FinJeHeW Finnish Journal of eHealth and eWelfare

SCIENTIFIC PAPERS

VERTAISARVIOITU
KOLLEGIALT GRANSKAD
PEER-REVIEWED
www.tsv.fi/tunnus

Preliminary validation of treatment relationship confirmed by event log applications

Tuula Ristimäki, M.Sc. (Admin.), Senior Coordinator[1], Maria Pohjanvuori, B.Sc. (Soc.), Healthcare Consultant[2], Ari Pätsi, M.Sc. (Tech.), CIO[1]

[1]Department of IT management, the South Ostrobothnia Hospital District, Seinäjoki, Finland, [2]Andrea FI, Riihimäki, Finland

Tuula Ristimäki, M.Sc. (Admin.), Senior Coordinator, the Department of IT management, the South Ostrobothnia Hospital District, Seinäjoki, FINLAND. Email: Tuula.Ristimaki@epshp.fi

Abstract

A relationship between patients and healthcare professional should be confirmed by an EHR system before the patients' medical records are made available to healthcare professionals. We have earlier presented a logical level description about how a connection between patients and healthcare professionals (i.e. a treatment relationship) could be established automatically by event log applications (SIEM) after patient data has been accessed via an EHR system or other applications. The purpose of this study was to analyze, if the data collected for automatic confirmation of treatment relationships by SIEM was valid and to decrease the need for manual analysis. The record access data was collected from various information systems for the event log analyzer. The analyzing principles established in this case were based on the hospital's core processes. The outcome substantiates the view that automation can be used to evaluate large numbers of events. There is, however, still the need to further specify and apply principles to the configuration, in order to improve the surveillance within indirect use of patient information.

Keywords: professional patient relationship, automatic data processing, health information technology

Introduction

The Personal Data Act includes the duty of planning, duty of caring and duty to protect personal data. According to the Act on Electronic Archiving of Patient Records (159/2007) and the Health Care Act (1326/2010), a relationship between patients and healthcare professionals should be confirmed by an EPR system before the patients' medical records are made available to healthcare professionals. [1] Over the last few years healthcare providers have acquired increasing numbers of healthcare solutions that store patient data and occasionally share it with other healthcare professionals. The need for surveillance is also increasing. The management of event logs[1] for this purpose must be based on good governance and planning, and the legislation on individuals´ rights must be diligently followed [2].

The literature referring to patient data security often deals with access control models. In Role-Based Access Control (RBAC) the control can be location-based (e.g. healthcare professional assigned to the same unit as patient), or based on responsibilities in the organization. There is also a need for extended flexibility in the healthcare environment since processes in healthcare are complex and involve multiple actors. [3] In Situation Based Access Control (SitBAC), access to specific sensitive data is based on circumstances that match predefined patterns. There is clearly a need to specify scenarios of patient data access via situation models. [4] The same principles could be interpreted for SIEM[2] systems, which can then automatically confirm the appropriate use of electronic health record (EHR) system. The feasibility of the proposed models are seldom tested on an operational clinical system [5].

Boxwala et al. (2011) developed an approach for utilizing statistical and machine-learning methods to identify suspicious accesses to electronic health records. The data was integrated from disparate sources into a single data mart. From the suspicious patterns, i.e. where the user didn't have treatment or other reason to access records, they were able to build prediction models for rare events. An advantage of using statistical and machine-learning models is that they produce scores indicating suspiciousness of access. [5]

Salazar-Kish et al. (2000) developed algorithms for determining appropriate access to EHR, using available User-Patient data. A user–patient relationship was based on data which included information about the user's role (Primary Care Physician, Scheduled Provider, Referring Provider) or her/his department. They studied the impact of the algorithm to assess how often the user attempted to access a record and a patient–user relationship was not found by the algorithm.[6] Coleman et al. (2004) used a multidimensional analysis tool to analyze audit logs from Radiology Information System (RIS) and Archiving and Communication System (PACS). The data included, for example, user demographics, dates of exam, requesting and relevant patient demographic dimensions. They noted that the analyzing system was able to improve the surveillance and security of patient data, but human intervention was still required. [7]

Treatment relationship confirmed by even log applications

We have earlier presented a logical level description about how a connection between patients and healthcare professionals (i.e. a treatment relationship) can be established automatically by event log applications (SIEM), after patient data has been accessed via an EHR system or other hospital applications. We modeled information resources and information flows in healthcare core processes and related IT solutions, to determine when the access of a workforce member to patients' electronic health information is appropriate. Furthermore, we described the roles of healthcare professionals and examined routinely recorded patient administration data (referrals, admissions etc.).We also described how the treatment relationship between a patient, healthcare professionals and patient data could be represented for monitoring applications. [8, see also

