Illegitimate HIS Access by Healthcare Professionals Detection System Applying an Audit Trail-based Model

Liliana Sá-Correia[1][a], Manuel E. Correia[2][b] and Ricardo Cruz-Correia[1,3][c]

[1]*HLTSYS, HealthySystems, lda, Porto, Portugal*

[2]*Faculdade de Ciências da Universidade do Porto, Portugal*

[3]*Center for Research in Health Technologies and Information Systems - CINTESIS, Porto, Portugal*

Keywords: Data Breach, Data Protection, Health Data Access, Illegitimate Access Detection.

Abstract: Complex data management on healthcare institutions makes very hard to identify illegitimate accesses which is a serious issue. We propose to develop a system to detect accesses with suspicious behavior for further investigation. We modeled use cases (UC) and sequence diagrams (SD) showing the data flow between users and systems. The algorithms represented by activity diagrams apply rules based on professionals' routines, use data from an audit trail (AT) and classify accesses as suspicious or normal. The algorithms were evaluated between 23rd and 31st July 2019. The results were analyzed using absolute and relative frequencies and dispersion measures. Access classification was in accordance to rules applied. "Check time of activity" UC had 64,78% of suspicious classifications, being 55% of activity period shorter and 9,78% longer than expected, "Check days of activity" presented 2,27% of suspicious access and "EHR read access" 79%, the highest percentage of suspicious accesses. The results show the first picture of HIS accesses. Deeper analysis to evaluate algorithms sensibility and specificity should be done. Lack of more detailed information about professionals' routines and systems, and low quality of systems logs are some limitations. Although we believe this is an important step in this field.

1 INTRODUCTION

Healthcare institutions typically imply complex data management processes, where a professional can have multiple roles during a certain period of time (physician, researcher, head of department), leading him or her to access many different patients' Eletronic Health Record (EHR), that in its turn are accessed by many professionals for different reasons. This complexity makes very hard distinguishing the legitimate accesses from the non-legitimate ones and it is becoming a serious issue for healthcare institutions to solve. Although audit trails (AT) are an important tool for some General Data Protection Regulation (GDPR) requirements' complience (EU, 2016), like audit and traceability (Gonçalves-Ferreira et al., 2018), we belive that they can have an important role on detection of suspicious actions on EHR that can be illegitimate access. Previous studies show that despite the complex environment of data management on healthcare providers it is possible to create rules associated to routines of healthcare professionals and to model their access to Health Information Systems (HIS) through use cases (UC). Taking advantage of information collected on previous investigation (L.Correia et al., 2019) we propose to implement algorithms for detection of suspicious actions on HIS by healthcare professionals giving clues for further investigation by the Data Protection Officer (DPO) and to ensure the patients data privacy.

[a] https://orcid.org/0000-0001-6174-3957
[b] https://orcid.org/0000-0002-2348-8075
[c] https://orcid.org/0000-0002-3764-5158

2 METHODS

Parting from previous studies (L.Correia et al., 2019) in which were modeled UC for scenarios that described situations of, or that could lead to, illegitimate access, we selected three to implement algorithms for detection of suspicious activity. The choice was based on the available logs in the AT of a hospital from North Portugal after an analysis of variables needed

Sá-Correia, L., Correia, M. and Cruz-Correia, R.
Illegitimate HIS Access by Healthcare Professionals Detection System Applying an Audit Trail-based Model.
DOI: 10.5220/0008991505390546
In *Proceedings of the 13th International Joint Conference on Biomedical Engineering Systems and Technologies (BIOSTEC 2020) - Volume 5: HEALTHINF*, pages 539-546
ISBN: 978-989-758-398-8; ISSN: 2184-4305

