Log analysis of human computer interactions regarding *Break The Glass* accesses to genetic reports

Ana Ferreira[1,2], Pedro Farinha[2], Cátia Santos-Pereira[2], Ricardo Correia[2], Pedro P Rodrigues[2], Altamiro Costa-Pereira[2] and Verónica Orvalho[3]
[1]*SnT, University of Luxembourg,Campus Kirchberg, Luxembourg*
[2]*CINTESIS, Faculty of Medicine, University of Porto, Portugal*
[3]*IT, Faculty of Science, University of Porto, Portugal*
ana.ferreira@uni.lu, {pedro_fa, catiap, rcorreia, pprodrigues, altamiro}@med.up.pt, veronica.orvalho@dcc.fc.up.pt

Keywords: Security usability, Human interaction log analysis, Electronic Health Records, Access control override.

Abstract: Patients' privacy is critical in healthcare but users of Electronic Health Records (EHR) frequently circumvent existing security rules to perform their daily work. Users are so-called the weakest link in security but they are, many times, part of the solution when they are involved in systems' design. In the healthcare domain, the focus is to treat patients (many times with scarce technological, time and human resources) and not to secure their information. Therefore, security must not interfere with this process but be present, nevertheless. Security usability issues must also be met with interdisciplinary knowledge from human-computer-interaction, social sciences and psychology. The main goal of this paper is to raise security and usability awareness with the analysis of users' interaction logs of a *BreakTheGlass* (BTG) feature. This feature is used to restrict access to patient reports to a group of healthcare professionals within an EHR but also permit access control override in emergency and/or unexpected situations. The analysis of BTG user interaction logs allows, in a short time span and transparently to the user, revealing security and usability problems. This log analysis permits a better choice of methodologies to further apply in the investigation and resolution of the encountered problems.

1 INTRODUCTION

Theoretically, a computer can be made secure if the three main security characteristics (e.g. confidentiality, integrity and availability) can be guaranteed. However, a crucial factor can bring a lot of entropy to this *secure* world: humans (Schneier, 2000). Yet, technology that is theoretically secure and not usable does little to improve information security because it pushes users away to less secure platforms. This is very common in healthcare where users of Electronic Health Records (EHR) frequently circumvent existing access control rules to perform their work (Lehoux, 1999), (Cranor, 2005).

In the healthcare domain, the focus is to treat patients (many times with scarce technological, time and human resources) and not to secure their information. