& \text{activerole}(p_2, \mathit{authorized\text{-}by\text{-}law}(u)) \land\\
& (t \in_{\mathcal{T}} \mathit{phi}) \land\\
& \exists p_3.\ (u \in_{\mathcal{U}} \mathit{oversight}(p_3)) \land\\
& \qquad (\text{activerole}(p_3, \mathit{health\text{-}care\text{-}system}) \lor\\
& \qquad\ \ \text{activerole}(p_3, \mathit{government\text{-}benefit\text{-}programs\text{-}health\text{-}eligibility}) \lor\\
& \qquad\ \ \text{activerole}(p_3, \mathit{government\text{-}regulated\text{-}entity\text{-}health\text{-}compliance}) \lor\\
& \qquad\ \ \text{activerole}(p_3, \mathit{subject\text{-}to\text{-}civil\text{-}rights\text{-}health\text{-}compliance})) \land\\
& \qquad ((p_3 = q) \supset\\
& \qquad\quad \text{related-to-receipt-health-care}(u) \lor\\
& \qquad\quad \text{related-to-public-health-benefits}(u) \lor\\
& \qquad\quad \text{related-to-public-benefits-qualification-depends-on-health}(u))
\end{aligned}$$

Admittedly, this weakens the correspondence with the text's structure, but that seems unavoidable.

164.512 (d)(3)

> *Notwithstanding paragraph (d)(2) of this section, if a health oversight activity or investigation is conducted in conjunction with an oversight activity or investigation relating to a claim for public benefits not related to health, the joint activity or investigation is considered a health oversight activity for purposes of paragraph (d) of this section.*

Again, it seems necessary to merge this paragraph into the norm for paragraph (d)(1):

$$\begin{aligned}
\varphi^{+}_{\texttt{164.512d}''} \triangleq\ & \text{activerole}(p_1, \mathit{covered\text{-}entity}) \land\\
& \text{belongstorole}(p_2, \mathit{health\text{-}oversight\text{-}agency}) \land\\
& \text{activerole}(p_2, \mathit{authorized\text{-}by\text{-}law}(u)) \land\\
& (t \in_{\mathcal{T}} \mathit{phi}) \land\\
& \exists p_3.\ (u \in_{\mathcal{U}} \mathit{oversight}(p_3)) \land\\
& \qquad (\text{activerole}(p_3, \mathit{health\text{-}care\text{-}system}) \lor\\
& \qquad\ \ \text{activerole}(p_3, \mathit{government\text{-}benefit\text{-}programs\text{-}health\text{-}eligibility}) \lor\\
& \qquad\ \ \text{activerole}(p_3, \mathit{government\text{-}regulated\text{-}entity\text{-}health\text{-}compliance}) \lor\\
& \qquad\ \ \text{activerole}(p_3, \mathit{subject\text{-}to\text{-}civil\text{-}rights\text{-}health\text{-}compliance})) \land\\
& \qquad ((p_3 = q) \supset\\
& \qquad\quad \exists u'.\ (\text{related-to-receipt-health-care}(u') \lor\\
& \qquad\qquad\quad \text{related-to-public-health-benefits}(u') \lor\\
& \qquad\qquad\quad \text{related-to-public-benefits-qualification-depends-on-health}(u')) \land\\
& \qquad\qquad\ ((u' = u) \lor\\
& \qquad\qquad\quad \text{joint-oversight}(u, u')))
\end{aligned}$$

164.512(d)(4)

> *If a covered entity also is a health oversight agency, the covered entity may use protected health information for health oversight activities as permitted by paragraph (d) of this section.*

Again, because our model does not support usage-based norms, we cannot handle this paragraph. However, we expect that, in such a model, it would be straightforward to modify the norms from paragraph (d) to apply to uses.

164.512(e)

164.512(e)(1)

> *A covered entity may disclose protected health information in the course of any judicial or administrative proceeding:*

164.512(e)(1)(i)

> *In response to an order of a court or administrative tribunal, provided that the covered entity discloses only the protected health information expressly authorized by such order; or*

$$
\begin{aligned}
\varphi^{+}_{\texttt{164.512e1i}} \triangleq\ & \text{activerole}(p_1, \textit{covered-entity}) \land \\
& (t \in_{\mathcal{T}} \textit{phi}) \land \\
& (u \in_{\mathcal{U}} \textit{judicial-administrative-proceeding}) \land \\
& \exists p_3, m'.\ (\text{activerole}(p_3, \textit{court}) \lor \\
& \qquad\quad \text{activerole}(p_3, \textit{administrative-tribunal})) \land \\
& \qquad\ \diamondminus \text{send}(p_3, p_1, m') \land \\
& \qquad\ \text{is-order}(m', p_1, p_2, (q, t))
\end{aligned}
$$

We rely on an oracle for the semantics of in-order.

164.512(e)(1)(ii)

> *In response to a subpoena, discovery request, or other lawful process, that is not accompanied by an order of a court or administrative tribunal, if:*
>
> *(A) The covered entity receives satisfactory assurance, as described in para. (e)(1)(iii) of this section, from the party seeking the information that reasonable efforts have been made by such party to ensure that the individual who is the subject of the protected health information that has been requested has been given notice of the request; or*
>
> *(B) The covered entity receives satisfactory assurance, as described in para. (e)(1)(iv) of this section, from the party seeking the information that reasonable efforts have been made by such party to secure a qualified protective order that meets the requirements of paragraph (e)(1)(v) of this section.*

We have the positive norm:

$$\begin{aligned}\varphi^{+}_{\texttt{164.512e1ii}} \triangleq\ & \text{activerole}(p_1, \textit{covered-entity}) \wedge \\ & (t \in_{\mathcal{T}} \textit{phi}) \wedge \\ & (u \in_{\mathcal{U}} \textit{judicial-administrative-proceeding}) \wedge \\ & \exists m'.\ \diamondminus \text{send}(p_2, p_1, m') \wedge \\ & \qquad \text{is-lawful-process}(m', p_1, p_2, (q, t)) \wedge \\ & \qquad (\text{received-satisfactory-assurances-164.512e1iii}(p_1, p_2, (q, t), u) \vee \\ & \qquad\ \ \text{received-satisfactory-assurances-164.512e1iv}(p_1, p_2, (q, t), u))\end{aligned}$$

We rely on an oracle for the semantics of is-lawful-process. The macros for receiving satisfactory assurances are defined in the following paragraphs.

164.512(e)(1)(iii)

> *For the purposes of paragraph (e)(1)(ii)(A) of this section, a covered entity receives satisfactory assurances from a party seeking protecting health information if the covered entity receives from such party a written statement and accompanying documentation demonstrating that:*
>
> *(A) The party requesting such information has made a good faith attempt to provide written notice to the individual (or, if the individual's location is unknown, to mail a notice to the individual's last known address);*
>
> *(B) The notice included sufficient information about the litigation or proceeding in which the protected health information is requested to permit the individual to raise an objection to the court or administrative tribunal; and*
>
> *(C) The time for the individual to raise objections to the court or administrative tribunal has elapsed, and:*
>
> *(1) No objections were filed; or*
>
> *(2) All objections filed by the individual have been resolved by the court or the administrative tribunal and the disclosures being sought are consistent with such resolution.*

$$\begin{aligned}& \text{received-satisfactory-assurances-164.512e1iii}(p_1, p_2, (q, t), u) \triangleq \\ & \quad \exists m'.\ \diamondminus \text{send}(p_2, p_1, m') \wedge \\ & \qquad \text{contains-evidence-of-attempt-to-sufficiently-notify}(m', p_1, p_2, (q, t), u) \wedge \\ & \qquad \text{contains-evidence-of-objection-time-elapsed}(m', p_1, p_2, (q, t), u) \wedge \\ & \qquad (\text{contains-evidence-of-no-objections}(m', p_1, p_2, (q, t), u) \vee \\ & \qquad\ \ \text{contains-evidence-of-all-objections-resolved}(m', p_1, p_2, (q, t), u))\end{aligned}$$

We revive the use of special purpose contains-... predicates. Our generic contains predicate requires that the attribute be given with respect to a particular subject principal. This is not the case here.

164.512(e)(1)(iv)

> *For the purposes of paragraph (e)(1)(ii)(B) of this section, a covered entity receives satisfactory assurances from a party seeking protected health information, if the covered entity receives from such party a written statement and accompanying documentation demonstrating that:*

> *(A) The parties to the dispute giving rise to the request for information have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or*
>
> *(B) The party seeking the protected health information has requested a qualified protective order from such court or administrative tribunal.*

$$\begin{aligned}
&\text{received-satisfactory-assurances-164.512e1iv}(p_1, p_2, (q,t), u) \triangleq \\
&\quad \exists m'.\ \diamondminus \text{send}(p_2, p_1, m') \wedge \\
&\qquad (\text{contains-evidence-of-parties-agreed-to-protective-order}(m', p_1, p_2, (q,t), u) \vee \\
&\qquad\ \text{contains-evidence-of-request-for-protective-order}(m', p_1, p_2, (q,t), u))
\end{aligned}$$

Again, we rely solely on predicates because the requirement is for evidence of a qualified protective order, not the actual order itself. We assume that the legal proceeding purpose u captures all of the information regarding parties in the dispute and the relevant court.

164.512(e)(1)(v)

> *For purposes of paragraph (e)(1) of this section, a qualified protective order means, with respect to protected health information requested under paragraph (e)(1)(ii) of this section, an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that:*
>
> *(A) Prohibits the parties from using or disclosing the protected health information for any purpose other than the litigation or proceeding for which such information was requested; and*
>
> *(B) Requires the return to the covered entity or destruction of the protected health information (including all copies made) at the end of the litigation or proceeding.*

By relying on predicates to check the *evidence* of a protective order, and not the existence of the protective order itself, this paragraph seems unnecessary.

164.512(e)(1)(vi)

> *Notwithstanding paragraph (e)(1)(ii) of this section, a covered entity may disclose protected health information in response to lawful process described in paragraph (e)(1)(ii) of this section without receiving satisfactory assurance under paragraph (e)(1)(ii)(A) or (B) of this section, if the covered entity makes reasonable efforts to provide notice to the individual sufficient to meet the requirements of paragraph (e)(1)(iii) of this section or to seek a qualified protective order sufficient to meet the requirements of paragraph (e)(1)(iv) of this section.*

$$\begin{aligned}
\varphi^{+}_{\texttt{164.512e1vi}} \triangleq\ & \text{activerole}(p_1, \textit{covered-entity}) \wedge \\
& (t \in_{\mathcal{T}} \textit{phi}) \wedge \\
& (u \in_{\mathcal{U}} \textit{judicial-administrative-proceeding}) \wedge \\
& \exists m'.\ \diamondminus \text{send}(p_2, p_1, m') \wedge \\
& \qquad \text{is-lawful-process}(m', p_1, p_2, (q,t), u) \wedge \\
& \qquad \text{made-reasonable-effort-to-notify}(p_1, p_2, (q,t), u)
\end{aligned}$$

164.512(e)(2)

> *The provisions of this paragraph do not supersede other provisions of this section that otherwise permit or restrict uses or disclosures of protected health information.*

In our opinion, this paragraph simply requires that all negative norms in this section apply to the positive norms from paragraph (e). This will automatically be the case due to our top-level formula and the fact that the positive norms of paragraph (e) will be injected there.

164.512(f)

> *A covered entity may disclose protected health information for a law enforcement purpose to a law enforcement official if the conditions in paragraphs (f)(1) through (f)(6) of this section are met, as applicable.*

This paragraph serves to factor out the constraint that paragraphs (f)(1)–(6) apply to disclosures for law enforcement purposes to a law enforcement official. Our norms in the following paragraphs take this into account.

164.512(f)(1)

> *A covered entity may disclose protected health information:*

164.512(f)(1)(i)

> *As required by law including laws that require the reporting of certain types of wounds or other physical injuries, except for laws subject to paragraph (b)(1)(ii) or (c)(1)(i) of this section; or*

$$\begin{aligned}\varphi^{+}_{\texttt{164.512f1i}} \triangleq\ & \text{activerole}(p_1, \textit{covered-entity}) \land \\ & \text{activerole}(p_2, \textit{law-enforcement-official}) \land \\ & (t \in_{\mathcal{T}} \textit{phi}) \land \\ & (u \in_{\mathcal{U}} \textit{law-enforcement}) \land \\ & \text{required-by-law}(p_1, p_2, (q, t), u) \land \\ & \neg\varphi^{+}_{\texttt{164.512b1ii}} \land \\ & \neg\varphi^{+}_{\texttt{164.512c1i}}\end{aligned}$$

164.512(f)(1)(ii)

> *In compliance with and as limited by the relevant requirements of:*
>
> *(A) A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer;*
>
> *(B) A grand jury subpoena; or*
>
> *(C) An administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, provided that:*
>
> *(1) The information sought is relevant and material to a legitimate law enforcement inquiry;*

(2) The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and

(3) De-identified information could not reasonably be used.

$$\begin{aligned}\varphi^{+}_{\texttt{164.512f1ii}} \triangleq\ & \text{activerole}(p_1, \textit{covered-entity}) \land \\ & \text{activerole}(p_2, \textit{law-enforcement-official}) \land \\ & (t \in_{\mathcal{T}} \textit{phi}) \land \\ & (u \in_{\mathcal{U}} \textit{law-enforcement}) \land \\ & (\text{in-compliance-with-court-order}(p_1, p_2, (q,t), u) \lor \\ & \ \text{in-compliance-with-grand-jury-subpoena}(p_1, p_2, (q,t), u) \lor \\ & \ (\text{in-compliance-with-administrative-request}(p_1, p_2, (q,t), u) \land \\ & \ \ \text{minimum-necessary}(p_1, p_2, m, u) \land \\ & \ \ \text{deidentified-information-not-sufficient}(u)))\end{aligned}$$

It seems that paragraph (f)(1)(ii)(C)(1) is redundant since the opening of paragraph (f) explicitly states that the disclosure must be for a law enforcement purpose.

164.512(f)(2)

Except for disclosures required by law as permitted by paragraph (f)(1) of this section, a covered entity may disclose protected health information in response to a law enforcement official's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, provided that:

(i) 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.

(ii) Except as permitted by paragraph (f)(2)(i) of this section, the covered entity may not disclose for the purposes of identification or location under paragraph (f)(2) of this section any protected health information related to the individual's DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue.

