Two patterns for HIPAA regulations

Eduardo B. Fernandez[1] and Sergio Mujica[2]

1 Florida Atlantic University, Boca Raton, FL, USA
2 Escuela de Ingeniería, Universidad Finis Terrae, Santiago, Chile

Abstract
We present two patterns to describe rules of the Health Insurance Portability & Accountability Act (HIPAA). Regulations are legal documents and must be faithfully followed. For example, in the USA, HIPAA must be followed by institutions that handle medical records. Our patterns describe the Privacy Rule and the Security Rule of HIPAA. We intend to add later the remaining three rules. These rules are policies and as such they can be described through patterns to let developers of health-related software have a precise representation of these policies.

Keywords: Regulations, HIPAA, Security patterns, Software architecture

Introduction
Regulations are legal documents and must be faithfully followed. For example, in the USA, the Health Insurance Portability and Accountability Act (HIPAA) [Hip], must be followed by institutions that handle medical records. Regulations define sets of policies that can be conveniently represented as patterns. It is possible to convert methodologies to build secure systems such as [Fer13] into methodologies that also are compliant with specific regulations if we add to them a catalog of patterns that describe the regulation(s). We have started work on patterns for HIPAA. HIPAA has five rules that can be represented by patterns. We intend to write patterns for all of them and we have started from the first two. We have shown that incorporating regulations described as patterns into reference architectures we can generate applications that comply with these regulations [Fer14].

Even if possible, does it make sense to describe the rules (policies) of regulations as patterns? We believe that the answer is yes, they will be implemented in many systems so a precise description of their structure can be considered a pattern in our view. A regulation pattern is similar to a security pattern and follows the standard POSA template [Bus96]. The main difference is that a security pattern intends to neutralize a threat while a regulation pattern realizes one or more policies from a regulation. We have already described web services standards as patterns and showed its value [Fer12]. We know of only one other way to describe precisely HIPAA rules [Lam09], but this is a formal approach, hard for developers to apply in their work. Imprecise implementations of regulations may lead to lawsuits and may harm patients.

In this paper we present patters for:

The Privacy Rule of HIPAA--Describe accurately the policy that prescribes that health providers must notify individuals of the use of their health information.

The Security Rule of HIPAA--Define a set of security mechanisms to protect patient health information (PHI) that is held or transferred in electronic form. This rule complements the Privacy Rule by defining ways to protect its information.

We describe these patterns using a modified POSA template [Bus96] and our audience are software architects and developers involved with health-related software. These patterns will be part of a catalog of patterns for regulations. They have, of course, value on their own.

The Privacy Rule of HIPAA

Intent
Describe accurately the policy that prescribes that health providers must notify individuals of the use of their health information.

Example.
A software house decided to market software to help private medical clinics and health providers comply with HIPAA regulations. They found that the regulations themselves were not clear and it was hard for their developers to implement the rules in the regulation. The developers read the regulations and interpreted them in their own way. The final product was a failure because some of the regulations were not correctly implemented and resulted in lawsuits and misunderstandings that violated the regulations.

Context
Covered entities are defined as health care clearinghouses, employer sponsored health plans, health insurers, and medical service providers that engage in certain transactions. The Privacy Rule of HIPAA establishes that covered entities should notify individuals of uses of their *Protected Health Information* (PHI), i.e., health providers should notify patients of the uses of their medical information. PHI is any information about health status, provision of health care, or payment for health care that can be linked to a specific individual. The PHI includes any part of a patient's medical record or payment history. Covered entities must appoint a Privacy Official and a contact person responsible for receiving complaints and train all members of their workforce in procedures regarding PHI [Hip]. .HIPAA applies specifically in the USA but other countries have similar regulations to protect health information.

Problem
Regulations are legal documents and must be faithfully followed. HIPAA must be followed in the US to handle medical records. A patient who has a problem because this regulation is not properly applied to his medical information may sue the company handling his records. We need to be sure that any software we use implements the regulations precisely and faithfully.

The solution to the problem of accurate representation of regulations is affected by the following **forces:**

Notification—there must be an automatic way to notify users
Completeness—the rule applies to all the health information kept by a health provider.

