Patient Data Confidentiality Issues of the Dutch Electronic Health Care Record

Perry Groot Ferry Bruijsten Martijn Oostdijk

Institute for Computing and Information Sciences,
Radboud University Nijmegen, P.O.Box 9010, 6500GL Nijmegen

Abstract

Health care is currently in a phase of transition. One of the recent developments that seems to be inescapable is the introduction of an Electronic Health care Record and a central service system that makes all medical data electronically accessible. Many issues, including patient data confidentiality, however, are still not solved satisfactorily. One possible approach to patient data confidentiality is a control and warning system that monitors all access to patient information and flags those requests that do not abide to the law health care providers are expected to follow. In this paper, we investigate the feasibility of a control and warning system at a Dutch hospital, and we analyse whether such an approach is practical and a viable option for providing patient data confidentiality. We provide a conceptual schema of the underlying domain and give empirical results by querying the hospital information system. Our empirical results show that the policy of the hospital for providing patient data confidentiality is unlikely to succeed when scaled up to a National level in its current form. Although experimental results show that the policy can be strengthened considerably by using additional supporting facts from the care process of a patient, this is still insufficient as the number of flagged requests for patient data is too high. Some of these results are, however, caused by the developments of the Dutch health care system, which are not fully reflected yet in the hospital information system analysed. Incorporating these developments may lead to better results with respect to patient data confidentiality.

1 Introduction

Health care is currently in a phase of transition. There is mounting pressure on health care organisations to improve efficacy and cost-effectiveness, without sacrificing quality of care. Information Technology (IT) is seen as an enabling technology and a major factor in steering these developments. So far, however, development of IT in health care has been lagging behind in comparison to other sectors of society [12]. Various initiatives, from governments, professional organisations, and from hospitals, are now actively trying to catch up on IT in health care.

One of these developments, the Electronic Health care Record (EHR) system, has already been a key research field in medical informatics in the last decade and several EHR standards have been developed over the years [3, 4]. The EHR is defined by [7] as “digitally stored health care information about an individual’s lifetime with the purpose of supporting continuity of care, education, and research, and ensuring confidentiality at all times”. In the Netherlands, the development and introduction of an EHR system is currently being coordinated by NICTIZ (National Institute for IT in Health Care; `www.nictiz.nl`). This will be accomplished through a central service system accessible through the Internet that links the medical data of various medical institutions [10]. The system will be developed in phases and is expected to be fully operational in the next decade.

Although, the EHR is expected to have a beneficial impact on the health care process by making patient information electronically available anywhere at any time for all care providers, there are still a number of issues (e.g., interoperability, content structure, security), that have not been dealt with satisfactorily. With respect to security, an EHR system could operate on a scale where on one end all roles of all care providers are specified that dictates in advance who may access what data [9], while at the other end all care providers are able to access all patient data, but a control and alarm system is used to monitor and log all data access. The latter option is currently specified by NICTIZ, but with no detail how such a system should be set up.

At this moment, it is not even clear if a control and warning system is even a viable option for providing patient data confidentiality. Although the EHR and accompanying infrastructure seem to be inescapable[1], medical institutions will be hard to convince in making their patient data electronically available when they are held responsible if security measures are found to be inadequate. In this paper, we therefore investigate whether a control and alarm system is a viable option for ensuring patient data confidentiality.

As the infrastructure and local service system are still under development and data is currently only available at a local level, we restrict our analysis of patient data confidentiality to the EHR of a Dutch hospital.[2] According to [8, 11], a control and alarm system should be supported with a clear policy and legal procedures that sanctions improper conduct. We therefore take a policy developed by the Dutch hospital as starting point and validate whether their policy and their current EHR implementation are adequate from a practical perspective and whether they are capable in abiding to the Dutch law.

Section 2 provides more background on Dutch law and the Dutch health care system. Section 3 discusses in more depth the Dutch hospital and their policy. Section 4 gives empirical results of the logging of patient data access classified as lawful and unlawful entries. Section 5 gives conclusions and Section 6 discusses future work.