We have the following positive norm:

$$\begin{aligned}\varphi^{+}_{\texttt{164.512f2}} \triangleq\ & \text{activerole}(p_1, \textit{covered-entity}) \land \\ & \text{activerole}(p_2, \textit{law-enforcement-official}) \land \\ & ((t \in_{\mathcal{T}} \textit{name-and-address}) \lor \\ & \ (t \in_{\mathcal{T}} \textit{date-and-place-of-birth}) \lor\end{aligned}$$

$$
\begin{aligned}
&\quad (t \in_{\mathcal{T}} \textit{social-security-number}) \lor \\
&\quad (t \in_{\mathcal{T}} \textit{ABO-blood-type-and-rh-factor}) \lor \\
&\quad (t \in_{\mathcal{T}} \textit{type-of-injury}) \lor \\
&\quad (t \in_{\mathcal{T}} \textit{date-and-time-of-treatment}) \lor \\
&\quad (t \in_{\mathcal{T}} \textit{date-and-time-of-death}) \lor \\
&\quad (t \in_{\mathcal{T}} \textit{distinguishing-physical-characteristics})) \land \\
&(u \in_{\mathcal{U}} \textit{law-enforcement-relevant-identification-or-location}(q)) \land \\
&(\exists m'.\ \diamondminus \mathrm{send}(p_2, p_1, m') \land \\
&\qquad \text{is-request-for}(m', p_1, p_2, (q, t), u))
\end{aligned}
$$

Since paragraph (f)(2)(i) does not mention DNA information, we believe that the "exception" given in paragraph (f)(2)(ii) is simply a statement of intent that serves to underscore the fact that DNA information is not mentioned in (f)(2)(i). As a result, we include no logical mention of DNA information.

We also do not understand the need for the "except for disclosures required by law as permitted by paragraph (f)(1)" exception. However, because this paragraph introduces no negative norms, the disjunctive character of positive norms will do the correct thing: these categories would only apply in $\varphi^{+}_{\texttt{164.512f2}}$. It seems that the authors of HIPAA may be confusing "if" with "only if".

164.512(f)(3)

> *Except for disclosures required by law as permitted by paragraph (f)(1) of this section, a covered entity may disclose protected health information in response to a law enforcement official'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 paragraph (b) or (c) of this section, if:*

Note that we will not need to handle the phrase "other than disclosures that are subject to paragraph (b) or (c) of this section". Even though this paragraph requires things (essentially agreement) beyond (b) and (c), these additional requirements need not occur for disclosures that fit (b) or (c): by their disjunctive nature, only one positive norm needs to be satisfied. Satisfying only paragraph (b) is enough, for example. This is similar to our previous comment.

164.512(f)(3)(i)

> *The individual agrees to the disclosure; or*

$$
\begin{aligned}
\varphi^{+}_{\texttt{164.512f3i}} \triangleq\ & \mathrm{activerole}(p_1, \textit{covered-entity}) \land \\
& \mathrm{activerole}(p_2, \textit{law-enforcement-official}) \land \\
& (\mathrm{belongstorole}(q, \textit{victim-of-crime}) \lor \\
& \ \mathrm{belongstorole}(q, \textit{suspected-victim-of-crime})) \land \\
& (t \in_{\mathcal{T}} \textit{phi}) \land \\
& (u \in_{\mathcal{U}} \textit{law-enforcement}) \land \\
& (\exists m'.\ \diamondminus \mathrm{send}(p_2, p_1, m') \land \\
& \qquad \text{is-request-for}(m', p_1, p_2, (q, t), u)) \land \\
& (\exists m''.\ \diamondminus \mathrm{send}(q, p_1, m'') \land \\
& \qquad \text{is-agreement-to}(m'', p_1, p_2, (q, t), u))
\end{aligned}
$$

164.512(f)(3)(ii)

> *The covered entity is unable to obtain the individual's agreement because of incapacity or other emergency circumstance, provided that:*
>
> *(A) 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;*
>
> *(B) The law enforcement official represents that immediate law 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; and*
>
> *(C) The disclosure is in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment.*

$$
\begin{aligned}
\varphi^{+}_{\texttt{164.512f3ii}} \triangleq\ & \text{activerole}(p_1, \textit{covered-entity}) \land \\
& \text{activerole}(p_2, \textit{law-enforcement-official}) \land \\
& (\text{belongstorole}(q, \textit{victim-of-crime}) \lor \\
& \ \ \text{belongstorole}(q, \textit{suspected-victim-of-crime})) \land \\
& (t \in_{\mathcal{T}} \textit{phi}) \land \\
& (u \in_{\mathcal{U}} \textit{law-enforcement}) \land \\
& (\exists m'.\ \diamondminus \text{send}(p_2, p_1, m') \land \\
& \qquad \text{is-request-for}(m', p_1, p_2, (q, t), u)) \land \\
& \text{belongstorole}(q, \textit{emergency-circumstance}) \land \\
& \text{represents-needed-to-determine-crime}(p_2, p_1, p_2, (q, t), u) \land \\
& \text{represents-not-used-against-victim}(p_2, p_1, p_2, (q, t), u) \land \\
& \text{represents-activity-adversely-affected-by-wait}(p_2, p_1, p_2, (q, t), u) \land \\
& \text{believes-in-best-interest}(p_1, p_1, p_2, (q, t), u)
\end{aligned}
$$

Again, the represents-... predicates and the believes-in-best-interest predicate rely on oracles for their semantics.

164.512(f)(4)

> *A covered entity may disclose protected health information about an individual who has died to a law enforcement official for the purpose of alerting law enforcement of the death of the individual if the covered entity has a suspicion that such death may have resulted from criminal conduct.*

$$
\begin{aligned}
\varphi^{+}_{\texttt{164.512f4}} \triangleq\ & \text{activerole}(p_1, \textit{covered-entity}) \land \\
& \text{activerole}(p_2, \textit{law-enforcement-official}) \land \\
& \text{belongstorole}(q, \textit{deceased}) \land \\
& (t \in_{\mathcal{T}} \textit{phi}) \land \\
& (u \in_{\mathcal{U}} \textit{suspicious-death-notification}(q)) \land \\
& \text{believes-death-may-be-result-of-crime}(p_1, q)
\end{aligned}
$$

The believes-death-may-be-result-of-crime predicate also uses an oracle for its semantics.

164.512(f)(5)

> *A covered entity may disclose to a law enforcement official protected health information that the covered entity believes in good faith constitutes evidence of criminal conduct that occurred on the premises of the covered entity.*

$$\begin{aligned}\varphi^{+}_{\texttt{164.512(f)(5)}} \triangleq\ & \text{activerole}(p_1, \textit{covered-entity}) \wedge \\ & \text{activerole}(p_2, \textit{law-enforcement-official}) \wedge \\ & (t \in_{\mathcal{T}} \textit{phi}) \wedge \\ & (u \in_{\mathcal{U}} \textit{report-possible-crime-on-premises}(p_1)) \wedge \\ & \text{believes-evidence-of-crime-on-premises}(p_1, (q, t))\end{aligned}$$

164.512(f)(6)

Since §164.512(f)(6)(ii) constitutes a local negative norm on §164.512(f)(6)(i), the norms are joined with conjunction, forming a new positive norm:

$$\varphi^{+}_{\texttt{164.512f6}} \triangleq \varphi^{+}_{\texttt{164.512f6i}} \wedge \varphi^{-}_{\texttt{164.512f6ii}}$$

164.512(f)(6)(i)

> *A covered health care provider providing emergency health care in response to a medical emergency, other than such emergency on the premises of the covered health care provider, may disclose protected health information to a law enforcement official if such disclosure appears necessary to alert law enforcement to:*
>
> *(A) The commission and nature of a crime;*
> *(B) The location of such crime or of the victim(s) of such crime; and*
> *(C) The identity, description, and location of the perpetrator of such crime.*

$$\begin{aligned}\varphi^{+}_{\texttt{164.512f6i}} \triangleq\ & \text{activerole}(p_1, \textit{provider}) \wedge \\ & \text{activerole}(p_2, \textit{law-enforcement-official}) \wedge \\ & (t \in_{\mathcal{T}} \textit{phi}) \wedge \\ & (u \in_{\mathcal{U}} \textit{alert-of-crime-commission-location-victims-perpetrator}) \wedge \\ & \text{providing-emergency-healthcare}(p_1, q) \wedge \\ & \text{appears-necessary-to-alert-of-crime-commission-location-victims-perpetrator}(p_1, p_2, (q, t), u)\end{aligned}$$

164.512(f)(6)(ii)

> *If a covered health care provider believes that the medical emergency described in paragraph (f)(6)(i) of this section is the result of abuse, neglect, or domestic violence of the individual in need of emergency health care, paragraph (f)(6)(i) of this section does not apply and any disclosure to a law enforcement official for law enforcement purposes is subject to paragraph (c) of this section.*

$$\varphi^{-}_{\texttt{164.512f6ii}} \triangleq \neg\text{believes-emergency-result-of-abuse-neglect-domestic-violence}(p_1, q)$$

Note that we have changed "a covered healthcare provider" to refer to *the* covered healthcare provider of the potential disclosure. We believe that this is the intended or implied meaning.

164.512(g)

164.512(g)(1)

> *A covered entity may disclose protected health information to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law. A covered entity that also performs the duties of a coroner or medical examiner may use protected health information for the purposes described in this paragraph.*

$$
\begin{aligned}
\varphi^{+}_{\texttt{164.512g1}} \triangleq\ & \text{activerole}(p_1, \mathit{covered\text{-}entity}) \land \\
& (\text{activerole}(p_2, \mathit{coroner}) \lor \\
& \ \text{activerole}(p_2, \mathit{medical\text{-}examiner})) \land \\
& \text{belongstorole}(q, \mathit{deceased}) \land \\
& (t \in_{\mathcal{T}} \mathit{phi}) \land \\
& ((u \in_{\mathcal{U}} \mathit{identification}(q)) \lor \\
& \ (u \in_{\mathcal{U}} \mathit{determining\text{-}cause\text{-}of\text{-}death}(q)) \lor \\
& \ \text{authorized-by-law}(p_2, u))
\end{aligned}
$$

We have taken the liberty of parameterizing the identification and cause of death purposes by the deceased individual q to more tightly reflect what we believe to be the intended meaning.

164.512(g)(2)

> *A covered entity may disclose protected health information to funeral directors, consistent with applicable law, as necessary to carry out their duties with respect to the decedent. If necessary for funeral directors to carry out their duties, the covered entity may disclose the protected health information prior to, and in reasonable anticipation of, the individual's death.*

$$
\begin{aligned}
\varphi^{+}_{\texttt{164.512g2}} \triangleq\ & \text{activerole}(p_1, \mathit{covered\text{-}entity}) \land \\
& \text{activerole}(p_2, \mathit{funeral\text{-}director}) \land \\
& (\text{belongstorole}(q, \mathit{deceased}) \lor \\
& \ (\Diamond(\downarrow y.\ (x \geq y - c) \land \\
& \qquad\qquad \text{belongstorole}(q, \mathit{deceased})) \land \\
& \quad \text{early-disclosure-necessary}(p_1, p_2, (q, t), u))) \land \\
& (t \in_{\mathcal{T}} \mathit{phi}) \land \\
& (u \in_{\mathcal{U}} \mathit{funeral\text{-}director\text{-}duties}(q)) \land \\
& \text{necessary-for-duties}(p_1, p_2, (q, t), u)
\end{aligned}
$$

Note that we use the $\Diamond$ operator to formalize disclosure prior to death, where c stands for a reasonable interval of time.

164.512(h)

> *A covered entity may use or disclose protected health information to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye or tissue donation and transplantation.*

$$\begin{aligned}\varphi^{+}_{\texttt{164.512h}} \triangleq\ & \text{activerole}(p_1, \textit{covered-entity}) \land \\ & (\text{activerole}(p_2, \textit{organ-procurement-organization}) \lor \\ & \ \text{activerole}(p_2, \textit{engaged-in-procurement-banking-transplantation-of-organs-eyes-tissue})) \land \\ & (t \in_{\mathcal{T}} \textit{phi}) \land \\ & (u \in_{\mathcal{U}} \textit{facilitate-organ-eye-tissue-donation-transplantation})\end{aligned}$$

Note that, in accordance with a literal reading of this paragraph, this norm allows arbitrary protected health information of any individual to be disclosed to transplant organizations. In our interpretation, the principle of minimum necessary disclosure for the purpose of facilitating organ donation and transplantation will appropriately constrain the particular classes of information that may be disclosed.

164.512(i)

164.512(i)(1)

> *A covered entity may use or disclose protected health information for research, regardless of the source of funding of the research, provided that:*
>
> *(i)* Board approval of a waiver of authorization. *The covered entity obtains documentation that an alteration to or waiver, in whole or in part, of the individual authorization required by §164.508 for use or disclosure of protected health information has been approved by either:*
>
> *(A) An Institutional Review Board (IRB), established in accordance with 7 CFR lc.107, 10 CFR 745.107, 14 CFR 1230.107, 15 CFR 27.107, 16 CFR 1028.107, 21 CFR 56.107, 22 CFR 225.107, 24 CFR 60.107, 28 CFR 46.107, 32 CFR 219.107, 34 CFR 97.107, 38 CFR 16.107, 40 CFR 26.107, 45 CFR 46.107, 45 CFR 690.107, or 49 CFR 11.107; or*
>
> *(B) A privacy board that:*
>
> *(1) Has members with varying backgrounds and appropriate professional competency as necessary to review the effect of the research protocol on the individual's privacy rights and related interests;*
>
> *(2) Includes at least one member who is not affiliated with the covered entity, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with any of such entities; and*
>
> *(3) Does not have any member participating in a review of any project in which the member has a conflict of interest.*
>
> *(ii)* Reviews preparatory to research. *The covered entity obtains from the researcher representations that:*
>
> *(A) Use or disclosure is sought solely to review protected health information as necessary to prepare a research protocol or for similar purposes preparatory to research;*
>
> *(B) No protected health information is to be removed from the covered entity by the researcher in the course of the review; and*
>
> *(C) The protected health information for which use or access is sought is necessary for the research purposes.*
>
> *(iii)* Research on decedent's information. *The covered entity obtains from the researcher:*

(A) Representation that the use or disclosure sought is solely for research on the protected health information of decedents;

(B) Documentation, at the request of the covered entity, of the death of such individuals; and

(C) Representation that the protected health information for which use or disclosure is sought is necessary for the research purposes.

We have the positive norm:

$$
\begin{aligned}
\varphi^{+}_{\texttt{164.512i1}} \triangleq\ & \text{activerole}(p_1, \textit{covered-entity}) \wedge \\
& \text{activerole}(p_2, \textit{researcher}) \wedge \\
& \text{belongstorole}(q, \textit{deceased}) \wedge \\
& (t \in_{\mathcal{T}} \textit{phi}) \wedge \\
& (u \in_{\mathcal{U}} \textit{research}) \wedge \\
& (\exists p_3, m'.\ (\text{activerole}(p_3, \textit{institutional-review-board}(p_1)) \vee \\
& \qquad\qquad \text{activerole}(p_3, \textit{privacy-board}(p_1, p_2, (q,t), u))) \wedge \\
& \qquad\qquad \diamondminus \text{send}(p_3, p_1, m') \wedge \\
& \qquad\qquad \text{is-approval-of-authorization-waiver}(m', p_3, p_1, p_2, (q,t), u)) \wedge \\
& \text{represents-disclosure-solely-for-research-preparation}(p_2, p_1, p_2, (q,t), u) \wedge \\
& \text{represents-no-information-removed-during-review}(p_2, p_1, p_2, (q,t), u) \wedge \\
& \text{represents-information-necessary-for-research}(p_2, p_1, p_2, (q,t), u) \wedge \\
& \text{represents-disclosure-solely-for-decedent-research}(p_2, p_1, p_2, (q,t), u) \wedge \\
& \text{represents-disclosure-necessary-for-research}(p_2, p_1, p_2, (q,t), u)
\end{aligned}
$$

and the constraint:

$$
\begin{aligned}
& \text{activerole}(p_3, \textit{privacy-board}(p_1, p_2, (q,t), u)) \Rightarrow \\
& \quad \text{is-varied-and-competent-to-review-research-effect-on-privacy}(p_3, p_1, p_2, (q,t), u) \wedge \\
& \quad \text{at-least-one-member-not-affiliated-covered-entity-or-sponsor}(p_3, p_1, p_2, (q,t), u) \wedge \\
& \quad \text{has-no-conflict-of-interest}(p_3, p_1, p_2, (q,t), u)
\end{aligned}
$$

Note that we leave the *institutional-review-board* role unconstrained since it will be defined by the other relevant laws. We also have constrained *privacy-board* as in paragraph (i)(B). Finally, the represents-... predicates rely on oracles to give their semantics.