Document realization—any documents prescribed by the rule must have an explicit representation.
Overseeing—. there must be a role in charge of verifying that the rules are applied

Solution
The notification obligation is intended to protect the privacy of patients by informing them of who has accessed their PHI. Explicit representation of the PHI for patients and its handling also helps prevent fraud and helps medical research. .

Structure
Figure 1 shows the representation in UML of the Privacy rule. A **Patient** has a **Protected Health Information (PHI),** which includes information such as her visits to a doctor and her payments. The PHI also includes the **Medical Record** of the patient. A **Covered Entity** can access the PHI (in different ways depending on the Covered Entity functions). **Privacy Official** represents an interface for this role such that a person in this role can verify that this regulation is being followed. **Privacy Information** includes additional or specific policies and procedures to enforce this regulation. Class **Obligation** reifies the policy of notification.

Dynamics
Figure 2 shows the use case: "Show a PHI of a patient to a non-covered entity". The Covered Entity allows the Police Department to access a patient record during a criminal investigation. After doing so, the Covered entity has the obligation to notify the Patient of this access.

Implementation
There are no prescribed system implementations of this rule. However,there are exceptions to the rule:

***Permitted Uses and Disclosures*.** A covered entity is permitted to use and disclose PHI, without an individual's authorization, for the following purposes or situations [Pri]: (1) To the Individual (unless required for access or accounting of disclosures); (2) Treatment, Payment, and Health Care Operations; (3) Opportunity to Agree or Object; (4) Incident to an otherwise permitted use and disclosure; (5) Public Interest and Benefit Activities; and (6) Limited Data Set for the purposes of research, public health or health care operations.

Known uses
The Florida Department of Health (FDOH) is implementing a system following HIPAA rules [Hil13].

Example resolved
Now the software house has a precise description of the information and procedures that must be included in their software products.

