Formalization of HIPAA

Simon Berring
Navya Rehani
Dina Thomas

HIPAA Overview

The Health Information Portability and Accountability Act (HIPAA) was passed in 1996, supplemented with the HHS Privacy Rule in 2000, and supplemented again in 2003. Its dual goal was to protect individuals' health information and to allow sufficient flow of information for maintaining high quality health care.

Objectives

We examined the text of the 2003 privacy rule with the goal of providing a formal description of the text using Linear Temporal Logic (LTL) and determining whether the rule met various desired/expected properties connected to those goals.

Previous Work

Our major references were BDMN[06] and GLM[Forthcoming]. Ideas for potentially interesting properties come from the latter, and our formalization framework comes from the former. The framework is as follows: translate from the text into the LTL grammar:

$$\varphi ::= \mathrm{send}(p_1, p_2, m) \mid \mathrm{contains}(m, q, t) \mid \mathrm{inrole}(p, r) \mid \mathrm{incontext}(p, c) \mid t \in t' \mid \varphi \wedge \varphi \mid \neg\varphi \mid \varphi \mathcal{U} \varphi \mid \varphi \mathcal{S} \varphi \mid \bigcirc\varphi \mid \exists x : \tau.\varphi$$

where each rule is interpreted as a "positive norm" or "negative norm", where positive norms specify allowed behavior and are inserted into the disjunction below, and negative norms specify disallowed behavior, and are inserted into the conjunction.

$$\sigma \models \Box\forall p_1, p_2, q : P.\forall m : M.\forall t : T.\, \mathrm{incontext}(p_1, c) \wedge \mathrm{send}(p_1, p_2, m) \wedge \mathrm{contains}(m, q, t) \rightarrow \bigvee_{\varphi^+ \in \mathrm{norms}^+(c)} \varphi^+ \wedge \bigwedge_{\varphi^- \in \mathrm{norms}^-(c)} \varphi^-$$

Verification Tool

SPIN stands for Simple Promela INterpreter. It is a verifier for parallel distributed systems with LTL model checking capability and non-deterministic scheduling of processes. Promela stands for PRocess/PRotocol MEta LAnguage. It provides an SPL-like environment, where communication between processes takes place via synchronous and asynchronous channels.

SPIN also had two conspicuous disadvantages. It does not support past temporal operators (which are necessary given the "norms" structure), and it has serious memory constraints. We dealt with the first by adding variables to the model to store state and using only future operators. We dealt with the second by creating separate models for each desired property, using only relevant roles/variables.

Our Approach
We formalized desired properties and relevant HIPAA rules using LTL. The relevant roles are modeled in Promela as processes communicating with each other. Our models allowed all possible communications between processes. We use SPIN to verify the property (□HIPAA → □Desired) on this model.

Results
We investigated several desired properties, and found that the following three were *not satisfied*:

- A friend cannot find out what medicine you're taking without your knowledge
  inrole(p1, pharmacist) ∧ inrole (q, patient) ∧ inrole (p2, friend[q]) ∧
  t ∈ prescription ∧ send(p1, p2, t) →
  (!send(q, p1, deny-identification) S send(q, p1, identify-friend))

- Your protected health information won't be transmitted to a third party who is not covered by HIPAA privacy rule
  inrole(p1, hcp) ∧ inrole(q, patient) ∧ t∈phi ∧ send(p1, p2, t) →
  incontext(p2, covered-entity)

- A doctor may not disclose a patient's record for TPO after the patient has denied consent.[1]
  inrole(q, patient) ∧ inrole(p1, hcp) ∧ t∈phi ∧ send(p1, p2, t) →
  (!send(q, p1, deny-consent) S send (q, p1, consent))

In each case, we modeled a relevant subset of HIPAA[2]. See the appendix for details.

Analysis
Traces violating the first property either take advantage of the rule's provision: **§164.510(b)(1)**, which does not require a patient to identify a family member or friend before they receive disclosures of protected health information (phi), or they take advantage of provision **§164.510(b)(3)**, which allows the use of "professional judgment" to authorize a disclosure of phi when a patient is unavailable.

Traces violating the second property use either **§164.506(c)(3)**, which allows the disclosure of phi to a (potentially non-covered) health care provider (hcp) for use in payment, or use **§164.506(c)(4)**, which allows disclosure to non-covered hcps that have relationships with the patient.

