MEDINFO 2015: eHealth-enabled Health
I.N. Sarkar et al. (Eds.)

© 2015 IMIA and IOS Press.
This article is published online with Open Access by IOS Press and distributed under the terms of the Creative Commons Attribution Non-Commercial License.
doi:10.3233/978-1-61499-564-7-3

Validating the Access to an Electronic Health Record: Classification and Content Analysis of Access Logs

Leandro Noer Alassia[a], Sonia Benítez[a], Daniel Roberto Luna[a], Fernán González Bernaldo de Quiros[a]

[a] *Health Informatics Department, Hospital Italiano de Buenos Aires, Buenos Aires, Argentina*

Abstract

Electronic Health Records (EHRs) have made patient information widely available, allowing health professionals to provide better care. However, information confidentiality is an issue that continually needs to be taken into account. The objective of this study is to describe the implementation of rule-based access permissions to an EHR system.. The rules that were implemented were based on a qualitative study. Every time users did not meet the specified requirements, they had to justify access through a pop up window with predetermined options, including a free text option ("other justification").

A secondary analysis of a deidentified database was performed. From a total of 20,540,708 hits on the electronic medical record database, 85% of accesses to the EHR system did not require justification. Content analysis of the "Other Justification" option allowed the identification of new types of access. At the time to justify, however, users may choose the faster or less clicks option to access to EHR, associating the justification of access to the EHR as a barrier.

Keywords

Access Logs; Confidentiality; Accessibility.

Introduction

The health record serves several purposes, such as clinical documentation, transmission of information between clinicians, student instruction, knowledge generation, monitoring developments, and justifying interventions [1]. Hence, the medical record must be accessed by many individuals with very different aims.

In the age of the Electronic Health Records (EHRs), confidentiality and accessibility become relevant [2-4], particularly when users are not part of the care process. These issues impact the patient population, since patient records can contain sensitive information ranging from diseases, to data concerning sexuality and personal habits, to basic demographic information. According to estimates made by the American Health Information Management Association (AHIMA), 150 people on average, have access to a patient medical record during an inpatient episode [5]. Given this volume of access, the need to protect the confidentiality of patient information is evident and important [6].

In the United States, the Office of Civil Rights has reinforced the privacy and security of personal health information though the Health Insurance Portability and Accountability Act (HIPAA), setting standards and national regulations to protect sensitive electronic health information; thus defining access rights [7]. The Data Protection Act in the UK is the European counterpart to HIPAA [8]. HIPAA establishes two categories of acceptable access: "Treatment Payment Operations in Healthcare (TPO)", and "healthcare related". It is understood that research processes involve the generation of deidentified health records, which are excluded from HIPAA.

From a technical point of view, the Roles-Based Access Control (RBAC) model has shown to be useful [9-11]. In this model, people with a potential need for access to information are given permissions according to their credentials. In this way, information remains available if needed, but the aforementioned problem remains.

Different strategies have been employed to protect patient information without severely impacting the availability of data. The so-called "blue light button" strategy represents the concept of an alternate path, which allows the user to access information. This model is necessary in the context of health care where the unpredictable often happens. Violating the access control model established by RBAC can lead to confidentiality violation. For this reason, it should be subjected to an audit process [12]. This has been called an "optimistic security approach" [13].

Understanding that it is not possible to fully abandon the optimistic approach, we seek to generate a solution to minimize its use, not only because, once breached, the patient's confidentiality has been permanently compromised, but also because the subsequent audit process is cumbersome and costly in terms of human resources [14].

Some reports show restrictive approaches to users whose credentials do not justify access [15]. In others, contextual information is required to grant access, which follows the RBAC model [16,17], while other approaches tried to establish relationships through the use of relational algorithms and machine learning [18,19].

Our approach was to first examine how professionals perceive the ideal access model for EHRs [20]. The project was planned based on the results of that study as well as on the results of a field survey. The goal of this paper is to describe the implementation of access permissions to EHR based on rules.

Methods

Design

This is a cross-sectional study. A secondary analysis of a deidentified database was performed.

Setting

Hospital Italiano de Buenos Aires (HIBA) is a high complexity teaching hospital with 750 inpatient beds, located in Buenos Aires, Argentina. HIBA is part of a health network that includes a second hospital, 25 outpatient centers, and 50 private clinics. HIBA's workforce consists of 2,800 doctors, 2,800 healthcare related personnel, and 1,900 administrative

personnel. Since 1998 HIBA has been using an "in house" Health Information System (HIS) that includes a unique, modular, problem-oriented, and patient-centered web based electronic health record (EHR). In the EHR system, all staff with valid credentials can access and review all medical records, regardless of the nature of their duties. Each entry has a potentially traceable access log.

Figure 1 shows the steps in the project. This work analyzed different justifications and categories of EHR access.

