REQUIREMENTS ENGINEERING TO AUDIT PRIVACY ISSUES IN MEDICAL AND HEALTH SOFTWARE

Miguel A. Martinez, Ambrosio Toval and Manuel Campos
Computer and Systems Departament, University of Murcia, Campus de Espinardo (Murcia), Spain

Keywords: Personal Data Protection, Audit, Requirements Engineering, Privacy, Reuse.

Abstract: In recent years, there has been a growing interest to guarantee that health organizations make a suitable treatment and protection of the personal data with which they deal in their daily activity. The privacy of personal data is regulated by law in many countries and is considered an important issue in a number of Quality Standards. This paper presents a systematic method to make an audit of the privacy in health sector software based on Requirements Engineering (RE). The aplication and validation of the method is ilustrated in a operative tool of report and clinical record management in the Intensive Care Unit (ICU) in a hospital.

1 INTRODUCTION

The Information Systems (IS) Audit is a discipline whose practice has increased considerably during the last few years. IS Audit is defined as the systematic process of gathering, grouping and evaluating evidences to determine whether an IS safeguards the assets, whether it maintains the integrity of the data, whether it effectively carries out the aims of the organization, and whether it uses the resources efficiently (Weber, 1988). A special type of audit within this discipline is the software audit. The purpose of auditing software is to verify that the software accomplishes the requirements (both functional and non-functional). A security audit is defined as "*an independent revision and examination of the registries and activities of a system in order to verify if the controls of the system are adapted to guarantee the fulfilment of the established policy and the operative procedures, to detect security problems, and to recommend possible changes in the control policy and procedures*" (ISO/IEC-7498-2:1989, 1989). A security audit can include many aspects, such as the protection level of the facilities or people, but this paper we will focus on the security related to data and information (privacy) of personal nature, that is a crucial aspect in the security of clinical IS and clinical software. More concretely, in this work we define a method to audit the aspects related to the privacy on clinical software, and we illustrate its use by means of an application to software for Electronic Clinical Record and report management for an Intensive Care Unit (ICU) that is being deployed in a hospital.

The method used to carry out the audit is based on SIREN, a general method of Requirements Engineering (RE) based on standards of this discipline (IEEE-Std.830-1998, 1998; IEEE-Std.1233-1998, 1998) and that is focused on the reusability of requirements. SIREN (*SImple REuse of software requiremeNts*) is a practical proposal to select and to specify the requirements of a software system. The key elements in SIREN are a spiral process model, requirements document templates and a reusable requirements repository which is organized by catalogs. The SIREN catalog related to privacy aspects is called PDP (Personal Data Protection) (Toval et al., 2002b).

At the moment, SIREN can be applied in four different ways:

1. As a method for RE (Toval et al., 2002a; Toval et al., 2002b) so that the fulfilment of the applicable norm (for example, on security and PDP) can be guaranteed from the beginning of the development of IS, by using suitable catalogs.
2. As guide and support to conduct an audit for determining the existence of security controls and its degree of fulfilment in an organization who deals with sensible data (Martinez et al., 2006).
3. As a method for auditing software (either developed by the organization or acquired) in operation.
4. As a method of consulting in the acquisition of

A. Martinez M., Toval A. and Campos M. (2008).
REQUIREMENTS ENGINEERING TO AUDIT PRIVACY ISSUES IN MEDICAL AND HEALTH SOFTWARE.
In *Proceedings of the First International Conference on Health Informatics*, pages 74-81

new software, so that it can be guaranteed that this software satisfies the expected level of security.

In this paper, we show a specialization of the method presented in (Martinez et al., 2006) that can be used in applications 3 and 4, that is, as a method for auditing and consulting. In order to conduct the audit in a simple and agile way, it is necessary to define a new method for auditing software that fulfils the standards of different disciplines, such as IEEE830 (IEEE-Std.830-1998, 1998) and CobiT (Control for Objectives Information Technologies) (CobiT, 2005), as well as the different laws in security and protection of personal data.

The rest of the paper is organized as follows: Section 2 describes briefly the method used for auditing. In Section 3, we describe the phase of practical application in our case study. In Section 4, some related works are presented and compared with our proposal. Section 5 describes the lessons learned after the application of the method proposed in the practical case. Finally, we enumerate the conclusions and the future work in this line.

