Patient Data Confidentiality Issues of the Dutch Electronic Health Care Record

Perry Groot Ferry Bruisten Martijn Oostdijk
perry@cs.ru.nl martijno@cs.ru.nl

Institute for Computing and Information Sciences, Radboud University Nijmegen, Toernooiveld 1, 6525 ED Nijmegen, The Netherlands

Problem Description

There is mounting pressure on health care organizations to improve efficacy and cost-effectiveness. Information Technology is seen as an enabling technology and a major factor in steering these developments. A recent development is the Electronic Health care Record (EHR), which is defined as

> digitally stored health care information about an individual's lifetime at all times with the purpose of care, education, and research, while ensuring confidentiality at all times

Many issues of the EHR, including patient data confidentiality, are still not resolved completely. For example, it is difficult to specify and enforce access control on a global scale. This can be dealt with by giving all care providers access to all patient data, but use a control and alarm system to monitor and log all data access. The latter option is currently used in the specification of the Dutch EHR, however, it is still an open issue how to model such a system. In our research, we investigate whether ***a control and alarm system is a viable option for ensuring patient data confidentiality***.

Background

A basic infrastructure has been specified by NICTIZ (national institute for ICT in health care), which uses a central service system to keep track of all available medical data from various medical institutions. Care providers can log on to the system using their UZI number linked to a chip card, the UZI pass. Patients are identified using their BSN number. The Dutch laws WBP and WGBO specify what medical personnel are allowed to do with patient data. Basically, a treatment agreement should exist between patient and care provider, but is seldom directly documented in practice.

Local Hospital

In our study, we were able to use the resources of a local hospital, who had developed their own local policy for increasing the internal control on patient data access. In this policy several types of care providers are identified for which the hospital prefers a system that can generate a warning whenever a care provider is accessing patient data that is (or was) not treated by the specialism of the care provider. In our study, we only focus on the group of medical specialists.