[1] In this article term event log refers to data collected by applications from user interactions in EPR systems

[2] In this article, term SIEM refers to monitoring applications which automatically analyze event logs

7] We have especially taken into account situations where the treatment relationship could not be confirmed beforehand by an application. The main purpose was to enable monitoring that would combine critical event log data from different systems, and provide real-time policy-based alerts of suspicious behavior. [8]

Modern IT infrastructure generates huge amount of logs every day, so data mining should be based on clear principles. For a treatment relationship to exist, the patient, the professional and the recorded event must exist in the same context or healthcare unit (or unit group). We also agreed that an event in violation of this principle should trigger an alert in the automated log monitoring run [9]. It should be logged as suspect and be reported to the responsible parties in administration. We then proceeded to pinpoint the key events that would enable us to corroborate this principle. [8]

Identifying the significant key events

Modeled healthcare core processes indicated, that the relationship between healthcare professionals and patients is mediated by and established through the organization, which both delivers care (to patients) and contracts (the professionals) [8]. In the Finnish healthcare system, professionals tend to work in three types of roles. From the treatment relationship perspective, each role is characterized by a particular way of accessing patient data:

• *Routine use in Routine Patient Processes.* For the most part patient data is used within health center and hospital core processes such as the Elective Surgery Patient Process. Core processes are iterative i.e. they follow the same pattern and consist of the same consecutive events with little deviation for every patient in a designated patient group. The Patient Information System (PIS) or EHR records routine events within every patient process e.g. referral received (date/unit), treatment reservation made (date/unit), admittance (date/unit), etc. Establishing a treatment relationship is relatively straightforward by connecting the patient with the professional through routine event data recorded in the organizational unit.

• *Routine use Outside Routine Patient Processes.* Certain healthcare professionals have a varying job description that requires them to respond to requests originating from several routine patient processes or outside patient processes. These requests may be connected to an on-going or active patient process in the PIS/EHR, or they may have no connection to any event record in the organization. Typically, such requests include specialist consultations by phone, prescription renewal requests, requests by patients to change the terms of their consent, and the like. A treatment relationship may be established at times when (1) the professional can be logically connected to an on-going patient process and (2) when the professional has a role that serves a wider range of organizational units or processes.

• *Role based use.* Finally, some healthcare professionals and supporting staff work in positions where a treatment relationship between the patient and themselves never exists from the viewpoint of the PIS/EHR event records. Roles like the Specialized Hygiene Nurse, PIS/EHR IT-support Specialist, Archivist, Biller / Controller, and Queue Manager are examples of such positions. All of these professionals have a legitimate reason to access patient data when performing the duties of their given job descriptions. Many of them use task related information systems which do not interface with the PIS/EHR. Establishing this legitimate relationship is somewhat more complicated for the SIEM system. To connect the patient with the professional the system must have information of (1) an active patient process in PIS/EHR; (2) the role and job description of the professional and (3) an active process in the task related information system for the patient in question. [8]

It is necessary to point out that in addition to recording the key events for establishing treatment relationship the event log monitoring system must also be capable of reporting on all events, if needed. For example, the patient is, upon request, entitled to know the individuals who have accessed her/his personal data.

In this article we give an example of implementing a SIEM application. The aim was to analyze, if the data needed by SIEM systems to automatically confirm a

treatment relationship was valid, and to decrease the need for manual analysis.

Materials and methods

From the perspective of evaluating the large amounts of event log data, it is important to use data from various systems. An organization must have a clear understanding about its information systems and processes, and it must ensure the quality and availability of the data. [10, 11]

When a SIEM-application is implemented, the healthcare organization has to make several important decisions:

> *(1) From which EPR applications do we start collecting event logs for the monitoring system?*
>
> *(2) Which patient administration data is valid for analyzing purposes?*
>
> *(3) Where do we find information about the healthcare worker's working unit, at the moment she or he accessed patient data?*
>
> *(4) Various administrative tasks are also required but they are not described in this article.*

In our case, event logs were collected from the main EHR system in the Conservative Service Sector, Operative Service Sector, Psychiatric Service Sector, Emergency Care Sector and all other Sectors (including support services, Administrative Sector) on two different days (June, September). Reports from the radiology information system (RIS) and the hospital infection report application (SAI) were also collected at the same times. We decided to start with the core process recorded routinely along every patient process e.g. referral received, treatment reservation made, admittance to a unit. Other legitimate information was not applied. Data from work shift planning was used to record the units where healthcare professionals worked during each shift. If work shift planning was not available, we used the unit where the healthcare professional is contracted. Grouping of the work units is essential, since most of the professionals work in several units on a daily basis. Grouping is based mainly on medical subspecialties or on smaller units, for example in psychiatry.

