

## Reusable Security Requirements for Healthcare Applications

Jostein Jensen, Inger Anne Tøndel,  
Martin Gilje Jaatun, Per Håkon Meland  
SINTEF ICT, Department of Software  
Engineering Safety and Security  
{Jostein.Jensen, Inger.A.Tondel,  
Martin.G.Jaatun, Per.H.Meland}@sintef.no

Herbjørn Andresen  
University of Oslo, Faculty of Law,  
Norwegian Research Center for Computers  
and Law  
Herbjorn.Andresen@jus.uio.no

### Abstract

*Healthcare information systems are currently being migrated from paper based journals to fully digitalised information platforms. Protecting patient privacy is thus becoming an increasingly complex task, where several national and international legal requirements must be met. These legal requirements present only high-level goals for privacy protection, leaving the details of security requirements engineering to the developers of electronic healthcare systems.*

*Our objective has been to map legal requirements for sensitive personal information to a set of reusable technical information security requirements. This paper presents examples of such requirements extracted from legislation applicable to the healthcare domain.*

### 1. Introduction

Healthcare information systems are currently being migrated from paper based journals to fully digitalised information platforms. A digital medium leads to new opportunities for data sharing, where distributed data access should have a positive impact on cost and availability of data [1]. However, the introduction of electronic healthcare information systems has also raised new security concerns.

The European Parliamentary Technology Assessment (EPTA) network says in a report on privacy related to ICT that: “*With the development of ICT applications in the health sector, privacy is challenged, as there will be an increase in data exchange...*” [2]. Others, such as van der Haak et al. [1] and Ilioudis and Pangalos [3], have expressed similar concerns. Possible misuse scenarios related to personal sensitive information are only limited by the imagination, and EPTA points to insurers, employers, family, media and

even authorities as actors with vested interest in such information.

Sensitive health information and electronic health systems are afforded special protection by European legislation [4], and computerised health applications have to make special provisions to ensure that the required level of protection is implemented. Nevertheless, the mentioned EPTA report lists a set of challenges that should be addressed to enhance privacy in software, where one of them states the following:

*“Systems development neglects privacy - Too often, privacy threats could be avoided if data protection concerns were integrated in information systems from the beginning. This implies both legislative and technical adaptations.” [2]*

From this, we deduce that software developers need help in order to successfully develop healthcare applications with sufficient protection of personal privacy to satisfy current legislation. Our contribution is the concept of legislation-based reusable security requirements which facilitates addressing security aspects from the very start of a development project.

### 2. Background

This paper draws upon results from a research project, MPOWER<sup>1</sup>, funded by the European Commission. Its objective is to define and implement a secure service platform that supports integration of “smart house” and sensor technology for persons with cognitive disabilities (e.g. dementia). Such a platform needs to handle personal health data, and thus automatically falls under the strict legislative privacy regulations of healthcare applications. As part of the design process of the platform’s security solutions, a

---

<sup>1</sup> <http://www.sintef.no/Projectweb/MPOWER/>

survey of legislative requirements with respect to processing of personal health data was performed. We studied the European Data Protection Directive, 95/46/EC [5], and the Norwegian implementations of this, as “*existing data protection legislation at EU level and its transposition at Member State level*” are believed to be “*sufficient to allow eHealth tools and applications to be used efficiently in health care*” [4]. From this legislation we extracted a set of security requirements, and ensured that each requirement could be traced back to its origin.

When deriving these security requirements, we found that there was a high potential for reuse of healthcare-related technical security requirements – especially as many of them are directly associated with existing legislation. Making these, and information about our work available is useful to help developers both to create software fulfilling legal requirements, and as such help them to create secure privacy-preserving software.

In the following sections we briefly discuss previous work on reusing security requirements as well as previous work on the use of legal requirements in the healthcare domain.

## 2.1 Reuse of Security Requirements

There is no universally accepted definition of security requirements in the literature. Security requirements are described as everything from high level goals to detailed specifications of which security mechanisms to use. In previous work we have suggested to specify security requirements that focus on *what* should be achieved – not *how*. Still they must be specific about things like who they concern and when they apply in order to be testable [6].