Traces violating the third property use **§164.506(b)(1)**, which makes the optional consent given by the patient non-binding on the hcp.

---

[1] This property was first investigated by Gunter, et al in GLM[Forthcoming].
[2] For a positive proof of a safety property on HIPAA, it is important to model all relevant positive norms. For a counter-example, it is important to have all relevant negative norms. We selected sections of the text we believed we could isolate in this latter sense.

Conclusions

We found the HIPAA Privacy Rule to be generally well-specified and documented. However, there were (unsurprisingly) ambiguous clauses in the prose descriptions. According to our analysis, the rule fails to make expected privacy guarantees in at least three ways.

References

BDMN[06] *Adam Barth, Anupam Datta, John C. Mitchell, Helen Nissenbaum. Privacy and Contextual Integrity: Framework and Applications. To appear: Proceedings of the 27th IEEE Symposium on Security and Privacy. ACM Press, 2006.*

GLM[Forthcoming] *Carl Gunter, Insup Lee, Michael May. Privacy APIs: Access Control Techniques to Analyze and Verify Legal Privacy Policies. To appear.*

OCR/HIPAA Privacy/Security/Enforcement Regulation Text. August 2003.

APPENDIX:

1. A friend cannot find out what medicine you're taking without your knowledge
□(HIPAA -> Desired Property) returns FALSE

a. Desired Property

inrole(p1, pharmacist) ∧ inrole (q, patient) ∧ inrole (p2, friend[q]) ∧ t ∈ prescription ∧ send(p1, p2, t) → (! send(q, p1, deny-identification) S send(q, p1, identify-friend))

---------removing past operators ---

inrole(p1, pharmacist) ∧ inrole (q, patient) ∧ inrole (p2, friend[q]) ∧ t ∈ prescription ∧ (!send(p1, p2, t) W send(q, p1, identify-friend)) ∧ □(send(q, p1, deny-identification) → (!send(p1, p2, t) W send(q, p1, identify-friend))

b. HIPAA

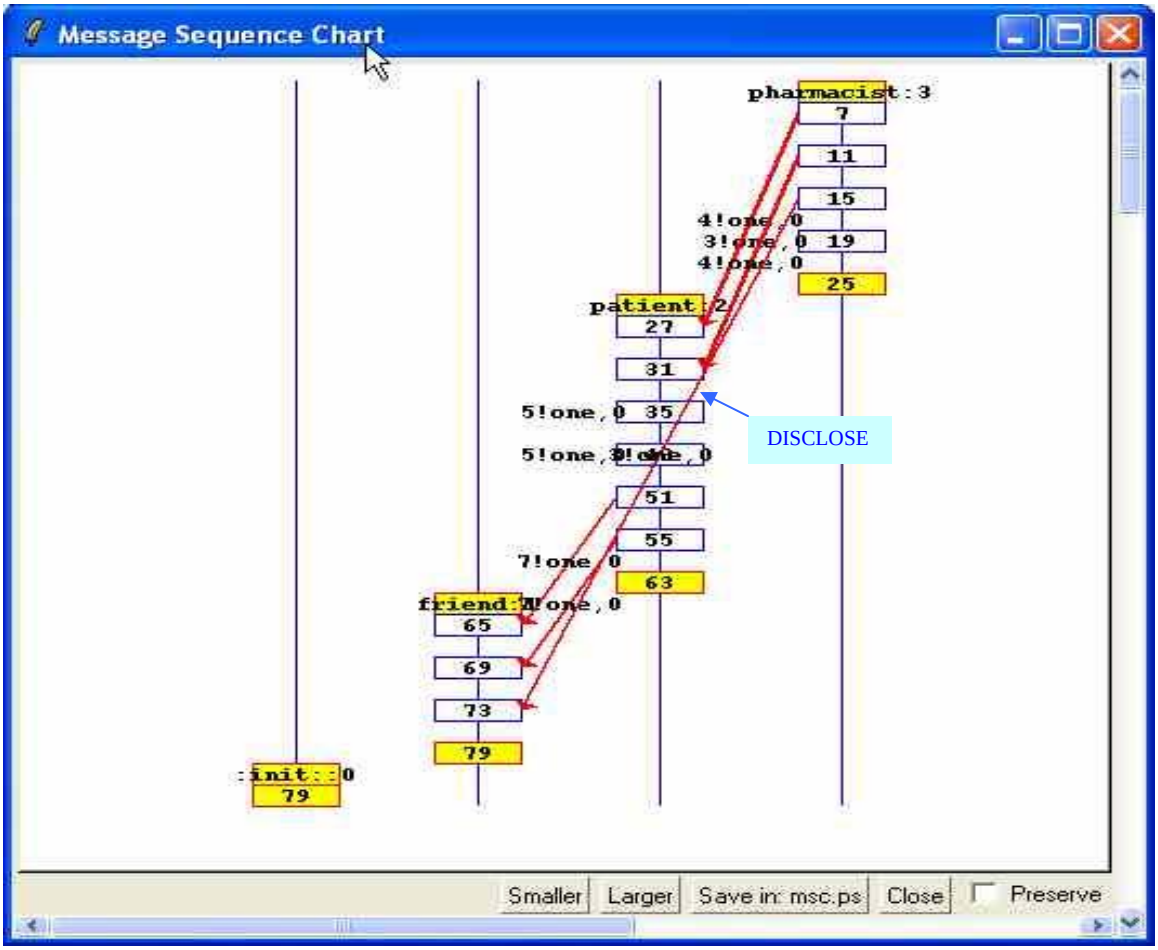
§ 164.510: Uses and disclosures requiring an opportunity for the individual to agree or to object.
[pp 24 of OCR/HIPAA Privacy/Security/Enforcement Regulation Text]
(b) Standard: uses and disclosures for involvement in the individual's care and notification purposes.
(1) *Permitted uses and disclosures.*
(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.
(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.
(2) *Uses and disclosures with the individual present.* 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.
(3) *Limited uses and disclosures when the individual is not present.* 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.