2 Background

NICTIZ has made specifications for a basic infrastructure with a central service system, the LSP ('Landelijk Schakel Punt'), that keeps track of the medical data that is available from various medical institutions. Using this system allows care providers to view patient data that is stored locally at different sites. Medical care providers can log on to the system after they identify themselves with their UZI number ('Unieke Zorgverlener Identificatienummer'). The UZI number is linked to a chip card, the UZI-pass, that can both be used for identification and authentication of a care provider. All information about UZI-passes are stored in the UZI-register (`www.uzi-register.nl`) maintained by CIBG (`www.cibg.nl`). Information about patients can be requested by providing their BSN number ('Burger Service Nummer'), which is a unique number equal to their SOFI number, but is used differently within Dutch law so that it has a wider use.

Technological advancements should, however, still operate within the context provided by the law. The Dutch law WBP ('Wet Bescherming Persoonsgegevens') gives rules for protecting the privacy of citizens. Citizens are given the right to view any personal data, to make corrections, or to make objections against processing their personal data, whereas organisations have the duty to make sure that any technical or organisational measure is taken to secure private data against loss or any form of unlawful processing. Who may lawfully view patient data is specified in the Dutch law WGBO ('Wet op de geneeskundige behandelovereenkomst'). When a care provider treats a patient, a treatment agreement is made. The WGBO specifies that the care provider needs to provide information about the treatment (nature, purpose, risks, options, prognosis, etc.) and needs to ask permission from the patient for treatment, although this may be presupposed when treatment is not radical. Also, when several care providers are directly involved in the care process of the patient, permission may be presupposed. Hence, to view patient data lawfully there should be a treatment agreement between care provider and patient, but is seldom documented in practice.

Nevertheless, many facts can be derived from the care process that strongly support or reject a treatment agreement between care provider and patient. For example, since ary 1, 2005, a DBC ('Diagnose Behandeling Combinatie') is used for all hospital financing. A DBC is a code of four parts (care type, care question, diagnosis, treatment) that describes the complaint of the patient, how the patient enters the hospital, which diagnosis has been made, and which treatment is supposed to take place (cf. `www.dbconderhoud.nl`). As the DBC is intended for financial purposes, it is unlikely to provide a sound and complete mechanism for establishing a treatment agreement between care provider and patient, but additional supporting facts may be derived from appointments, medical actions, visitations, hospital stays, etc. Such supporting facts may provide a solid base for a control and warning system.

3 Local Hospital

The Dutch hospital investigated developed a local policy to increase the internal control on patient data access. Within this policy, six types of care providers are identified. Here, we will only focus on the group

[1] K. Loohuis. Nictiz: 'Stoppen met EPD is geen optie', *Computable*, September 2005.

[2] Because of privacy concerns, the name of the hospital can not be disclosed and all data used within this paper has been anonimised.

of medical specialists. This group is currently able to access all patient data irrespective of whether the patient was treated by this specialism. The hospital preferres a situation in which the medical specialist is given a warning when he or she tries to access patient data when the patient is not (or was not) treated by the specialism of the medical specialist. For this, the hospital has developed a policy and it it the goal of this paper to validate the feasibility of this policy to increase internal control in the hospital.

3.1 Object-Role Model of Universe of Discourse

Object-Role Modelling (ORM) is a methodology for modelling and querying an information system at the conceptual level, which improves correctness, clarity, and adaptability [5]. ORM pictures the world as *objects* (entities and values) that play *roles* (parts in relationships, i.e., n-ary predicates), possibly augmented with additional constraints like totality (one or more) and uniqueness (zero or one) as shown in Figure 1. Here, we present a conceptual schema of the health care domain, adapted from [6], using ORM.

