Integrity of Electronic Patient Records

Joris Hulstijn, Jan van Der Jagt, Pieter Heijboer

Integrity of Electronic Patient Records[1]

Joris Hulstijn[1], Jan van der Jagt[2], Pieter Heijboer[3]

[1] Delft University of Technology, Delft, The Netherlands
[2] Amsterdam, The Netherlands
[3] Ricoh Europe, Amsterdam, The Netherlands
j.hulstijn@tudelft.nl, janvanderjagt@ziggo.nl, p-heijboer@hetnet.nl

Abstract. We discuss a reference model for security measures to preserve integrity of information. Unlike traditional approaches which focus on an defensive approach to preserving integrity, we also present offensive measures to stimulate integrity of information, by providing feedback from usage. The reference model is used to analyze the security measures proposed in the design of the Dutch national Electronic Patient Dossier (EPD), in particular the projected application for medication records. We conclude that much of the defensive measures were covered, but that some offensive measures are lacking, in particular measures related to trust. This may have harmed adoption.

Keywords: health care information systems, information security, integrity

1 Introduction

Electronic Patient Records are information systems for storing and retrieving information about the medical treatment of a patient. In developing such systems, countries have come up with different solutions regarding the trade-offs between budget, usability, security and acceptance. This is far from easy [7]. Also in the Netherlands there has been much controversy surrounding the development of a national Electronic Patient Dossier (EPD). In April 2011 the Dutch First Chamber of Parliament voted against the obligatory use of the national EPD, ending a project that started in 2002 and cost about 300 million euro [27]. The main reasons for rejection were the continued controversy over the security of patient records, combined with the inability of the government to convince senators of the necessity of a system at this scale. It is expected that local EPD initiatives will continue to be developed, taking over parts of the national infrastructure

This controversy shows that information security is an important concern in the development of electronic patient records, because it relates to their acceptance by the public. Public opinion is mostly concerned about privacy: are the records well protected? Of the quality aspects of security (confidentiality, integrity and availability), confidentiality therefore receives most of the attention (e.g. [3],[2],[19]). Less is published about integrity of patient records: can the contents be relied upon? This is an omission, because information integrity is crucial for meeting the objectives

[1] The research in this paper was conducted as part of the graduate thesis project of Jan van der Jagt and Pieter Heijboer at the IT Auditing department of VU University, Amsterdam [12].

of electronic patient records, namely to facilitate reliable exchange of information and thereby reduce the number of preventable medical errors [26]. Preventing medication errors will likely save lives and reduce health care spending [14]. Also in information security in general, there has been relatively little research on integrity, compared to confidentiality. This paper aims to address this omission.

We follow Boritz [4] and define integrity as representational faithfulness: does the information stored in a system correspond to reality? Integrity concerns both accuracy and completeness and therefore timeliness too, as well as validity with respect to regulations and procedures. Integrity is therefore closely related to the notion of reliability as used in accounting [15].

When security experts or auditors assess the security of an information system, they commonly test against a norm: the reference model. In this paper we report on our experiences in developing a reference model for assessing the integrity of electronic patient records [12]. Usually, reference models are developed on the basis of information security guidelines like ISO 27001, NIST 800-53 or COBIT 4.1. These guidelines do mention integrity, but we found them not specific enough. In particular, on the basis of Boritz's [4] characteristics, we selected all control objectives in the COBIT 4.1 guidelines which are relevant to integrity. We identified 48 of them [12]. However, it turned out that most of these control objectives address enabling conditions, such as base level security or auditability, but do not address integrity itself. This makes such control objectives impractical as a norm: difficult to test against. What is needed is an organizing principle to structure the reference model.

Guidelines for information security define information integrity as: "… guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity"[9]. This shows a rather defensive approach: once information is stored reliably it should be protected to keep it that way. The well known Clark and Wilson [8] model is an exponent of this view.

In this paper, we would like to argue that such a defensive view is necessary, but not sufficient. People are bound to make mistakes. Defensive measures do nothing to detect or correct errors once they have been made. Moreover, integrity may actually be served by transparency and openness. For example, the Wikipedia model of ensuring reliability of encyclopedia entries is based on openness and feedback. Therefore we propose to use offensive measures too, which aim to enhance integrity.