2 A METHOD FOR AUDITING SOFTWARE BASED ON SIREN

The method proposed belongs to the scope of the Spanish legislation (LOPD, 1999; SMR, 1999), which is an adaptation of the European Union legislation (Directive-1995/46/CE, 1995). Nevertheless, the proposal is easily generalizable since this legislation has been adapted in a similar way by other European countries. For example, in Italy, the law that regulates the personal data protection is the *Italian Law 196*, of 30 of June of 2003, in Germany the counterpart is the *Federal Law of Data Protection* (BDSG), and in the United Kingdom, it is the *Data Protection Act* of 24 from October of 1998. In the United States, there is a sectorial conception of the law and has as source a mixture of legislation, regulation and self-regulation. Rights of information privacy in a variety of sectorial laws have been granted, like for example the law *The Privacy Act* of 1974, the *Fair Credit Reporting Act* of 1970, or the *Electronic Communications Privacy Act* of 1986.

In addition, our method has a direct correspondence with the referential frame of CobiT in its more recent version (CobiT, 2005), which is widely accepted by the international community of IS auditors. With this proposal, we intend to help to fulfil the CobiT Control Objectives that deal with privacy aspects, since the identification and verification of the fulfilment of the requirements related to these aspects is facilitated by the use of the requirements of the SIREN PDP catalog.

The method for auditing software based on SIREN contemplates the following phases (see Figure 1):

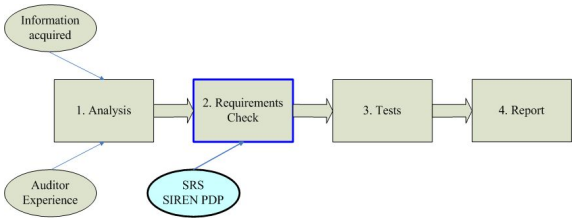

Figure 1: Phases of the method for auditing data protection in software.

Phase 1. - Analysis of the situation of the software. This phase consists of a first interview for establishing the scope of the audit so that an initial budget can be elaborated. The objective is to gather all kind of information about the treatment of the data used by the software. The information comes from two sources: on the one hand, the information facilitated by the development team of the software (manual of use, UML diagrams, etc.), and, on the other hand, from the experience acquired by the auditor after testing the software.

Phase 2. - Requirements verification with the SRS (Software Requirements Specifications) of the SIREN PDP catalog. The auditor verifies the fulfilment or breach of the requirements contained in the SRS of the catalog. Personnel responsible in the organization should support and facilitate, as much as possible, this verification. The verification consists of choosing those requirements of the SIREN PDP catalog that can be applied to the organization and of verifying whether they are fulfilled or not in the software. For example, if the software is going to be used in an organization to whom a high level of data protection is going to be demanded, according to the SMR (Security Measures Regulation), the auditor will extract from the SRS those requirements necessary to reach this protection level and will verify if these requirements are present in the tool. This extraction or filter of requirements of the catalog is possible thanks to the use of the meta-information associated to each requirement (in this case, through the attribute ”security level”).

Phase 3. - Execution tests. In this phase, the auditor must check the proper operation of the software once

it has been integrated in the system. In case that some of the evaluated measures are not fulfilled in the tool, the auditor must describe the risks that exist in the IS of the organization where the software is going to be used. In order to perform the tests, the *Software Test Specification* (STS) of the SIREN PDP catalog will be used. In this way, any person (even with little experience) could make the tests systematically.

Phase 4. - Preparation and writing of the final report. The product of the audit is a final report where all aspects from the evaluation are written. At least the report will have the following information:

- *Situation*: which describes briefly the resultant weakness after the analysis carried out in the software tool.
- *Threats*: where the possible risks which the software tool are exposed to, are enumerated.
- *Recommendations and action plans* proposed to the development team.

The aim of the SRS used for the audit is to gather the requirements about the functionality of the system, external interfaces, performance, design restrictions and attributes of software (portability, maintenance, security, availability and reliability). This specification of requirements has been made in agreement with the IEEE 830-98 Standard that is responsible for defining the characteristics and contents of a good software requirements specification.