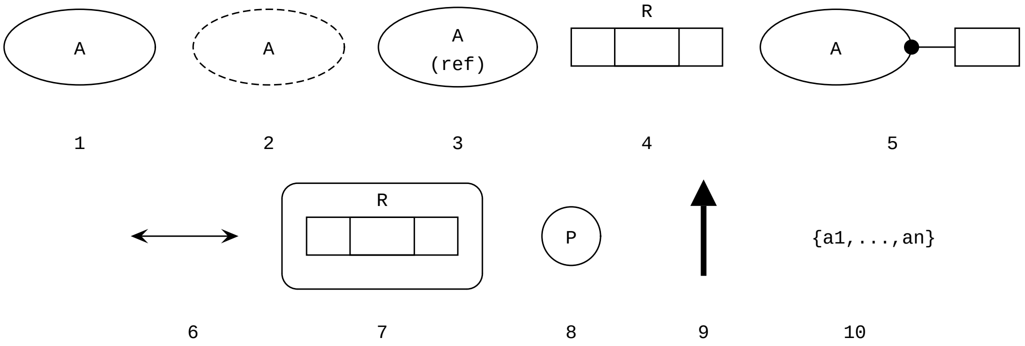


Figure 1: ORM notation. 1. Entity type, 2. value type, 3. uniquely identifiable entity type with bracketed value type, 4. role, 5. totality constraint, 6. uniqueness constraint, 7. objectified role, 8. primary external uniqueness constraint, 9. subtype, 10. value constraint.

The Object-Role Model of our UoD is shown in Figure 2. A care provider is uniquely identified with his UZI number and has one of the six identified roles in the hospital's policy (i.e., medical specialist, specialist in training, nurse, apothecary, paramedic, secretary). A medical specialist is a subtype of care provider having a specialism, belonging to some hospital specialism, who is responsible for the care given to some patient. In practice, the role of treating specialist may be fulfilled by more than one medical specialist, as a specific specialist may not be present at all time. A patient may also have to deal with several specialisms, who may be involved in one or more care questions, possibly overlapping in time. A patient is treated by a certain hospital specialism if there is an open or completed DBC for that specialism. As stated in Section 2, a DBC is created for a patient for each care question, but it may be the case that a DBC has not yet been created for a patient. To model the log that keeps track of patient data access, each entry should at least contain four entries denoting the date, the time, the patient identification number (BSN), and the care provider identification number (UZI). These four entries form a minimal set that is needed to identify the care provider and moment of access for a certain patient record. Each log entry should be unique.

According to Figure 2, a treatment agreement between care provider and patient is supported when one of the specialisms of the medical specialist who viewed the EHR also occurs in one of the DBCs that were created for the corresponding patient. Additional information about specialisms involved in the care process of the patient, which may not be found in the DBC, can be obtained using additional facts about the patient. Figure 2 shows two of those additional facts, namely the appointments made for the patient and the medical actions involving the patient.

4 Empirical Results

The conceptual schema of Section 3 could, in principle, be used to query the hospital information system in order to obtain information about lawful and unlawful accesses to patient information. ORM allows a conceptual schema to be mapped into a relational schema that can be queried using SQL, or, for some extensions, ORM can automatically generate SQL code from queries specified at the conceptual level. However,