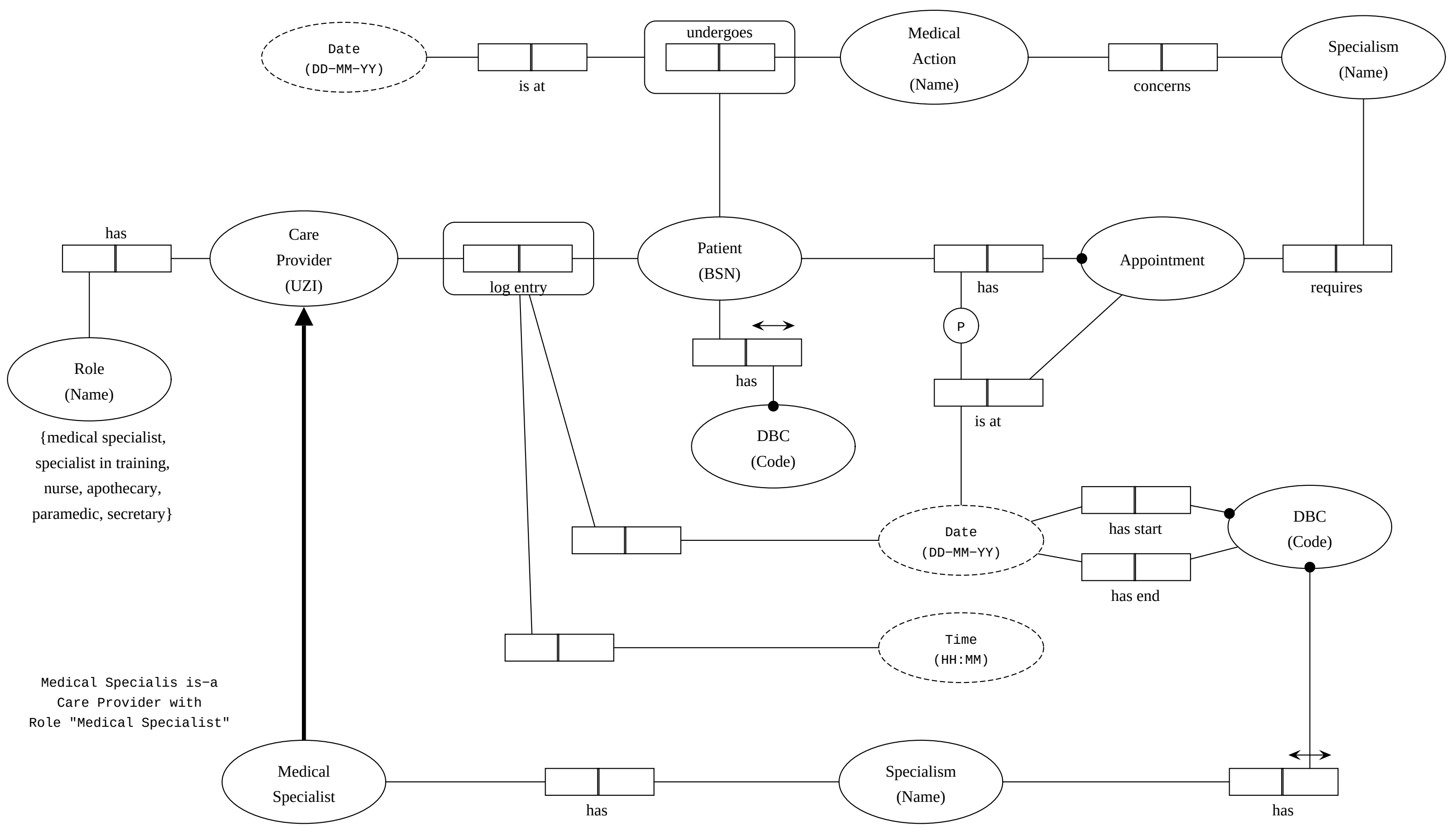