164.512(i)(2)

For a use or disclosure to be permitted based on documentation of approval of an alteration or waiver, under paragraph (i)(1)(i) of this section, the documentation must include all of the following:

We have the following macro which describes the conditions under which a message is a valid approval of a waiver of authorization:

$$
\begin{aligned}
& \text{is-approval-of-authorization-waiver}(m', p_3, p_1, p_2, (q,t), u) \triangleq \\
& \quad \text{is-approval-of-authorization-waiver-164.512i2i}(m', p_3, p_1, p_2, (q,t), u) \wedge \\
& \quad \text{is-approval-of-authorization-waiver-164.512i2ii}(m', p_3, p_1, p_2, (q,t), u) \wedge \\
& \quad \text{is-approval-of-authorization-waiver-164.512i2iii}(m', p_3, p_1, p_2, (q,t), u) \wedge \\
& \quad \text{is-approval-of-authorization-waiver-164.512i2iv}(m', p_3, p_1, p_2, (q,t), u) \wedge \\
& \quad \text{is-approval-of-authorization-waiver-164.512i2v}(m', p_3, p_1, p_2, (q,t), u)
\end{aligned}
$$

164.512(i)(2)(i)

> Identification and date of action. *A statement identifying the IRB or privacy board and the date on which the alteration or waiver of authorization was approved;*

We have another macro:

$$\begin{aligned}&\text{is-approval-of-authorization-waiver-164.512i2i}(m', p_3, p_1, p_2, (q,t), u) \triangleq\\&\quad \text{contains-statement-identifying-privacy-board}(m', p_3) \land\\&\quad \exists\tau{:}\mathsf{time}.\ \text{contains-date-of-approval}(m', \tau)\end{aligned}$$

164.512(i)(2)(ii)

> Waiver criteria. *A statement that the IRB or privacy board has determined that the alteration or waiver, in whole or in part, of authorization satisfies the following criteria:*
>
> *(A) The use or disclosure of protected health information involves no more than a minimal risk to the privacy of individuals, based on, at least, the presence of the following elements:*
>
> *(1) An adequate plan to protect the identifiers from improper use and disclosure;*
>
> *(2) An adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and*
>
> *(3) Adequate written assurances that the protected health information will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of protected health information would be permitted by this subpart;*
>
> *(B) The research could not practicably be conducted without the waiver or alteration; and*
>
> *(C) The research could not practicably be conducted without access to and use of the protected health information.*

And another macro:

$$\begin{aligned}&\text{is-approval-of-authorization-waiver-164.512i2ii}(m', p_3, p_1, p_2, (q,t), u) \triangleq\\&\quad \text{contains-statement-of-minimal-risk}(m', p_3, p_1, p_2, (q,t), u) \land\\&\quad \text{contains-statement-of-protection-plan-is-adequate}(m', p_3, p_1, p_2, (q,t), u) \land\\&\quad \text{contains-statement-of-destruction-plan-is-adequate}(m', p_3, p_1, p_2, (q,t), u) \land\\&\quad \text{contains-statement-of-assurances-of-no-redisclosure-are-adequate}(m', p_3, p_1, p_2, (q,t), u) \land\\&\quad \text{contains-statement-of-waiver-is-necessary}(m', p_3, p_1, p_2, (q,t), u) \land\\&\quad \text{contains-statement-of-phi-is-necessary}(m', p_3, p_1, p_2, (q,t), u)\end{aligned}$$

164.512(i)(2)(iii)

> Protected health information needed. *A brief description of the protected health information for which use or access has been determined to be necessary by the IRB or privacy board has determined, pursuant to paragraph (i)(2)(ii)(C) of this section;*

$$\begin{aligned}&\text{is-approval-of-authorization-waiver-164.512i2iii}(m', p_3, p_1, p_2, (q,t), u) \triangleq\\&\quad \text{contains-description-of-phi-necessary}(m', (q,t))\end{aligned}$$

164.512(i)(2)(iv)

Review and approval procedures. *A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures, as follows:*

(A) An IRB must follow the requirements of the Common Rule, including the normal review procedures (7 CFR 1c.108(b), 10 CFR 745.108(b), 14 CFR 1230.108(b), 15 CFR 27.108(b), 16 CFR 1028.108(b), 21 CFR 56.108(b), 22 CFR 225.108(b), 24 CFR 60.108(b), 28 CFR 46.108(b), 32 CFR 219.108(b), 34 CFR 97.108(b), 38 CFR 16.108(b), 40 CFR 26.108(b), 45 CFR 46.108(b), 45 CFR 690.108(b), or 49 CFR 11.108(b)) or the expedited review procedures (7 CFR 1c.110, 10 CFR 745.110, 14 CFR 1230.110, 15 CFR 27.110, 16 CFR 1028.110, 21 CFR 56.110, 22 CFR 225.110, 24 CFR 60.110, 28 CFR 46.110, 32 CFR 219.110, 34 CFR 97.110, 38 CFR 16.110, 40 CFR 26.110, 45 CFR 46.110, 45 CFR 690.110, or 49 CFR 11.110);

(B) A privacy board must review the proposed research at convened meetings at which a majority of the privacy board members are present, including at least one member who satisfies the criterion stated in paragraph (i)(1)(i)(B)(2) of this section, and the alteration or waiver of authorization must be approved by the majority of the privacy board members present at the meeting, unless the privacy board elects to use an expedited review procedure in accordance with paragraph (i)(2)(iv)(C) of this section;

(C) A privacy board may use an expedited review procedure if the research involves no more than minimal risk to the privacy of the individuals who are the subject of the protected health information for which use or disclosure is being sought. If the privacy board elects to use an expedited review procedure, the review and approval of the alteration or waiver of authorization may be carried out by the chair of the privacy board, or by one or more members of the privacy board as designated by the chair; and

$$
\begin{aligned}
&\text{is-approval-of-authorization-waiver-164.512i2iv}(m', p_3, p_1, p_2, (q,t), u) \triangleq \\
&\quad \text{contains-statement-of-review-and-approval-under-...}(m', p_3, p_1, p_2, (q,t), u) \land \\
&\quad (\text{contains-statement-of-adherence-to-regular-review}(m', p_3, p_1, p_2, (q,t), u) \lor \\
&\quad\ \text{contains-statement-of-adherence-to-expedited-review}(m', p_3, p_1, p_2, (q,t), u))
\end{aligned}
$$

164.512(i)(2)(v)

Required signature. *The documentation of the alteration or waiver of authorization must be signed by the chair or other member, as designated by the chair, of the IRB or the privacy board, as applicable.*

$$
\begin{aligned}
&\text{is-approval-of-authorization-waiver-164.512i2v}(m', p_3, p_1, p_2, (q,t), u) \triangleq \\
&\quad \text{contains-signature}(m', p_3)
\end{aligned}
$$

164.512(j)

164.512(j)(1)

> *A covered entity may, consistent with applicable law and standards of ethical conduct, use or disclose protected health information, if the covered entity, in good faith, believes the use or disclosure:*

164.512(j)(1)(i)

> *(A) Is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; and*
>
> *(B) Is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat; or*

$$\begin{aligned}
\varphi^{+}_{\texttt{164.512j1i}} \triangleq\ & \text{activerole}(p_1, \textit{covered-entity}) \wedge \\
& (t \in_{\mathcal{T}} \textit{phi}) \wedge \\
& (u \in_{\mathcal{U}} \textit{lessen-health-threat}) \wedge \\
& \text{consistent-with-applicable-law}(p_1, p_2, (q,t), u) \wedge \\
& \text{believes-necessary-to-lessen-health-threat}(p_1, p_1, p_2, (q,t), u) \wedge \\
& \text{believes-can-lessen-threat}(p_1, p_2, u)
\end{aligned}$$

As usual, the new predicates are given semantics by oracles.

164.512(j)(1)(ii)

> *Is necessary for law enforcement authorities to identify or apprehend an individual:*

164.512(j)(1)(ii)(A)

> *Because of a statement by an individual admitting participation in a violent crime that the covered entity reasonably believes may have caused serious physical harm to the victim; or*

We have the positive norm:

$$\begin{aligned}
\varphi^{+}_{\texttt{164.512j1iiA}} \triangleq\ & \text{activerole}(p_1, \textit{covered-entity}) \wedge \\
& \text{activerole}(p_2, \textit{law-enforcement-official})??? \wedge \\
& (t \in_{\mathcal{T}} \textit{phi}) \wedge \\
& (u \in_{\mathcal{U}} \textit{identify-apprehend}(q)) \wedge \\
& \text{consistent-with-applicable-law}(p_1, p_2, (q,t), u) \wedge \\
& (\exists m'.\ \diamondminus \text{send}(q, p_1, m') \wedge \\
& \qquad \text{is-admission-of-crime}(m') \wedge \\
& \qquad \text{believes-crime-caused-serious-harm}(p_1, m'))
\end{aligned}$$

Although it is not stated explicitly in the text, we believe that this paragraph applies only when the information is disclosed to a law enforcement official. Therefore, we have constrained the recipient appropriately in our norm.

As we will see in the following paragraphs, local negative norms constrain this positive norm. Therefore, we form the new positive norm:

$$\begin{aligned}\varphi^{+}_{\texttt{164.512j1iiA'}} \triangleq\ & \varphi^{+}_{\texttt{164.512j1iiA}} \land \\ & (\varphi^{-}_{\texttt{164.512j2i}} \land \varphi^{-}_{\texttt{164.512j2ii}} \land \varphi^{-}_{\texttt{164.512j3}})\end{aligned}$$

164.512(j)(1)(ii)(B)

> *Where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody, as those terms are defined in §164.501.*

We have the positive norm:

$$\begin{aligned}\varphi^{+}_{\texttt{164.512j1iiB}} \triangleq\ & \text{activerole}(p_1, \textit{covered-entity}) \land \\ & \text{activerole}(p_2, \textit{law-enforcement-official})??? \land \\ & (t \in_{\mathcal{T}} \textit{phi}) \land \\ & (u \in_{\mathcal{U}} \textit{identify-apprehend}(q)) \land \\ & \text{consistent-with-applicable-law}(p_1, p_2, (q, t), u) \land \\ & \text{believes-escaped-lawful-custody}(p_1, q)\end{aligned}$$

Again, we believe that the intended recipient is a law enforcement official.

164.512(j)(2)

> *A use or disclosure pursuant to paragraph (j)(1)(ii)(A) of this section may not be made if the information described in paragraph (j)(1)(ii)(A) of this section is learned by the covered entity:*

164.512(j)(2)(i)

> *In the course of treatment to affect the propensity to commit the criminal conduct that is the basis for the disclosure under paragraph (j)(1)(ii)(A) of this section, or counseling or therapy; or*

$$\varphi^{-}_{\texttt{164.512j2i}} \triangleq \neg\text{learned-while-treating-propensity-for-crime}(p_1, (q, t))$$

164.512(j)(2)(ii)

> *Through a request by the individual to initiate or to be referred for the treatment, counseling, or therapy described in paragraph (j)(2)(i) of this section.*

$$\varphi^{-}_{\texttt{164.512j2ii}} \triangleq \neg\text{learned-through-request-for-treatment-of-propensity-for-crime}(p_1, (q, t))$$

164.512(j)(3)

> *A disclosure made pursuant to paragraph (j)(1)(ii)(A) of this section shall contain only the statement described in paragraph (j)(1)(ii)(A) of this section and the protected health information described in paragraph (f)(2)(i) of this section.*

We have the following negative norm, which is local to paragraph (j)(1)(ii)(A):

$$\begin{aligned}\varphi^{-}_{\mathtt{164.512j3}} \triangleq\ & (\exists m'.\ \diamondminus \text{send}(q, p_1, m') \land \\ & \qquad\quad \text{is-admission-of-crime}(m', q) \land \\ & \qquad\quad \text{contains-msg}(m, m') \land \\ & \qquad\quad \text{contains}(m', q, t)) \lor \\ & (t \in_{\mathcal{T}} \textit{name-and-address}) \lor \\ & (t \in_{\mathcal{T}} \textit{date-and-place-of-birth}) \lor \\ & (t \in_{\mathcal{T}} \textit{social-security-number}) \lor \\ & (t \in_{\mathcal{T}} \textit{ABO-blood-type-and-rh-factor}) \lor \\ & (t \in_{\mathcal{T}} \textit{type-of-injury}) \lor \\ & (t \in_{\mathcal{T}} \textit{date-and-time-of-treatment}) \lor \\ & (t \in_{\mathcal{T}} \textit{date-and-time-of-death}) \lor \\ & (t \in_{\mathcal{T}} \textit{distinguishing-physical-characteristics})\end{aligned}$$

Although this paragraph refers back to paragraph (f)(2)(i), it does not do so with the intent of referencing the permitted disclosure there. Instead, the reference is to the list of allowable attribute classes. Therefore, we choose to copy those attributes here.

164.512(j)(4)

> *A covered entity that uses or discloses protected health information pursuant to paragraph (j)(1) of this section is presumed to have acted in good faith with regard to a belief described in paragraph (j)(1)(i) or (ii) of this section, if the belief is based upon the covered entity's actual knowledge or in reliance on a credible representation by a person with apparent knowledge or authority.*

We believe that this paragraph is making a "meta-level" comment that is applicable only if legal complaints are brought against the covered entity for an alleged failure to act in good faith. Consequently, we do not include any norms here.

164.512(k)

164.512(k)(1)

164.512(k)(1)(i)

> *A covered entity may use and disclose the protected health information of individuals who are Armed Forces personnel for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission, if the appropriate military authority has published by notice in the FEDERAL REGISTER the following information:*
>
> *(A) Appropriate military command authorities; and*
> *(B) The purposes for which the protected health information may be used or disclosed.*

We have the positive norm:

$$\begin{aligned}\varphi^{+}_{\mathtt{164.512k1i}} \triangleq\ & \text{activerole}(p_1, \textit{covered-entity}) \land \\ & \text{belongstorole}(q, \textit{armed-forces-personnel}) \land \\ & (t \in_{\mathcal{T}} \textit{phi}) \land\end{aligned}$$

$$\begin{aligned}(\exists p_3.\ & \text{deemed-necessary-for-mission}(p_3, p_1, p_2, (q, t), u) \land \\ & \text{published-in-FR-command-authority-for-disclosure}(p_3, p_1, p_2, (q, t), u) \land \\ & \text{published-in-FR-purpose-for-disclosure}(u, p_1, p_2, (q, t), u))\end{aligned}$$

As usual, the new predicates depend on oracles.