A particular characteristic of the SIREN method is that in the requirements specification there exist what we call *parameterized requirements*. A parameterized requirement contains some parts that must be adapted to each application or system when they are reused in a concrete project. For example, the following requirement extracted from the SIREN PDP catalog "*the system will not conserve the data, once cancelled, so that the identification of the subject interested is not allowed during a period no inferior to [time in months] on the basis of which they had been successfully obtained or registered*", gives the analyst the possibility of choosing a period of suitable time to the necessities of the concrete project.

The SRS of the PDP catalog used for the audit presented in this work is currently composed by 48 requirements. In addition to the statement, each requirement of the catalog contains meta-information (attributes with information about each requirement) that enriches the requirement. Among the 18 attributes that have been defined up to now, we can point out the following ones: *source, exceptions, security level, motivation and fulfilment*.

3 CASE STUDY

In this work, we present a concrete application of the method to a software tool for clinical record management that deal with personal data and, therefore, needs a high protection level in its data. The tool used is called CH4 and has been developed by the Artificial Intelligence and Knowledge Engineering research group of the University of Murcia and is being deployed at the moment in the ICU of the *Hospital Universitary of Getafe (Madrid)*.

With the objective of taking advantage of the case study as an experience to validate the proposed method, we have decided to use a method of qualitative investigation in software engineering, denominated Action-Research (Baskerville, 1999) (the use of this method will be explained in Section 4.1).

CH4 has the aim of managing the clinical record as much as facilitating the daily work and communication between medical staff in an ICU. CH4 is centered in the process of patient management along their stay in the ICU by registering personal and clinical data, and allowing the staff to automatically generate reports. In this way, a documentary database with admittance, evolution and discharge report is created and available for its later access.

In the development of this report oriented tool, three scenarios have been considered: the admittance, the daily evolution and the discharge. In each one of them, data relative to tests (physical, complementary examinations, analytical explorations, classifications, ...) treatments and diagnoses can be introduced. The tool includes facilities, as the treatment profiles, to easy the management of the most habitual cases. Each diagnosis or problem can be related to the concrete results of tests, to the treatments or even to other problems, allowing in this way a traceability of all the aspects defined for a patient.

3.1 Design of the Experiment

The application of Action-Research gives rise to a cyclical process in which the different implied parts participate, examining the existing situation (which they consider of some problematic way) with the objective to change it and to improve it (Wadsworth, 1998). Action-Research is one of the few approaches valid to study the effects of specific alterations in development methodologies and maintenance of systems in human organizations (Baskerville and Wood-Harper, 1996). Following the terminology of Action-Research, in this case study the following participants are considered:

- The "researcher" is the research group in Software

Engineering of the University of Murcia.

- The "researched" object is the application of the PDP catalog in a method for auditing a software tool for clinical record management that needs a high protection level in the files of personal data that handles.
- The "critical reference group" (CRG), in other words, the one for which the research is carried out, is formed by the members of the development team of the tool, is the research group of Artificial Intelligence and Knowledge Engineering of the University of Murcia. According to Action-Research, the CRG must also participate in the research process, although less actively than the researcher.
- The "stakeholders" will be all those organizations who can benefit from the results of the research, in particular, the members themselves of the CRG and, in general, other groups whose development activities are similar to those of the tool audited.

In this research, a participative application of Action-Research has been made, in which the CRG puts into practice the recommendations made by the researcher, and shares its effects and results.

3.2 Audit of Software for Clinical Record Management in an ICU

Within IS Audit, we distinguished two basic types of audit: system audits and software audits. The first one corresponds to verifications on the own IS (an example of real application using method SIREN can be seen in (Martinez et al., 2006)). The second type is centered in verifying that the software tools accomplish to the requirements, both functional and non-functional (norms, laws, etc.). This work belongs to the second type, where the tool audited is a practical case of a software tool related to the clinical sector. We have used the SRS of the SIREN PDP catalog as guide to make the audit process shown in Figure 1.

After analyzing the information obtained in the different interviews with the development team of the tool made in Phase 1 of the audit, and after the test of the tool made by the auditor, we pass to Phase 2. Since we have at our disposal the SRS of SIREN PDP catalog, only two meetings were necessary to complete this phase. In these meetings, the fulfilment or breach of the requirements of SIREN PDP catalog has been checked one by one in the tool.