for each UC. Since we had logs just from the applicational system Obscare we excluded the UC that depend other type of logs. The rules and tresholds applyed to algorithms were based on the information gathered on discussions with experts and interviews to healthcare professionals (L.Correia et al., 2019). We used the Unified Model Language (UML) to design the UC and activity diagrams (AD), and coded in JAVA programming language. Tests were conducted between 23rd and 31st of July 2019, with logs of one applicational system - Obscare that were being collect by the AT HS.REGISTER on an hospital from North Portugal. We analysed the obtained datasets in order to find erros on dates and calculations, inconsistencies and access misclassifications. For each, it was removed duplicated records and it was analysed the impact of N/A existence. For the dataset of UC "Check time of activity" was produced a summary table by professional category with the metrics: (1) total of results, (2) number of professionals without identification, (3) minimum time of activity, (4) 1st and 3rd quartiles and median values of time of activity, (5) mean of time of activity, (6) maximum time of activity; (7) standard deviation and (8) number of results classified as "suspicious". For the dataset of UC "Check days of activity" we produced a summary table by professional category with the metrics: (1) total of results, (2) minimum days of activity, (3) 1st and 3rd and median days of activity, (4) mean of days of activity, (5) maximum of days of activity; (6) standard deviation and (7) number of results classified as "suspicious". For dataset of UC "EHR read access" we produced a summary table by date with the metrics: (1) total of results, (2) total of results without professional ID, (3) total of results with null patient ID, (4) total of suspicious access classifications, (5) total of suspicious access classifications without professional ID and (6) total of suspicious access classifications with null patient ID, and a table comparing the accesses by professional category.

3 RESULTS

3.1 Use Case "Check Time of Activity"

First, we think of identifying professionals' activity periods that are longer or shorter than expected for a work shift, since professionals have a schedule to work and should not access to HIS when they are off (Diário da Republica, 2005).

Scenario 1. *A professional uses his credentials during his shift to accomplish his tasks. In the end of his shift, he goes home and he did not logout his session on the computer. A colleague uses his open session to access the HIS and take a look at a patient's EHR that he was curious about.*

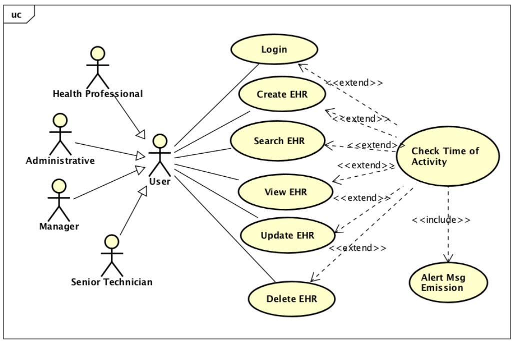

Figure 1: Use case "Check time of activity".

For this UC we propose to track all activities of a professional and monitor the consecutive time of activity, checking if the total time of activity is normal for a shift duration, or is shorter or longer insted, as showed in the UC (figure 1) and on the SD (figure 2).

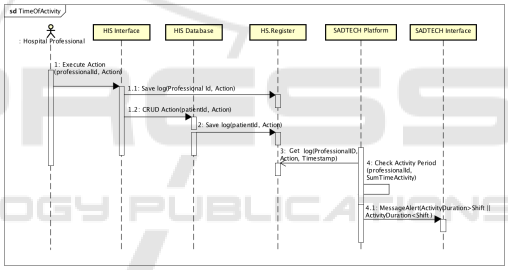

Figure 2: Sequence diagram "Check time of activity".

Our algorithm requests the data to AT between two dates, analyses the data and produces a report with the classification of the results corresponding to periods of consecutive time of activity. As we cannot afirm that the result obtained is in fact an illegitimat access, we classified the access as "suspicious" if it is shorter or longer than expected for a work shift and an alert is launched. The AD (figure 3) shows the proposed algorithm. For each professional, the events are ascending ordered by timestamp. It adds the time between two consecutive timestamps of event logs, if the difference between them is less than six hours. Other wise we consider that the professional is off and it starts counting a new period of consecutive time of actvity. If the total of added time is greater than thirteen hours or shorter than five hours it may indicate that the user is not accessing only during the work shift.