164.512(k)(1)(ii)

> *A covered entity that is a component of the Departments of Defense or Transportation may disclose to the Department of Veterans Affairs (DVA) the protected health information of an individual who is a member of the Armed Forces upon the separation or discharge of the individual from military service for the purpose of a determination by DVA of the individual's eligibility for or entitlement to benefits under laws administered by the Secretary of Veterans Affairs.*

$$\begin{aligned}\varphi^{+}_{\mathtt{164.512k1ii}} \triangleq\ & \text{activerole}(p_1, \textit{covered-entity}) \land \\ & \text{belongstorole}(p_1, \textit{component-of-DoD-or-DoT}) \land \\ & \text{activerole}(p_2, \textit{DVA}) \land \\ & \diamondminus\text{belongstorole}(q, \textit{armed-forces-member}) \land \\ & (t \in_{\mathcal{T}} \textit{phi}) \land \\ & (u \in_{\mathcal{U}} \textit{eligibility-determination-for-veterans-benefits})\end{aligned}$$

Note the use of the temporal $\diamondminus$ operator on belongstorole to ensure that the individual was a member of the Armed Forces.

Also, it is not clear to us whether there is (or should be) a distinction between the terms "member" and "personnel" as used in paragraphs (k)(1)(i) and (ii). We choose to follow the vocabulary used in law.

164.512(k)(1)(iii)

> *A covered entity that is a component of the Department of Veterans Affairs may use and disclose protected health information to components of the Department that determine eligibility for or entitlement to, or that provide, benefits under the laws administered by the Secretary of Veterans Affairs.*

We have the positive norm:

$$\begin{aligned}\varphi^{+}_{\mathtt{164.512k1iii}} \triangleq\ & \text{activerole}(p_1, \textit{covered-entity}) \land \\ & \text{activerole}(p_1, \textit{component-of-DVA}) \land \\ & \text{activerole}(p_2, \textit{component-of-DVA}) \land \\ & (t \in_{\mathcal{T}} \textit{phi}) \land \\ & ((u \in_{\mathcal{U}} \textit{eligibility-determination-for-veterans-benefits}) \lor \\ & \ (u \in_{\mathcal{U}} \textit{provision-of-veterans-benefits}))\end{aligned}$$

Because this paragraph makes no mention of q's role, we leave q's role unconstrained. It is possible that this paragraph intends that q is a former member of the Armed Forces, as is explicitly required in (k)(1)(ii). However, we choose to be conservative and follow the text literally.

164.512(k)(1)(iv)

> *A covered entity may use and disclose the protected health information of individuals who are foreign military personnel to their appropriate foreign military authority for the same purposes for which uses and disclosures are permitted for Armed Forces personnel under the notice published in the FEDERAL REGISTER pursuant to paragraph (k)(1)(i) of this section.*

$$\begin{aligned}\varphi^{+}_{\texttt{164.512k1iv}} \triangleq\ & \text{activerole}(p_1, \textit{covered-entity}) \wedge \\ & \text{belongstorole}(q, \textit{foreign-military-personnel}) \wedge \\ & (t \in_{\mathcal{T}} \textit{phi}) \wedge \\ & (\exists p_3.\ \text{deemed-necessary-for-mission}(p_3, p_1, p_2, (q,t), u) \wedge \\ & \qquad \text{published-in-FR-command-authority-for-disclosure}(p_3, p_1, p_2, (q,t), u) \wedge \\ & \qquad \text{published-in-FR-purpose-for-disclosure}(u, p_1, p_2, (q,t), u))\end{aligned}$$

Note that this is the same as paragraph (k)(1)(i), with the exception of q's role, which is now *foreign-military-personnel*.

164.512(k)(2)

> *A covered entity may disclose protected health information to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act (50 U.S.C. 401, et seq.) and implementing authority (e.g., Executive Order 12333).*

We have the positive norm:

$$\begin{aligned}\varphi^{+}_{\texttt{164.512k2}} \triangleq\ & \text{activerole}(p_1, \textit{covered-entity}) \wedge \\ & (t \in_{\mathcal{T}} \textit{phi}) \wedge \\ & (u \in_{\mathcal{U}} \textit{national-security-activities}) \wedge \\ & \text{NSA-authorized-recipient}(p_2) \wedge \\ & \text{NSA-authorized-purpose}(u)\end{aligned}$$

164.512(k)(3)

> *A covered entity may disclose protected health information to authorized federal officials for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056, or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or to for the conduct of investigations authorized by 18 U.S.C. 871 and 879.*

$$\begin{aligned}\varphi^{+}_{\texttt{164.512k3}} \triangleq\ & \text{activerole}(p_1, \textit{covered-entity}) \wedge \\ & \text{activerole}(p_2, \textit{authorized-federal-official}) \wedge \\ & (t \in_{\mathcal{T}} \textit{phi}) \wedge \\ & ((\exists p_3.\ (u \in_{\mathcal{U}} \textit{provision-of-protective-services}(p_3)) \wedge \\ & \qquad (\text{authorized-to-receive-protection-18USC3056}(p_3) \vee \\ & \qquad\ \text{authorized-to-receive-protection-22USC2709a3}(p_3))) \vee \\ & \ (u \in_{\mathcal{U}} \textit{conduct-investigations-18USC871-and-879}))\end{aligned}$$

164.512(k)(4)

A covered entity that is a component of the Department of State may use protected health information to make medical suitability determinations and may disclose whether or not the individual was determined to be medically suitable to the officials in the Department of State who need access to such information for the following purposes:

(i) For the purpose of a required security clearance conducted pursuant to Executive Orders 10450 and 12698;
(ii) As necessary to determine worldwide availability or availability for mandatory service abroad under sections 101(a)(4) and 504 of the Foreign Service Act; or
(iii) For a family to accompany a Foreign Service member abroad, consistent with section 101(b)(5) and 904 of the Foreign Service Act.

$$\begin{aligned}\varphi^{+}_{\texttt{164.512k4}} \triangleq\ & \text{activerole}(p_1, \textit{covered-entity}) \wedge \\ & \text{activerole}(p_1, \textit{component-of-DoS}) \wedge \\ & \text{activerole}(p_2, \textit{DoS-official}) \wedge \\ & (t \in_{\mathcal{T}} \textit{medical-suitability}(u)) \wedge \\ & ((u \in_{\mathcal{U}} \textit{security-clearance-EO-10450-and-12698}) \vee \\ & \ (u \in_{\mathcal{U}} \textit{determine-availability-for-foreign-service-FSA-101a4-and-504}) \vee \\ & \ (u \in_{\mathcal{U}} \textit{determine-family-accompaniment-FSA-101b5-and-904}))\end{aligned}$$

164.512(k)(5)

164.512(k)(5)(i)

A covered entity may disclose to a correctional institution or a law enforcement official having lawful custody of an inmate or other individual protected health information about such inmate or individual, if the correctional institution or such law enforcement official represents that such protected health information is necessary for:

(A) The provision of health care to such individuals;
(B) The health and safety of such individual or other inmates;
(C) The health and safety of the officers or employees of or others at the correctional institution;
(D) The health and safety of such individuals and officers or other persons responsible for the transporting of inmates or their transfer from one institution, facility, or setting to another;
(E) Law enforcement on the premises of the correctional institution; and
(F) The administration and maintenance of the safety, security, and good order of the correctional institution.

$$\begin{aligned}\varphi^{+}_{\texttt{164.512k5i}} \triangleq\ & \text{activerole}(p_1, \textit{covered-entity}) \wedge \\ & (\text{activerole}(p_2, \textit{correctional-institution}) \vee \\ & \ \text{activerole}(p_2, \textit{law-enforcement-official})) \wedge \\ & \text{belongstorole}(q, \textit{in-lawful-custody}(p_2)) \wedge \\ & (t \in_{\mathcal{T}} \textit{phi}) \wedge \\ & \text{represents-necessary-for-providing-healthcare}(p_2, p_1, p_2, (q, t), u) \wedge\end{aligned}$$

$$\begin{aligned}
&\text{represents-necessary-for-health-safety-of-inmates}(p_2, p_1, p_2, (q, t), u) \wedge \\
&\text{represents-necessary-for-health-safety-of-employees}(p_2, p_1, p_2, (q, t), u) \wedge \\
&\text{represents-necessary-for-health-safety-of-transportation-officers}(p_2, p_1, p_2, (q, t), u) \wedge \\
&\text{represents-necessary-for-law-enforcement-on-premises}(p_2, p_1, p_2, (q, t), u) \wedge \\
&\text{represents-necessary-for-safety-security-order}(p_2, p_1, p_2, (q, t), u)
\end{aligned}$$

164.512(k)(5)(ii)

> *A covered entity that is a correctional institution may use protected health information of individuals who are inmates for any purpose for which such protected health information may be disclosed*

Because our model does not support usage-based norms, we cannot handle this paragraph. However, given an appropriately extended model, we believe that it would be relatively straightforward to include modified versions of the corresponding disclosure-based norms.

164.512(k)(5)(iii)

> *For the purposes of this provision, an individual is no longer an inmate when released on parole, probation, supervised release, or otherwise is no longer in lawful custody.*

Given that we used the role *in-lawful-custody*(p_2) in paragraph (k)(5)(i), this paragraph seems to suggest that $\neg$belongstorole$(q, \textit{in-lawful-custody}(p_2))$ characterizes the fact that an individual is not in lawful custody. This seems completely trivial, and so we do not include any norms or constraints here.

164.512(k)(6)

164.512(k)(6)(i)

> *A health plan that is a government program providing public benefits may disclose protected health information relating to eligibility for or enrollment in the health plan to another agency administering a government program providing public benefits if the sharing of eligibility or enrollment information among such government agencies or the maintenance of such information in a single or combined data system accessible to all such government agencies is required or expressly authorized by statute or regulation.*

$$\begin{aligned}
\varphi^{+}_{\texttt{164.512k6i}} \triangleq\ &\text{activerole}(p_1, \textit{health-plan}) \wedge \\
&\text{activerole}(p_1, \textit{government-public-benefits-program}) \wedge \\
&\text{activerole}(p_2, \textit{government-public-benefits-program}) \wedge \\
&(t \in_{\mathcal{T}} \textit{phi}) \wedge \\
&\text{relates-to-eligibility-enrollment-in-health-plan}((q, t), p_1) \wedge \\
&\text{disclosure-required-or-authorized-by-statute-or-regulation}(p_1, p_2, (q, t), u)
\end{aligned}$$

164.512(k)(6)(ii)

> *A covered entity that is a government agency administering a government program providing public benefits may disclose protected health information relating to the program to another covered entity that is a government agency administering a government program providing public benefits if the programs serve the same or similar populations and the disclosure of protected health information is necessary to coordinate the covered functions of such programs or to improve administration and management relating to the covered functions of such programs.*

$$\begin{aligned}\varphi^{+}_{\texttt{164.512k6ii}} \triangleq \exists p_3, p_4.\ & \text{activerole}(p_1, \textit{covered-entity}) \land \\ & \text{activerole}(p_1, \textit{government-agency-administering}(p_3)) \land \\ & \text{activerole}(p_2, \textit{covered-entity}) \land \\ & \text{activerole}(p_2, \textit{government-agency-administering}(p_4)) \land \\ & \text{belongstorole}(p_3, \textit{government-public-benefits-program}) \land \\ & \text{belongstorole}(p_4, \textit{government-public-benefits-program}) \land \\ & (t \in_{\mathcal{T}} \textit{phi}) \land \\ & \text{relates-to-program}((q,t), p_3) \land \\ & \text{serve-similar-populations}(p_3, p_4) \land \\ & (\text{necessary-for-coordination}(p_3, p_4, p_1, p_2, (q,t), u) \lor \\ & \ \text{necessary-for-improve-management}(p_3, p_4, p_1, p_2, (q,t), u))\end{aligned}$$

164.512(l)

> *A covered entity may disclose protected health information as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault.*

$$\begin{aligned}\varphi^{+}_{\texttt{164.512l}} \triangleq\ & \text{activerole}(p_1, \textit{covered-entity}) \land \\ & (t \in_{\mathcal{T}} \textit{phi}) \land \\ & \text{authorized-and-necessary-for-workers-compensation-laws}(p_1, p_2, (q,t), u)\end{aligned}$$

4.7 §164.514 Other requirements relating to uses and disclosures of protected health information.

164.514(a)

> *Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.*

This paragraph appears to state an intent and so requires no formalization.

164.514(b)

> *A covered entity may determine that health information is not individually identifiable health information only if:*

We require the following constraint:

$$\neg(t \in_{\mathcal{T}} \mathit{phi}) \Rightarrow \\ \quad \varphi_{\texttt{164.514b1}} \lor \\ \quad \varphi_{\texttt{164.514b2}}$$

164.514(b)(1)

> *A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:*
>
> *(i) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and*
>
> *(ii) Documents the methods and results of the analysis that justify such determination; or*

We have the macro:

$$\varphi_{\texttt{164.514b1}} \triangleq \exists p.\ \text{has-experience-with-deidentified-info}(p) \land \\ \qquad \text{determines-and-documents-reidentification-risk-is-small}(p, t)$$

164.514(b)(2)

> *(i) The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed:*
>
> *(A) Names;*
>
> *(B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:*
>
> *(1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and*
>
> *(2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.*
>
> *(C) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;*

(D) Telephone numbers;
(E) Fax numbers;
(F) Electronic mail addresses;
(G) Social security numbers;
(H) Medical record numbers;
(I) Health plan beneficiary numbers;
(J) Account numbers;
(K) Certificate/license numbers;
(L) Vehicle identifiers and serial numbers, including license plate numbers;
(M) Device identifiers and serial numbers;
(N) Web Universal Resource Locators (URLs);
(O) Internet Protocol (IP) address numbers;
(P) Biometric identifiers, including finger and voice prints;
(Q) Full face photographic images and any comparable images; and
(R) Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section; and