When writing *reusable* requirements it is even more important to leave out information on how security should be achieved. In most cases there will be several mechanisms that can be used to achieve the same or similar objectives. It is often impossible to make general recommendations for what mechanisms to choose, as it will depend on technology choices etc. This claim is supported by Firesmith [7] and Sindre et al. [8], among others.

Firesmith argues that where functional requirements generally vary between applications, security requirements are often more standardised. Applications “*tend to have the same basic kinds of valuable and potentially vulnerable assets*” which again “*tend to be subject to the same basic kinds of security threats from attacks by the same basic kinds of attackers*” [7]. We believe this to be even more true for applications within one single domain, and especially for domains

which are subject to extensive formal regulations, such as the healthcare domain.

Much of the existing work on reuse of security requirements is focused on misuse and threat recognition, e.g. through misuse cases [8]. Though this is a valid approach, and supports risk management, our starting point is quite different since we focus on legislation rather than threats. We therefore find the work on security requirements representation more relevant for our work, in particular the work of Firesmith [7] [9] on how to create reusable templates for security requirements and on grouping requirements into categories.

To achieve maximum reuse of requirements it is important to make the reusable requirements easily available. Security repositories containing requirements have been suggested by among others Sindre et al. [8] and Toval et al. [10]. Meland et al. [11] have, in the SHIELDS project<sup>2</sup>, defined an architecture for a repository that together with other software security artefacts can contain a security requirements catalogue.

## 2.2 Legal Requirements Reuse

van der Haak et al. [1] have previously looked at legal requirements concerning protection of sensitive health data in cross institutional electronic patient records. They studied the European Data Protection Directive 95/46/EC and the German implementations of this, and proposed technical measures that could be used to meet the legislative requirements for healthcare applications. However, they do not say which measures address which part of the legislation. Such lack of traceability is pointed out by Otto and Antón [12] as a common problem for much of the existing work within this topic. As a result we must take van der Haak et al.’s word that their proposed solution in fact addresses all relevant legal requirements. We believe the lack of traceability makes it hard to determine what the consequences will be if deciding to solve problems with other security measures than what is proposed. Additionally, it will be difficult to determine what the consequences will be if legislation or its interpretation changes. As legal texts “*contain numerous ambiguities, cross-references, domain-specific definitions, and acronyms, and are frequently amended via new regulations and case law*” [12], lack of traceability between requirements and legislation is a major weakness.

Also relevant to our work is the security policy framework suggested by Ilioudis and Pangalos [3]. This framework can be applied to systems processing and transmitting medical data through the Internet. The

---

<sup>2</sup> <http://www.shields-project.eu/>

authors claim that major legislative directives, technical reports and recommendations from EU, USA and Canada are taken into account for the development of the framework. However, also in this case traceability between the different parts of the policy and the legislation is missing.

Even though it is not specific for the healthcare domain, the work of Toval et al. [13] on creating a catalogue with requirements from personal data-protection laws is relevant. In their catalogue they have the possibility to state the source of each requirement to ensure traceability. This information is, however, not included in the example requirements they provide.

### 3. Relevant Laws and Regulations

In this section we introduce legislation applicable to the healthcare domain, which is used as basis for the reusable security requirements presented in section 4. We use the European Data Protection Directive as a starting point, and then list and refer to the Norwegian legislation used in our work as example of a national implementation of the Directive. Legal requirements are high-level by nature, and we claim that there is a need to map these to more technical software security requirements that can be utilised directly by software developers.

#### 3.1 The European Data Protection Directive

For the European Union, the Data Protection Directive 95/46/EC is intended to protect individuals with regard to the processing of personal data. The Directive is also aimed at permitting warrantable movement of personal data between member states. As also pointed out by van der Haak et al. [1], articles 7 and 8 of the Directive are essential for the regulation of personal data processing. Article 7 sets the criteria for making processing of personal data legitimate, while article 8 treats special categories of processing. The latter specifically refer to the treatment of data related to healthcare (Article 8 (3)).