Summarizing, the research questions of the paper are as follows:

1. Can we develop a security reference model specifically addressing integrity, which includes measures to both maintain and improve information integrity?
2. Can the usefulness and adequacy of such a reference model be established in a case study, namely an infrastructure for exchanging electronic patient records?

The paper is structured as follows. We will first discuss the definitions (Section 2). Then we will develop a reference model containing both defensive and offensive measures (Section 3). We illustrate the usefulness and adequacy of the reference model by analyzing the security measures proposed in the design of the Dutch National Electronic Patient Dossier (EPD), focusing on medication data (Section 4).

2 Defining Integrity

What are the main characteristics of integrity? Accounting practice traditionally focuses on reliability, i.e. *correctness* (or accuracy): does the information correspond to reality, and *completeness:* are all relevant aspects of reality represented? [22][15]. These concerns have been taken over in information security. Thus the 'Code of Practice' regards integrity as "the property of safeguarding the accuracy and completeness of assets" [12]. Both correctness and completeness crucially depend on *timeliness*: failure to update when reality is changing leads to misrepresentation. Information is generated from raw data by processing steps like calculation, selection or aggregation. The more processing is needed, the harder it becomes to trace representational faithfulness. Therefore the *validity* of information, i.e. whether it has been generated according to authorized procedures, is crucial. Consider for example the exam results in a university administration. There is no reality outside university records, which is why there is an elaborate system of procedures for submitting exam results, and segregation of duties between lecturer, student and administration.

Maintaining absolute integrity is impossible. In consultation with stakeholders, tolerances must be set. For example, in a hospital, inaccuracy or incompleteness of medication data has more severe effects, than mistakes in the patient's name and address. A classification of the impact of errors leads to so called *integrity levels* [4]. A system should be designed in such a way that components with a lower integrity level cannot compromise high integrity components.

As we stated in the introduction, we distinguish two strategies. They can now be defined more precisely. The *defensive strategy* is aimed at keeping the current level of integrity. The *offensive strategy* aims to increase the current level of integrity.

3 Defensive Strategy

For any information system, the data definition and information structure should follow from the underlying semantics (meaning). The semantics determines which data types make sense, which data values are accepted, and specifies relational constraints between data entries (reconciliation). For example: a date of birth is always prior to the present date, or the total amount of travel expenses aggregated over projects must be equal the total amount of travel expenses aggregated over employees. Such conditions are called *integrity constraints*. Integrity constraints can be formalized and automatically maintained by a database management system [11]. Automated enforcement of integrity constraints requires that users may only access the data through the automated system. This principle of *encapsulation* prevents improper modification.

When an information system meets its integrity constraints, we say it is *internally consistent*. There are also constraints about the relation of the data with the external world. For instance, in a hospital there is a policy that no treatment may be started without first registering the patient's identification number. However, in this case, computer systems are unable to enforce that the number actually belongs to the patient (correctness), or that all actual treatments are being registered (completeness). When also such external demands are met, for instance by workflow procedures and verification, we obtain *external consistency* [22].

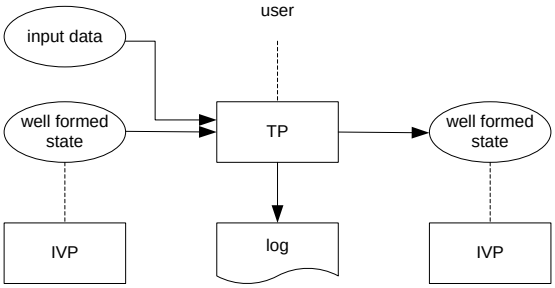

Figure 1. Integrity policies according to Clark and Wilson [8]. Arrows depict information flow and dashed lines depict control.

The defensive strategy can be explained with reference to the influential model of Clark and Wilson [8]. An integrity policy consists of two kinds of procedures. An integrity verification procedure (IVP) verifies whether a data set is well formed, i.e., meets the applicable integrity constraints. A transformation procedure (TP) has two functions. First, for newly entered input data, it verifies whether the data meets the applicable integrity constraints. Second, for all transformations, it will guarantee that the data will remain well formed and integrity constraints are preserved (Figure 1).

The process is regulated by two kinds of rules: certification and enforcement rules. Certification is done by the user of the information: in practice the security officer, system owner or data owner. Enforcement is done automatically by the computer system (encapsulation). We follow the original numbering of the article, but for ease of explanation we use a different order of presentation.