(ii) The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

We have the macro:

$$
\begin{array}{l}
\varphi_{\texttt{164.514b2}} \triangleq \neg(\textit{name} \in_{\mathcal{T}} t) \wedge \\
\qquad ((t \in_{\mathcal{T}} \textit{geographic-subdivision}) \wedge \\
\qquad\; \text{smaller-than-State}(t) \supset \\
\qquad\qquad (t \in_{\mathcal{T}} \textit{first-three-zip-code-digits}) \wedge \\
\qquad\qquad \text{population-of-first-three-zip-code-digits-larger-than-20000}(t)) \wedge \\
\qquad (\forall t'.\ (t' \in_{\mathcal{T}} t) \wedge (t' \in_{\mathcal{T}} \textit{date}) \supset \\
\qquad\qquad\quad (t' \in_{\mathcal{T}} \textit{year})) \wedge \\
\qquad \neg(\textit{telephone-numbers} \in_{\mathcal{T}} t) \wedge \\
\qquad \neg(\textit{fax-numbers} \in_{\mathcal{T}} t) \wedge \\
\qquad \neg(\textit{email-addresses} \in_{\mathcal{T}} t) \wedge \\
\qquad \neg(\textit{social-security-numbers} \in_{\mathcal{T}} t) \wedge \\
\qquad \neg(\textit{medical-record-numbers} \in_{\mathcal{T}} t) \wedge \\
\qquad \neg(\textit{health-plan-beneficiary-numbers} \in_{\mathcal{T}} t) \wedge \\
\qquad \neg(\textit{account-numbers} \in_{\mathcal{T}} t) \wedge \\
\qquad \neg(\textit{license-numbers} \in_{\mathcal{T}} t) \wedge \\
\qquad \neg(\textit{vehicle-identifiers} \in_{\mathcal{T}} t) \wedge \\
\qquad \neg(\textit{device-identifiers} \in_{\mathcal{T}} t) \wedge \\
\qquad \neg(\textit{URLs} \in_{\mathcal{T}} t) \wedge \\
\qquad \neg(\textit{IP-addresses} \in_{\mathcal{T}} t) \wedge \\
\qquad \neg(\textit{biometric-identifiers} \in_{\mathcal{T}} t) \wedge \\
\qquad \neg(\textit{full-face-images} \in_{\mathcal{T}} t) \wedge \\
\qquad (\forall t'.\ (t' \in_{\mathcal{T}} \textit{unique-identification-number}) \wedge \\
\qquad\qquad (t' \in_{\mathcal{T}} t) \supset \\
\qquad\qquad\quad \varphi_{\texttt{164.514c}}) \wedge
\end{array}
$$

$\neg$has-knowledge-of-identification-risk(t)

164.514(c)

> *A covered entity may assign a code or other means of record identification to allow information deidentified under this section to be reidentified by the covered entity, provided that:*
>
> *(1) The code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and*
>
> *(2) The covered entity does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.*

We have the macro:

$$\begin{aligned}\varphi_{\texttt{164.514c}} \triangleq\ & (t' \in_{\mathcal{T}} \textit{reidentification-code}) \land \\ & \neg\text{code-derived-from-phi}(t') \land \\ & \neg\Diamond\exists p', m'.\ \text{send}(p_1, p', m') \land \\ & \qquad\qquad \text{contains}(m', p_1, t') \land \\ & \qquad\qquad \text{contains}(m', p_1, \textit{reidentification-mechanism})\end{aligned}$$

164.514(d)

164.514(d)(1)

> *In order to comply with §164.502(b) and this section, a covered entity must meet the requirements of paragraphs (d)(2) through (d)(5) of this section with respect to a request for, or the use and disclosure of, protected health information.*

$$\begin{aligned}&\text{believes-minimum-necessary-for-purpose}(p_1, p_2, (q, t), u) \triangleq \\ &\quad \varphi_{\texttt{164.514d2}} \land \\ &\quad \varphi_{\texttt{164.514d3}} \land \\ &\quad \varphi_{\texttt{164.514d4}} \land \\ &\quad \varphi_{\texttt{164.514d5}}\end{aligned}$$

164.514(d)(2)

> *(i) A covered entity must identify:*
>
> *(A) Those persons or classes of persons, as appropriate, in its workforce who need access to protected health information to carry out their duties; and*
>
> *(B) For each such person or class of persons, the category or categories of protected health information to which access is needed and any conditions appropriate to such access.*

(ii) A covered entity must make reasonable efforts to limit the access of such persons or classes identified in paragraph (d)(2)(i)(A) of this section to protected health information consistent with paragraph (d)(2)(i)(B) of this section.

We have the macro:

$$\begin{aligned}\varphi_{\texttt{164.514d2}} \triangleq\ & \text{identifies-workforce-members-needing-phi}(p_1) \land \\ & \text{reasonably-limits-phi-access}(p_1)\end{aligned}$$

164.514(d)(3)

(i) For any type of disclosure that it makes on a routine and recurring basis, a covered entity must implement policies and procedures (which may be standard protocols) that limit the protected health information disclosed to the amount reasonably necessary to achieve the purpose of the disclosure.

(ii) For all other disclosures, a covered entity must:

(A) Develop criteria designed to limit the protected health information disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is sought; and

(B) Review requests for disclosure on an individual basis in accordance with such criteria.

(iii) A covered entity may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when:

(A) Making disclosures to public officials that are permitted under §164.512, if the public official represents that the information requested is the minimum necessary for the stated purpose(s);

(B) The information is requested by another covered entity;

(C) The information is requested by a professional who is a member of its workforce or is a business associate of the covered entity for the purpose of providing professional services to the covered entity, if the professional represents that the information requested is the minimum necessary for the stated purpose(s); or

(D) Documentation or representations that comply with the applicable requirements of §164.512(i) have been provided by a person requesting the information for research purposes.

We have the macro:

$$\begin{aligned}\varphi_{\texttt{164.514d3}} \triangleq\ & \text{implements-policies-for-routine-disclosures}(p_1) \land \\ & \text{implements-criteria-for-limiting-phi}(p_1) \land \\ & (\text{meets-policies-and-criteria}(p_1, p_2, (q,t), u) \lor \\ & \ (\text{activerole}(p_2, \textit{public-official}) \land \\ & \ \ \text{represents-minimum-necessary}(p_2, p_1, p_2, (q,t), u)) \lor \\ & \ \text{activerole}(p_2, \textit{covered-entity}) \lor \\ & \ ((\text{activerole}(p_2, \textit{workforce-member}(p_1)) \lor\end{aligned}$$

$$\begin{aligned}&\text{activerole}(p_2, \textit{business-associate}(p_1))) \land\\ &(u \in_{\mathcal{U}} \textit{providing-professional-services}(p_1)) \land\\ &\text{represents-minimum-necessary}(p_2, p_1, p_2, (q,t), u)) \lor\\ &((u \in_{\mathcal{U}} \textit{research}) \land\\ &\text{represents-minimum-necessary-164.512i}(p_2, p_1, p_2, (q,t), u)))\end{aligned}$$

164.514(d)(4)

(i) A covered entity must limit any request for protected health information to that which is reasonably necessary to accomplish the purpose for which the request is made, when requesting such information from other covered entities.

(ii) For a request that is made on a routine and recurring basis, a covered entity must implement policies and procedures (which may be standard protocols) that limit the protected health information requested to the amount reasonably necessary to accomplish the purpose for which the request is made.

(iii) For all other requests, a covered entity must:

(A) Develop criteria designed to limit the request for protected health information to the information reasonably necessary to accomplish the purpose for which the request is made; and

(B) Review requests for disclosure on an individual basis in accordance with such criteria.

We do not handle this paragraph.

164.514(d)(5)

For all uses, disclosures, or requests to which the requirements in paragraph (d) of this section apply, a covered entity may not use, disclose or request an entire medical record, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request.

We have the macro:

$$\varphi_{\texttt{164.514d5}} \triangleq (\textit{full-medical-record} \in_{\mathcal{T}} t) \supset \text{full-record-specifically-justified}(p_1, p_2, (q,t), u)$$

164.514(e)

164.514(e)(1)

A covered entity may use or disclose a limited data set that meets the requirements of paragraphs (e)(2) and (e)(3) of this section, if the covered entity enters into a data use agreement with the limited data set recipient, in accordance with paragraph (e)(4) of this section.

We have the following positive norm:

$$
\begin{aligned}
\varphi^{+}_{\texttt{164.514e1}} \triangleq\ & \text{activerole}(p_1, \textit{covered-entity}) \land \\
& \varphi_{\texttt{164.514e2}} \land \\
& \varphi_{\texttt{164.514e3}} \land \\
& \text{has-limited-data-use-agreement}(p_1, p_2, (q, t), u)
\end{aligned}
$$

164.514(e)(2)

> *A limited data set is protected health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:*
>
> *(i) Names;*
> *(ii) Postal address information, other than town or city, State, and zip code;*
> *(iii) Telephone numbers;*
> *(iv) Fax numbers;*
> *(v) Electronic mail addresses;*
> *(vi) Social security numbers;*
> *(vii) Medical record numbers;*
> *(viii) Health plan beneficiary numbers;*
> *(ix) Account numbers;*
> *(x) Certificate/license numbers;*
> *(xi) Vehicle identifiers and serial numbers, including license plate numbers;*
> *(xii) Device identifiers and serial numbers;*
> *(xiii) Web Universal Resource Locators (URLs);*
> *(xiv) Internet Protocol (IP) address numbers;*
> *(xv) Biometric identifiers, including finger and voice prints; and*
> *(xvi) Full face photographic images and any comparable images.*

We have the macro:

$$
\begin{aligned}
\varphi_{\texttt{164.514e2}} \triangleq\ & (t \in_{\mathcal{T}} \textit{phi}) \land \\
& \neg(\textit{name} \in_{\mathcal{T}} t) \land \\
& (\forall t'.\ (t' \in_{\mathcal{T}} \textit{postal-address}) \land \\
& \qquad (t' \in_{\mathcal{T}} t) \supset \\
& \qquad\quad (t' \in_{\mathcal{T}} \textit{city}) \lor \\
& \qquad\quad (t' \in_{\mathcal{T}} \textit{State}) \lor \\
& \qquad\quad (t' \in_{\mathcal{T}} \textit{zip-code})) \land \\
& \neg(\textit{telephone-numbers} \in_{\mathcal{T}} t) \land \\
& \neg(\textit{fax-numbers} \in_{\mathcal{T}} t) \land \\
& \neg(\textit{email-addresses} \in_{\mathcal{T}} t) \land \\
& \neg(\textit{social-security-numbers} \in_{\mathcal{T}} t) \land \\
& \neg(\textit{medical-record-numbers} \in_{\mathcal{T}} t) \land \\
& \neg(\textit{health-plan-beneficiary-numbers} \in_{\mathcal{T}} t) \land \\
& \neg(\textit{account-numbers} \in_{\mathcal{T}} t) \land \\
& \neg(\textit{license-numbers} \in_{\mathcal{T}} t) \land \\
& \neg(\textit{vehicle-identifiers} \in_{\mathcal{T}} t) \land \\
& \neg(\textit{device-identifiers} \in_{\mathcal{T}} t) \land
\end{aligned}
$$

$$\begin{aligned}
&\neg(\mathit{URLs} \in_{\mathcal{T}} t) \land \\
&\neg(\mathit{IP\text{-}addresses} \in_{\mathcal{T}} t) \land \\
&\neg(\mathit{biometric\text{-}identifiers} \in_{\mathcal{T}} t) \land \\
&\neg(\mathit{full\text{-}face\text{-}images} \in_{\mathcal{T}} t)
\end{aligned}$$

164.514(e)(3)

> *(i) A covered entity may use or disclose a limited data set under paragraph (e)(1) of this section only for the purposes of research, public health, or health care operations.*
>
> *(ii) A covered entity may use protected health information to create a limited data set that meets the requirements of paragraph (e)(2) of this section, or disclose protected health information only to a business associate for such purpose, whether or not the limited data set is to be used by the covered entity.*

We have the macro:

$$\begin{aligned}
\varphi_{\texttt{164.514e3}} \triangleq\ &(u \in_{\mathcal{U}} \mathit{research}) \lor \\
&(u \in_{\mathcal{U}} \mathit{public\text{-}health}) \lor \\
&(u \in_{\mathcal{U}} \mathit{healthcare\text{-}operations})
\end{aligned}$$

Note that we cannot handle paragraph (ii) since our model does not support an action for creating a limited data set. In other words, there is nothing in our model that paragraph (ii) can constrain.

164.514(e)(4)

164.514(e)(4)(i)

> *A covered entity may use or disclose a limited data set under paragraph (e)(1) of this section only if the covered entity obtains satisfactory assurance, in the form of a data use agreement that meets the requirements of this section, that the limited data set recipient will only use or disclose the protected health information for limited purposes.*

Because this paragraph simply restates the final part of paragraph (e)(1), there is nothing new to handle here.

164.514(e)(4)(ii)

> *A data use agreement between the covered entity and the limited data set recipient must:*
>
> *(A) Establish the permitted uses and disclosures of such information by the limited data set recipient, consistent with paragraph (e)(3) of this section. The data use agreement may not authorize the limited data set recipient to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity;*
>
> *(B) Establish who is permitted to use or receive the limited data set; and*

(C) Provide that the limited data set recipient will:

(1) Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law;

(2) Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement;

(3) Report to the covered entity any use or disclosure of the information not provided for by its data use agreement of which it becomes aware;

(4) Ensure that any agents, including a subcontractor, to whom it provides the limited data set agrees to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and

(5) Not identify the information or contact the individuals.

We use the following macro to specify the conditions under which a limited data use agreement exists:

$$\begin{aligned}
&\text{has-limited-data-use-agreement}(p_1, p_2) \triangleq \\
&\quad \diamondminus(\exists m'.\ \text{send}(p_2, p_1, m') \wedge \\
&\qquad\qquad \text{is-limited-data-use-agreement}(m') \wedge \\
&\qquad\qquad \text{contains-permitted-uses-disclosures}(p_1, p_2, m') \wedge \\
&\qquad\qquad \text{contains-permitted-recipients}(p_1, p_2, m') \wedge \\
&\qquad\qquad \text{contains-agreement-to-no-further-disclosures}(p_1, p_2, m') \wedge \\
&\qquad\qquad \text{contains-agreement-to-safeguards}(p_1, p_2, m') \wedge \\
&\qquad\qquad \text{contains-agreement-to-report-further-disclosures}(p_1, p_2, m') \wedge \\
&\qquad\qquad \text{contains-agreement-to-subcontractor-agreements}(p_1, p_2, m') \wedge \\
&\qquad\qquad \text{contains-agreement-to-no-contact-or-identification}(p_1, p_2, m'))
\end{aligned}$$

Note the use of special purpose contains-... predicates. This is because the ordinary contains predicate requires that the information attribute be given with respect to a subject principal. This is not the case here, so we cannot use ordinary contains.

164.514(e)(4)(iii)

(A) A covered entity is not in compliance with the standards in paragraph (e) of this section if the covered entity knew of a pattern of activity or practice of the limited data set recipient that constituted a material breach or violation of the data use agreement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful:

(1) Discontinued disclosure of protected health information to the recipient; and

(2) Reported the problem to the Secretary.

(B) A covered entity that is a limited data set recipient and violates a data use agreement will be in noncompliance with the standards, implementation specifications, and requirements of paragraph (e) of this section.

There does not appear to be anything to add here; this paragraph seems to describe “meta-level” operations that must occur when an entity is in noncompliance.