§ 164.510(b)(1)
[Positive Norm]
inrole(q, patient) ∧ inrole(p1, hcp) ∧ t∈phi ∧ inrole(p2, familyfriend[q]) ∧ send(p1, p2, t)

[Positive Norm]
inrole(q, patient) ∧ inrole(p1, hcp) ∧ t∈phi ∧ send(p1, p2, t) ∧ (!send(q, p1, deny-identification) S send(q, p1, identify-friend))

§ 164.510(b)(2)
[Negative Norm]
inrole(q, patient) ∧ inrole(p1, hcp) ∧ t∈phi ∧ available-sane-agrees(q) ∧ send(q, p1, object-disclosure[t])
→ □!send(p1, p2, t)

§ 164.510(b)(3)
[Positive Norm]
inrole(q, patient) ∧ inrole(p1, hcp) ∧ t∈phi ∧ !available-sane-authorize(q) ∧
uses-professional-judgment(p1) ∧ !send(p1, p2, t)



2. Your protected health information won't be transmitted to a third party who is not covered by HIPAA privacy rule
[] (HIPAA -> Desired Property) returns FALSE

a. Desired Property
inrole(p1, hcp) ∧ inrole(q, patient) ∧ t∈phi ∧ send(p1, p2, t) → incontext(p2, covered-entity)

b. HIPAA

§ 164.506 Uses and disclosures to carry out treatment, payment, or health care operations.
[pp 22of OCR/HIPAA Privacy/Security/Enforcement Regulation Text]
(c) *Implementation specifications: Treatment, payment, or health care operations.*
(1) A covered entity may use or disclose protected health information for its own treatment, payment, or health care operations.
(2) A covered entity may disclose protected health information for treatment activities of a health care provider.
(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.
(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
(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.