Evaluation. The algorithm was tested between 23rd and 31st July 2019. The results for each professional

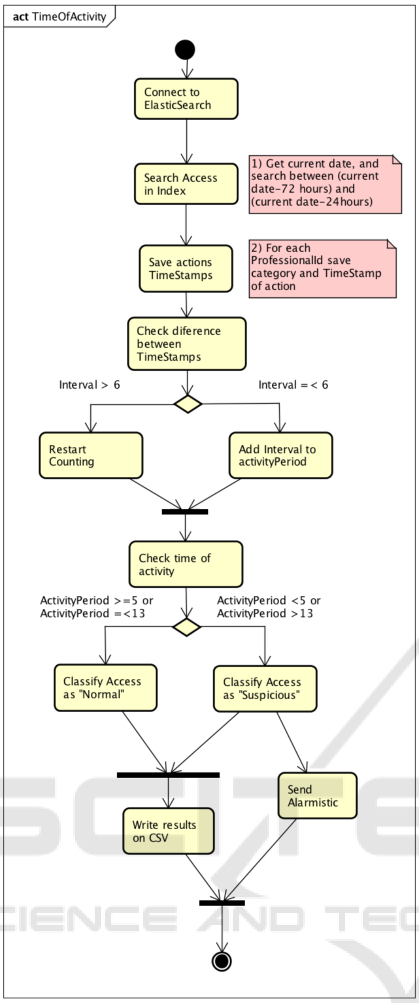

Figure 3: Activity diagram “Check time of activity”.

and classification as suspicious are shown in table 1. If a professional accesses a period of time less than five hours ($\leq$ 299 minutes) and greater than thirteen hours ($\geq$781 minutes) it is classified as “suspicious”, else the system classifies the access as normal. In the referred period, which counts nine days, after removing the duplicated ones, we got 276 results, of which 176 were classified as suspicious. The data presented show two outliers with different behaviours. For the category “No identified” all cases have a duration completely distinct from the others, but all 6 occurrences have the same behaviour. This happens because this category represent automatic processes that run in system’s background, acording the provider of Obscare system. Another outlier is in “Nurse” category and is similar to “No identified” category, because there are some automatic processes associated to “Nurse” category, as well. Categories associated to management and research tasks have activities with very short duration and few occurrences. Looking to categories that are more related to healthcare delivery and removing the automatic processes from “Nurse” category we can see that the results presented, generally, do not exceed the superior limit fixed as suspicious access. However the categories “physician” and “specialist phyisician” have some results that exceed that limit. It is also possible to see that there are many accesses that do not go over the inferior limit and those are responsible for most of the suspicious access classifications.

3.2 Use Case “Check Days of Activity”

Secondly, we tried to identify professionals’ consecutive days of activity that are longer than expected for a week work, since professionals are off after a week of work, that can be up to seven consecutive days and in some exceptions even longer, and should not access to HIS when they are off (Diário da Republica, 2005). **Scenario 2.** *A professional uses his credentials during his shift to accomplish his tasks. In the end of work week, when he is off, another user uses his credential to access a HIS, to take a look at a patient EHR.*

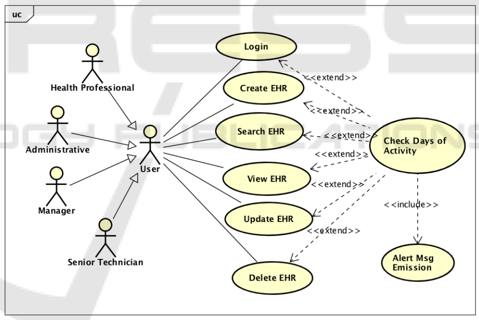

Figure 4: Use case “Check days of activity”.

For this UC we propose to track all activities of a professional and monitor the consecutive days of his or her work, checking if the total consecutive days of activity is normal for a work week, or longer, as showed in the UC (figure 4). The SD (figure 5) shows that for every activity in the system done by a professional, it is sent a event log for the AT which identifies the professional, his profile, the timestamp, the patient accessed, the action executed among other data. Our algorithm requests the data to the AT between two dates, analyses the data and produces a report with the classification of the results corresponding to the number of consecutive days of activity. Also, as we cannot afirm that the result obtained is in fact an illegitimate access, we classified the accesses as “suspicious” if it is longer than expected for a work week. For each

Table 1: Results for UC “Days of Activity”.