(C1) IVPs are certified to verify the relevant *integrity constraints* for a given data set. If they do, the data set is called valid.
(C2) TPs are certified to be *valid*, i.e., each applicable TP must be shown to transform a valid data set into another valid data set. To this end, for all data sets a list of TPs which are certified for that data set is maintained.
(C5) TPs which deal with newly entered input data must make sure the data respect the relevant integrity constraints, or else reject the data.
(E1) The system enforces that users can't alter the data directly, but only through TPs which are certified to be valid for the relevant data set (*encapsulation*).

These rules can ensure internal consistency. To assure a certain level of external consistency, also the following control measures must be adopted by the organization.

(E2) The system maintains *authorization* tables to enforce that users can only carry out a TP on a data set for which they have been authorized.
(C3) Authorization tables are certified to conform to the principle of *segregation of duties*. The job descriptions, roles and the specification of the segregation of duties, which are used to generate the authorization tables, are validated beforehand and formally accepted by the responsible employee.
(C5') Additional verification or reconciliation procedures are implemented to ensure external consistency when new data enter into the system, as part of C5.

These certification and enforcement rules only work under certain background assumptions about the audit environment, the computer system and the employees. Some of those assumptions are already made explicit by Clark and Wilson.

(E3) All users are uniquely *identified* and *authenticated* by the system.
(C4) All TPs must preserve an *audit trail* through logging.
(E4) The *maintenance* of the certification and enforcement rules themselves is subject to *segregation of duties*. In particular, only people authorized to certify TPs or IVPs may alter the list of data sets for which they are certified, and no person who is authorized to certify TPs may have executive rights for those TPs.

In subsequent research, more background assumptions have been added, see e.g. Adams et al [1]. We briefly list them here. (E5) Automated *DBMS facilities* should generate an audit trail and allow recovery of transformation procedures. (C6) *Change management* procedures (as in ITIL) should make sure that all changes to a computer system have been certified, and the risks addressed. (C7) Basic *security measures* like hardening are required. (C8) *Data definitions* must be *maintained* by the data owner. (C9) Integrity of data from an *external party* must be *validated* before being accepted. (C10) A person must be made *responsible* for data quality [9]. (E6) The system makes sure that an employee who is *authorized* by another employee, may only execute TPs on data sets for which the second employee is also authorized. (C11) A system should be *available* for authorized employees, when needed. This avoids a 'shadow registrations'. (C12) *Back-up* and *recovery* measures must ensure that after a calamity the system can be restored.

4 Offensive Strategy

Human errors are unavoidable. An error is defined as a situation in which a planned sequence of activities does not produce the intended result, where this failure cannot be attributed to external influence [21; p 9]. There are two types of errors. The first type is misunderstanding, resulting in the sequence of activities not being executed according to plan. The second type displays a wrong understanding, resulting in the creation of a plan which is incapable of achieving the intended results [21; p 17]. Both types of error undermine the defensive strategy. For instance, errors of the first type may lead to incorrect execution of procedures. Errors of the second type lead to incorrect specification of TPs. The defensive framework cannot prevent users from omitting data, or registering data which are not externally consistent. This also applies to the data needed to preserve the framework itself, such as authorization tables.

Generally, there are three ways in which humans address errors [21; p 148]. First, by exercising *self control*, such as the correction of typing mistakes (subconscious), or checking whether the right document is attached to an email (conscious). Second, by signals from the *environment* before the error has been made. We distinguish warnings from blocking functions. Blocking functions force one to perform in the right way. For instance, the wrong key won't open the door. Warnings only guarantee detection. A timely warning may allow for a recovery before any great harm is done. Third, by feedback from *another person*. Consider the 'four-eyes' verification procedure, in which a colleague verifies some task before it is finalized. For instance,

in pharmacies, a colleague must routinely verify whether the medication matches the prescription, before it is handed to the patient.

We have taken recommendations from the literature on information quality, such as Boritz [4; p 81-85] and English [9; p 337-339]: awareness, trust, simplicity, proactive measures and automated support tools. They will now be explained in full.

Awareness. Security policies should address integrity of data and rewarding schemes.

A1. Participants should understand what is meant by integrity, its impact on the organization, and how they can improve it (awareness). (Boritz 2004; p86).