164.514(f)

164.514(f)(1)

> *A covered entity may use, or disclose to a business associate or to an institutionally related foundation, the following protected health information for the purpose of raising funds for its own benefit, without an authorization meeting the requirements of §164.508:*
>
> *(i) Demographic information relating to an individual; and*
>
> *(ii) Dates of health care provided to an individual.*

$$\begin{aligned}\varphi^{+}_{\texttt{164.514f1}} \triangleq\ & \text{activerole}(p_1, \textit{covered-entity}) \wedge \\ & (\text{activerole}(p_2, \textit{business-associate}(p_1)) \vee \\ & \ \text{activerole}(p_2, \textit{related-foundation}(p_1))) \wedge \\ & ((t \in_{\mathcal{T}} \textit{demographic-info}) \vee \\ & \ (t \in_{\mathcal{T}} \textit{healthcare-dates})) \wedge \\ & (u \in_{\mathcal{U}} \textit{fundraising})\end{aligned}$$

164.514(f)(2)

> *(i) The covered entity may not use or disclose protected health information for fundraising purposes as otherwise permitted by paragraph (f)(1) of this section unless a statement required by §164.520(b)(1)(iii)(B) is included in the covered entity's notice;*
>
> *(ii) The covered entity must include in any fundraising materials it sends to an individual under this paragraph a description of how the individual may opt out of receiving any further fundraising communications.*
>
> *(iii) The covered entity must make reasonable efforts to ensure that individuals who decide to opt out of receiving future fundraising communications are not sent such communications.*

We have the macro:

$$\begin{aligned}\varphi_{\texttt{164.514f2}} \triangleq \diamondminus(\exists m'.\ & \text{send}(p_1, p_2, m') \wedge \\ & \text{is-notice}(m', p_1, p_2, (q, t), u) \wedge \\ & \text{contains-statement-of-possible-fundraising}(m', p_1, p_2) \wedge \\ & \text{contains-opt-out-instructions}(m', p_1, p_2))\end{aligned}$$

We choose not to formalize paragraph (iii) because it is unclear how to capture such "reasonable efforts". In PrivacyLFP, we can only require (or not) that something is sent or not sent.

164.514(g)

> *If a health plan receives protected heath information for the purpose of underwriting, premium rating, or other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and if such health insurance or health benefits are not placed with the health plan, such health plan may not use or disclose such protected health information for any other purpose, except as may be required by law.*

$$\begin{array}{l}
\varphi^{-}_{\texttt{164.514g}} \triangleq (\exists p'.\ \text{activerole}(p_1, \textit{health-plan}) \wedge \\
\qquad\qquad \diamondminus (\exists m', u'.\ \text{send}(p', p_1, m') \wedge \\
\qquad\qquad\qquad\qquad\qquad \text{contains}(m', (q,t), u') \wedge \\
\qquad\qquad\qquad\qquad\qquad ((u' \in_{\mathcal{U}} \textit{health-insurance-contract-creation}) \vee \\
\qquad\qquad\qquad\qquad\qquad\ (u' \in_{\mathcal{U}} \textit{health-insurance-contract-renewal}) \vee \\
\qquad\qquad\qquad\qquad\qquad\ (u' \in_{\mathcal{U}} \textit{health-insurance-contract-replacement}))) \wedge \\
\qquad\qquad \neg\text{health-insurance-placed-with}(p', p_1)) \supset \\
\qquad\quad (u \in_{\mathcal{U}} \textit{health-insurance-contract-creation}) \vee \\
\qquad\quad (u \in_{\mathcal{U}} \textit{health-insurance-contract-renewal}) \vee \\
\qquad\quad (u \in_{\mathcal{U}} \textit{health-insurance-contract-replacement}) \vee \\
\qquad\quad \text{required-by-law}(p_1, p_2, (q,t), u)
\end{array}$$

164.514(h)

164.514(h)(1)

> *Prior to any disclosure permitted by this subpart, a covered entity must:*
>
> *(i) Except with respect to disclosures under §164.510, verify the identity of a person requesting protected health information and the authority of any such person to have access to protected health information under this subpart, if the identity or any such authority of such person is not known to the covered entity; and*
>
> *(ii) Obtain any documentation, statements, or representations, whether oral or written, from the person requesting the protected health information when such documentation, statement, or representation is a condition of the disclosure under this subpart.*

Given the level of detail of our model, we do not handle explicit authentication actions. Instead, our model relies on roles having been previously assigned to the principals. This is analogous to the way that authorization logics assume that authentication has already occurred.

164.514(h)(2)

164.514(h)(2)(i)

> *If a disclosure is conditioned by this subpart on particular documentation, statements, or representations from the person requesting the protected health information, a covered entity may rely, if such reliance is reasonable under the circumstances, on documentation, statements, or representations that, on their face, meet the applicable requirements.*
>
> *(A) The conditions in §164.512(f)(1)(ii)(C) may be satisfied by the administrative subpoena or similar process or by a separate written statement that, on its face, demonstrates that the applicable requirements have been met.*
>
> *(B) The documentation required by §164.512(i)(2) may be satisfied by one or more written statements, provided that each is appropriately dated and signed in accordance with §164.512(i)(2)(i) and (v).*

Again, because our model provides roles for the principals, this paragraph seems unnecessary.

164.514(h)(2)(ii)

> *A covered entity may rely, if such reliance is reasonable under the circumstances, on any of the following to verify identity when the disclosure of protected health information is to a public official or a person acting on behalf of the public official:*
>
> *(A) If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status;*
>
> *(B) If the request is in writing, the request is on the appropriate government letterhead; or*
>
> *(C) If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.*

The same analysis applies here as for paragraphs (h)(1) and (h)(2)(i).

164.514(h)(2)(iii)

> *A covered entity may rely, if such reliance is reasonable under the circumstances, on any of the following to verify authority when the disclosure of protected health information is to a public official or a person acting on behalf of the public official:*
>
> *(A) A written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority;*
>
> *(B) If a request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal is presumed to constitute legal authority.*

See paragraph (h)(2)(ii).

164.514(h)(2)(iv)

> *The verification requirements of this paragraph are met if the covered entity relies on the exercise of professional judgment in making a use or disclosure in accordance with §164.510 or acts on a good faith belief in making a disclosure in accordance with §164.512(j).*

See paragraph (h)(2)(ii).

4.8 §164.524 Access of individuals to protected health information.

164.524(a)

164.524(a)(1)

> *Except as otherwise provided in paragraph (a)(2) or (a)(3) of this section, an individual has a right of access to inspect and obtain a copy of protected health information*

> *about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set, except for:*
>
> *(i) Psychotherapy notes;*
> *(ii) Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; and*
> *(iii) Protected health information maintained by a covered entity that is:*
> *(A) Subject to the Clinical Laboratory Improvements Amendments of 1988, 42 U.S.C. 263a, to the extent the provision of access to the individual would be prohibited by law; or*
> *(B) Exempt from the Clinical Laboratory Improvements Amendments of 1988, pursuant to 42 CFR 493.3(a)(2).*

In our opinion, this paragraph describes the *intent* of §164.524. As a result, it introduces no norms directly. The relevant norms will be obtained from the following paragraphs.

164.524(a)(2)

> *A covered entity may deny an individual access without providing the individual an opportunity for review, in the following circumstances.*

Paragraph (a)(2) describes the valid reasons that a covered entity may have for denying an access request without an opportunity for review. These reasons will be used in paragraph (b)(2)(i)(B), and so this macro is used there. Note that this paragraph is not yet describing a requirement; that will appear in (b)(2)(i)(B).

$$\begin{aligned}
&\text{may-deny-without-review-164.524a2}(p_2,(p_1,t')) \triangleq \\
&\quad \text{may-deny-without-review-164.524a2i}(p_2,(p_1,t')) \lor \\
&\quad \text{may-deny-without-review-164.524a2ii}(p_2,(p_1,t')) \lor \\
&\quad \text{may-deny-without-review-164.524a2iii}(p_2,(p_1,t')) \lor \\
&\quad \text{may-deny-without-review-164.524a2iv}(p_2,(p_1,t')) \lor \\
&\quad \text{may-deny-without-review-164.524a2v}(p_2,(p_1,t'))
\end{aligned}$$

164.524(a)(2)(i)

> *The protected health information is excepted from the right of access by paragraph (a)(1) of this section.*

$$\begin{aligned}
&\text{may-deny-without-review-164.524a2i}(p_2,(p_1,t')) \triangleq \\
&\quad (t' \in_{\mathcal{T}} \textit{psychotherapy-notes}) \lor \\
&\quad \text{compiled-for-action-or-proceeding}(p_2,(p_1,t')) \lor \\
&\quad \text{prohibited-by-42USC263a}(p_2,(p_1,t')) \lor \\
&\quad \text{exempt-pursuant-to-42CFR493.3a2}(p_2,(p_1,t'))
\end{aligned}$$

164.524(a)(2)(ii)

> *A covered entity that is a correctional institution or a covered health care provider acting under the direction of the correctional institution may deny, in whole or in part, an inmate's request to obtain a copy of protected health information, if obtaining such copy would jeopardize the health, safety, security, custody, or rehabilitation of the individual or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for the transporting of the inmate.*

We have the macro:

$$
\begin{array}{l}
\text{may-deny-without-review-164.524a2ii}(p_2, (p_1, t')) \triangleq \\
\quad \exists p_2'.\ \text{activerole}(p_2', \textit{correctional-institution}) \wedge \\
\qquad ((p_2' = p_2) \vee \\
\qquad\ (\text{activerole}(p_2, \textit{provider}) \wedge \\
\qquad\quad \text{under-direction-of}(p_2, p_2'))) \wedge \\
\qquad \text{activerole}(p_1, \textit{inmate}(p_2')) \wedge \\
\qquad \text{jeopardizes-health-safety-security-custody-rehabilitation}(p_2', p_2, (p_1, t'))
\end{array}
$$

164.524(a)(2)(iii)

> *An individual's access to protected health information created or obtained by a covered health care provider in the course of research that includes treatment may be temporarily suspended for as long as the research is in progress, provided that the individual has agreed to the denial of access when consenting to participate in the research that includes treatment, and the covered health care provider has informed the individual that the right of access will be reinstated upon completion of the research.*

We have the macro:

$$
\begin{array}{l}
\text{may-deny-without-review-164.524a2iii}(p_2, (p_1, t')) \triangleq \\
\quad \text{created-or-obtained-for-current-research}(p_2, (p_1, t')) \wedge \\
\quad \text{activerole}(p_2, \textit{provider}) \wedge \\
\quad \text{agreed-to-denial-of-access}((p_1, t'), p_2) \wedge \\
\quad \text{informed-of-future-reinstatement}(p_2, (p_1, t'))
\end{array}
$$

Although not stated explicitly in the law, it seems reasonable to have:

$$
\begin{array}{l}
\text{agreed-to-denial-of-access}((p_1, t'), p_2) \triangleq \\
\quad \exists m'.\ \diamondminus \text{send}(p_1, p_2, m') \wedge \\
\qquad\quad \text{is-agreement-to-denial}(m', p_2, (p_1, t'))
\end{array}
$$

and:

$$
\begin{array}{l}
\text{informed-of-future-reinstatement}(p_2, (p_1, t')) \triangleq \\
\quad \exists m'.\ \diamondminus \text{send}(p_2, p_1, m') \wedge \\
\qquad\quad \text{is-notice-of-future-reinstatement}(m', p_2, (p_1, t'))
\end{array}
$$

164.524(a)(2)(iv)

> *An individual's access to protected health information that is contained in records that are subject to the Privacy Act, 5 U.S.C. 552a, may be denied, if the denial of access under the Privacy Act would meet the requirements of that law.*

$$\begin{array}{l}
\text{may-deny-without-review-164.524a2iv}(p_2, (p_1, t')) \triangleq \\
\quad \text{subject-to-5USC552a}(p_2, (p_1, t')) \wedge \\
\quad \text{may-deny-under-5USC552a}(p_2, (p_1, t'))
\end{array}$$

164.524(a)(2)(v)

> *An individual's access may be denied if the protected health information was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.*

$$\begin{array}{l}
\text{may-deny-without-review-164.524a2v}(p_2, (p_1, t')) \triangleq \\
\quad \exists p_3, m'.\ \diamondminus \text{send}(p_3, p_2, m') \wedge \\
\qquad\qquad \text{contains}(m', (p_1, t')) \wedge \\
\qquad\qquad \neg\text{activerole}(p_3, \mathit{provider}) \wedge \\
\qquad\qquad \text{sent-under-promise-of-confidentiality}(p_3, p_2, m') \wedge \\
\qquad\qquad \text{would-reveal-source}(p_2, (p_1, t'), p_3)
\end{array}$$

164.524(a)(3)

> *A covered entity may deny an individual access, provided that the individual is given a right to have such denials reviewed, as required by paragraph (a)(4) of this section, in the following circumstances:*

This paragraph states the valid reasons that a covered entity may give for denying an access request, given that an opportunity for review is provided. As in paragraph (a)(2), we express these conditions as a series of macros. However, no norms are present in this paragraph. Instead, these macros are used in paragraph (b)(2)(i)(B).

$$\begin{array}{l}
\text{may-deny-with-review-164.524a3}(p_2, (p_1, t')) \triangleq \\
\quad \text{may-deny-with-review-164.524a3i}(p_2, (p_1, t')) \vee \\
\quad \text{may-deny-with-review-164.524a3ii}(p_2, (p_1, t')) \vee \\
\quad \text{may-deny-with-review-164.524a3iii}(p_2, (p_1, t'))
\end{array}$$

164.524(a)(3)(i)

> *A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;*

We have the macro:

$$\begin{array}{l}
\text{may-deny-with-review-164.524a3i}(p_2, (p_1, t')) \triangleq \\
\quad \text{determines-access-would-endanger-physical-safety}(p_2, p_2, (p_1, t'))
\end{array}$$

164.524(a)(3)(ii)

> *The protected health information makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or*

We have the macro:

$$
\begin{aligned}
&\text{may-deny-with-review-164.524a3ii}(p_2, (p_1, t')) \triangleq \\
&\quad \exists q'', t'', p_3.\ \text{contains}(t', (q'', t'')) \land \\
&\qquad\qquad \neg(q'' = p_1) \land \\
&\qquad\qquad \neg\text{belongstorole}(q'', \mathit{provider}(p_1)) \land \\
&\qquad\qquad \text{activerole}(p_3, \mathit{health\text{-}care\text{-}professional}) \land \\
&\qquad\qquad \text{determines-likely-to-cause-harm}(p_3, p_2, (p_1, t'), q'')
\end{aligned}
$$

164.524(a)(3)(iii)

> *The request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.*

$$
\begin{aligned}
&\text{may-deny-with-review-164.524a3iii}(p_2, (p_1, t)) \triangleq \\
&\quad \exists q, q'.\ \text{belongstorole}(p_1, \mathit{personal\text{-}representative}(q)) \land \\
&\qquad\quad \text{likely-to-harm-individual}(p_2, (p_1, t), q')
\end{aligned}
$$

164.524(a)(4)

> *If access is denied on a ground permitted under paragraph (a)(3) of this section, the individual has the right to have the denial reviewed by a licensed health care professional who is designated by the covered entity to act as a reviewing official and who did not participate in the original decision to deny. The covered entity must provide or deny access in accordance with the determination of the reviewing official under paragraph (d)(4) of this section.*

We again interpret this paragraph as stating the *intent* of this part of the law. The particular implementation specifications are given in paragraph (d), and so this paragraph yields no norms directly.

164.524(b)

164.524(b)(1)

> *The covered entity must permit an individual to request access to inspect or to obtain a copy of the protected health information about the individual that is maintained in a designated record set. The covered entity may require individuals to make requests for access in writing, provided that it informs individuals of such a requirement.*

We have no norms here. However, the fact that a covered entity must allow requests for access is captured by the particulars of our top-level formula. If the individual sends a request to the covered entity, the $(m = \text{req\_for\_access}(p_1, t)) \supset$ fragment of our top-level formula.