EU member states are expected to implement the Directive (Article 17) e.g. through national legislation. The PRIVIREAL<sup>3</sup> research project examined the implementation of the Data Protection Directive across Europe. Norway is committed to this directive as it is included in the European Economic Area (EEA) Agreement. PRIVIREAL describes the Norwegian Personal Data Act [14] as the Norwegian implementation of Directive 95/46/EC and states that: “*The Act is EC-compatible, and in many respects it*

*goes beyond the Directive, offering an even greater level of protection*” [15].

Norwegian laws and regulations are thus believed to be representative for European requirements within this domain. The following section presents Norwegian legislation that is used to protect the privacy of individuals with respect to health related data.

#### 3.2 Relevant Norwegian Legislation

The purpose of the **Personal Data Act**<sup>4</sup> [14] is to protect natural persons from violation of their right to privacy through the processing of personal data. The Act shall ensure that personal data are processed in accordance with fundamental respect for the right to privacy, including the need to protect personal integrity, and ensure that personal data are of adequate quality. The Personal Data Act is elaborated via the **Personal Data Regulation** [16].

The objective of the **Health Personnel Act** [17] is to contribute to safety for patients and quality of health services, and also trust between the patient and both health personnel and health services. The different sections in this act focus on subjects like requirements on how the health personnel work, how the organisation is structured, professional authorisations and licensing, professional secrecy, duties to inform other agencies in some special circumstances, and duty of documentation.

The objective of the **Patients’ Rights Act** [18] is to contribute to ensuring the population equal access to health care of good quality. The provision of this act shall contribute to the promotion of a relationship based on trust between the patient and the health service while having respect for the individual patient’s life, integrity and human dignity.

The objective of the **Personal Health Data Filing System Act** [19] is “*to contribute towards providing public health services and the public health administration with information and knowledge without violating the right to privacy, so as to ensure that medical assistance may be provided in an adequate, effective manner*”. This act also complies with Directive 95/46/EC, and it has many important features in common with the general Personal Data Act.

The **Regulation of Patient Records** [20] presents the rules for keeping and maintaining patient record systems.

The **Security Act** [21] is aimed at the central and local government administration and covers a spectrum

---

<sup>3</sup> <http://www.privireal.org/>

---

<sup>4</sup> In the following we refer to a number of Norwegian laws by unofficial English titles; for the authoritative Norwegian title, see the references.

of preventive security measures against threats that affect security of the realm. Information security is a specific subtopic of this act which sets requirements for document classification and handling. Information security aspects are elaborated in the **Regulations on Information Security** [22], which presents detailed regulations for handling classified data (i.e. in our case sensitive personal information) in both local and distributed information system.

The Security Act and its associated Regulations on Information Security are only loosely related to the healthcare domain through the **Protection Decree** [23]. Generally, though, they are not applicable to most IT systems containing patient data, yet we find that they provide a relevant source of practical recommendations. The Protection Decree is used when public authorities handle documents that need protection for other reasons than mentioned in the Security Act or its associated regulations.

#### 4. Reusable Security Requirements

From the legislation presented above, we have extracted a set of security requirements for the MPOWER platform. We present these in Table 1 and use them as examples of reusable security requirements that can be extracted from legislation; we do not claim to provide an exhaustive list. The meaning of the terms MUST and SHOULD that are used in the requirements follow the definitions given in RFC 2119 [24].

For each requirement we provide references to the laws and regulations from which the requirements originate, thus providing the traceability which seems lacking in previous work. By detailing the requirements to the same level as done in the table, we are able to reuse them in future software projects related to healthcare applications. We believe that even the small set of requirements provided can set the basis for creating a security architecture and support the design of information systems handling personal sensitive data. The requirements are written according to recommendations for security requirements engineering by Firesmith [9], and they are grouped according to his requirements categories.