Professional Category	Nr results	Professional identified	Min.	1st Qu.	Median	Mean	3rd Qu.	Max.	Stsndard Deviation	Suspicious access
			nr of consecutive minutes worked							
No identified	6	0	4305	4305	4305	4308	4305	4328	6.12	6 (100%)
Admin Sirai	5	5	4.00	4.00	6.00	6.40	8.00	10.00	2.60	5 (100%)
Admin VCOBSGYNV3,Create users	1	1	2.00	2.00	2.00	2.00	2.00	2.00	0	1 (100%)
Administrative	56	56	1.00	96.75	338.00	307.54	364.25	713.00	210.83	24 (43%)
Nurse	108	105	0.00	50.25	210.50	335.45	361.75	4320.00	194.41	71 (66%)
Nurse,Admin VCInt,Physician, Development team	1	1	1.00	1.00	1.00	1.00	1.00	1.00	0.00	1 (100%)
Nurse,Administrative,Admin Physician,Admin Sirai, Admin_Backoffice	4	4	0.00	2.25	8.00	13.00	18.75	36.00	16.31	4 (100%)
Management, Admin, VCOBSGYNV3,Creat Users,Physician	1	1	137.00	137.00	137.00	137.00	137.00	137.00	0.00	1 (100%)
Indicators Sirai,Admin Sirai	1	1	0.00	0.00	0.00	0.00	0.00	0.00	0	1 (100%)
Physician	28	28	0.00	74.5	230.00	314.60	399.00	1543.00	345.88	21 (75%)
Physician_Specialist,Physician	65	65	0.00	124.00	338.00	436.40	669.00	1431.00	365.68	41 (63%)
	276	267	0.00	67.00	266.00	422.80	448.50	4320.00	766.37	176 (63%)

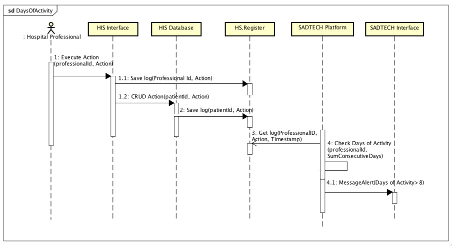

Figure 5: Sequence diagram “Check Days of activity”.

classification as “suspicious” an email is sent to the CIS and to the DPO.

The AD (figure 6) shows the proposed algorithm. For each professional, the events are ascending ordered by timestamp and it counts consecutive days using the timestamps of event logs. If the difference between them is more than one day, we consider that the professional was off and it starts counting a new period of consecutive days of actvity. If the total of added days is greater than eight days it may indicate that the user is not accessing only during the work shift.

Evaluation. The algorithm was tested between 23rd and 31st July 2019. The results of days of activity for each professional and classification as suspicious are shown in table 2. If a professional accesses a period of days greater than 8 days it is classified as “suspicious”, else the system classifies the access as normal. In the referred period, which counts nine days, we got 213 results, of which 17 were classified as “suspicious”. The data presented shows two outliers with different behaviours. For the category “No identified” all the cases have a duration completely distinct from the others, but all the 6 occurrences have the same behaviour. This happens because this category represent automatic processes that run in system’s background. Another outlier is in “Nurse” category and is similar to “No identified” category, because there are some automatic processes associated to “Nurse” category, as well. Categories associated to management and research tasks have activities with very short duration

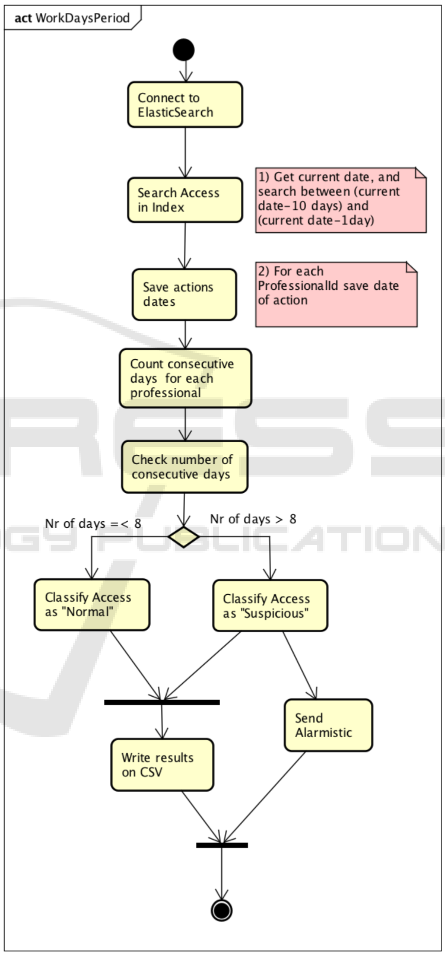

Figure 6: Activity diagram “Check days of activity”.

and few occurrences. We can see that automatic processes run every day having no associated category, and there are accesses associated to management and research accesses that occurs generally once or twice a week. Observing the categories that are directly related to delivery of healthcare, such “Administrative”, “Nurse”, “Phisician” and “Specialist Phisitian”, similarly to what happens in the results of the UC “Check time of activity”, the suspicious accesses are associated to “specialist physician” category.