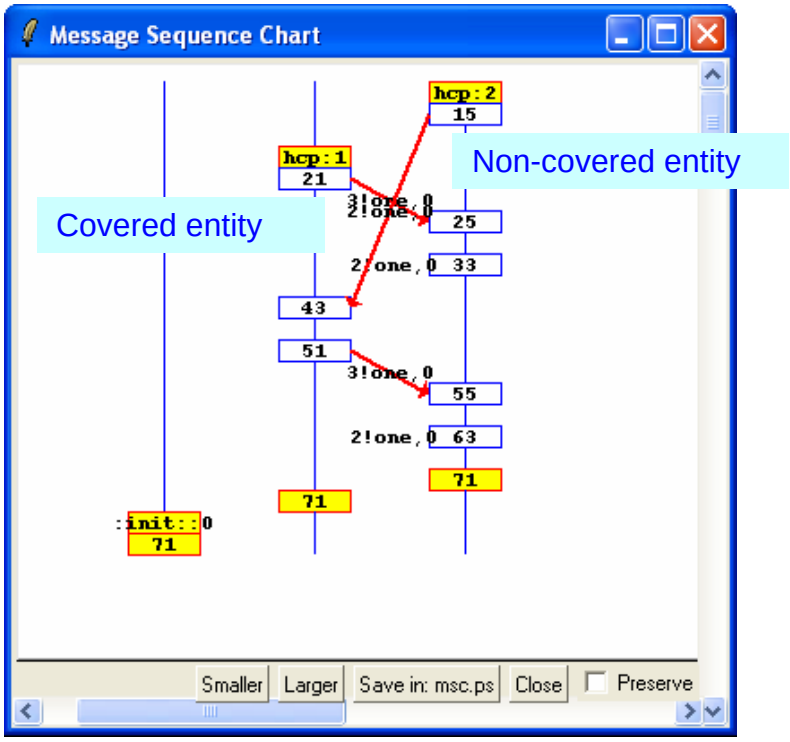
§ 164.506(c)(1)
[Positive Norm]
$inrole(p1, hcp) \wedge inrole(p2, hcp) \wedge t \in phi \wedge send(p1, p2, t) \wedge disclosure\text{-}for\text{-}TPO(p1, t)$

§ 164.506(c)(2)
[Positive Norm]
$inrole(p1, hcp) \wedge inrole(p2, hcp) \wedge t \in phi \wedge send(p1, p2, t) \wedge disclosure\text{-}for\text{-}T(p2, t)$

§ 164.506(c)(3)
[Positive Norm]
$inrole(p1, hcp) \wedge (inrole(p2, hcp) \vee incontext(p2, covered\text{-}entity)) \wedge t \in phi \wedge send(p1, p2, t) \wedge disclosure\text{-}for\text{-}P(p2, t)$

§ 164.506(c)(4)
[Positive Norm]
$inrole(p1, hcp) \wedge inrole(p2, hcp) \wedge inrole(q, patient) \wedge t \in phi \wedge has\text{-}relationship(q, p2) \wedge send(p1, p2, t) \wedge disclosure\text{-}for\text{-}TPO(p2, t)$

§ 164.506(c)(5)
[Positive Norm]
$inrole(p1, hcp) \wedge inrole(p2, hcp) \wedge t \in phi \wedge send(p1, p2, t) \wedge incontext(p1, covered\text{-}entity) \wedge incontext(p2, covered\text{-}entity) \wedge disclosure\text{-}for\text{-}O(p2, t)$



3. A doctor may not disclose a patient's record for TPO even though the patient has denied consent.
[] (HIPAA -> Desired Property) returns FALSE

a. Desired Property

inrole(q, patient) ∧ inrole(p1, hcp) ∧ t∈phi ∧ send(p1, p2, t) → *(!send(q, p1, deny-consent) S send (q, p1, consent))*

--- Remove Past Operators ---

inrole(q, patient) ∧ inrole(p1, hcp) ∧ t∈phi ∧ send(q, p1, deny-consent)) → *(!send(p1, p2, t) W send (q, p1, consent))*

b. HIPAA

> **§ 164.506 Uses and disclosures to carry out treatment, payment, or health care operations.**
> *[pp 22of OCR/HIPAA Privacy/Security/Enforcement Regulation Text]*
> (b) *Standard: Consent for uses and disclosures permitted.*
> (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.
> (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.

§164.506(b)(1) [Positive Norm]
inrole(q, patient) ∧ inrole(p1, hcp) ∧ t∈phi ∧
(<->send(p1, q, consent-request) ∨ !<->send(p1, q, consent-request)) ∧ send(p1, p2, t)

§164.506(b)(2) [Negative Norm]
inrole(q, patient) ∧ inrole(p1, hcp) ∧ t ∈ authorization-requiring-phi ∧ require-authorization(t) ∧ !<-> send(q,p1, authorization) → !send(p1,p2,t)