Note that the requirements presented in Table 1 are written for a service platform based on a service oriented architecture. Similar requirements should be written for other types of information platforms accordingly.

**Table 1: Reusable security requirements extracted from laws and regulations applicable to healthcare**

Requirement type	Description
Identification and authentication requirements	Services should identify and verify the identity of all of its human users before allowing them access to their resources. [17] §21,[20] §14,[18] §3-6, [16] §2-11 and §2-12
	Services should identify and verify the identity of corresponding services before they are allowed to communicate. [22] §5-4, [20] §14
Authorisation requirements	Services should verify the authorisation level of users before access to sensitive data can be given. [17] §21, §22 [18] §3-6 [16] §2-11,§2-12
Integrity requirements	The platform should support integrity protection of sensitive personal data while it is stored. [22] §5-5, [19] §16, [14] §13, [16] §2-13
	The platform should be able to detect unauthorised manipulation of data that is being transmitted. [22] §5-5, [19] §16, [14] §13, [16] §2-13
Privacy requirements	The platform must protect any stored sensitive personal data from unauthorised access. [18] §3-6 and §5-3, [19] §16, [14] §13, [16] §2-11
	Personal sensitive data must be confidentiality protected while transmitted over open, untrusted communication lines. [22] §5-5, [18] §3-6 and §5-3, [19] §16, [14] §13, [16] §2-11
Security Auditing Requirements	The platform should be able to log security incidents, such as failed login attempts or unauthorised access attempts to services in order to discover and trace system abuse. [16] §2-14
	The platform should be able to log activities related to access of sensitive information. [16] §2-14
Survivability requirements	Input validation should be performed at time of data reception to reduce threats represented by malicious content and malformed packets. [22] §5-9
	Multiple levels of security should be ensured to avoid a single point of failure. [22] §5-4
	Data freshness should be controlled to prevent chances of replay attacks. [22] §5-5
Non-repudiation requirements	A patient journal should show who has added content, e.g. through electronic signatures. [17] §40, [20] §7

#### 5. Discussion

Toval et al. [13] says that it makes sense to consider reuse of legal requirements for personal data protection because: 1) it is difficult to understand and extract requirements directly from legal documents, 2) it will make it possible to ensure beforehand that the information system to be built will fulfil regulations,

and 3) reuse will enable high efficiency because many applications will have similar needs.

Concerning the first point, an approach using a security repository concept such as those presented by Meland et al. [11] and Ardi et al. [25] allows security experts together with legal professionals to share the results of the complex requirements elicitation process. To include a feedback system in such repositories will allow both developers and other security experts to review the requirements, and constantly improve the repository content. However, such repositories will of course need a critical mass of content before being really usable, something that must be done by receiving quality-assured input over time.

The second point is related to the possibility of tracing, and thus the ability to determine, the fulfilment of legal requirements. Our work is very much related to that of van der Haak et al. [1] and Ilioudis and Pangalos [3], in that we study legislation in order to derive requirements for health systems. However, we address what we believe is a major weakness of their work, i.e. that the traceability between legislation and solution is missing. Like Ilioudis and Pangalos we focus on reusability, though our approach is more similar to that of Toval et al. in that we suggest reusable security requirements that should be available through a repository whereas Ilioudis and Pangalos present a security policy. In our approach, where we explicitly state the relation between legislation and requirement, traceability to legislation is possible throughout the software development lifecycle by keeping track of requirements fulfilment. Our approach can thus be used to ease the job of documenting that a healthcare application satisfies legal requirements. As such, it may help various governments in the process of accrediting healthcare software systems for treatment of sensitive personal data.

Toval et al.'s third point says that reuse of legal requirements will enable efficiency. This can be seen in relation to Zuccato et al [26] who claim that finding the right security requirements is challenging because they are often "*perceived as self-evident or even annoying*". The result is often a small set of fuzzy requirements that development teams can make little practical use of. We believe that a lot of similar projects should be able to share and reuse many of the same security requirements, and plan to use the repository developed by Meland et al. for this. As such, we should be able both to increase efficiency and quality in the requirements elicitation phase for healthcare applications.