Once the two first phases of the audit method have been completed, the pertinent tests were made to verify the operation of the tool once it has been integrated in the IS.

Table 1: Results of the audit of the software.

	Software requirement
Fulfilled	22
Not fulfilled	10
Undetermined	16

Finally, all the results of the evaluation were written in a final report. This final report was given to the development team and they included in the tool the improvements and safety measures proposed in the audit. It is important to emphasize that implantation of such measures is not part of the audit, since a basic principle of the audits is that these finalize with conclusions and possible solutions, but never get to implement solutions as part of the audit.

In this way, after maintaining several interviews with the development team of the tool and the person in charge of security of the system, we have collected the data shown in Table 1.

According to the results of the Table 1, we see that the tool fulfils 45.8% of the referring requirements to the SRS of the SIREN PDP catalog. If we do not take into account the requirements that can not be applied to this tool (those marking like undetermined), a fulfilment of 68.7% with respect to the SRS of SIREN PDP catalog is obtained.

Some examples of requirements of the SIREN PDP catalog that were not fulfilled in the audited tool are the following ones:

- SRSL2. *The application will warn the user that a password needs to be changed.*
- SRSL6. *The [identification procedure] and [authentication procedure] will limit the possibility of repeatedly trying a non-authorized access to the application.*
- SRSL9. *The subsystem implementing the [identification procedure] and [authentication procedure], or other system related to this one, will log all accesses to the application. The log will consist of: user identification, timestamp of the access, file accessed, access type, and the result of the access.*
- SRSL14. *The application will allow the cancellation of the registered personal data (within the ten following days to its request by the interested part). The data will be accessible only by Public Administration and Courts for the investigation of possible responsibilities due to the treatment during the term of prescription of these responsibilities.*

The breach of these requirements is caused by diverse reasons. For example, requirement SRSL2 is

not fulfilled since the application did not provide a control to automatically warn the users about the necessity of changing the passwords. The breach of requirement SRSL6 put in serious danger the security of the application, because a user without permissions granted in the application could try to access many times; instead of only closing the session if an attempt of no authorized access takes place, the user login must be blocked and the attempts of no authorized access must be registered. Requirement SRSL9 is breached since the application did not consider registering the access information; as a solution, we proposed to use the database and application logging facilities to store the user accesses. Finally, requirement SRSL14 is not fulfilled since the application eliminates the data completely when a cancellation is required; instead of that, the data should be marked as unavailable or stored in a temporary database so that could be accessed in case they are required by the Public Administration.

4 RELATED WORK

In this section, we make a review of the most outstanding papers related to our proposal. In order to facilitate its reading, we have organized these works by topics, according to the essential related aspect treated. These topics are: 1) Personal data protection audits applied to the health sector; 2) Software tools audits; 3) Principles of the data protection in the European Union; 4) RE applied to the security field.

4.1 Personal Data Protection Audits Applied to the Health Sector

In (Sandhu and Samarati, 1996), an introduction to the personal data audit is provided, emphasizing its importance in the organizations that deal with them. Here, audit is understood like the process that gathers data on the system activities to analyze them in search of security violations. In (Hughes, 2005), the authors make a study about the relations between audits and research methods applied to the health sector of the United Kingdom. More concretely they apply Action-Research, which is a method with a special relevance in the health sector, where there is an important social factor. Nevertheless, in these papers, the approach is different from ours, since they do not audit a specific tool but the stored personal data in a system, and because neither application to a study case appears, nor the specific phases of an audit process are distinguished.

4.2 Software Tools Audits

Some of the software audit tools (in general, not only of the health sector) more used are GASP and WebCensus, both available in trial version in the BSA (*Business Software Alliance*) website[1], that is the main organization dedicated to the development of legal and safe computer science. These tools allow the auditors to identify and to track licensed and unlicensed software installed in a computer. Both tools are easy to use (WebCensus can be run through Web, without requiring installation by the user) and their high degree of accuracy has converted them in audit tools standard in numerous companies and governmental bureau worldwide. These tools have a different approach from the methodology that we propose, since they exclusively are limited to make a testing of the software installed in a system, contributing data related to the licenses and manufacturers, but they do not cover in any way the audit of software specific concerns (functional or non-functional requirements).