164.524(b)(2)

164.524(b)(2)(i)

> *Except as provided in paragraph (b)(2)(ii) of this section, the covered entity must act on a request for access no later than 30 days after receipt of the request as follows.*

We have the negative norm:

$$\begin{aligned}
\varphi^{-}_{\mathtt{164.524b2i}} \triangleq {\downarrow}x.\ & \text{accessible-on-site}(p_2, (p_1, t)) \supset \\
& \Diamond({\downarrow}y.\ (y \leq x + 30) \wedge \\
& \qquad (\text{respond-164.524b2iA}(p_2, (p_1, t)) \vee \\
& \qquad\ \ \text{respond-164.524b2iB}(p_2, (p_1, t))))
\end{aligned}$$

Note that this negative norm is not installed with most of the other negative norms. Instead it only applies to the $(m = \text{req\_for\_access}(p_1, t)) \supset$ part of our top-level formula. This is the negative norm that ensures that covered entities respond to all access requests.

164.524(b)(2)(i)(A)

> *If the covered entity grants the request, in whole or in part, it must inform the individual of the acceptance of the request and provide the access requested, in accordance with paragraph (c) of this section.*

We define an accepting response using the macro:

$$\begin{aligned}
& \text{respond-164.524b2iA}(p_2, (p_1, t)) \triangleq \\
& \quad \text{request-accepted}(p_2, (p_1, t)) \wedge \\
& \quad (\exists m'.\ \text{send}(p_2, p_1, m') \wedge \\
& \qquad\quad \text{is-notice-of-request-accepted}(m', p_2, (p_1, t))) \wedge \\
& \quad \text{access-provided-164.524c}(p_2, (p_1, t))
\end{aligned}$$

Note that the predicate request-accepted is left undefined; we rely on an oracle for its semantics. The macro access-provided-164.524c is defined in paragraph (c).

164.524(b)(2)(i)(B)

> *If the covered entity denies the request, in whole or in part, it must provide the individual with a written denial, in accordance with paragraph (d) of this section.*

We define a denying response using the macro:

$$\begin{aligned}
& \text{respond-164.524b2iB}(p_2, (p_1, t)) \triangleq \\
& \quad \text{request-denied}(p_2, (p_1, t)) \wedge \\
& \quad (\text{may-deny-without-review-164.524a2}(p_2, (p_1, t)) \vee \\
& \quad\ \ \text{may-deny-with-review-164.524a3}(p_2, (p_1, t))) \wedge \\
& \quad (\exists m'.\ \text{send}(p_2, p_1, m') \wedge \\
& \qquad\quad \text{is-notice-of-request-denied}(m', p_2, (p_1, t))) \wedge \\
& \quad \text{access-denied-164.524d}(p_2, (p_1, t))
\end{aligned}$$

Again, we do not give a definition to request-denied since that depends on the covered entity's decision. The macro access-denied-164.524d is defined in paragraph (d). Note that we make use here of the macros from paragraphs (a)(2) and (3).

164.524(b)(2)(ii)

> *If the request for access is for protected health information that is not maintained or accessible to the covered entity on-site, the covered entity must take an action required by paragraph (b)(2)(i) of this section by no later than 60 days from the receipt of such a request.*

$$\begin{aligned}\varphi^{-}_{\texttt{164.524b2ii}} \triangleq {\downarrow}x.\ &\neg\text{accessible-on-site}(p_2,(p_1,t)) \supset \\ &\Diamond({\downarrow}y.\ (y \leq x+60) \wedge \\ &\quad(\text{respond-164.524b2iA}(p_2,(p_1,t)) \vee \\ &\quad\ \text{respond-164.524b2iB}(p_2,(p_1,t))))\end{aligned}$$

164.524(b)(2)(iii)

> *If the covered entity is unable to take an action required by paragraph (b)(2)(i)(A) or (B) of this section within the time required by paragraph (b)(2)(i) or (ii) of this section, as applicable, the covered entity may extend the time for such actions by no more than 30 days, provided that:*
>
> *(A) The covered entity, within the time limit set by paragraph (b)(2)(i) or (ii) of this section, as applicable, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request; and*
>
> *(B) The covered entity may have only one such extension of time for action on a request for access.*

We have the macro:

$$\begin{aligned}&\text{respond-164.524b2iii}(p_2,(p_1,t),d) \triangleq \\ &\quad\exists m'.\ \text{send}(p_2,p_1,m') \wedge \\ &\qquad\text{is-notice-of-extension}(m',p_2,(p_1,t)) \wedge \\ &\qquad\Diamond({\downarrow}z.\ (z \leq d+30) \wedge \\ &\qquad\quad(\text{respond-164.524b2iA}(p_2,(p_1,t)) \vee \\ &\qquad\quad\ \text{respond-164.524b2iB}(p_2,(p_1,t))))\end{aligned}$$

We must go back and update the norms $\varphi^{-}_{\texttt{164.524b2i}}$ and $\varphi^{-}_{\texttt{164.524b2ii}}$ to reflect this new possibility. For example, $\varphi^{-}_{\texttt{164.524b2i}}$ would become:

$$\begin{aligned}\varphi^{-}_{\texttt{164.524b2i}'} \triangleq {\downarrow}x.\ &\text{accessible-on-site}(p_2,(p_1,t)) \supset \\ &\Diamond({\downarrow}y.\ (y \leq x+30) \wedge \\ &\quad(\text{respond-164.524b2iA}(p_2,(p_1,t)) \vee \\ &\quad\ \text{respond-164.524b2iB}(p_2,(p_1,t)) \vee \\ &\quad\ \text{respond-164.524b2iii}(p_2,(p_1,t),y)))\end{aligned}$$

164.524(c)

> *If the covered entity provides an individual with access, in whole or in part, to protected health information, the covered entity must comply with the following requirements.*

We have the following macro which characterizes what must occur when access is provided:

$$
\begin{aligned}
&\text{access-provided-164.524c}(p_2, (p_1, t)) \triangleq \\
&\quad \exists m'.\ \text{send}(p_2, p_1, m') \wedge \\
&\qquad ((\text{access-provided-164.524c1}(p_2, (p_1, t), m') \wedge \\
&\qquad\ \ \text{access-provided-164.524c2i}(p_2, (p_1, t), m')) \vee \\
&\qquad\ \text{access-provided-164.524c2ii}(p_2, (p_1, t), m')) \wedge \\
&\qquad \text{access-provided-164.524c3}(p_2, (p_1, t), m') \wedge \\
&\qquad \text{access-provided-164.524c4}(p_2, (p_1, t), m')
\end{aligned}
$$

164.524(c)(1)

> *The covered entity must provide the access requested by individuals, including inspection or obtaining a copy, or both, of the protected health information about them in designated record sets. If the same protected health information that is the subject of a request for access is maintained in more than one designated record set or at more than one location, the covered entity need only produce the protected health information once in response to a request for access.*

$$
\begin{aligned}
&\text{access-provided-164.524c1}(p_2, (p_1, t), m') \triangleq \\
&\quad \text{contains}(m', (p_1, t))
\end{aligned}
$$

164.524(c)(2)

164.524(c)(2)(i)

> *The covered entity must provide the individual with access to the protected health information in the form or format requested by the individual, if it is readily producible in such form or format; or, if not, in a readable hard copy form or such other form or format as agreed to by the covered entity and the individual.*

We have the macro:

$$
\begin{aligned}
&\text{access-provided-164.524-c2i}(p_2, (p_1, t), f, m') \triangleq \\
&\quad (\text{producible-in-format}(p_2, (p_1, t), f) \wedge \\
&\quad\ \text{in-format}(p_2, p_1, m', f)) \vee \\
&\quad (\neg\text{producible-in-format}(p_2, (p_1, t), f) \wedge \\
&\quad\ \exists f'.\ \text{producible-in-format}(p_2, (p_1, t), f') \wedge \\
&\qquad \text{has-agreed-to-format}(p_2, p_1, (p_1, t), f') \wedge \\
&\qquad \text{has-agreed-to-format}(p_1, p_2, (p_1, t), f') \wedge \\
&\qquad \text{in-format}(p_2, p_1, m', f'))
\end{aligned}
$$

where has-agreed-to-format$(p, p', (p_1, t), f')$ is defined in an unspecified way. However, it is natural to have

$$
\begin{aligned}
&\text{has-agreed-to-format}(p, p', (p_1, t), f') \triangleq \\
&\quad \exists m''.\ \diamondminus \text{send}(p, p', m'') \land \\
&\qquad\quad \text{is-agreement-to-format}(m'', p, p', (p_1, t), f')
\end{aligned}
$$

164.524(c)(2)(ii)

> *The covered entity may provide the individual with a summary of the protected health information requested, in lieu of providing access to the protected health information or may provide an explanation of the protected health information to which access has been provided, if:*
>
> *(A) The individual agrees in advance to such a summary or explanation; and*
>
> *(B) The individual agrees in advance to the fees imposed, if any, by the covered entity for such summary or explanation.*

We have the macro:

$$
\begin{aligned}
&\text{access-provided-164.524-c2ii}(p_2, (p_1, t), m') \triangleq \\
&\quad \exists x.\ \text{is-summary-of}(m', (p_1, t)) \land \\
&\qquad \text{has-agreed-to-summary}(p_1, p_2, (p_1, t)) \land \\
&\qquad \text{fees-for-summary}(p_2, (p_1, t), \$x) \land \\
&\qquad ((\$x > \$0) \supset \text{has-agreed-to-summary-fees}(p_1, p_2, (p_1, t), \$x))
\end{aligned}
$$

where the has-agreed-to-... predicates are left undefined by the law. However, it is again natural to permit definitions following the above example of has-agreed-to-format.

164.524(c)(3)

> *The covered entity must provide the access as requested by the individual in a timely manner as required by paragraph (b)(2) of this section, including arranging with the individual for a convenient time and place to inspect or obtain a copy of the protected health information, or mailing the copy of the protected health information at the individual's request. The covered entity may discuss the scope, format, and other aspects of the request for access with the individual as necessary to facilitate the timely provision of access.*

This is handled by paragraph (b)(2).

164.524(c)(4)

> *If the individual requests a copy of the protected health information or agrees to a summary or explanation of such information, the covered entity may impose a reasonable, cost-based fee, provided that the fee includes only the cost of:*
>
> *(i) Copying, including the cost of supplies for and labor of copying, the protected health information requested by the individual;*
>
> *(ii) Postage, when the individual has requested the copy, or the summary or explanation, be mailed; and*
>
> *(iii) Preparing an explanation or summary of the protected health information, if agreed to by the individual as required by paragraph (c)(2)(ii) of this section.*

We do not handle this paragraph since it is unclear what counts as a reasonable fee.

164.524(d)

> *If the covered entity denies access, in whole or in part, to protected health information, the covered entity must comply with the following requirements.*

To comply with the requirements of (d) for access denial, a covered entity must comply with all of the subparagraphs: (d)(1)–(4).

access-denied-164.524d$(p_2, (p_1, t), m') \triangleq$
access-denied-164.524d1$(p_2, (p_1, t), m') \wedge$
access-denied-164.524d2$(p_2, (p_1, t), m') \wedge$
access-denied-164.524d3$(p_2, (p_1, t), m') \wedge$
access-denied-164.524d4$(p_2, (p_1, t), m')$

164.524(d)(1)

> *The covered entity must, to the extent possible, give the individual access to any other protected health information requested, after excluding the protected health information as to which the covered entity has a ground to deny access.*

Because we have structured access requests to be over individual attributes, we have no notion of partial access denial. Therefore, there is nothing to do here:

access-denied-164.524d1$(p_2, (p_1, t), m') \triangleq \top$

164.524(d)(2)

> *The covered entity must provide a timely, written denial to the individual, in accordance with paragraph (b)(2) of this section. The denial must be in plain language and contain:*
>
> *(i) The basis for the denial;*
> *(ii) If applicable, a statement of the individual's review rights under paragraph (a)(4) of this section, including a description of how the individual may exercise such review rights; and*
> *(iii) A description of how the individual may complain to the covered entity pursuant to the complaint procedures in §164.530(d) or to the Secretary pursuant to the procedures in §160.306. The description must include the name, or title, and telephone number of the contact person or office designated in §164.530(a)(1)(ii).*

access-denied-164.524d2$(p_2, (p_1, t'), m') \triangleq$
contains-basis-for-denial$(m', p_2, (p_1, t)) \wedge$
(review-permitted$(p_2, (p_1, t'))$ $\supset$
contains-statement-of-review-rights$(m')) \wedge$
contains-description-how-to-complain$(m', p_2) \wedge$
contains-contact-info-164.530a1ii(m', p_2)

164.524(d)(3)

> *If the covered entity does not maintain the protected health information that is the subject of the individual's request for access, and the covered entity knows where the requested information is maintained, the covered entity must inform the individual where to direct the request for access.*

$$
\begin{array}{l}
\text{access-denied-164.524d3}(p_2, (p_1, t), m') \triangleq \\
\quad \text{not-maintained-by}((p_1, t), p_2) \wedge \\
\quad (\exists p_3, m''.\ \diamondminus \text{send}(p_3, p_2, m'') \wedge \\
\qquad\qquad \text{contains-location-of}(m'', p_1, t)) \wedge \\
\quad \text{contains-location-of}(m', p_1, t)
\end{array}
$$

Note the use of the $\diamondminus$ operator to track knowledge that a principal has: the covered entity knows where the requested information is maintained if it previously recieved a message containing the location of that requested information.

164.524(d)(4)

> *If the individual has requested a review of a denial under paragraph (a)(4) of this section, the covered entity must designate a licensed health care professional, who was not directly involved in the denial to review the decision to deny access. The covered entity must promptly refer a request for review to such designated reviewing official. The designated reviewing official must determine, within a reasonable period of time, whether or not to deny the access requested based on the standards in paragraph (a)(3) of this section. The covered entity must promptly provide written notice to the individual of the determination of the designated reviewing official and take other action as required by this section to carry out the designated reviewing official's determination.*

We have the macro:

$$
\begin{array}{l}
\text{access-denied-164.524d4}(p_2, (p_1, t), m') \triangleq \\
\Box(\downarrow x. \forall m_2.\ \text{send}(p_1, p_2, m_2) \wedge \\
\qquad\qquad \text{is-request-for-review}(m_2, p_2, (p_1, t)) \supset \\
\qquad\qquad\quad \Diamond(\downarrow y.\ (y \leq x + c_1) \wedge \\
\qquad\qquad\qquad\quad \exists p_3, m_3.\ \text{send}(p_2, p_3, m_3) \wedge \\
\qquad\qquad\qquad\qquad\qquad \text{is-referral-to-review-denial}(m_3, p_2, (p_1, t), m') \wedge \\
\qquad\qquad\qquad\qquad\qquad \Diamond(\downarrow z.\ (z \leq y + c_2) \wedge \\
\qquad\qquad\qquad\qquad\qquad\qquad \exists m_4.\ \text{send}(p_3, p_2, m_4) \wedge \\
\qquad\qquad\qquad\qquad\qquad\qquad\quad ((\text{is-agreement-with-denial}(m_4, p_2, (p_1, t), m') \wedge \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad \Diamond(\downarrow w.\ (w \leq z + c_3) \wedge \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \exists m_5.\ \text{send}(p_2, p_1, m_5) \wedge \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \text{is-notice-of-review-result}(m_5, m_4) \wedge \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \text{access-provided-164.524c}(p_2, (p_1, t)))) \vee \\
\qquad\qquad\qquad\qquad\qquad\qquad\quad (\text{is-disagreement-with-denial}(m_4, p_2, (p_1, t), m') \wedge \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad \Diamond(\downarrow w.\ (w \leq z + c_3) \wedge \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \exists m_5.\ \text{send}(p_2, p_1, m_5) \wedge \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \text{is-notice-of-review-result}(m_5, m_4)))))))
\end{array}
$$

There are quite a few steps in this rule, but this seems to be unavoidable due to the length and detail of this paragraph. This paragraph makes crucial use of the freeze quantifier, $\downarrow_{-}.$, which was not present in prior work.