3.3 Use Case “Check EHR Read Access”

In this UC, we tried to identify accesses by professionals to read patients’ EHR and did not create or update them. The lack of evidences that can justify such access is already spotted as an issue to solve by healthcare institutions. According to GDPR and Joint Commission International (JCI) for hospitals certification on Management of Information (MOI) 11.5 this type of access should be addressed to mitigate problems related to data breaches (Joint Commission International, 2017).

Scenario 3. *A professional access to a patient EHR. Why does he access? What are the evidences of the healthcare delivering of that professional.*

For this UC we propose to track all accesses of a professional and monitor the patient accessed and the type of action excuted between 72 hours (three consecutive days). A EHR may be updated after the end of shift or in the begining of the shift and the information updated may need to be checked in the end of the shift. If between 72 hours there is an access to read an EHR and there is any update or create action, the access is classified as “suspicious”, else is classified as normal, as showed in the UC (figure 7). The SD (figure 8) shows that for every activity in the system done by a professional, it is sent an event log for the AT which identifies the professional, his profile, timestamp, patient accessed, action executed, among other data. Our algorithm requests the data to the AT between two dates, analyses the data and produces a report with the read actions (yes or no), write actions (yes or no) and results of access classification. Again, as we cannot afirm that the result obtained is in fact an illegitimate access, we classified the accesss as “suspicious” if there is any update or create actions. For each classification as “suspicious” an email is sent to the CIS and to the DPO.

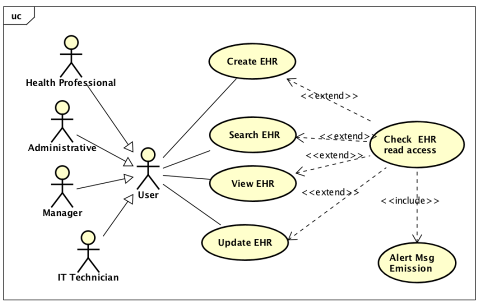

Figure 7: Use case “Check EHR read access”.

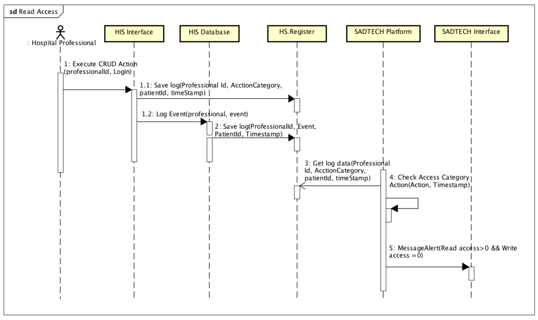

Figure 8: Sequence diagram “EHR read access”.