A2. The primary recording of data should be given more status, reflected in rewards. Rewards to stimulate efficiency may negatively affect quality (Boritz 2004;p 80).

Trust and feedback. Many enterprises are nowadays organized as chains or networks of relatively independent organizations which need to cooperate. Business processes cut across these organizational boundaries, so they require frequent exchange of information. This requires trust. Trust is needed for cooperation [16]. Cooperation in turn implies that people are using each others' data, and help each other to correct or improve its quality. It is well known that feedback generated by actual usage is crucial for maintaining data quality [20].

In organizations, trust and feedback can be influenced, for instance as follows:

T1. Resolve borderline disputes and organizational barriers between departments, for instance by frequent meetings about interoperability issues [4; p 86].

T2. When specifying integrity constraints, take all known information needs into account, also those from beyond the own organization (English 1996; p 44). This avoids organizations setting up 'shadow administrations', which do not align.

T3. Initiate frequent meetings in which all stakeholders discuss data definitions, and the required integrity level. This promotes mutual trust in the information.

T4. Allow employees to participate in the design of systems and processes, to make systems easier to use and thereby make it easier to record data reliably.

T5. Stimulate feedback of employees on the actual usage of the information based on the data they have recorded [20].

Trust provides a basis for cooperation and thereby for improved integrity. However, there is also a risk of too much confidence. In our experience, people may accept poor quality data just to avoid conflicts. A healthy balance between trust and skepticism regarding the quality of data of other parties, will improve integrity of information.

Simplicity. Business process reengineering may contribute to the improvement of integrity. A simpler process will reduce the chance of making an error and will make it easier to correct detected errors. A process can be simplified by reducing the number of steps or by reducing the number of people involved.

S1. Stimulate that data are actually being used: "Use it or lose it!" [20]. Data which are not being used will not get feedback needed to improve accuracy.

S2. Record original data in one unique location, as close to the source as possible. Avoiding intermediate processing will avoid new errors [9; p 58].

S3. Deliver information immediately to the end-user from the system itself, to avoid information getting lost or being manipulated in between by others.

S4. Make sure that procedures and agreements regarding integrity are accessible and available. Make sure users can review the data definitions of the data they use.

Proactive measures. Maintaining integrity also requires proactive efforts to verify and correct errors.

P1. Make sure all entered or modified data is being verified. The lack of an explicit control in a routine procedure is a common cause of errors [21;p 59]. Verification can be achieved by the so called four-eyes principle, or by a party with an 'opposed interest': e.g. the client verifying the quality of a service, before paying. Controls must be integrated in the workflow.
P2. Instruct employees to take each contact with a customer or end-user as an opportunity to verify data. A time-stamp of the latest modification is crucial.
P3. Make sure that standards and agreements about data definitions are obeyed. Data pollution caused by not following standards is hard to clean up.
P4. Repeatedly verify whether routines, procedures, protocols or controls aiming to stimulate integrity are still effective.
P5. Carefully analyze all integrity related complaints, so root causes can be traced.
P6. Actively search for errors and defects on a regular basis. Use data mining and data analysis tools and knowledge of the semantics (reconciliation), to detect irregularities and patterns of usage which deviate from what is to be expected.

Information System Support. Information systems themselves can also play a role in the offensive strategy, by supporting users to follow procedures.

I1. Introduce additional records to a data collection to be able to determine integrity and repair data when needed. Examples are serial numbers, time stamps of the latest update, or the name of person who made the latest update.
I2. Introduce functionality to support users in assessing the current level of integrity. Examples are control totals, intuitively designed forms, or the use of colors to distinguish different risk categories. For example, in a pharmacy prescriptions for 'dangerous' drugs can be printed on pink rather than white paper.
I3. Implement opportunities for eliciting feedback in the information system, in order to relay errors to the source, and allow corrections to be made.
I4. Implement warnings or signals about the current status of the integrity into the information system.
I5. Record source documents (e.g. paper medicine prescriptions) electronically and make them available when access is necessary for validation.

These measures can be implemented in a Workflow Management System (WfMS).

In addition, there are many best practices regarding information systems management, such as incident management and problem management (ITIL).

I6. Set up the complaints department or the helpdesk in such a way that it gives insight in common causes of integrity related incidents (incident management).
I7. Set up technical departments in such a way that they analyze common underlying root causes of incidents, and give systematic solutions (problem management).