4.3 Principles of the Data Protection in the European Union

In (Van der Haak et al., 2003) and (Massacci et al., 2005), two practical applications about the use of personal data protection law in different European countries (concretely, Germany and Italy) are described. The first paper focuses on the identification of specific legal requirements related to data security and data protection of patients included in electronic clinical records. It is based on the set of German laws on data protection. The second paper presents a practical case of the application of a RE methodology for the fulfilment of the Italian legislation in privacy and data protection.

In these papers, authors do not provide the requirements engineers with a PDP requirements catalog (or similar) related to data privacy in a easily understandable language. So, the application of the data protection law in IS becomes a more tedious and difficult task for the requirements engineer.

The PDP requirements catalog that we have used (and improved) in this paper, is valid, with slight modifications, in any country of the European Union, since it is based on, among others, (Directive-1995/46/CE, 1995) and on (Directive-2002/58/CE, 2002). As (Lusignan et al., 2006) exposes, these directives are the base of the privacy laws of any European Union country. The authors show a table with the chronological order of the different treaties the

[1] www.bsa.org

fundamental principles of personal data protection of the European Union, and another table with a comparison of these principles (including general principles of the ethics in health computer systems).

4.4 Requirements Engineering applied to the Security Field

In the line of RE, we draw attention to the work by Firesmith (Firesmith, 2003), which provides examples and directives for requirements engineers to specify suitably security requirements. The different types of security requirements are identified and defined, among which privacy, security audit and physical protection requirements are highlighted. (Olvingson et al., 2002) presents a minimal data set for requirements elicitation in the area of public health. This minimal data set is a data collection that supports the elicitation of users' voices that later will constitute the foundation on which to identify the true requirements and describes the problems found by health professionals in their daily activities in countries like Sweden and the United States. Thus, it is possible to prioritize the requirements in an early phase of the construction of the system, e.g. the RE phase, and thus capture the most important characteristics to be implemented in IS. In these two papers, proposals are made considering thinking only RE and without following any RE methodology. On the contrary, we have followed the SIREN methodology and made a proposal for conduct audits.

In contrast to with the works described previously, our paper offers an integrated and repeatable systematic method to make an audit of software tools based on international standards of audit (CobiT) and good practices of Software Engineering (SIREN and international standards of RE). This method has been validated in a real study case where personal data are treated. In this way, our work complements other current proposals in the audit area but is new because allows the auditor to verify the fulfilment of privacy laws in software tools which deal with personal data.

5 LESSONS LEARNED

After carrying out this work we can identify three main lessons learned of our experience as software tools auditors.

On the one hand, this type of audits supposes a decisive aid to improve the used tools so that they adjust to the norms used as base; for example, in this case, the norms are the personal data protection laws. On the other hand, we have realized that thanks to the existence of a previous requirements catalog, we have been able to reduce the time dedicated to meetings and other activities of the audit. The interviews with the development team and board of directors of the organization (usually with very just a short time available) can be focused and guided directly to the crucial points that concern the audit.

Finally, we have detected weak points in the requirements catalog used in the audit. The inconsistencies consist fundamentally of the existence of ambiguities in the writing of certain requirements, which impede to the auditor team to make a firm decision on his fulfilment or breach in the software tool.

In relation to this last point, in addition to being able to detect what requirements were fulfilled or not in the current version of the developed tool, and thanks to the feedback obtained from the development team of the audit tool, ambiguous requirements and bad-written requirements in the SRS of the SIREN PDP catalog have been identified during the audit.

Of the 48 requirements that composed the SRS of the SIREN PDP catalog, 7 of them were identified by the development team of the audit tool, like candidates to a possible modification since they were not clear and precise enough. Some examples of these requirements, along with its corresponding improvement, are showed next:

SRSL2-Old. *The software will have to warn that a password needs to be changed.*

SRSL2-New. *In case that the authentication mechanism is based on the existence of passwords, the software will warn that a password needs to be changed, once finished the validity period set to [time in days].*

SRSL5-Old. *The software will allow that the Information Systems and data processing facilities can be subjected to an internal or external audit, at least every two years.*