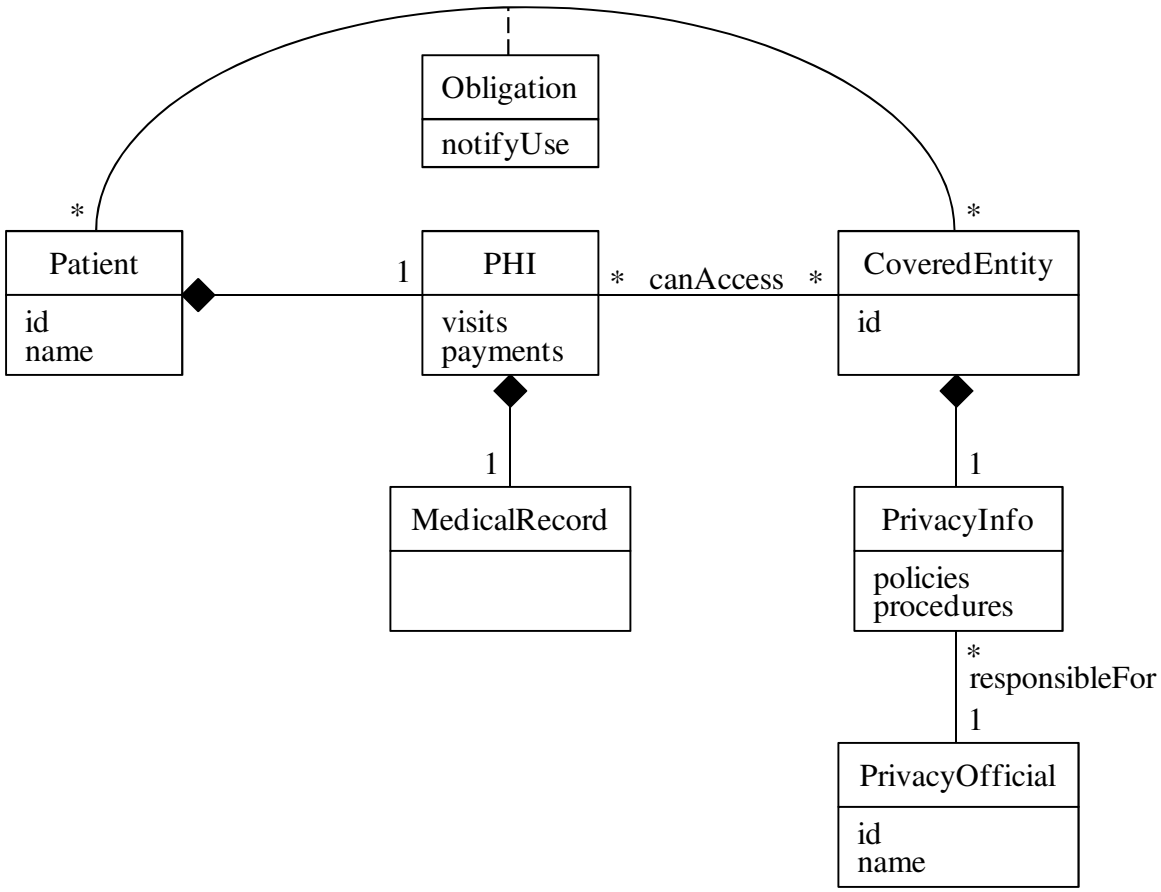

Figure 1. Class diagram for HIPAA's Privacy rule

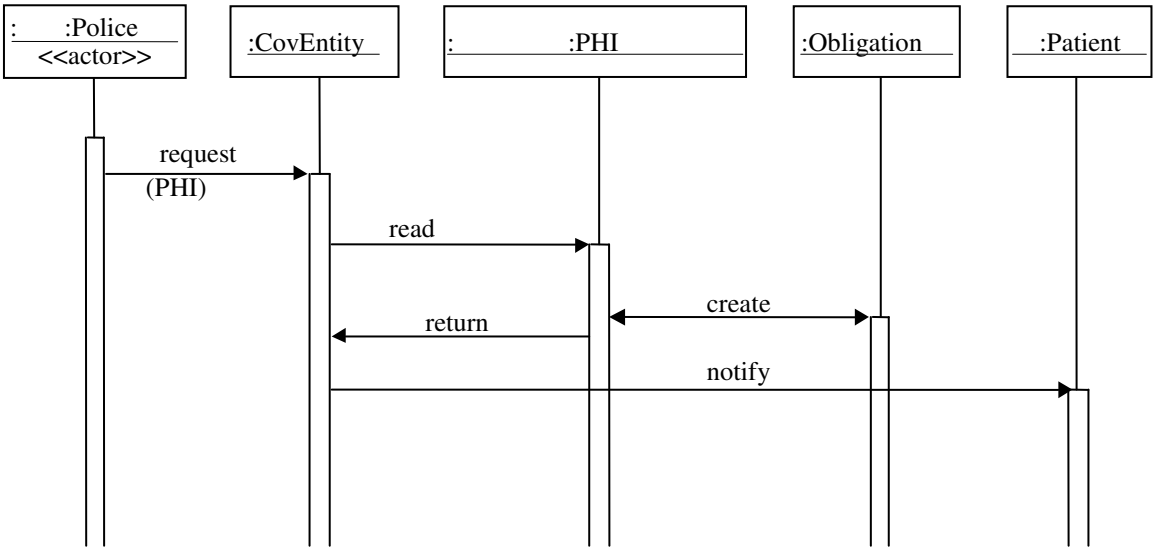

Figure 2. Use case: show a PHI od a patient to a non-covered entity

Consequences
This pattern has the following advantages:

- ***Completeness*—**the pattern describes explicitly all the requirements of the rule**.**
- ***Document realization***—Every document mentioned in the rule has a explicit representation (a class0 in the model.
- ***Notification*—**the model includes an obligation to notify users
- ***Overseeing***—. The Privacy Official is a role in charge of verifying that the rules are applied to the Privacy Information.

Liabilities include some extra overhead to keep all the extra information and for notification.

See also
[Sor05] describes a common form of medical records.

The Security Rule of HIPAA

Intent
Define a set of security mechanisms to protect patient health information (PHI) that is held or transferred in electronic form. This rule complements the Privacy Rule by defining ways to protect its information.

Example.
A software house decided to market software to help private medical clinics and health providers comply with HIPAA regulations. Using the previous pattern they were able to get a good description of the requirements of the Privacy Rule. However, they need to build in their products appropriate security mechanisms or the privacy recommendations will not be able to be enforced when their product is deployed.