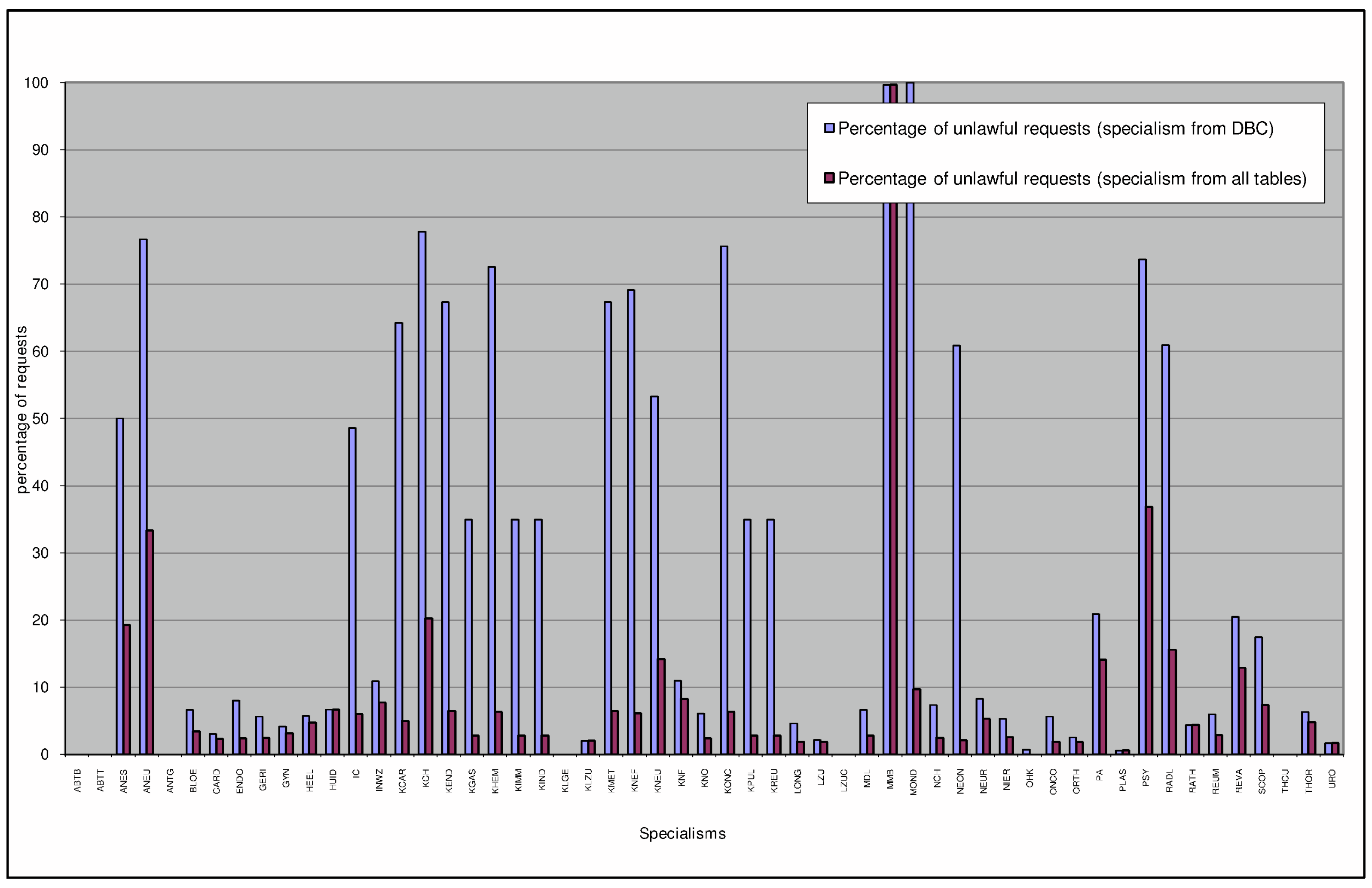