SRSL5-New. *As much as every two years, the software will warn of the need to make an audit (internal or external) of the Information Systems and data processing facilities to verify the fulfilment of the Security Measures Regulations.*

SRSL26-Old. *The software will allow the people in charge of treatments of public and private ownership, as well as the organizations in which they group themselves, to formulate codes of ethics.*

SRSL26-New. In this case the requirement remains equal, it is necessary to add the following additional information in the attribute "*Rationale*" of the requirement: *The aim of codes of ethics is to establish the conditions of organization, operating conditions, applicable procedures, norms of security of the surroundings, use and obligations of the software and*

hardware implied in the treatment and use of the personal information, as well as the guarantees, in its scope, for the exercise of the people rights and its development norms.

6 CONCLUSIONS AND FURTHER WORK

Finally, we show the most important conclusions, obtained after carrying out this research:

- A systematic method has been extended to make a data protection audit to a software tool which deals with specially protected data. More specifically, we have applied the method to audit a tool for clinical record management in an ICU at a hospital that deals with sensible data.
- With the application of the proposed method, we helped to adapt the tool audited to the security measures and to the regulations demanded by law.
- An improvement of the PDP requirements catalog has been obtained (Toval et al., 2002b), which corresponds with one of the SIREN method phases. In this sense, the quality of the existing requirements has been improved: some requirements, identified as necessary or advisable, have been inserted in the PDP SIREN catalog.
- The use of "good practices" in Software Engineering considerably facilitates the subsequent audit work.
- As a result of the audit, we can provide a precise degree (in %) of fulfilment of a software tool with respect to the requirements document.
- With the application of the method, the treatment of legal requirements and the audit process implied is contemplated in the organization that uses the software tool. This process is considered important in Quality Standards like ISO 9001 or ISO 9004.
- The result of the audit provide the development team with a very useful and direct set of suggestions to be included in the software tool in order to accomplish the norms.

As limitation of our proposal, we can say that although our method is generalizable to other functional and non-functional software concerns, it is necessary to have a requirements catalog similar to the one used in this paper. At the moment, we have developed the following reusable requirements catalog:

- Personal Data Protection (PDP) (Toval et al., 2002b).
- Security in Information System (Toval et al., 2002a).
- Teleoperated Systems (Nicolas et al., 2006).

In lack of a predefined specific requirements catalog on the concern or concerns that we want to audit, some other alternative sources of broad acceptance could be used. For example, standard ISO/IEC 9126 (ISO/IEC-9126-1, 2001) could be used as guide for an audit of software quality.

As future work, we are already working on the development of a more specific requirements catalog of Electronic Clinical Record (ECR). This catalog will not only cover the legal aspects in the LOPD and the SMR but will also bring together the obligations imposed in the General Health Law (Law 14/1986) and the Law on the Autonomy of the Patient (Law 41/2002). Finally, we have developed a website where it is possible to consult the results obtained after audit, to download the SIREN PDP catalog and to request a change of the current catalog requirements.

ACKNOWLEDGEMENTS

This work has been partially financed by the Spanish Ministry of Science and Technology, project DEDALO (Desarrollo de sistEmas De calidad bAsado en modeLos y requisitOs), TIN2006-15175-C05-03, by the project FoMDAs (Formalizacion de (Meta-) Modelos y transformaciones en un marco MDA para el Desarrollo Automatico de SIW), URJC-CM-2006-CET-0387, by the project IDEATIO (Herramientas inteligentes para el control de la calidad asistencial en procesos de seguimiento integrado intra/extrahospitalario de pacientes: Una aproximacion basada en guias de practica clinicas), TIN2006-15460-C04-01, and by the Junta de Castilla-La Mancha (Spain), project DESERT (DEveloping Secure systEms through Requirements and Tools), PBC-05-012-3.

REFERENCES

Baskerville, R. L. (1999). Investigating information systems with action research. *Communications of the Association for Information Systems*, 2(3):4.

Baskerville, R. L. and Wood-Harper, A. T. (1996). A critical perspective on action research as a method for information systems research. *Journal of Information Technology*, 11(3):235–246.

CobiT (2005). *Control Objectives for Information and related Technology. 4th Edition*. http://www.isaca.org/cobit.htm.