For automated treatment relationship monitoring three types of log information is needed [8]. We used all three types of log data in our preliminary analysis.

(1) Patient Process Information (key events), from PIS, EHR, and /or task related systems

a. Date/Time, system ID
b. Patient name, patient ID, patient location (organizational unit)
c. User name, user ID, user login location

(2) User Information from the identity and access management system

a. User profession (manual analysis)
b. User role/profile (with access rights) (manual analysis)
c. User working unit(s)/organization

(3) Work shift planning and time management systems

a. User working time, (from work shift planning)
b. User working time, actualized; time-stamps from access-control systems

In the case hospital, we worked in cooperation with the IT provider who provides event data collection from several EHR systems, healthcare professionals´ time management systems and patients' processes from PIS. The data from those systems was analyzed by a SIEM application. We compared how event log rows varied in different Sectors of the hospital and in applications (RIS, SAI). We also compared the ratio between all the event log rows and the rows where the treatment relationship was not confirmed automatically. For security reasons we will not publish actual figures. We also want to emphasize that we are not reporting misuse, but are reporting examples of how the quality of data may be improved.

Finally, we analyzed the results from the Conservative Service Sector one-by-one to find out, which aspects we should explore next to improve the automatic analyz-

ing. We grouped reasons (i.e. why the treatment relationship was not established) into three categories: information about working unit, healthcare professional's role and all other reasons.

Results

The balance of the event log rows within different sectors of the hospital and in the applications are presented in table 1. The ratio of the collected event log rows in a particular sector of the hospital or application is presented in the column two. The third column is the percentage of those rows where the treatment relationship was not established by the SIEM application, in that particular sector of the hospital or application in question. In the last column are the same results (the relationship is not established) compared with all event logs at the time.

We further analyzed results from the Conservative Service Sector to find out what principles we should explore next to improve automatic analyzing. The reasons why the treatment relationship was not established are presented in table 2.

Table 1. Balance (%) of the event log rows within Sectors of the hospital (EHR) and applications (RIS, SAI).

Hospital sector or application	% of Event log rows (EHR by sectors, RIS, SAI)	Treatment relationship could not be established by SIEM /% rows inside sectors or applications	Treatment relationship could not be established by SIEM/ % of all event log rows
Conservative Service Sector	28,5	1,6	0,4
Operative Service Sector	41,2	1,9	0,8
Psychiatric Service Sector	12,4	2,5	0,3
Emergency Care Sector	9,2	3,2	0,3
Other units using EPR	4,7	-	-
RIS application	4,0	7,2	0,3
SAI	0,1	5,1	0,01

(- =not observed)

Table 2. Variation of the reasons where the SIEM could not find the treatment relationship in Conservative Service Sector (only the rows where user has viewed the EHR).

Conservative Service Sector (one- by-one analysis)		
	Category (the treatment relationship was not established)	% of rows in sector
1	Information from user's working unit	
	1.1 Working unit is not available	0,01
	1.2 Unit group is missing or not adequate	0,12
	1.3 Working unit is incorrect	0,05
2	User's role	
	2.1 User works in medical support services	0,23
	2.2 User works in non-medical support services	0,02
3	Other	
	3.1 Incorrect SIEM protocol	0,02
	3.2 All other reasons	0,24

Discussion and conclusions

An organization collects and processes information from a number of information systems and solutions. The analysis of separate pieces of information from separate information systems is highly resource-intensive. [2, 10] It requires knowledge, planning and investment [9]. Those who make configurations for SIEM applications or analyze results must have extensive knowledge of the organization and processes inside it, since no application has any business intelligence in itself.

In care units where the routine patient processes follow the same pattern, the relationship between patient and user is more easily established than in other units. In Emergency Care Sector, Psychiatric Care Sectors and specific applications (RIS, SAI) the treatment relationship could not be established as often. The outcome is partly due to the nature of the medical support services units. Radiology is part of medical support services, and RIS is one of the task related applications where we should look for active processes for the same patient, in both RIS and EHR/PIS. In the Emergency Care Sector, the situation is complex due to paramedics and many other professionals on call from different sectors, and using different applications. In the Psychiatric Service Sector healthcare professionals work across unit groups, so the principles of grouping healthcare/work units should be studied again more carefully.

The results are not scientifically significant, but they are an example of how to empower further analysis of event logs. The analyzer could not find the treatment relationship mostly because working unit information was inadequately grouped or insufficient. However, the main reason was that users worked under medical support services, so different analyzing guidelines need to be established there (Routine use Outside Routine Patient Processes or Role based use). The other reasons category is a collection of different things which need further analysis and principles. When healthcare professionals had responsibilities in observation units (which cannot be grouped under just one medical specialty), data is not currently or readily identifiable (Routine use Outside Routine Patient Processes).