This concludes our overview of the measures to maintain and improve integrity. These measures can be used as a reference model in an information security assessment, focusing on integrity. In our case study we discuss one such audit.

5. Case Study: Dutch national Electronic Patient Dossier

In this section we discuss the information integrity measures proposed in the design of the Dutch national Electronic Patient Dossier (EPD), focusing specifically on the application for exchanging medication data, the Electronic Medication Dossier (EMD). Although the national EPD has been rejected by parliament, its design does remain a representative instance of a system for electronic patient records.

The purpose of this initial case study is to test the usefulness and adequacy of the reference model for assessing security measures specifically focusing on integrity, in particular the distinction between defensive and offensive measures. Proper validation would involve many more case studies, also in other domains, and should contain comparisons with other security reference models.

5.1 Research Approach

Data for the case study were collected by means of semi-structured interviews with representatives of the major stakeholders to analyze the decision making process around the Dutch national EPD, focusing on integrity aspects. We spoke with representatives of several patient organizations, physicians, pharmacies, project managers, health informatics experts and software providers. In addition, we studied the proposed architecture and security measures by means of publicly accessible data. On the basis of this we made an overview of the security measures taken or proposed in the infrastructure design. These security measures were compared with those suggested by the reference model, and compared with the concerns raised by stakeholders in the interviews. The results were validated with two security experts.

5.2 Case Description

The Dutch national EDP is being developed by NICTIZ, a subsidiary of the Dutch Ministry of Health. An *electronic patient dossier* (EPD) is defined in the context of this project as a collection of electronic data related to the medical treatment of a patient. An EPD is maintained by care providers for the benefit of other care providers. It differs from a Personal Health Record (PHR), which is maintained by the patient. The Dutch national EPD has two functionalities: (1) data exchange and communication between care providers related to the current joint treatment of a patient, and (2) retrieving historical patient data, recorded as a result of other current and prior treatments, to improve the current treatment of a patient .

This means that the Dutch national EPD is not unique. Many kinds of EPDs are already being used at local level, by general practitioners, pharmacies and in hospitals. The national solution was supposed to improve upon these local initiatives, because of improved scope, security, and privacy protection. Note however that these advantages are related to security, not usability or content. Content must be provided by the health professionals themselves. The main characteristics of the EPD are:

- *Virtual Dossier*. All patient data remain stored in the original source systems. At a central level only a reference index is being developed, which allows access to particular patient data upon request. The EPD only provides a virtual dossier.
- *Closed Network*. Access to the EPD is only possible through a closed network, the so called AORTA (see below). All messages are being encrypted and communication over the network takes place according the HL7 standard.

– *Identification and authentication*. Each care practitioner needs a special identification pass to log onto AORTA. This pass contains encryption keys for authentication and secure message exchange.
– *Unique patient identification*. Patient's records must be stored under the patient's unique citizen service number (BSN), which allows data about from different sources to be identified, and combined.

In principle, a national infrastructure set up along these lines could host several EPD services. Even at the end of the project, only two of those services were operational: the medication dossier, and the dossier for transfer of records among general practitioners, for instance after a stand-in or weekend service. In this paper we focus on the medication dossier.

The network infrastructure for information exchange between care providers is called AORTA. Each health care provider (general practitioner, pharmacy, hospital) can connect through the so called National Switchboard (LSP), mediated by so called Healthcare Information Brokers. A requirement is that the existing system has been classified as a "well maintained healthcare system" (GBZ). Connection of a well-maintained healthcare system to the national infrastructure is realized through data communication networks maintained by certified Healthcare-related Service Providers (ZSP). Hospitals typically provide their own ICT services.

Previous attempts to link medical data lacked a unique way of identifying patients. The existing social security number was 'upgraded' to citizen service number (BSN) and is now used as identification throughout the healthcare sector. The number appears on passports and identity cards, to allow authentication. The wide usage of the BSN greatly enhances integrity of the EPD: making a correct link between the patient and his or her dossier (external consistency) has become a lot easier.

Within each electronic patient dossier, NICTIZ distinguishes the following types of data, each with different requirements concerning privacy and storage period: personal data (name, address, residence), logistic data (appointments, reservations), medical data (diagnoses, lab results, x-ray images, medication), financial data (insurance, invoices) [17]. Clearly, these categories require different integrity levels.