Directive-1995/46/CE (1995). *Directive Num. 95/46/CE of the European Parliament and Council, dated October 24th: about People protection regarding the personal data management and the free circulation of these data. DOCE no. L281, 23/11/1995, P.0031-0050.*

Directive-2002/58/CE (2002). *Directive Num. 2002/58/CE of the European Parliament and Council, of July 12, 2002, relative to the processing of personal data and the protection of privacy in the electronic communications industry (Official Gazette of the European Union L 201 of 31.7.2002).*

Firesmith, D. (2003). Engineering security requirements. *Journal of Object Technology (JOT)*, 2(1):53–68.

Hughes, R. (2005). Is audit research? the relationships between clinical audit and social research. *International Journal of Health Care Quality Assurance*, 18(4):289–299.

IEEE-Std.1233-1998 (1998). *Guide for Developing System Requirements Specifications. In Volume 1: Customer and Terminology Standards The Institute of Electrical and Electronics Engineers, Inc. IEEE Software Engineering Standards Collection*.

IEEE-Std.830-1998 (1998). *Guide to Software Requirements Specifications (ANSI). In Volume 4: Resource and Technique Standards The Institute of Electrical and Electronics Engineers, Inc. IEEE Software Engineering Standards Collection*.

ISO/IEC-7498-2:1989 (1989). *Information processing systems. Open Systems Interconnection. Basic Reference Model. Part 2: Security Architecture*.

ISO/IEC-9126-1 (2001). *Software Engineering - Product Quality - Part1: Quality Model.*

LOPD (1999). *Spanish Constitutional Law 15/1999, December 13th, on Personal Data Protection. BOE no. 298, 14/12/1999 (In Spanish).* http://www.agpd.es.

Lusignan, S., Chan, T., Theadom, A., and Dhoul, N. (2006). The roles of policy and professionalism in the protection of processed clinical data: A literature review. *International Journal of Medical Informatics*.

Martinez, M. A., Lasheras, J., Toval, A., and Piattini, M. (2006). An Audit Method of Personal Data Based on Requirements Engineering. In *Proceedings of the 4th International Workshop on Security in Information Systems, (WOSIS'06), In conjunction with ICEIS'06, Paphos, Cyprus*, pages 217–231.

Massacci, F., Prest, M., and Zannone, N. (2005). Using a security requirements engineering methodology in practice: The compliance with the italian data protection legislation. *Computer Standards and Interfaces*, 27:445–455.

Nicolas, J., Lasheras, J., Toval, A., Ortiz, F. J., and Alvarez, B. (2006). A collaborative learning experience in modelling the requirements of teleoperated systems for ship hull maintenance. In *Proceedings of the Learning Software Organizations + Requirements Engineering (LSO+RE 2006), Hannover, Germany*, pages 71–80.

Olvingson, C., Hallberg, N., Timpka, T., and Greenes, R. (2002). Using the critical incident technique to define a minimal data set for requirements elicitation in public health. *International Journal of Medical Informatics*, 68:165–174.

Sandhu, R. and Samarati, P. (1996). Authentication, Access Control and Audit. *ACM Computing Surveys (CSUR)*, 28(1):241–243.

SMR (1999). *Spanish Royal Decree 994/1999, June 11th, by means of which the Security Measures Regulations of Automated Files which contain personal data is approved. BOE no. 151, 25/06/1999, page 24241 (In Spanish).* http://www.agpd.es.

Toval, A., Nicolás, J., Moros, B., and Garcia, F. (2002a). Requirements Reuse for Improving Information Systems Security: A Practitioner's Approach. *RE J.*, 6(4):205–219.

Toval, A., Olmos, A., and Piattini, M. (2002b). Legal Requirements Reuse: A Critical Success Factor for Requirements Quality and Personal Data Protection. In *RE*, pages 95–103. IEEE Computer Society.

Van der Haak, M., Wolff, A., Brandner, R., Drings, P., Wannenmacher, M., and Wetter, T. (2003). Data security and protection in cross-institutional electronic patient records. *International Journal of Medical Informatics*, 70:117–130.

Wadsworth, Y. (1998). What is participatory action research? *Action Research International. Paper 2,*, 2004.

Weber, R. (1988). *EDP Auditing: Conceptual Foundations and Practice. 2nd Edition.* Mc Graw Hill.