Analyzing event log data is an ongoing process, and we must remind readers that every principle described earlier is not yet in use. Modeling the core processes should produce principles that enable reporting on most of the real-time policy-based alerts of suspicious behavior. As we presented earlier in a logical level description about establishing a treatment relationship, there are also two major exceptions to these core processes [8]. First, different principles should be applied to medical support services, operating room units and research units or applications, because patient administration data is not always available in these units. Secondly, there are certain professionals whose roles include using patient data, even if they are not directly connected to the patient.

The outcomes of our case substantiate the view, that automation can be used to evaluate large numbers of events, and the data collected was valid to decrease the need for manual analysis. The automatic analyzing application can help in regular evaluation of information security, as part of an annual plan. It is also important to thoroughly analyze all of the events from EHR and other applications, in order to decrease errors in the applied principles. In specific applications where the number of users is small and relationships are direct, automatic control can easily be used. However, implementing a SIEM application requires specifications and solid principles of configuration, to actually improve the surveillance of indirect use of patient information.

The writers all agree that the ideal improvement would be to have role based user interaction and access control with added ability for handling dynamic events in health care IT [11]. In the meantime, we believe the best practice is to constantly remind employees of their responsibilities to protect patients' personal information. Writers also agree that the process can be automated, and want to encourage other institutions to create models that facilitate the process of identifying inappropriate accesses [4].

References

[1] Ajantasainen lainsäädäntö. http://finlex.fi. Act on Electronic Archiving of Patient Records (laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä, 159/2007) and the Health Care Act (terveydenhuoltolaki, 1326/2010)

[2] Valtionvarainministeriö. Valtion tietoturvallisuuden johtoryhmä. Lokiohje 2009; 3. [cited 2014 Nov 11]. Available from: http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20090511Lokioh/Vahti_3_NETTI.pdf

[3] Wilikens M, Feriti S, Sanna A, Masera M. A Context-Related Authorization and Access Control Method Based on RBAC: A case study from the healthcare domain. SACMAT 02 Proceedings of the seventh ACM symposium on Access control models and technologies 2002 [cited 2015 Feb 12]. Available from: https://scholar.google.fi/scholar?cluster=2285804118864534072&hl=fi&as_sdt=0,5

[4] Peleg M, Beimel D, Don D, Denekamp Y. Situation-Based Access Control: Privacy management via modeling of patient data access scenarios. Journal of Biomedical Informatics 2008; 41 (6) [cited 2015 Feb 10]. Available from: http://www.sciencedirect.com/science/article/pii/S1532046408000506

[5] Boxwala AA, Kim J, Grillo JM, Ohno-Machado L. Using statistical and machine learning to help institutions detect suspicious access to electronic health records. Journal of the American Medical Informatics Association 2011; 18 (4) [cited 2015 Jan 31]. Available from: http://jamia.oxfordjournals.org/content/18/4/498

[6] Salazad-Kish J, Tate D, Hall PD, Homa K. Development of CPR security using impact analysis. Proc AMIA symposium 2000 [cited 2015 Feb 11]. Available from: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2243941/pdf/procamiasymp00003-0784.pdf

[7] Coleman RM, Ralston MD, Szafran A, Beaulieu DM. Multidimensional Analysis: A Management Tool for Monitoring HIPAA Compliance and Departmental Performance. J Digit Imaging 2004; 17 (3) [cited 2015 Feb 8]. Available from: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3046603/

[8] Pohjanvuori M, Ristimäki T, Valtonen R, Salminen J. Lokivalvontaan perustuva hoitosuhteen varmistus – hanke, loppuraportti [unpublished]. Finnish Hospital Districts of South Ostrobothnia, Helsinki and Uusimaa and Itä-Savo, the Association of Finnish Local and Regional Authorities and the National Institute for Health and Welfare 2012.

[9] Ipswitch, Inc. Network Management Division. Event Log Management & Compliance Best Practices: For Government & Healthcare Industry Sectors. Government Health IT, HIMMS Media 2010 Sep [cited 2014 Oct 25]. Available from: http://www.govhealthit.com/sites/govhealthit.com/files/resource-media/pdf/elm_-_compliance_best_practices_govt_-_healthcare.pdf

[10] The Office of the Data Protection Ombudsman. Prepare a Data Balance Sheet 2012 [cited 2014 Oct 25]. Available from: http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/publications/PlaGcyked/Prepare_a_data_balance_sheet.pdf

[11] Røstad L, Edsberg O. A Study of Access Control Requirements for Healthcare Systems Based on Audit Trails from Access Logs. Norwegian University of Science and Technology (NTNU), Department of Computer and Information Science, Trondheim 2006 [cited 2014 Nov 1]. Available from: http://www.acsac.org/2006/papers/77.pdf.