Context
Today, providers are using clinical applications such as computerized physician order entry (CPOE) systems, electronic health records (EHR), and radiology, pharmacy, and laboratory systems. Health plans are providing access to claims and care management, as well as member self-service applications. While this means that the medical workforce can be more mobile and efficient (i.e., physicians can check patient records and test results from wherever they are), the rise in the adoption rate of these technologies increases the potential security risks for the PHI.

Problem
Regulations are legal documents and must be faithfully followed. HIPAA must be followed in the US to handle medical records. A patient who has a problem because this regulation is not properly applied to his medical information may sue the company handling his records. We need to protect the medical information of all patients.

Forces
Completeness—the rule applies to all the health information kept by a health provider.
Security—there must be a security mechanism that controls the proper ue of this information; otherwise, illegal accesses cannot be stopped.
Document protection—any documents prescribed by the rule must have an appropriate protection of its contents.
Notification—there must be an automatic way to notify users

Solution
The Security Rule requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI. Specifically, covered entities must:

- Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
- Identify and protect against reasonably anticipated threats to the security or integrity of the information;
- Protect against reasonably anticipated, impermissible uses or disclosures; and
- Ensure compliance by their workforce.

The covered entities must perform risk analysis and apply the appropriate defenses. A method such as [Bra08] could be used to enumerate threats and define the corresponding defenses.

Structure
Figure 3 shows the representation in UML of the Security Rule. A **Patient** has a **Protected Health Information (PHI),** which includes information such as her visits to a doctor and her payments. The PHI also includes the **Medical Record** of the patient. A **Covered Entity** can access the PHI (in different ways depending on the Covered Entity functions). The model shows two instantiations of the Role-Based Access control pattern to define rights of Covered Entities with respect to PHIs and rights of Patients with respect to their PHIs. A Security Logger/Auditor pattern keeps trach of all the PHIs accesses so that patients can be properly notified of accesses by non-covered entities.

Dynamics
Figure 4 shows the sequence diagram for the use case “Access a PHI in a Covered Entity”. A doctor requests access to a PHI of a patient that belongs to a Covered Entity. The PHI is returned to her and the access is logged.