We have used Firesmith's categories [9] to group related requirements. The grouping of similar requirements is done to ease the task of finding related and relevant requirements in the repository. However,

when the number of requirements increase it may be necessary with relations beyond Firesmith's categories, e.g. to:

- create new groups of requirements that naturally belong together
- connect requirements to specific technologies, e.g. SOA
- identify which requirements are in conflict or are overlapping

Otto and Antón point out that a requirements catalogue or repository must be updated each time a new law changes. Otherwise, there may be doubts whether the repository content is of sufficient quality. Consequently, there must be well defined routines for keeping the repository up to date and changes must be reported. This is a challenge within this domain, as information security and data protection legislation is relatively new and still an emerging field. There exist little case law to guide requirements engineers with the legal interpretation [12], yet we conjecture that an alternative sorting of the repository, allowing us to trace all requirements connected to each fragment of legal text, could offer some help in monitoring needs for update if the law changes.

Considering the perspective of legal protection related to personal data, we believe reuse of legislation-based requirements will contribute to a uniform interpretation of the legislation protecting against unintended differences between systems. However, laws are not primarily designed as system requirements, but rather more as a balancing of boundaries, processes, duties and rights. When deriving reusable technical requirements from legislation and making them available in a repository it is prudent to ask a number of questions: Should the requirements themselves be considered as regulations, and if so, should there be any sanctions if they are violated? Is there a risk of incorrect use of the requirements? Who should be responsible for controlling them? These are open questions that need further research. However, we consider our proposed approach more as a support and guide for software developers to implement secure software, where the traceability between technical security requirements and legislation help documenting that necessary measures are included to satisfy legislation.

In this paper we have used Norwegian legislation to exemplify our work. Similar should be performed for other European implementations of The European Data Protection Directive.

## 6. Conclusion

We have elicited technical security requirements from legislation applicable to the healthcare domain. They are written to support reuse and provide traceability to the legislation from which they were derived.

## Acknowledgements

We would like to thank Ulrik Johansen and Lillian Røstad at SINTEF ICT – Ulrik for input on relevant legislation and requirements extraction, and Lillian for a final proof reading and valuable input. Further, we would like to thank the project manager of MPOWER<sup>1</sup>, Marius Mikalsen and technical manager Ståle Walderhaug for support. A fruitful collaboration with the SHIELDS project<sup>2</sup> is also appreciated.