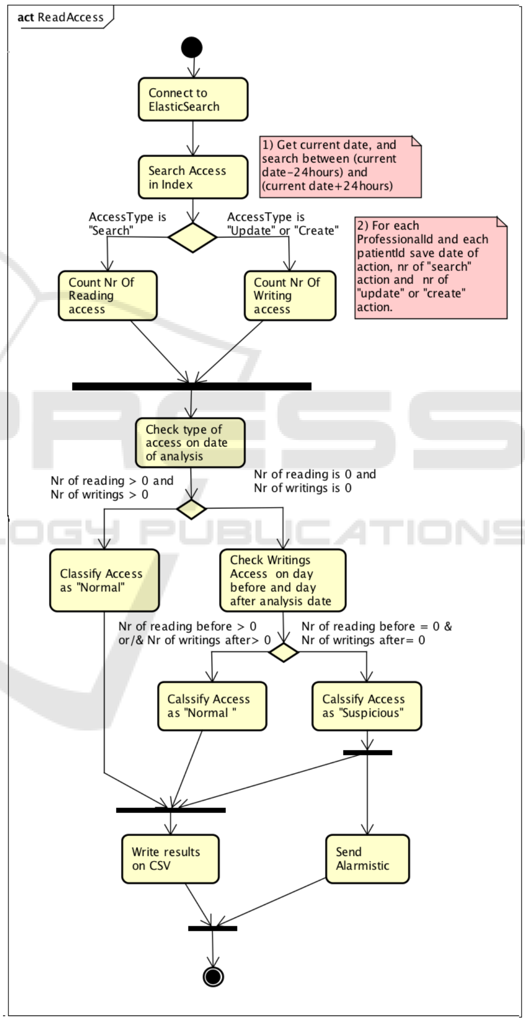

Figure 9: Activity diagram “EHR read access”.

The AD (figure 9) shows the proposed algorithm. For each professional, it is analysed the patient accessed, and, for each, verifies the action, counts the number of readings and the number of writings. For each patient, if the number of readings is greater than zero and the number of writings are equal to zero the

Table 2: Results for UC “Days of Activity”.

Professional Category	Nr results	nr of consecutive days Min.	1st Qu.	Median	Mean	3rd Qu.	Max.	Standard deviation	Suspicious access
No identified	9	11	11	11	11	11	11	0.00	9 (100%)
Admin Sirai	18	1.00	1.00	1.00	1.11	1.00	2.00	0.32	0
Admin VCOBSGYNV3,Create users	1	1.00	1.00	1.00	1.11	1.00	1.00	N/A	0
Administrative	61	1.00	1.00	2.00	2.18	3.00	7.00	1.46	0
Nurse	101	1.00	1.00	1.00	1.67	2.00	5.00	0.99	0
Nurse,Admin SIRAI	1	1.00	1.00	1.00	1.11	1.00	1.00	N/A	0
Nurse,Admin VCInt,Physician, Development team	2	1.00	1.00	1.00	1.11	1.00	1.00	0.00	0
Nurse,Administrative,Admin Physician,Admin Sirai, Admin_Backoffice	5	1.00	1.00	1.00	1.60	2.00	3.00	0.89	0
Management, Admin, VCOBSGYNV3,Creat Users,Physician	1	1.00	1.00	1.00	1.11	1.00	1.00	N/A	0
Indicators Sirai,Admin Sirai	7	1.00	1.00	1.00	1.43	1.50	3.00	0.78	0
Physician	30	1.00	1.00	2.00	2.03	2.00	5.00	1.19	0
Physician_Specialist,Physician	82	1.00	1.00	2.00	2.57	2.00	11.00	2.64	8 (9.7%)
	318	1.00	1.00	1.00	1.93	2.00	11.00	2.25	17(5,3%)

access is classified as “suspicious”, else it is classified as “normal”.

Evaluation. The algorithm was tested between 23rd and 31st July 2019. The results for UC “EHR read access” are shown in table 3. In the referred period, which counts nine days, we obtained 378 results, of which 300 (79%) were classified as “suspicious”. This means that, during this period, there were 300 sets of professionals’ accesses to EHR’s patient without any registry being made. Analysing the results we can see that 32 accesses classified as “normal” do not have professional ID and 28 others do not have patient ID.

Table 3: Results for UC “EHR read access”.

Analysis date	Total of results	No Prof. Id	Null Patient Id	Suspicious access classification by system Total	Null Prof. Id	Null Patient Id
2019-07-22	49	10 (20%)	11 (22%)	39 (80%)	4(10%)	9 (23%)
2019-07-23	38	6 (16%)	13 (34%)	30 (79%)	4 (13%)	8 (27%)
2019-07-24	49	7 (14%)	13 (27%)	44 (90%)	4 (9%)	12 (27%)
2019-07-25	59	9 (15%)	11 (19%)	43 (73%)	5 (12%)	7 (16%)
2019-07-26	31	11 (35%)	10 (32%)	24 (77%)	6 (25%)	8 (33%)
2019-07-27	31	10 (32%)	7 (23%)	24 (77%)	7 (29%)	4 (17%)
2019-07-28	29	6 (21%)	6 (21%)	22 (76%)	4 (18%)	2 (9%)
2019-07-29	44	10 (23%)	9 (20%)	34 (77%)	4 (12%)	7 (21%)
2019-07-30	48	8 (17%)	14 (29%)	40 (83%)	7 (18%)	9 (22%)
	378	77 (20%)	94 (25%)	300 (79%)	45 (15%)	66 (0,22%)

The results show that 77 classifications (20%) do not have the professional ID. Such occurrences are related to automatic processes, that run in parallel, to check, get and retrieve necessary data on EHR. The results with N/A “patitents id” are 94 (25%), and they are users’ processes that are not related with patients but to other type of reports instead. So we adjusted the values excluding the results of automatic processes and we obtain the values on table 4, which shows that the results classified as “suspicious” grow to 92%.