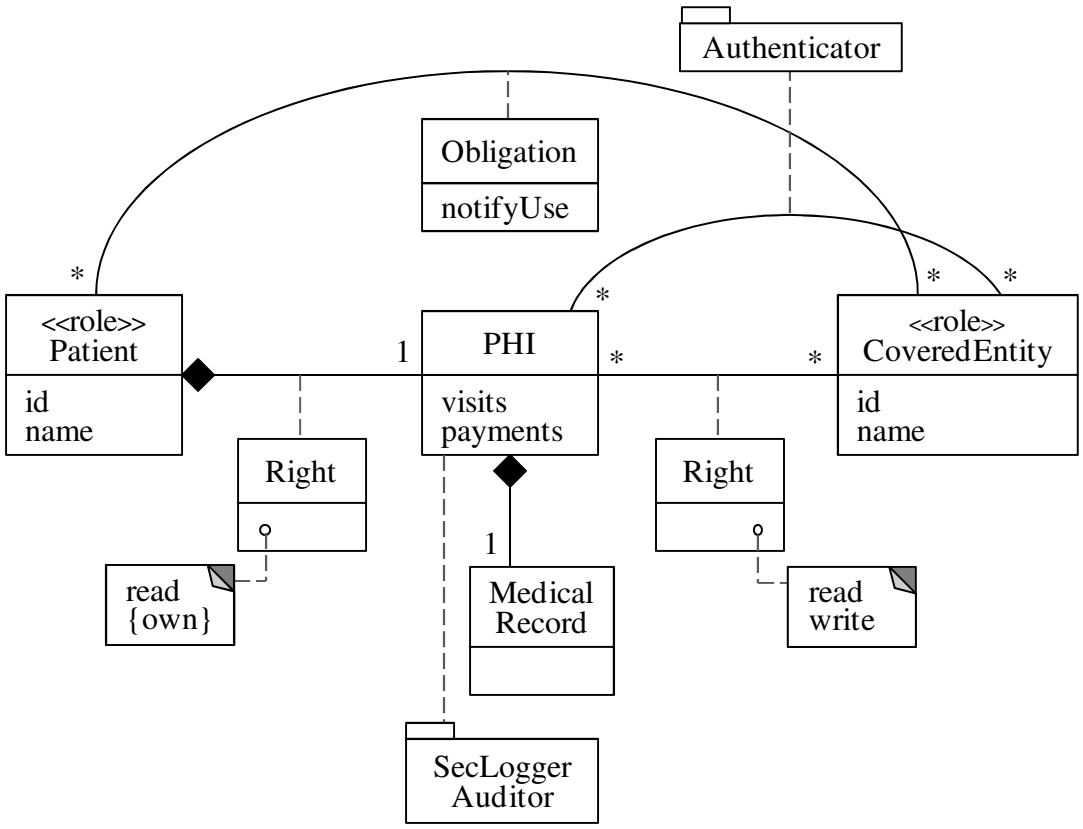

Figure 3. Class diagram for HIPAA's Security Rule

Implementation

The Office for Civil Rights HHS has responsibility for enforcing the Privacy and Security Rules with voluntary compliance activities and civil money penalties.

Given that the health care marketplace is diverse, the Security Rule is designed to be flexible and scalable so a covered entity can implement policies, procedures, and technologies that are appropriate for the entity's particular size, organizational structure, and risks to consumers' e-PHI.

Therefore, when a covered entity is deciding which security measures to use, the Rule does not dictate those measures but requires the covered entity to consider:

- Its size, complexity, and capabilities,
- Its technical, hardware, and software infrastructure,
- The costs of security measures, and
- The likelihood and possible impact of potential risks to e-PHI.

A covered entity must adopt reasonable and appropriate policies and procedures to comply with the provisions of the Security Rule. A covered entity must maintain, until six years after the later

of the date of their creation or last effective date, written security policies and procedures and written records of required actions, activities or assessments.

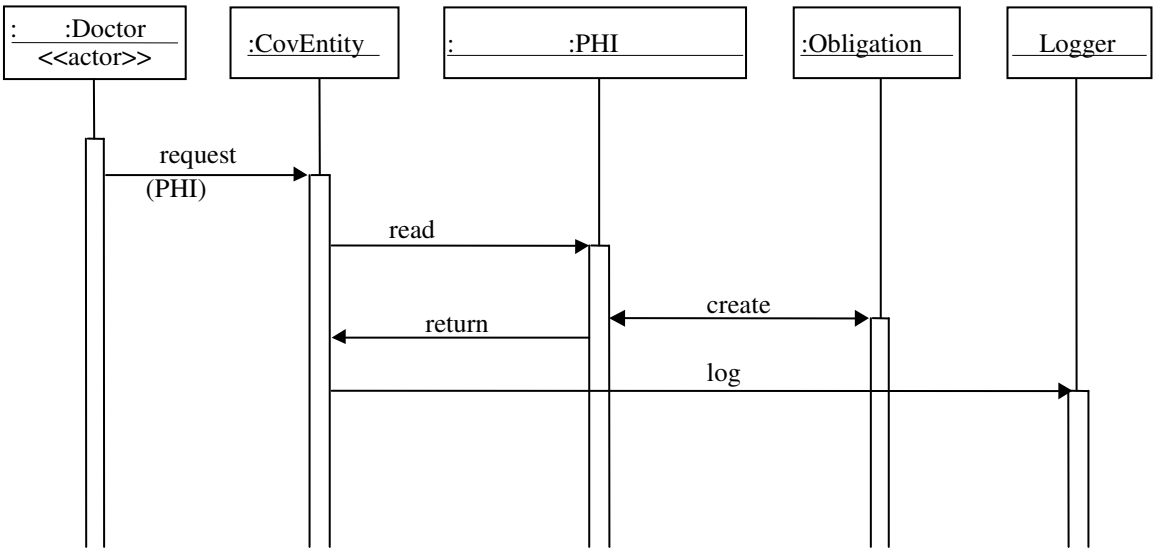

Figure 4. Use case "Access a PHI in a Covered Entity"

Known uses

- The Florida Department of Health (FDOH) is implementing a system following HIPAA rules [Hil13].