## References

- [1] M. van der Haak, A. C. Wolff, R. Brandner, P. Drings, M. Wannemacher, and T. Wetter, "Data security and protection in cross-institutional electronic patient records," *International Journal of Medical Informatics*, vol. 70, pp. 117-130, 2003.
- [2] EPTA, "ICT and Privacy in Europe, Experiences from technology assessment of ICT and Privacy in seven different European countries " European Parliamentary Technology Assessment (EPTA), 2006, <http://epub.oecaw.ac.at/ita/ita-projektberichte/e2-2a44.pdf>.
- [3] C. Ilioudis and G. Pangalos, "A framework for an institutional high level security policy for the processing of medical data and their transmission through the Internet," *Journal of Medical Internet Research*, vol. 3, 2001.
- [4] C. van Doosselaere, P. Wilson, J. Herveg, and D. Silber, "eHealth..... but is it legal?," in *Eurohealth*, vol. 13, 2007, pp. 1 - 4.
- [5] "Directive 95/94/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data," 1995, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML>.
- [6] I. A. Tondel, M. G. Jaatun, and P. H. Meland, "Security Requirements for the Rest of Us: A Survey," *Software, IEEE*, vol. 25, pp. 20-27, 2008.
- [7] D. Firesmith, "Specifying Reusable Security Requirements," *Journal of Object Technology*, vol. 3, pp. 61 - 74, 2004.
- [8] G. Sindre, D. Firesmith, and A. Opdal, "A Reuse-Based Approach to Determining Security Requirements," in *International Workshop on Requirements Engineering: Foundation for Software Quality (REFSQ 2003)*, 2003.
- [9] D. Firesmith, "Engineering Security Requirements," *Journal of Object Technology*, vol. 2, pp. 53 - 68, 2003.
- [10] A. Toval, J. Nicolás, B. Moros, and F. García, "Requirements Reuse for Improving Information Systems Security: A Practitioner's Approach," *Requirements Engineering*, vol. 6, pp. 205 - 219, 2002.
- [11] P. H. Meland, S. Shanai, J. Jensen, E. Rios, T. Sanchez, N. Shamehri, I. A. Tøndel, "An architectural foundation for security model sharing and reuse", to be presented at *The Fourth International Conference on Availability, Reliability and Security (ARES 2009), SecSE Workshop 2009*
- [12] P. N. Otto and A. I. Antón, "Addressing Legal Requirements in Requirements Engineering," in *15th IEEE International Requirements Engineering Conference*, 2007.
- [13] A. Toval, A. Olmos, and M. Piattini, "Legal Requirements Reuse: a Critical Success Factor for Requirements Quality and Personal Data Protection," in *IEEE Joint International Conference on Requirements Engineering*, 2002, pp. 95-103.
- [14] LOV-2000-04-14-31, "Personopplysningsloven," 2001, <http://www.lovdato.no/cgi-wift/wiftldles?doc=/usr/www/lovdato/all/nl-20000414-031.html>.
- [15] "PRIVIREAL Privacy in Research Ethics & Law," <http://www.privireal.org/content/dp/norway.php>
- [16] FOR-2000-12-15-1265, "Personopplysningsforskriften," 2007, <http://www.lovdato.no/cgi-wift/wiftldles?doc=/sf/sf/sf-20001215-1265.html>.
- [17] LOV-1999-07-02-64, "Helsepersonelloven," 2007, <http://www.lovdato.no/cgi-wift/wiftldles?doc=/usr/www/lovdato/all/nl-19990702-064.html>.
- [18] LOV-1999-07-02-63, "Pasientrettighetsloven," 2007, <http://www.lovdato.no/cgi-wift/wiftldles?doc=/usr/www/lovdato/all/nl-19990702-063.html>.
- [19] LOV-2001-05-18-24, "Helseregisterloven," 2007, <http://www.lovdato.no/cgi-wift/wiftldles?doc=/usr/www/lovdato/all/nl-20010518-024.html>.
- [20] FOR-2000-12-21-1385, "Forskrift om pasientjournal," 2001, <http://www.lovdato.no/cgi-wift/wiftldles?doc=/sf/sf/sf-20001221-1385.html>.
- [21] LOV-1998-03-20-10, "Sikkerhetsloven," 1998, <http://www.lovdato.no/cgi-wift/wiftldles?doc=/usr/www/lovdato/all/nl-19980320-010.html>.
- [22] FOR-2001-07-01-744, "Forskrift om informasjonssikkerhet," 2001, <http://www.lovdato.no/cgi-wift/wiftldles?doc=/sf/sf/sf-20010701-0744.html>.
- [23] FOR-1972-03-17-3352, "Beskyttelsesinstruksen," 2001, <http://www.lovdato.no/cgi-wift/wiftldles?doc=/sf/sf/sf-19720317-3352.html>.
- [24] "RFC 2119 - Key Words for Use in RFCs to Indicate Requirement Level," 1997, <http://www.ietf.org/rfc/rfc2119.txt>.
- [25] S. Ardi, D. Byers, P. H. Meland, I. A. Tondel, and N. Shahmehri, "How can the developer benefit from security modeling?," in *The Second International Conference on Availability, Reliability and Security (ARES 2007), SecSE Workshop 2007*, pp. 1017-1025.
- [26] A. Zuccato, V. Endersz, and N. Daniels, "Security Requirement Engineering at a Telecom Provider " in *Third International Conference on Availability, Reliability and Security, SecSE Workshop*, 2008.