The crucial data structure of the EPD is the *reference index*. This index keeps track of which data records about a patient are available at which source. The reference index is maintained through four basic functions: entering new data, modifying data, requesting data and protecting data. Protected data will not be exchanged over the national infrastructure. Data can be protected when a care practitioner has decided to not (yet) provide access on the basis of his or her professional secrecy, or when the patient has indicated that he does not want data to be published, for privacy reasons. Here we see the contradictory demands of integrity and confidentiality, because this feature will harm completeness of records, and hence integrity.

5.3 Application: Electronic Medication Records

We focus on the electronic medication dossier (EMD). The functionality of this dossier is to support the medication therapy process, in particular for care outside of the hospital, shown in Figure 2. The process consists of five steps which are typically performed in a loop, until the patient has recovered. Note that although the physician is in charge and coordinates the process, all consecutive steps are performed by different actors. This may lead to problems of transfer of information and distribution

of responsibilities. Only the patient is a constant factor in the process. This means that when the patient is less alert, communication problems may arise.

The first three steps involve a verification of medication safety; these steps could benefit from an EMD to reduce preventable errors. For instance, when a physician has an overview of all the drugs recently taken by a patient, she may be able to detect possibly harmful combinations. The system could also provide a warning in case of dangerous combinations, or in case of a dosage which differs from common usage. Similarly, the pharmacy could use a system like this to warn patients for medication interference, or simply refuse to provide the drugs in case of danger. As a matter of fact such warnings are already given on the basis of the local pharmacy sales data.

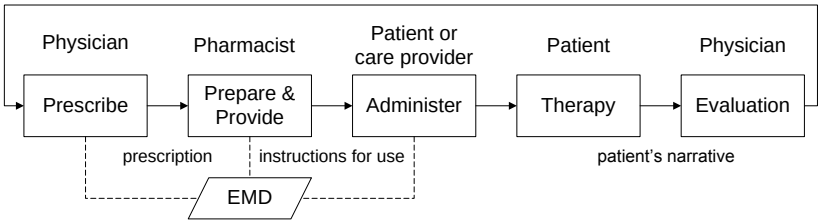

Figure 2. Medication Therapy Process, with potential benefit of an EMD indicated

The main rationale behind the EMD functionality is a finding of the HARM study [14], which states that out of a total of 41.000 medication-related hospital admissions each year in the Netherlands, that is about 2.4 % of all admissions, about 19.000 are preventable. The objective of the EMD is to reduce the number of such medication related incidents. The study also identified three specific risk areas: (i) Elderly patients are more likely to face medication safety problems. (ii) Some particular types of medicine have an increased likelihood of problems. (iii) Therapy loyalty, the condition of the patient and cognition are important factors.

To deal with these risk areas, a full scale national EMD may not be necessary. Other more targeted measures may be just as effective. For example, for elderly patients a physician in the role of so called care orchestrator could help to make transfers between care providers more smoothly. In fact many medication errors are related to the transition of hospital to home. However, hospitals and hospital pharmacies are not involved in the current phase of the project. For those people using the specific risky types of medicine, a paper or plastic EMD with RFID carried by the patient him or herself may be more effective. Finally, therapy loyalty and the conditions of the patient remain the responsibility of patient and physician anyway.

The medication safety functionality of the EMD was not ready at the time of the research. Despite the efforts the developers, there will always be limitations to automated medication safety verification. We list a few. First, there are fundamental technical difficulties with aligning brand names with the chemicals actually provided. A similar problem relates to communication of dosage. Currently there is no standard naming or dosing convention. Second, there are reasons the EMD may never be completely accurate or remain incomplete. Prescription and actual usage of a medication by the patient may not align, for example because the patient does not know how to administer the medicine well. The patient might have used medication which is available without prescription. Relevant data such as lab results are not

provided. And finally, the medication history may be incomplete, because some EMD sources may have been temporarily unavailable, or the patient could have used his right to protect his data. For these reasons, an EMD could at best only support medication safety verification by a human (physician at prescription; pharmacist at provision; nurse or patient at administering) who must be trained to work with possible incomplete data.