- Modernizing Medicine is a cloud-based company that handles medical records for medical practices and follows these regulations [Mod].

Example resolved

This pattern provides the company developers a guide about where to add security mechanisms in their products so that the privacy requirements are always enforced.

Consequences

The advantages of this pattern include:

- ***Completeness—***the pattern describes explicitly all the requirements of the rule**.**
- ***Security—***Authentication and RBAC Authorization control access to the PHI.
- ***Document protection***—Every document mentioned in the rule has a explicit representation (a class) in the model and it has a corresponding protection of its content..
- ***Notification—***the model includes an obligation to notify users

Liabilities include the extra complexity and overhead of the security mechanisms as well as their acquisition and operational costs.

See also

- Authenticator [Fer13]
- Authorizer [Fer13]--Describe who is authorized to access specific resources in a system, in an environment in which we have resources whose access needs to be controlled. It indicates for each active entity, which resources it can access, and what it can do with them.
- Security Logger/Auditor [Fer13]--How can we keep track of user's actions in order to determine who did what and when? Log all security-sensitive actions performed by users and provide controlled access to records for Audit purposes.
- Secure Channel [Fer13].

Conclusions

HIPAA is an important health regulation in the USA and variants of it have been adopted also in other countries. Any software dealing with health information and any institution dealing with medical records must comply with its rules. We have started from its two most fundamental rules and we will add the rest of the rules in future work. Additional future work is finding patterns that encompass more than one type of regulation; for example we have found analogies between medical rules and financial rules.

Acknowledgements

We thank Prof. Hironori Washizaki for his useful comments that isignificantly improved the paper. Our shepherd Prof. Hongyu Zhang provided three useful references.

References

[Bus96] F. Buschmann, R. Meunier, H. Rohnert, P. Sommerland, and M.Stal, *Pattern- oriented software architecture*, Wiley 1996.

[Fer12] E.B.Fernandez, O.Ajaj, I.Buckley, N.Delessy-Gassant, K.Hashizume, M.M. Larrondo-Petrie, " A Survey of Patterns for Web Services Security and Reliability Standards". *Future Internet* 2012, *4*, 430-450. http://www.mdpi.com/1999-5903/4/2/430/

[Fer13] E. B. Fernandez, *Security patterns in practice - Designing secure architectures using software patterns*. Wiley Series on Software Design Patterns, Wiley 2013.

[Fer14] E.B.Fernandez and Sergio Mujica, "From domain models to secure and compliant applications", submitted for publication

[Gar12] Syeda U. Gardazi, Arshad A. Shahid, and Christine Salimbene. 2012. "HIPAA and QMS Based Architectural Requirements to Cope with the OCR Audit Program". In Proceedings of the 2012 Third FTRA International Conference on Mobile, Ubiquitous, and Intelligent Computing(MUSIC '12). IEEE Computer Society, Washington, DC, USA, 246-253.

[Hil13] G. Hilgenberg, "ITSW and its Role in Emerging Technologies at the Department of Health", report for a course at Florida Atlantic University, Dec. 2013.

[Hip] Health Insurance Portability and Accountability Act, http://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act

[Lam09] Peifung E. Lam, John C. Mitchell, Sharada Sundaram, “A Formalization of HIPAA for a Medical Messaging System”, Trust, Privacy and Security in Digital Business, *Lecture Notes in Computer Science*, Volume 5695, 2009, 73-85

[Mod] Modernizing Medicine, http://www.modmed.com/

[Nah08] Nahra, K.J., "HIPAA Security Enforcement Is Here," *IEEE Security & Privacy*, vol.6, no.6, Nov.-Dec. 2008, 70-72

[Pri] U.S. Dept. of Health & Human Services, Summary of the HIPAA Privacy Rule, http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/

[SeR] Summary of the HIPAA Security Rule http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html

[Sor05] T. Sorgente, E.B.Fernandez, and M.M. Larrondo-Petrie, "The SOAP pattern for medical charts", in *Proceedings of the 12th Pattern Languages of Programs Conference (PLoP2005)*, Monticello, Illinois, 7-10 September 2005. http://hillside.net/plop/2005/proceedings/PLoP2005_tsorgente0_1.pdf