Outline of a surveillance service for drug prescription

C. Eikemeier, R. Grüter, W. Fierz

a DIMSA Working Group, Department of Mathematics and Informatics, University of Bremen, Germany
b University of St. Gallen, Switzerland
c LogoLab AG, Zurich, Switzerland

Introduction

The missing integration of data in different areas of the healthcare domain is reason for a significant number of drug interactions and side effects [1–5]. At least a significant reduction of the number of serious adverse events (SAE) is demanded because of ethical and also because of economical reasons.

The need for information exchange between the healthcare providers is evident [6]. Different regional and even national projects implement and evaluate solutions to implement an electronic patient record. They include card-based solutions, peer-to-peer networks and even server-centric solutions [7–13, cf. SMI 52]. In only few projects the complete patient record is directly made accessible. There is always a chance that parts of the patient data remain hidden. Thus, treatment or medication surveillance can only report problems unimpeachable: if a problem is reported, it will be there. But in general, the negation is not true.

Additionally, providing the patient data to the physician does not automatically result in a higher medical treatment quality [14]. The healthcare provider needs some kind of decision support by an automatic system to cope with the amount of data. The use of a clinical decision support system results in improved care [15].

Overview and basic idea

The surveillance of medical treatment decisions based on a consolidated data pool (e.g. in a hospital setting) can be carried out automatically [16–18]. It is similar to checking the adherence to clinical guidelines and both systems can be combined. But today data often is not yet concentrated; often each physician keeps his own data repository. Currently accessing the patient record demands to manually request each single part of the record. This is impractical and among the reasons why double examinations occur.

In conclusion, one approach to meet with the above-mentioned requirements (to counter information glut, to keep the existing data infrastructure, help to benefit from additional information) is to use the VETO! principle [19]. VETO! is a reactive group decision support system that checks if a decision of one member of the community complies with the knowledge of other community members. A prescription of a medication triggers a surveillance process (fig. 1 [1]) that checks as much information of the distributed patient record as possible and comments on the physician's decision.

The VETO! principle exploits the ideas from peer-to-peer systems to collect the data but uses a central Clearinghouse to evaluate it. Data is encrypted throughout the whole process except for the evaluation in the Clearinghouse. A hash code (HC) identifies groups of patients and therefore prevents from unveiling the true patient identity. Other physicians only will see the HC uncoded, the actual data (A, B1, B2 in fig. 1) is encrypted. The identity of the physicians can be obscured likewise by using known P2P techniques [20]. The other physicians add their contributions to all patients that match the HC and send these (now filled) messages to the Clearinghouse (fig. 1 [2, 3]).

The Clearinghouse employs rules and basic facts and explores possible risks in the treatment (fig. 1 [4]). In case of predicted problems, a message is sent back to the initiating physician (fig. 1 [5]). Because the Clearinghouse is the only point where the data is uncovered, only this special entity needs additional means for data protection. It is anticipated that the Clearinghouse is run by a governmental or "neutral" organization like FDA, BfArM or Swissmedic. They are already involved in the control of drugs and issue new official drug-related announcements and maintain the related expert knowledge.
Important parts revisited: the P2P like network and the Clearinghouse

When a prescription is issued the demand for additional relevant information is spread in the network in a P2P way [21]. Even if the surveillance system is using beneficial characteristics of P2P systems, it significantly differs from traditional P2P systems like Napster or Gnutella [22]. The use of the central Clearinghouse in the processing phase violates P2P definitions (“direct exchange of messages between the nodes”). But the phase when the query is spread differs significantly from traditional client-server systems and is similar to characteristics of P2P systems.

The reasoning system in the Clearinghouse is to be maintained by experts that define “Gold Standards” based on current research. These rules are dynamically adapted to new findings and as the computation is done in real time, only up-to-date knowledge is used.

Providing a central entity for processing the queries demands for a powerful IT system at the Clearinghouse. But it prevents from the burden to update the functional logic in all IT systems of the physicians. This would be necessary if in a true P2P manner the collected data has to be evaluated at the peer that initiated the question.

Security aspects

As this system deals with patient data, data safety is of high importance. Neither the issuing physician is allowed to see pieces of data that do not originate from himself, nor may other providers that add information (e.g. old prescriptions) to the message see any other data of the patient. Only the CH is able to uncover all data and check the message content. Today’s security software libraries provide public key infrastructure mechanisms, means to encrypt data and offer the ability to build hash keys to avoid data fraud [23]. It is a predominantly political/legal question how the transmission of medical data has to be secured. Perhaps current legal restrictions have to be reconsidered to match the public needs but not to restrict the possibilities of healthcare telematics too much.

The architecture of the VETO! system offers full anonymity of the patient identification. This is achieved by assigning a patient to a group of patients (having a common group hash key) and collecting all data of that group upon a query. Hence the provider of additional data does not know if his contribution really matches the patient in the query. Not until the identities in the two parts of the message are uncovered in the Clearinghouse, two completely different parts can be linked together.