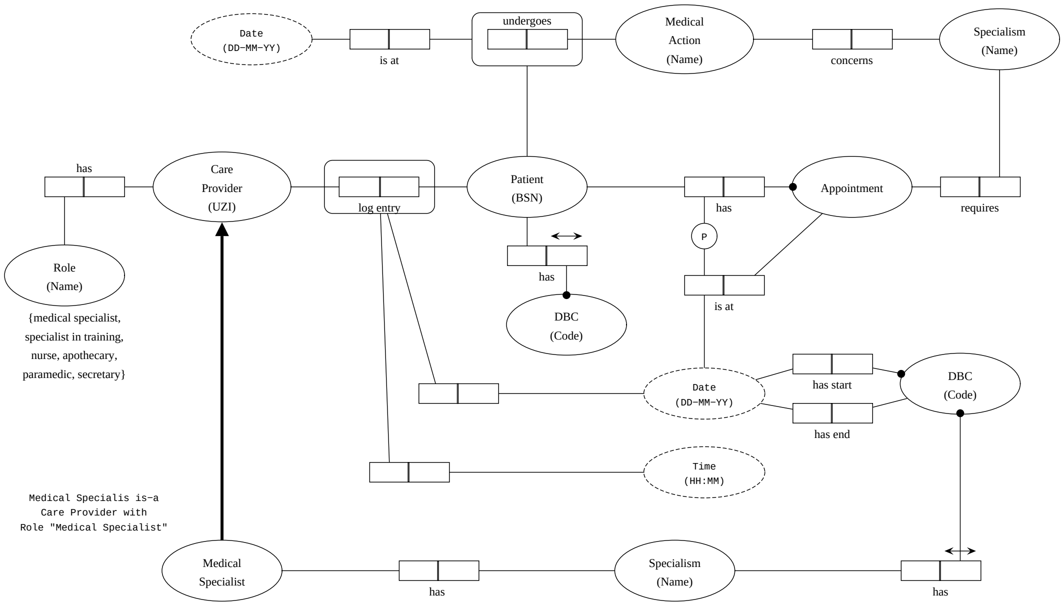


Figure 2: Simplified ORM model of the Universe of Discourse (adapted from [6]).

as the hospital under study was not constructed according to the conceptual schema in Figure 2, but instead uses databases with many table structures that have evolved over time, we had to construct SQL queries by hand. In this section we describe in more detail the experimental results obtained by querying the hospital information system for lawful and unlawful accesses to patient information.

Although the SQL queries were hand constructed, in essence we follow the schema in Figure 2 for obtaining lawful and unlawful accesses to patient information. We try to obtain evidence justifying patient data access by recovering the DBC and corresponding specialism such that it is identical to the specialism of the medical professional accessing the patient record. Mainly, three tables were queried, (1) the DBC table, containing, among others, the DBC code, the patient BSN, a specialism code, a start date, and an end date; (2) the specialism table, which maps medical specialists to specialisms; and (3) log entries, containing the time and date of request, the patient BSN, and the medical specialists UZI number. The specialism table in fact needed to be constructed from various tables as it was not available as a single table. A fourth table was needed to join records from the DBC table to the specialism table as both had a different coding scheme in place. To give an impression of the complexity of the queries constructed an example is given in Figure 3. Summarising, the complexity of the SQL queries is due to a number of factors: (1) different codings schemes were in place, (2) medical specialists may have several specialisms, (3) information may be missing (i.e., no DBC for a patient, no personnel number, no end date for a DBC, etc.), and (4) medical specialists should only view patient data information within the start and end of their profession.

The results of the SQL query in Figure 3 on the hospital information system are shown in Figure 4. The unlawful requests (according to a mismatch of the DBC specialism and medical specialists specialism) are shown as a percentage of the total number of requests for each specialism in the hospital. Clearly, there is a high variability among specialisms. For some specialisms, even all requests are possibly unlawful as no justifiable evidence could be retrieved from the DBCs. These results show that a DBC in itself is not enough for providing evidence to justify access to patient data. For some cases this can be explained by the fact that a DBC is not created for each patient. Sometimes, the patient undergoes diagnostics and treatments for which no DBC is opened, and therefore several specialisms involved in the care process of the patient can not be retrieved in this way, although they could, in principle, be retrieved from other supporting facts.