5.4 Interview Results

Interviews with stakeholders revealed that there are diverging views on the EMD. Pharmacists generally welcome the initiative. Patient organizations do welcome the idea, but have doubts about protection of privacy. General practitioners generally do not trust the system, and are reluctant to use it. The main concern is that they have no control over the accuracy and completeness of the data being entered at another source. Part of this results from their training. Doctors are trained to trust only what they see in front of them. Doctors often do use local EMD initiatives, in which they are in a position to know the other participants (physicians, pharmacists), which would allow them to telephone and ask for clarification, when needed.

5.5 Testing against the Reference Model

The previous description highlights the design principles and main security measures proposed in the design of the national EPD. In a larger study, resembling an audit of the set-up of the security measures, these design principles were compared against the reference model. For details we refer to Van der Jagt and Heijboer [12].

Summarizing the outcomes, we could say that the Dutch National EPD does satisfy most of the defensive measures to preserve integrity. See also Van 't Noordende [19] who made a survey of the security measures. In particular we mention:

- the certification of information systems of care providers, before being allowed on the AORTA infrastructure. This is an example of authorization (E2),
- the obligatory use of a citizen service number for unique identification of patient and record. This measure helps to ensure external consistency (C5') ,
- personal identification for care practitioners (E3) to enforce authorizations (E3).

However, regarding the offensive measures, it appears the project has not done enough. Some user groups, in particular general practitioners, generally do not trust the reliability of the data in the system and are reluctant to use it (T3-T5). One reason is the limited functionality (S1). Moreover, electronic patient records will by nature always be incomplete and inaccurate, because patients do not always take the medicine being prescribed in the dosage being described. Physicians must therefore verify medication usage with their patients, reducing usability of the system (T2). Another important issue is trust in the procedures of other care providers, to ensure reliability of data (T1). One of the reasons is that a natural feedback-loop concerning potential errors, as would exist in a local situation by telephone, is absent (T5). Moreover, due to privacy concerns, doctors or patients can block publication of some records. It is impossible to see that some data is missing. This harms the known completeness of data, and therefore the usefulness in practice (T2).

5.6 Usefulness and Adequacy of the Reference Model

A measurement instrument such as a reference model, is useful and adequate, when its distinctions help to bring out and explain aspects of a case which are also deemed relevant by stakeholders. Our interviews showed that stakeholders, in particular general practitioners, were concerned with trust and usability of the system. The reference model, especially the chapter on trust, did reveal these doubts as potential weaknesses of the design. Similar worries also motivated the rejection in parliament.
Concerning the distinction between defensive and offensive measures, we found that the defensive measures were relatively easy to assess, being specific and easily identifiable in the design specifications. The offensive measures were harder to locate. They are more about a design philosophy. This is in line with findings about assessing soft controls and organizational culture in the context of a security assessment [25].

6 Conclusions

Integrity of information is crucial, in particular in healthcare. In this paper we have developed an information security reference model specifically for integrity, and applied it to electronic patient records. We addressed two research questions.

1. Can we develop a security reference model specifically addressing integrity, which includes measures to both maintain and improve information integrity?
2. Can the usefulness and adequacy of such a reference model be established in a case study, namely an infrastructure for exchanging electronic patient records?

With regard to question (1), we have indeed developed a reference model, centering around the distinction between defensive measures, to preserve a given integrity level, and what we have called offensive measures, to create an environment and stimulate behavior which will increase the given integrity level.

We argue that defensive measures are necessary, but not sufficient. Humans are bound to make mistakes. Therefore one needs systematic ways of detecting and correcting errors. Feedback from the user will increase trust that errors will not go unnoticed. Especially in modern networked information systems, an important aspect of trust are the measures to ensure the integrity of data obtained from others.

With regard to question (2), our case study of the Dutch national EPD shows that most of the defensive measures have been covered in the design of the infrastructure. However, interviews show that key users do not trust the integrity of the data provided by the system, because they have no control over the provenance. They prefer local EPD initiatives in which they know participants and can trust their work. The case also highlights the trade-off between confidentiality and integrity: measures to withhold data for privacy reasons will harm completeness and reduce integrity.

This illustrates that the reference model, as developed by Van der Jagt and Heijboer [12], is useful and adequate for assessing integrity of patient records. Useful, because relevant stakeholder doubts about the design of the EPD were indeed brought out by the model (trust, provenance). As a matter of fact, these may have contributed to rejection of the national EPD by parliament, in addition to worries about privacy of patient records. Adequate, because the concepts in the model capture distinct aspects of reality. This is in particular true for the defensive measures concerning identification and authentication, but also for the offensive principle to capture data as close to the source as possible (S2), a key design feature of the EPD.