Analysing the results by catogories (table 5), we have those that typically access data for management and research tasks. All these accesses were considered suspicious because they are query actions. Nonetheless all the other categories have a high percentage of access classified as “suspicious”. This indicates that there are a several number of EHR accessed that did not had information updated, and were just consulted.

Table 4: Adjusted results for UC “EHR read access”.

Date	Total results nr = 216	Suspicious access nr= 198 (92%)
2019-07-22	29	27 (93%)
2019-07-23	20	19 (95%)
2019-07-24	30	29 (97%)
2019-07-25	40	32 (80%)
2019-07-26	11	11 (100%)
2019-07-27	15	14 (93%)
2019-07-28	18	17 (94%)
2019-07-29	26	24 (92%)
2019-07-30	27	25 (93%)

Table 5: Results for UC “EHR read access” by professional category.

Professional Category	**Nr Accesses** nr=378	**Nr Suspicious** nr=300 (79,3%)
No identified	50	30 (60)
Admin Sirai	7	7 (100)
Admin VCOBSGYNV3,Creat User	2	2 (100)
Administrative	52	38 (73)
Nurse	117	93 (79,5)
Nurse,Admin VCInt,Physician, Development team	1	1 (100)
Nurse,Administrative,Admin Physician,Admin Sirai, Admin_Backoffice	12	12 (100)
Management, Admin, VCOBSGYNV3,Creat Users,Physician	2	2 (100)
Indicators Sirai,Admin Sirai	2	2 (100)
Physician	25	18 (72)
Physician_Specialist,Physician	108	95 (88)

The categories related to healthcare delivery like “Administrative”, “Nurse”, “Phisician” and “Specialist Physician” have a high percentage of suspicious access classification, all above 70%.

4 DISCUSSION

Previous work showed that there are many reasons for existig concerns about health data access on healthcare institutions (L.Correia et al., 2019) and the health data flow complexity is such that turns very hard to evaluate the ligitimacy of the accesses to EHR. However, despite the complexity of health data management processes, it is possible to describe scenarios, UC and the data flow of the access between users and systems through SD. Based on this information we could develop three algorithms for suspicious activity dectection that used the data from AT, which has the users and systems activity logs. However, at this point, we just had available logs from one applicational system (Obscare) that were being collected to HS.Register in a hospital from North Portugal. So we developed three algorithms for suspicious activity dectection that could be tested. The results immediately show that there are some aspects in common to the three analysis. There are events that do not have the professional identification or category. This actions are automatic processes running in system's background and all of them are classified as suspicious in “Check time of activity” and “Check days of activity” UC, because of their continuous behaviour that exceeds the time limits imposed by algorithm's rules. For UC “EHR read access”, as it depends on the type of action of the automatic processes, not all are suspicious. Some are just to check information and others update the EHR. Being automatic processes they probably do not represent a threat, nonetheless they should be identified to make easier to spot and interpret them. We can also see that there are various professional categories of management responsibilities, and they are not used regularly. So their accesses appear classified as suspicious accesses due to their pattern of very short usage, specially when comparing with the expected duration for a shift. Even seeming normal at a first glance, it would be recommendable to track the behaviour of these accesses in particular, once they provide confidencial data. We think that a detailed analysis of the pattern of these accesses may give further indication of their legitimacy.

By the point of view of the professional category of the staff that access to HIS, the main categories that access are administrative, nurses, physicians and specialist physicians. In general, they present normal activity in what concerns to activity longer than expected ($\leq$780 minutes), 27 in 276 which represent 9,78% of the results. Physicians and Specialist physicians are the categories that have more cases of this type of activity, longer than expected. Some of these suspicious accesses may be explained by the fact that Obscare system is also used in emergency context, and not only for consulting or hospital stay context. In emergency context shifts may be longer than 12 hours, up to 24 hours (L.Correia et al., 2019). The suspicious accesses detected are in most cases for activities shorter than expected ($\geq$300 minutes), 152 in 276 representing 55% of the results and it is common to all categories. We supose that the consecutive time of activity on HIS by professionals in general probably may be shorter than six hours.