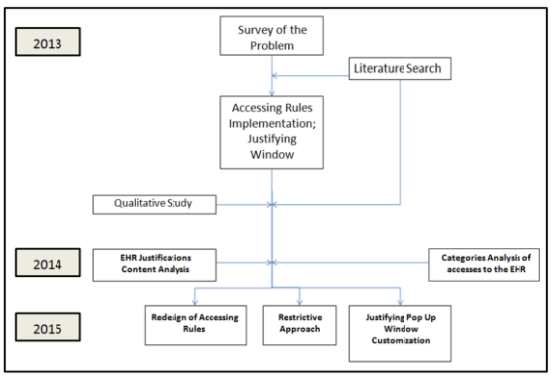

Figure 1- Data Confidentiality Project

Implementation of Access rules

Access permissions to the EHR based on specific rules were implemented in July 2013. The rules considered the most frequent use cases depending of the level of care. Ambulatory-level family physicians and physicians with a visit occurring within the last 180 days or with a scheduled visit do not need to justify access to the EHR. Attending physicians, nurses, pharmacists in the emergency department, and home care providers had the same privileges. At the inpatient level, physicians from the medical department where the inpatient was admitted, referral physicians with a referral request in the EHR, nurses working in the ward where patient is located, and pharmacists all have access to the EHR without any explanation. The qualitative study carried out in the first semester of 2013 helped to construct the different use cases [20].

Every time users did not meet the requirements listed above, they had to justify access through a pop up window with predetermined options (See Figure 2). Some options were: "medical auditor", "health informatics", "patient in my care", and "other justification". The "other justification" option allows the user to declare the reason of access in free text format. These options were chosen for different reasons. Most of them were sourced from the previous survey, in which we asked different types of users for the reasons they access the EHR. Some of them were included after the discussion, with the rest of the Medical Informatics team. We left the "other justification" option to capture not previously considered use cases. For more information, see http://www.hospitalitaliano.org.ar/infomed/index.php?contenido=ver_curso.php&id_curso=17942 .

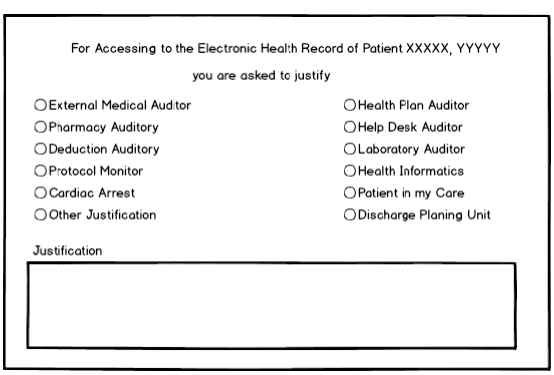

Figure 2- Pop Up Justification Window

Analysis Plan

Data from July 2013 to June 2014 were analyzed comparing both semesters, and descriptive statistics were performed. Categorical variables were presented as percentages. Free text from the "other justification" option was evaluated via content analysis. Because we did not make any adjustments in the short term, we looked for large variations occuring in the annual data over two periods.

Results

The total log accesses included 9,755,752 hits for the first period, representing an average of 62,536 hits per day, and 10,784,956 for the subsequent period (average of 59,916 daily). Of a total of 20,540,708 hits on electronic medical records, we found that 85% of access to the EHR did not need to be justified. In the remaining 15%, there were variations in the occurrences of the "patient under my care" and "other justification" options in both semesters.

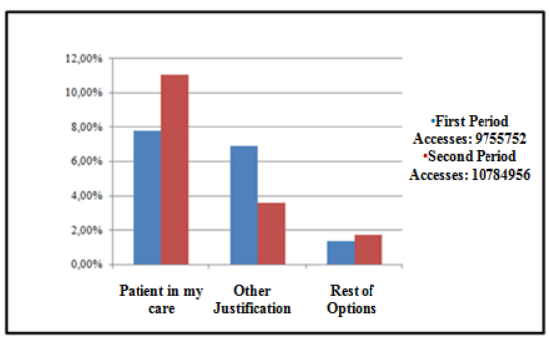

Figure 3. Remaining 15% of accesses by semester

Finally, from the content analysis of the "other justification" field, the new categories of access identified are shown in Table 1. Over all types of users, 52% of all written justifications corresponded to nonsensical text or acronyms with uncertain meaning.

Table 1 - Content analysis of the "other justification" option

Identified Case	Repetitions n=1060217 (%)
Nutrition Personnel Access	203, 693 (19.21)
Referral	131, 946 (12.44)
Billing Access	124, 681 (11.76)

Discussion

In this paper, data regarding justification of access to EHRs were analyzed. The majority (85%) of accesses responded to the rules, and users did not need to clarify the reason to access the EHR. Of the remaining 15%, the two predominant categories were "patient under my care" and "other Justification", the latter of which instructed the user to write additional information in free text.