References

1. M.D. Abrams, E.G. Amoroso, L.J. LaPadula, T.F. Lund, and J. G. Williams (1993) Report of an integrity research study group. Computers and Security, 12:679-689.
2. R. Agrawal, T. Grandison, C. Johnson, J. Kiernan (2007) Enabling the 21st century health care information technology revolution, Communications of the ACM 50 (2):34-42.
3. R. C. Barrows Jr and P. D. Clayton (1996) Privacy, confidentiality, and electronic medical records, Journal of the American Medical Informatics Association 3: 139-148.
4. K. J. Biba (1977) Integrity Considerations for Secure Computer Systems, technical report MTR-3153, The Mitre Corporation.
5. J. Efrim Boritz (2004) Managing Enterprise Information Integrity: Security, Control and Audit Issues, IT Governance Institute.
6. J. Efrim Boritz (2005) IS practitioners' views on core concepts of information integrity. International Journal of Accounting Information Systems, 6(4):260–279.
7. Sean Brennan (2007) The biggest computer programme in the world ever. How is it going? Journal of Information Technology (2007) 22, 202–211
8. David D. Clark, and Andrew Wilson (1987) A comparison of commercial and military computer security policies. IEEE Symposium on Security and Privacy, pages 184–194.
9. Larry P. English (1999) Improving Data Warehouse and Business Information Quality. New York: John Wiley & Sons, Inc.
10. FIPS (2006) Minimum Security Requirements for Federal Information and Information Systems, Federal Information Processing Standards Publication 200.
11. Paul W.P.J. Grefen and Peter M.G. Apers (1993) Integrity control in relational database systems - an overview. Data and Knowledge Engineering 10:187–223.
12. Jan van der Jagt and Pieter Heijboer (2009) Integriteit van Patientgegevens binnen het Landelijk EPD, Graduate Thesis, IT Audit Department, Vrije Universiteit, Amsterdam.
13. ISO/IEC 27001 (2005), Information technology – Security techniques – Information security management systems, International Organization for Standardization, Geneva
14. A. Leendertse, P. M.L.A. van den Bemt, T.C.G. Egberts (2006), Hospital Admissions related to Medication (HARM), Utrecht Institute for Pharmaceutical Sciences.
15. Laureen A. Maines and James M. Wahlen (2006) The Nature of Accounting Information Reliability, Accounting Horizons 20(4): 399–425.
16. D.H. McKnight; L L. Cummings; N.L. Chervany (1998) Initial trust formation in new organizational relationships, The Academy of Management Review 23(3):473--490.
17. Nictiz (2008) EPD Documentation, version 6.0.0.0, Technical Report, May—Dec 2008.
18. NIST (2010) Recommended Security Controls for Federal Information Systems and Organizations, NIST 800-53, revision 3, National Institute of Standards and Technology.
19. Guido van 't Noordende (2010) Security in the Dutch Electronic Patient Record System, Proceedings of SPIMACS'2010, Chicago, Illinois, USA, pp. 21-31.
20. Ken Orr (1998) Data Quality and Systems Theory. Comm. of the ACM 41(2): 66-71.
21. James Reason (1990) Human Error, Cambridge University Press.
22. B. Romney, P.J. Steinbart (2003) Accounting Information Systems (9th). Prentice Hall.
23. A. Silberschatz, and R.B. Kieburtz (1980) The external consistency of abstract data types. ACM SIGPLAN Notices 15(2):64-73.
24. R.W. Starreveld, O.C. van Leeuwen, H. van Nimwegen (2002) Bestuurlijke informatieverzorging, 1: Algemene grondslagen (5th ed.) Wolters-Noordhoff, Groningen.
25. Da Veiga J.H.P. Eloff (2010) A framework and assessment instrument for information security culture, Computers & Security 29(2): 196-207
26. VWS (2009) Wijziging van de Wet gebruik burgerservicenummer in de zorg, Nota 31466, Ministerie van Volksgezondheid, Welzijn en Sport.
27. VWS (2011) Antwoorden van de minister van VWS op de vragen van het lid Leijten (SP), Nota 3057071, Ministerie van Volksgezondheid, Welzijn en Sport.