164.524(e)

> *A covered entity must document the following and retain the documentation as required by §164.530(j):*
>
> *(1) The designated record sets that are subject to access by individuals; and*
>
> *(2) The titles of the persons or offices responsible for receiving and processing requests for access by individuals.*

Because our model does not account for retaining documentation and/or records, we cannot handle this paragraph. Anyway, this seems to be primarily an administrative requirement, not directly related to disclosures.

Chapter 5

Related Work and Conclusion

At this point, we have given logical formalizations of the Gramm-Leach-Bliley Act (GLBA), §§6802 and 6803, and the Health Insurance Portability and Accountability Act (HIPAA), §§164.502, 164.506, 164.508, 164.510, 164.512, 164.514, and 164.524 in our PrivacyLFP logic. Before concluding, we overview other related work in the area of formalizing privacy regulations.

5.1 Related Work

We divide the closely related work into three distinct categories: formalization efforts for HIPAA and GLBA, other privacy logics, and privacy languages.

Other Formalization Efforts for HIPAA and GLBA. There are five related efforts for formalizing HIPAA and GLBA.

First, because PrivacyLFP is based on Barth *et al.*'s Logic of Privacy and Utility (LPU) [BDMN06, BDMS07, Bar08], our formalization of HIPAA is most closely related to their proof-of-concept examples of five HIPAA clauses. Our formalization covers a *much* larger part of HIPAA, and is more expressive, most notably due to our addition of disclosure purposes and real-time features.

Second, Lam *et al.* describe a formalization of HIPAA §§164.502, 164.506, and 164.510 in a fragment of stratified Datalog with one alternation of negation, which they name pLogic [LMS09]. To formalize a given HIPAA clause, they write a pair of pLogic rules that decide if an action is permitted by that clause and if an action is forbidden by that clause. This approach has the advantage of maintaining a close correspondence with the law's text, which is useful when auditing.

Although Lam *et al.*'s formalization has significantly larger coverage than the example clauses of Barth *et al.*, it is not as complete as ours, partly for reasons of expressiveness. Due to the lack of temporal modalities in Datalog, they cannot express HIPAA clauses containing obligations, such as those in §164.524(b) which obligate a covered entity to respond to access requests within 60 days. (Lam *et al.* can handle constraints that depend on *past* actions by linking a kind of historical record to each action.) On the other hand, by using Datalog, they were able to quickly obtain a prototype implementation without much technical trouble. Our formalization does not yet have an implementation due to the nonstandard nature of our PrivacyLFP logic [DGJ$^+$10].

Third, Breaux and Antón have developed a methodology for extracting rights and obligations from natural language privacy laws, and applied the methodology to the entire text of HIPAA [BA08]. Their approach is quite different from ours and the others we have discussed.

Rather than producing a logical formalization intended for use with model checking and other tools, their methodology produces a catalog of constraints on requirements, cross references, role hierarchies, and priorities between clauses. This catalog is intended to assist engineers in designing software that complies with the privacy regulations. As an opportunity for future work, we believe that it might prove very profitable to combine these two approaches: by cataloging the law's components, Breaux and Antón's methodology would likely ease the logician's task of translating a privacy regulation into a logic for formal verification.

Fourth, May *et al.* [MGL06] advocate the use of privacy APIs as a means of capturing the privacy components of HIPAA. Privacy APIs are an extension of the traditional matrix model of access control with constructs for logging. Temporal and obligation features can only be expressed as uninterpreted strings, making the expressiveness strictly weaker than a system based on temporal logic. To evaluate their design of privacy APIs, they formalized §164.506 of two versions of HIPAA, and analyzed it using model checking, uncovering an ambiguity in the law. May *et al.* did not formalize a larger fragment of HIPAA. (May *et al.* also use a GLBA clause as an example, but do not appear to have pursued a large-scale formalization of GLBA.)

Finally, to the best of our knowledge, the only other formalization of GLBA clauses appears in the work on the Logic of Privacy and Utility (LPU) by Barth *et al.* [BDMN06, Bar08]. However, their formalization is limited to just four clauses. In addition, our formalization correctly handles clauses involving constraints on information sharing (via fixed points) and annual notices (via real-time features) that are not possible in LPU.

Other Privacy Logics. As previously noted, most closely related to PrivacyLFP is the Logic of Privacy and Utility (LPU) [BDMN06, BDMS07, Bar08]. As discussed in Section 2.2, we have made several extensions, including the addition of purposes, fixed point operators, and real-time features. These extensions improved the expressive power so that new clauses of GLBA and HIPAA could be formalized.

Choosing deontic logic, rather than temporal logic, as a foundation, Dinesh *et al.* have developed a logic for reasoning about conditions and exceptions in privacy laws [DJLS08]. This is distinct from the simple-minded way we handle exceptions by disjunctively joining them to the relevant clauses. The approach of Dinesh *et al.* is advantageous in that it does not require this kind of foresight: there is no need to modify previously formalized clauses if exceptions appear in later paragraphs. Further investigation is needed to determine whether their ideas can be adapted to PrivacyLFP.

Privacy Languages. There are numerous privacy languages described in the literature, including the Enterprise Privacy Authorization Language (EPAL) and the eXtensible Access Control Markup Language (XACML), the Platform for Privacy Preferences (P3P), and role-based access control languages (RBAC).

EPAL [BKBS04, BPS03] and XACML [ANP$^+$04], upon which EPAL was based, are privacy languages formulated as access control frameworks. For example, in EPAL, a user makes a "access" request (which may include sending data), which the system allows or denies according to the privacy policy. Unfortunately, EPAL and XACML do not possess first-class temporal modalities. Instead, they have a much weaker uninterpreted obligation symbol for representing future requirements. Our PrivacyLFP logic inherits the richer temporal and obligation constructs from LPU, and is therefore more expressive than EPAL and XACML.

P3P [RC99, BCK03, ACR99] is a privacy language targeted exclusively to web sites. As such, the sender and recipient are fixed to be the web site and web site visitor, respectively, making P3P unsuitable for the formalization of HIPAA, GLBA, and general privacy laws. Moreover, P3P cannot express temporal modalities.

RBAC languages (e.g., [Cra03, JSSS01, LMW02]) tackle the access control problem from the standpoint of roles: a principal's access rights are determined by the roles she holds. Unfortunately, RBAC generally lacks a notion of data attribute, and so cannot express privacy policies that take attributes into account when making an allow-deny decision. In addition, RBAC, too, does not include temporal modalities.

5.2 Conclusion

In this work, we have designed a novel privacy logic, PrivacyLFP, based on the Logic of Privacy and Utility [BDMN06, BDMS07, Bar08] but extended with purposes, real-time features, and fixed points. Using PrivacyLFP, we have given formalizations of GLBA and HIPAA, which we believe to be the most complete formalizations of these laws in a logic to date. Studies of HIPAA's effect on privacy practices have suggested that HIPAA has paradoxically weakened privacy [AEV$^+$07]. We sincerely hope that our formalizations may prove useful in designing and using practical tools to combat this effect in the financial and healthcare contexts.

5.3 Acknowledgements

The authors wish to thank Limin Jia for pointing out several simplifications to some of our GLBA and HIPAA norms, Rob Simmons for discussions on fixed points, and Helen Nissenbaum and Deborah Peel for discussions on HIPAA regulations.

Bibliography

[ACR99] Mark S. Ackerman, Lorrie F. Cranor, and Joseph Reagle. Privacy in e-commerce: Examing user scenarios and privacy preferences. In *Proceedings of the 1st ACM Conference on Electronic Commerce*, pages 1–8, 1999.

[AEV$^+$07] Annie I. Antón, Julia B. Eart, Matthew W. Vail, Neha Jain, Carrie M. Gheen, and Jack M. Frink. HIPAA's effect on web site privacy policies. *IEEE Security and Privacy*, 5(1):45–52, 2007.

[AH94] Rajeev Alur and Thomas A. Henzinger. A really temporal logic. *Journal of the ACM*, 41(1):181–203, January 1994.

[AHK02] Rajeev Alur, Thomas A. Henzinger, and Orna Kupferman. Alternating-time temporal logic. *Journal of the ACM*, 49(5):672–713, September 2002.

[ANP$^+$04] A. Anderson, A. Nadalin, B. Parducci, D. Engovatov, E. Coyne, F. Siebenlist, H. Lockhart, M. McIntosh, M. Kudo, P. Humenn, R. Jacobson, S. Proctor, S. Godik, S. Anderson, and T. Moses. Extensible access control markup language (xacml) version 2.0, 2004.

[BA08] Travis Breaux and Annie Antón. Analyzing regulatory rules for privacy and security requirements. *IEEE Transactions on Software Engineering*, 34(1):5–20, January 2008.

[Bar08] Adam Barth. *Design and Analysis of Privacy Policies.* Phd thesis, Stanford University, 2008.

[BCK03] Simon Byers, Lorrie F. Cranor, and David Kormann. Automated analysis of P3P-enabled web sites. In *Proceedings of the 5th International Conference on Electronic Commerce*, pages 326–338, 2003.

[Bd03] Torben Braüner and Valeria de Paiva. Towards constructive hybrid logic. In *Electronic Proceedings of Methods for Modalities 3 (M4M3)*, 2003. Online at http://m4m.loria.fr/M4M3/Papers/brauner.ps.gz.

[BDMN06] Adam Barth, Anupam Datta, John C. Mitchell, and Helen Nissenbaum. Privacy and contextual integrity: Framework and applications. In *Proceedings of the 27th IEEE Symposium on Security and Privacy*, pages 184–198, May 2006.

[BDMS07] Adam Barth, Anupam Datta, John C. Mitchell, and Sharada Sundaram. Privacy and utility in business processes. In *Proceedings of the 20th IEEE Computer Security Foundations Symposium*, pages 279–294, July 2007.

[BKBS04] Michael Backes, Günter Karjoth, Walid Bagga, and Matthias Schunter. Efficient comparsion of enterprise privacy policies. In *Proceedings of the 2004 ACM Symposium on Applied Computing*, pages 375–382, 2004.

[Bla00] Patrick Blackburn. Representation, reasoning, and relational structures: A hybrid logic manifesto. *Logic Journal of IGPL*, 8(3):339–365, 2000.

[BPS03] Michael Backes, Birgit Pfitzmann, and Matthias Schunter. A toolkit for managing enterprise privacy policies. In *European Symposium on Research in Computer Security*, volume 2808 of *LNCS*, pages 101–119, 2003.

[BS06] Julian Bradfield and Colin Stirling. *The Handbook of Modal Logic*, chapter Modal Mu-Calculi, pages 721–756. Elsevier, 2006.

[CMS06] Rohit Chadha, Damiano Macedonio, and Vladimiro Sassone. A hybrid intuitionistic logic: Semantics and decidability. *Journal of Logic and Computation*, 16:27–59(33), 2006.

[Cra03] Jason Crampton. On permissions, inheritance, and role hierarchies. In *Proceedings of the 10th ACM Conference on Computer and Communication Security*, pages 85–92, 2003.

[DGJ$^+$10] Henry DeYoung, Deepak Garg, Limin Jia, Dilsun Kaynar, and Anupam Datta. Privacy policy specification and audit in a fixed-point logic: How to enforce HIPAA, GLBA, and all that. Technical Report CMU-CyLab-10-008, Carnegie Mellon University, April 2010.

[DJLS08] Nikhil Dinesh, Aravind K. Joshi, Insup Lee, and Oleg Sokolsky. Reasoning about conditions and exceptions to laws in regulatory conformance checking. In *Proceedings of the Ninth International Conference on Deontic Logic in Computer Science*, volume 5076 of *LNAI*, pages 110–124, July 2008.

[JSSS01] Sushil Jajodia, Pierangela Samarati, Maria Luisa Sapino, and V. S. Subrahmanian. Flexible support for multiple access control policies. *ACM Transactions on Database Systems*, 26(2):214–260, 2001.

[LMS09] Peifung E. Lam, John C. Mitchell, and Sharada Sundaram. A formalization of HIPAA for a medical messaging system. In *Proceedings of the 6th International Conference on Trust, Privacy, and Security in Digital Business*, volume 5695 of *LNCS*, pages 73–85, 2009.

[LMW02] Ninghui Li, John C. Mitchell, and William H. Winsborough. Design of a role-based trust management framework. In *Proceedings of the 2002 IEEE Symposium on Security and Privacy*, pages 114–130. IEEE Computer Society Press, May 2002.

[MGL06] Michael J. May, Carl A. Gunter, and Insup Lee. Privacy APIs: Access control techniques to analyze and verify legal privacy policies. In *Proceedings of the IEEE Workshop on Computer Security Foundations*, pages 85–97, 2006.

[MP95] Zohar Manna and Amir Pnueli. *Temporal Verification of Reactive Systems: Safety*. Springer-Verlag, 1995.

[Nis04] Helen Nissenbaum. Privacy as contextual integrity. *Washington Law Review*, 79(1):119–158, 2004.

[Räs02] Thoralf Räsch. *Automata, Logics, and Infinite Games*, volume 2500 of *LNCS*, chapter Introduction to Guarded Logics, pages 321–342. Springer-Verlag, 2002.

[RC99] Joseph Reagle and Lorrie F. Cranor. The platform for privacy preferences. *Communications of the ACM*, 42(2):48–55, 1999.

[Sta] Stanford Privacy Group. HIPAA compliance checker. `http://crypto.stanford.edu/privacy/HIPAA`.

[Tar55] Alfred Tarski. A lattice-theoretical fixpoint theorem and its applications. *Pacific Journal of Mathematics*, 5(2):285–309, 1955.

[US 99] US Congress. Gramm-Leach-Bliley Act, Financial Privacy Rule. 15 USC §6801–§6809, November 1999. Available at `http://www.law.cornell.edu/uscode/usc_sup_01_15_10_94_20_I.html`.

[US 02] US Congress. Health Insurance Portability and Accountability Act of 1996, Privacy Rule. 45 CFR 164, August 2002. Available at `http://www.access.gpo.gov/nara/cfr/waisidx_07/45cfr164_07.html`.