The data is collected in a message container that consists of three parts: the hash key (readable), the query data (encrypted) and at a later stage the additional data (encrypted).

The first part of the security system is the building of a hash key from the patient’s metadata. For example the first, last character of the name and the month (numerical value) of the date of birth can be used: -MR10- if Miller is the name and October is data of birth. The encrypted name and the intended prescription form the query data. They are encrypted with the public key of the Clearinghouse. Together with

Figure 1 Overview of the VETO! system.
the unencrypted hash code this message is spread around to all peers in the network. Their IT systems automatically check for all patients with the same hash key. It is intended that this will also include Maier, also born in October. Therefore the provider of the additional data cannot be sure that the information will match in the end. He sends the received data together with his contributions to the Clearinghouse. There the two encrypted parts of the message are decrypted and it is checked if the different parts belong together. If this is the case, the expert knowledge rules are applied and a possible problematic outcome is issued to the initiating physician.

The Clearinghouse has a special role: for not creating a bottleneck the performance has to meet an average demand for processing power. Examples like eBay.com or google.com show that it is possible to build and manage such systems.

Implementation issues
One basic problem is the embedding into the information systems of the healthcare providers. Some kind of a general purpose adapter (hardware/software) will become the interface between the telematics network and the local information system. These adapter systems (e.g. called “connector”) link the platform services to the concrete data in the healthcare information systems (commonly based on HL/7). HL/7 medication orders directly point to relevant information. Rules of guideline applications written in the Arden syntax can be linked with HL/7 data by using the GELLO language [24]. The implementation of surveillance systems based on local data already offered the solution. This is not specific to the VETO! approach.

Another problem is error handling to cope with typos. The VETO! can partly deal with such errors. The expert knowledge rules issue a VETO! warning if a medication with a similar name exists and seems to be more appropriate in the current situation. The physician then can reconsider the prescription.

Possible barriers
A key requirement for the VETO! system is the availability of structured electronic patient data with the providers. This requirement will be gradually fulfilled over time, with drug data probably being at the forefront of this development. In fact, as soon as a provider is prepared to use an online drug ordering system he will very likely store the ordering event in the electronic patient record in a structured way and thereby providing the bases for being successfully addressed by other members of the P2P system. However, for other clinical data like SAE a similar incentive for structuring – if not demanded by legal requirements – is less likely. Information might be hidden in free-text entries to the patient records.

Furthermore, even when data are well structured, there might be semantic barriers that make the task of the Clearinghouse difficult to fulfil. It would be important then, that the Clearinghouse provides a commonly used vocabulary of drug names, dosage schemes, and if possible also for SAEs and laboratory data. MedDRA is one currently followed approach [25].

Another possible problem is related to the anonymity of the providers. Since the physician has to rely his decision in case of a warning coming from the Clearinghouse on foreign information, he might well want to know where the information is coming from. If transparency of the source of information is required, the Clearinghouse can provide this information. The advantages of anonymity and the trustworthiness of information have to be balanced.

Results and discussion
The presented concept is base for an efficient system to avoid serious adverse events in drug prescription. All pieces of the patient record will remain where they were created. This is one of the main advantages of this system compared to others. The Clearinghouse approach allows keeping the data encrypted as long as possible. The used hash key mechanism protects the original data from being exploited. They remain encrypted until being processed in the Clearinghouse.
Introduction in real life is evolutionary, that means, it can start on a regional test project and will improve the more providers are connected and the more structured data is fed into the system. Further optimisations allow tuning the base concept. The usage of a patient healthcare card [10] will simplify the overall system and enhance the matching performance. The VETO! system will benefit from a unique patient ID. The clinical expert knowledge can be taken from existing databases. Only the adaptation to the concrete usable form is needed.

Open questions for the introduction most likely stem from an economical and political point of view: the question of incentives to participate. As mentioned earlier a huge group of patients will benefit from the introduction of such system. So there is an ethical obligation to use the better system. Life and health insurances will also get monetary advantages and will likely pay for the better treatment quality even if it is hardly possible to measure the concrete effects. The introduction of an online surveillance system itself can be forced by official authorities. It needs to be discussed how to deal with ignorance against VETO! warnings.

This system could lead to a new high quality service that has not been realized before even if the underlying problems already are known for a longer time and the solution were generally available. It is remarkable that exploiting the benefits of peer-to-peer systems leads to such simple, yet powerful solution.

Literature

4 Lutterrotti N. Wenn Arzneimittel mehr schaden als nützen. NZZ 17.11.2004, 269.
10 Bales S. Welche Möglichkeiten bringt die neue elektronische Gesundheitskarte den Patienten? www.dimdi.de/de/ehealth/karte (accessed on 2004/03/10).
19 VETO Homepage. www.veto.ch/vu.