Figure 1: Simplified ORM model of the Universe of Discourse.

The first step in our study was to make an ORM model of the local hospital, which is shown in Figure 1. 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. 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.

Empirical Results

In the second step of our study we used SQL to query the databases from the local hospital, which were roughly created according to the scheme in Figure 1. With the SQL queries 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. This provides a reasonable indication of the number of (un)lawful accesses to patient data. To improve results we also retrieved specialism from additional supporting facts such as appointments, performed medical actions, hospital stays, visitations, etc.



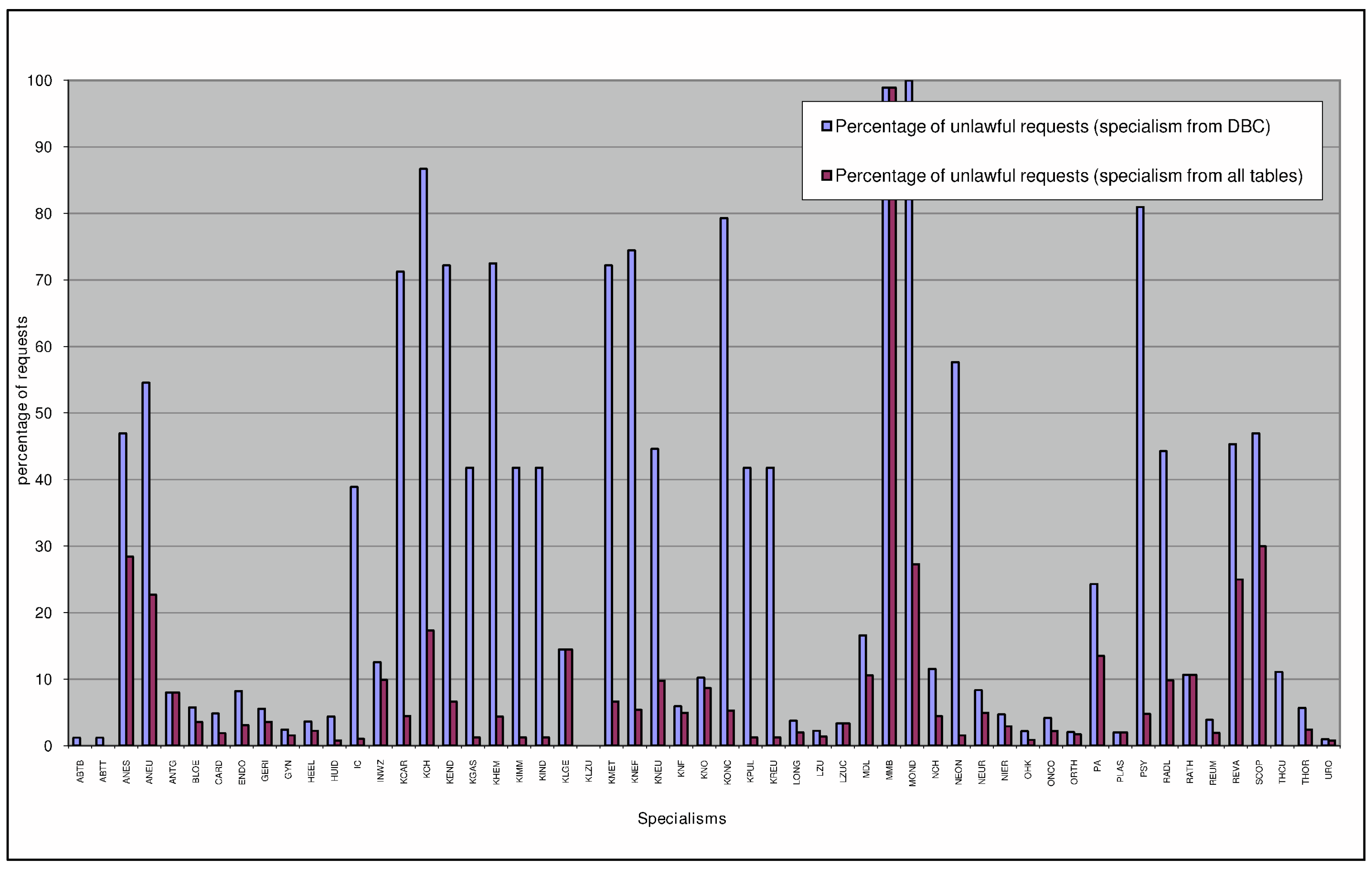


Figure 2: Percentage of (un)lawful entries per week (measured for two separate weeks) based on matching the specialism of the medical specialist with (1) the specialism corresponding to a DBC and (2) with the specialisms retrieved from all facts involving the patient.

Conclusions

Clearly there is a lot of variability between different specialisms, but matching specialisms of the DBC and medical professional is in itself not a good measure for providing patient data confidentiality. Additional supporting facts considerably improved results, but the total number of unlawful requests of patient data still ranged between 8% and 9% of the total number of requests. This is too high for practical purposes as the number of requests typically ranged in the order of 50.000 requests per week. In our study, many unlawful requests are generated by gateway specialisms, i.e., specialisms that are consulted or that act as a gateway to other specialisms as tests need to be performed first before one can determine certain diseases. 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 result in a drop of unlawful entries.

Abbreviations

BSN: Burger Service Nummer
DBC: Diagnose Behandeling Combinatie
ORM: Object-Role Model
UZI: Unieke Zorgverlener Identificatienummer
WBP: Wet Bescherming Persoonsgegevens
WGBO: Wet op de geneeskundige behandelovereenkomst

Reference

[1] Perry Groot, Ferry Bruisten, and Martijn Oostdijk. Patient Data Confidentiality Issues of the Dutch Electronic Health Care Record, In *the 19th Belgium-Netherlands Conference on Artificial Intelligence (BNAIC)*, 2007.