There was a marked decrease in the selection of the "other justification" option between the first and second periods of the study. We considered that this could be due to user adaptation. This phenomenon may be considered similar to alert fatigue [21,22]. Given the repeated appearance of the pop up window, it is possible that it disrupted workflow, such that many professionals who initially justified access eventually transitioned to selecting the "patient under my care" option, which allowed entry with only two clicks. This may also explain the nonsensical text in the "other justification" option, which may have been entered in order to access records more expeditiously. Further research will help to understand the problem. On the other hand, new residents begin their training at our hospital every June/July, increasing the probability of this option being used more frequently in the first period.

With respect to the "other justification" option, content analysis allowed us to find new use cases not covered before, which led to their addition to the rules of validity for access in the next phase of the project. Comparing our experience to those in other publications, we see that the RBAC model – the major paradigm for access control over the last fifteen years – is frequently adapted to different settings. In some cases, the model is applied to make access more restrictive [15], while in others it is to allow access in the combined context of team collaboration [23], using captured information on context metadata to optimize control permissions [16,17] or even trying to predict association rules between users and patients [18]. We think that a qualitative approach followed by a content analysis of the information (provided by users, even when not formally verified because of the deidentified data use), can offer a solution to find new rules, enabling a continuous quality improvement cycle and engaging users with regard to this important topic. Further research would be useful to evaluate the accuracy of the "other justification" option, if necessary.

This study has some limitations. It is a cross sectional study, and information is from a single academic healthcare center, therefore the results cannot be generalized without validation. Additionally, we cannot ensure that the selected options in the analysis corresponded to the real reason of access, because the categories outlined in Figure 2 could be accessed by all users without any validation.

Based on data from this study, we plan to make access to the EHR more restrictive, allowing access only if the user is a family doctor or a member of a registered care team. We will maintain a "blue light button" for emergencies, accompanied by an agile and effective audit. This option will trigger a self-audit mechanism through institutional e-mail. The rules of access will be extended according to the content analysis of written justifications. Finally, we will customize the options in the pop up window according to the department and/or service where the user belongs, to allow a more accurate granularity and to reduce the need to write extra text. With these changes, we aim to improve the workflow in the newly identified use cases, improve the fidelity of structured options for justification, and reduce the need for justification in free text.

Finally, it must not to be overlooked that an EHR provides the technical infrastructure to aggregate information and establishes a longitudinal record of health information for individual patients. This accessibility of information has already opened the debate about who should grant permission for a user to access the information in the EHR. For several years, it has been postulated that the patient, as owner of the information, is the one who should define who can access their record. This permission, in turn, must be sufficiently flexible to allow the patient to set the privacy level from accessible only to a few professionals, to having no privacy restrictions, according to each owner's preferences [24]. In this sense, open questions remain about what measures can be taken to protect patients' information, such as clarifying who can access and why they are accessing the clinical data repository, while interfering as little as possible with the workflow of each healthcare professional.

Conclusion

In this analysis of access permissions to the EHR based on rules, the majority of users did not need to clarify the reason why they needed access. Rules implemented were based on a qualitative approach, and content was analyzed using information provided by users. At the time of justification, however, users may consider access justification a disruptive barrier, often choosing the faster (or "fewer clicks") option to access the information.

References

[1] Reiser, S. The clinical record in medicine. Part 1:Learning from cases. (1991)*Annals of Internal Medicine,114* (10), 902–907

[2] Bradley A Malin, Khaled El Emam, Christine M O'Keefe. Biomedical data privacy: problems, perspectives, and recent advances. J Am Med Inform Assoc. 2013 Jan-Feb; 20(1): 2–6. doi: 10.1136/amiajnl-2012-001509 PMCID: PMC3555341

[3] Gkoulalas-Divanis, A., Loukides, G., Xiong, L., & Sun, J. Informatics methods in medical privacy. (2014) Journal of Biomedical Informatics, 50, 1–3. doi:10.1016/j.jbi.2014.07.010

[4] Barrows, R. C., & Clayton, P. D. (n.d.). Privacy, confidentiality, and electronic medical records. *Journal of the American Medical Informatics Association : JAMIA*, *3*(2), 139–48.