In addition to matching the specialism of the medical specialist with the specialism of the DBC, we therefore also matched the specialism to specialisms obtained from appointments, performed medical actions, hospital stays, visitations, operations, etc. In practice, medical actions are only attached to a DBC after they are closed for validation. The connection is determined by an algorithm based on, among others, execution date, requesting specialism, and execution specialism [1]. In practice, making this connection can be problematic because (1) several DBCs run in parallel, (2) a DBC was never opened, or (3) the DBC has already been closed and declared. Several medical actions may therefore be impossible to connect to a DBC.

```
SELECT [EHR_log].[perssnr], [EHR_log].[BSN], [EHR_log].[time], [EHR_log].[date]
FROM [EHR_log], [medical specialists]
WHERE [EHR_log].[date] BETWEEN “2006-11-27” AND “2006-12-03”
AND [EHR_log].[perssnr] = [medical specialists].[perssnr]
AND NOT EXISTS (SELECT [EHR].[perssnr], [EHR].[BSN], [EHR].[time], [EHR].[date]
      FROM [EHR_log] AS [EHR], [medical specialists] AS [medical Specialists_2]
      WHERE [EHR].[date] BETWEEN “2006-11-27” AND “2006-12-03”
      AND [EHR].[perssnr] = [medical specialists_2].[perssnr]
      AND [EHR].[BSN] = [EHR_log].[BSN]
      AND [EHR].[perssnr] = [EHR_log].[perssnr]
      AND [EHR].[date] >= (SELECT MIN([DBC_2].[start_date])
            FROM [RADAR dbo_gestelde_dbc_wei_view] AS [DBC_2]
            WHERE [DBC_2].[BSN]= [EHR].[BSN])
      AND [EHR].[date] < [medical Specialists_2].[end_date]
      AND [medical specialists_2].[specialism] IN (SELECT [dbo_specialisms].[specialism_mnemonic]
            FROM [RADAR dbo_gestelde_dbc_wei_view] AS [DBC],[specialisms]
            WHERE [DBC].[spcm_code_dbc] = [dbo_specialisms].[specialismcode_int]
            AND [DBC].[BSN] = [EHR].[BSN]
            GROUP BY [dbo_specialisms].[specialism_mnemonic])
      GROUP BY [EHR].[perssnr], [EHR].[BSN], [EHR].[time], [EHR].[date])
GROUP BY [EHR_log].[perssnr], [EHR_log].[BSN], [EHR_log].[time], [EHR_log].[date];
```

Figure 3: SQL code for retrieving all unlawful log entries for which the patient has no DBC with matching specialism to the specialism of the medical specialist who viewed the patients EHR in a certain week.

5 Conclusions

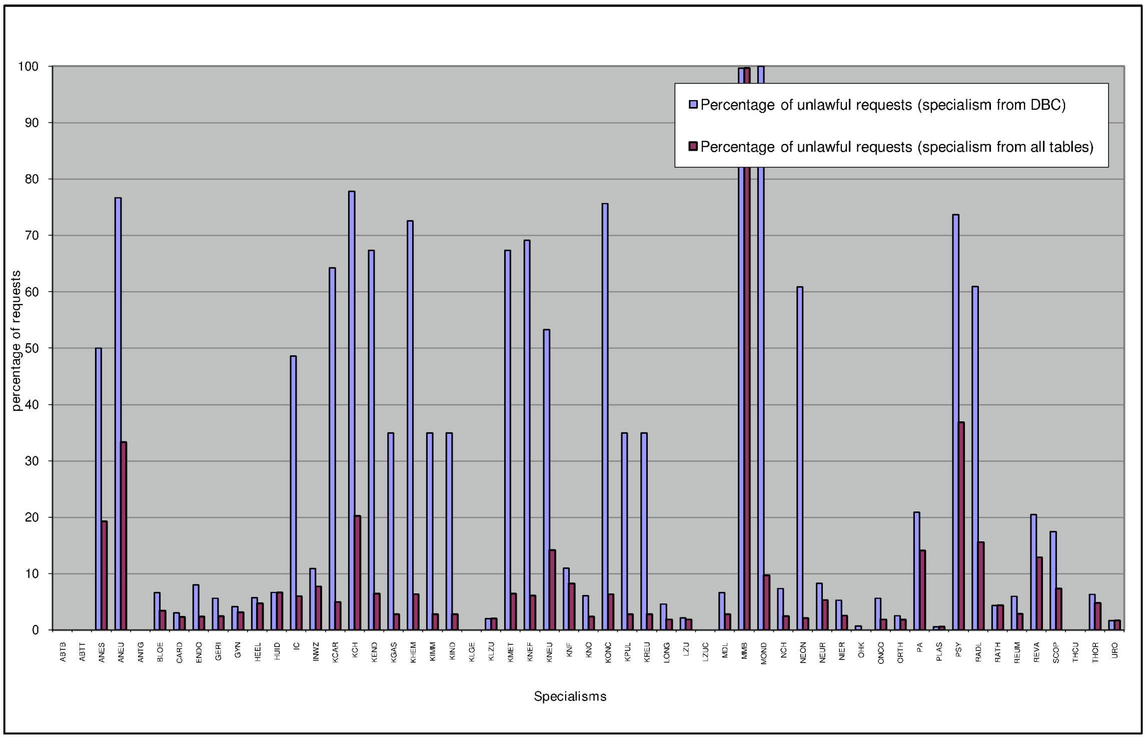
This study began with the premise that the EHR infrastructure is inescapable, i.e., that it is just a matter of time before it is introduced to the general public. However, several issues, including patient data confidentiality, related to the EHR, have not yet been dealt with satisfactorily. In this study we therefore analysed the feasibility of a system that allows all care providers to access all patient data, but are monitored by a control and alarm system as currently stated in the specifications of the Dutch health care infrastructure [10].

In our study, we have created a conceptual schema of the health care domain, which, together with a Dutch hospitals policy, we used for formulating requirements for lawful and unlawful requests for patient information. These requirements were stated as SQL queries in terms of a matching specialism between the medical specialist and a DBC of the patient (and other supporting facts), which were then executed against the database of the hospital information system.

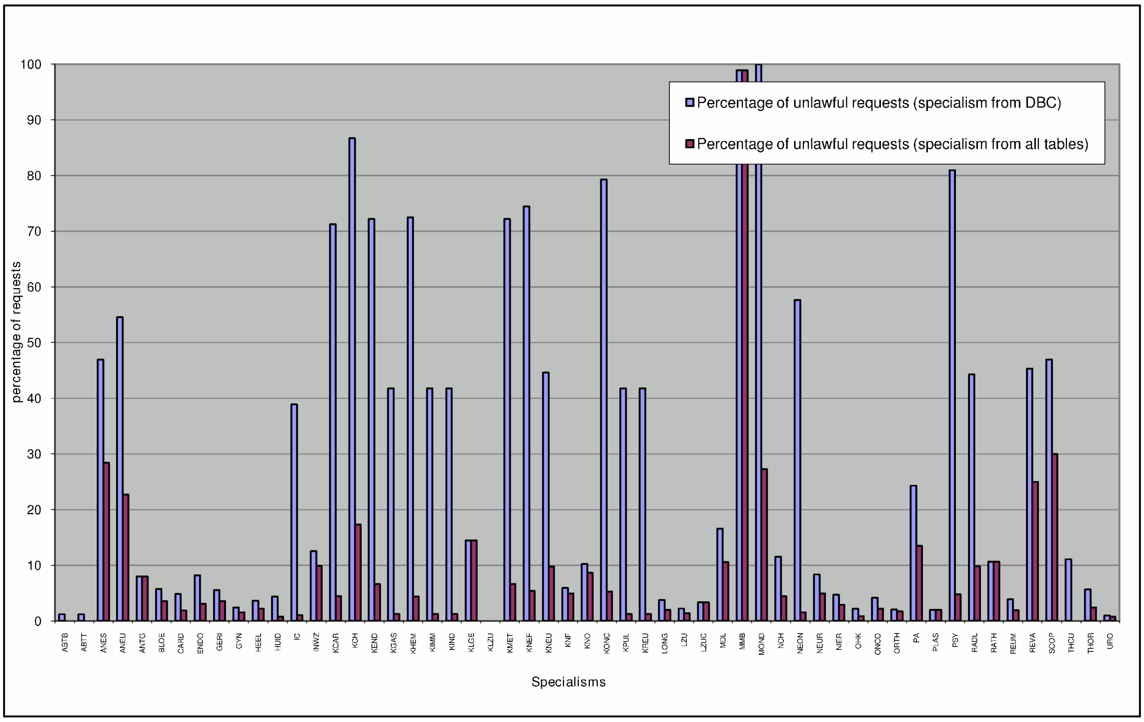
From the results follows that the DBC, as it is currently used, is in itself not a good measure for obtaining evidence that supports the requests of patient data information. Using this measure, many of the requests were classified as possibly unlawful, sometimes even up to 100% of the total number of requests. Using additional facts to obtain justifiable evidence considerably decreased the number of possibly unlawful requests, but the total number still ranged between 8% and 9% of the total number of requests. This is too high for practical purposes as the number of requests for patient data ranged in the order of 50.000 requests per week in the hospital under study (measured by the number of log entries).

Our empirical study shows that many of the unlawful entries generated are caused by specialisms that act as a gateway for other specialisms or are asked for consultation by other specialisms. For example, pediatrics is, in our case, subdivided into a number of subspecialisms that often consult each other. Taking pediatrics instead as specialism for all these subdivisions, would allow for a drop in unlawful entries.

As a final note, it is unclear whether the current law can be forced upon medical care providers in the current setting. In our study we did not directly aim for a one to one mapping between the law and our notion of (un)lawful access to patient data. This relation seems to be impossible to define with certainty when a treatment agreement is never stated somewhere in the system. It is still an open question if this would be practically feasible as patients often see several medical specialists, who may not be known in advance.



(a)



(b)

Figure 4: Percentage of (un)lawful entries per week (measured for two separate weeks shown in (a) and (b)) based on matching the specialism of the medical specialist with (1) the specialism corresponding to a DBC and (2) with the specialisms retrieved from all facts involving the patient.

6 Future work

Although the DBC is already being used in health care, there are still a number of problems. For example, ‘gate specialisms’, i.e., specialisms that act as a gate for the patient to enter the hospital, often provide support services, like endoscopic views, for which no DBC is opened and therefore cannot be attached to a DBC. As such specialisms often produce extra costs it is imperative that they are transparent. An extended data model is being developed that allows for the creation of care trajectories for all the different types of care such that all activities and services can be attached [2]. Having a model that clearly connects all facts about a patients care process together clearly would benefit the internal consistency of the hospital information system and provide a more solid base for validating patient data confidentiality.

In addition, the conceptual schema used within this paper is somewhat simplified. For example, in the schema used, EHRs are always retrieved completely, whereas one would like to structure the EHR such that parts from it can be requested. It is expected that certain medical personnel are not allowed to view the complete EHR, but are allowed to view some of its parts. For example, a secretary would be allowed to view patient information like name, gender, birth, etc., but not any data related to the medical condition of the patient.

Acknowledgements

We acknowledge the hospital staff for making the anonimised medical data available. Furthermore, we acknowledge Bas van Gils for checking the syntax of the ORM model.

References

[1] DBC Onderhoud. *Aanpassingen DBC Systeem per 1-1-2006 – Specificaties en toelichting bij de registratie, validatie en declaratie, version 1.4.1*, October 2005.

[2] DBC Onderhoud. *Uitbreiding DBC Systeem 2007 – Specificaties en toelichting bij de registratie, validatie en declaratie*, Juli 2006.

[3] M. Eichelberg, T. Aden, J. Riesmeier, A. Dogac, and G.B. Laleci. A survey and analysis of electronic healthcare record standards. *ACM Computing Surveys*, 37(4):277–315, December 2005.

[4] J. Grimson, W. Grimson, and W. Hasselbring. The SI challenge in health care. *Communications of the ACM*, 43(6), June 2000.

[5] T.A. Halpin. *Information Modeling and Relational Databases*. Morgan Kaufmann, 2001.

[6] A. Hamakers. Het waarborgen van de confidentialiteit van elektronische patiëntendossiers. Master’s thesis, Radboud University Nijmegen, 2007.

[7] I. Iakovidis. Towards personal health records: Current situation, obstacles and trends in implementation of Electronic Healthcare Records in Europe. *Int. J. Medical Informatics*, 52:105–117, 1998.

[8] E.H. Kluge. Informed consent and the security of the electronic health record (ehr): some policy considerations. *International Journal of Medical Informatics*, 73(3):229–234, March 2004.

[9] C. Lovis, S. Spahni, N. Cassoni, and A. Geissbuhler. Comprehensive management of the access to the electronic patient record: Towards trans-institutional networks. *International Journal of Medical Informatics*, 76(5–6):466–470, 2006.

[10] NICTIZ. *Specificatie van de basisinfrastructuur in de zorg, version 2.4*, August 2006.

[11] T.C. Rindfleisch. Privacy, information technology, and health care. *Communications of the ACM*, 40(8):92–100, August 1997.

[12] K. Spaink. *Medische Geheimen*. Nijgh & Ditmar, 2005.