In the case of consecutive days of work, excluding automatic processes which are 9 of 318 (2,83%), only specialist physician category exceeds the expected number of consecutive days of activity, which are 7 of 309(2,27%). The constraints of patient data access to care delivery it is usually used the credentials of physicians because most of the times they do not have EHR access limitations. These occurrences might explain the values obtained. In general, we see that accesses that show the highest percentage of being suspicious are the ones associated to physicians categories and are in line with our expectations. However a deeper analysis would be necessary to have further conclusions about these results. Relatively to accesses made to read medical records, the mean of suspicious access is 79% of the total accesses, and when analysing by category we can see that this high percentage is transversal to all categories. Even when excluding the categories that normally access to get reports, every type of management and research categories that access to extrat data and do not update records, the percentage of suspicious access grows to 93%, which means that only 7% of the records are accessed and updated. For this UC we should evaluate again the data that it is being analysed, test it during a longer period of time and find out whether this numbers are correct, performing an analysis on the field.

5 CONCLUSIONS

The scope of this study is very complex and requires a very thorough analysis. Although the difficulties we found it was possible to create a proof of concept of a system to detect suspicious accesses by professionals from healthcare institutions.

Some limitations we have are the lack of detail of the tasks performed by healthcare professionals to create more precise rules for algorithms. An analysis on the field, would be also very useful to better understand the results and, probably, change the classification of some accesses. Another limitation is the availability and quality of HIS logs. Obscare system has already logs prepared for GDPR compliance, but many systems have not and institutions need to make a great effort on providers to have this information. The period of test should be longer than nine days to detect more patterns in the results obtained.

Nonetheless it was possible to model the scenarios of undue access and create algorithms to detect suspicious accesses. The results obtained gave a first glance of what is happening at the level of HIS access. A strength of using Obscare system was the fact that it is used on hospital stay, consulting and emergency context. It may explain some of the outliers detected, as the emergency shifts may have different durations. These results must be confirmed at an initial stage and, than, take advantage of this information to create a knowledge base that will allow to apply Artificial Intelligence (AI) models.

Even at this stage, which is still in a very embryonic stadium, the project reveals to be very useful to IS department and to DPO. They are having the first picture of the accesses by professionals in the presented format. Having the results of access classification based on the rules created according to staff routines, the identification number of the professional that made the access, the time the access was made and the patient accessed, it gives clues for DPO and CIS investigate whether the access was in fact illegitimate. Further work must be performed to completely accomplish the main goal of this project, like perform a more detailed analysis to verify the correctness of classifications, determine its sensibility and specificity and detect the suspicious accesses in almost real time. It would be very interesting and useful althought the caracteristics of technology used in hospitals may be a barrier. Finally, the production of a knowledge base its recommended so that it will be possible to apply AI models in the future.

ACKNOWLEDGEMENTS

This article is a result of the project HS.Register Demonstrator, NORTE-01-0247-FEDER-033756, supported by Norte Portugal Regional Operational Programme (NORTE 2020), under the PORTUGAL 2020 Partnership Agreement, through the European Regional Development Fund (ERDF).

REFERENCES

Diário da Republica (2005). Informação genética pessoal e informação de saúde, Lei n.º 12/2005 - Diário da República n.º 18/2005).

EU (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Gonçalves-Ferreira, D., Leite, M., Santos-Pereira, C., Correia, M. E., Antunes, L., and Cruz-Correia, R. (2018). HS.Register - An Audit-Trail Tool to Respond to the General Data Protection Regulation (GDPR). *Stud. Health Technol. Inform.*, 247:81–85.

Joint Commission International (2017). JCI Accreditation Standards for Hospitals, 6th Edition.

L.Correia, R.Cruz-Correia, and P.Rodrigues (2019). Illegitimate his access by healthcare professionals: scenarios, use cases and audit trail-based detection model. SCITEPRESS.