[5] Steward, M. (2005). Electronic medical records. Privacy, confidentiality, liability. *The Journal of Legal Medicine*, *26*(4), 491–506. doi:10.1080/01947640500364762

[6] O'Brien J, Chantler C. Confidentiality and the duties of care. *Journal of Medical Ethics* 2003;29(1):36-40. doi:10.1136/jme.29.1.36

[7] U.S. Department of Health and Human Services Office for Civil Rights HIPAA Administrative Simplification Regulation Regulation Text 45 CFR Parts 160, 162, and 164 (Unofficial Version, as amended through March 26, 2013

[8] UK data protection act; 1998. http://www.legislation.gov.uk/ukpga/1998/29/ contents

[9] Ferraiolo, D. F., Sandhu, R., Gavrila, S., Kuhn, D. R., & Chandramouli, R. Proposed NIST standard for role-based access control. (2001).*ACM Transactions on Information and System Security*, *4*(3), 224–274. doi:10.1145/501978.501980

[10] Carrión Señor, I., Fernández Alemán, J. L., & Toval, A. Access control management in electronic health records: a systematic literature review. (2011). *Gaceta Sanitaria / S.E.S.P.A.S*, *26*(5), 463–8. doi:10.1016/j.gaceta.2011.11.019

[11] Le XH, Doll T, Barbosu M, Luque A, Wang D. Evaluation of an enhanced role- based access control model to manage information access in collaborative processes for a statewide clinical education program. J Biomed Info 2014;50: 184–95

[12] Lillian Røstad, Øystein Nytrø. Towards Dynamic Access Control for Healthcare Information Systems. Stud Health Technol Inform. 2008;136:703-8.

[13] D. Povey. Optimistic security: a new access control paradigm. Proceedings of the 1999 workshop on New security paradigms. ACM Press, Caledon Hills, Ontario, Canada, 2000. ISBN: 1581131496

[14] Boxwala, A. a, Kim, J., Grillo, J. M., & Ohno-Machado, L.Using statistical and machine learning to help institutions detect suspicious access to electronic health records. (2011) *Journal of the American Medical Informatics Association : JAMIA*, *18*(4), 498–505. doi:10.1136/amiajnl-2011-000217

[15] Lovis C, Spahni S, Cassoni N, Geissbuhler A. Comprehensive management of the access to the electronic patient record: towards trans-institutional networks Int J Med Inform. 2007 May-Jun;76(5-6):466-70. Epub 2006 Nov 3.

[16] Motta GH1, Furuie SS. A contextual role-based access control authorization model for electronic patient record. IEEE Trans Inf Technol Biomed. 2003 Sep;7(3):202-7.

[17] Koufi V, Vassilacopoulos G. Context-aware access control for pervasive access to process-based healthcare systems. Stud Health Technol Inform. 008;136:679-84.

[18] Chen K, Chang YC, Wang DW. Aspect-oriented design and implementation of adaptable access control for electronic medical records. Int J Med Inform. 2010 Mar;79(3):181-203. doi: 10.1016/j.ijmedinf.2009.12.007. Epub 2010 Feb 1.

[19] Boxwala, A. a, Kim, J., Grillo, J. M., & Ohno-Machado, L. Using statistical and machine learning to help institutions detect suspicious access to electronic health records. (2011) *Journal of the American Medical Informatics Association : JAMIA*, *18*(4), 498–505. doi:10.1136/amiajnl-2011-000217

[20] Alassia, L. N., García, M. G., Dawidowsky, A., Budalich, C. M., Benítez, S., Luna, D. R., & González Bernaldo de Quiros, F. (2014). Percepciones de los médicos frente a la legitimidad de los accesos a la historia Clínica Electrónica. In *XIV Congresso Brasileiro de Informática em Saúde. Santos, Brasil*.

[21] Jung, M., Hoerbst, a, Hackl, W. O., Kirrane, F., Borbolla, D., Jaspers, M. W. Ammenwerth, E. (2013). Attitude of physicians towards automatic alerting in computerized physician order entry systems. A comparative international survey. *Methods of Information in Medicine*, *52*(2), 99–108. doi:10.3414/ME12-02-0007

[22] Bates, D. W., Baysari, M. T., Dugas, M., Haefeli, W. E., Kushniruk, a W., Lehmann, C. U. Westbrook, J. I. (2013). Discussion of "attitude of physicians towards automatic alerting in computerized physician order entry systems". *Methods of Information in Medicine*, *52*(2), 109–27.

[23] Le, X. H., Doll, T., Barbosu, M., Luque, A., & Wang, D. (2012). An enhancement of the Role-Based Access Control model to facilitate information access management in context of team collaboration and workflow. Journal of Biomedical Informatics, 45(6), 1084–1107. http://doi.org/10.1016/j.jbi.2012.06.001

[24] Mandl, K. D., Szolovits, P., & Kohane, I. S. (2001). Public standards and patients ' control : how to keep electronic medical records accessible but private, 322(February).

Address for Correspondence

Leandro Noer Alassia, MD

Juan D. Peron 4190 (C1199ABD), Edificio DIS

Ciudad Autónoma de Buenos Aires, Argentina

leandro.alassia@hospitalitaliano.org.ar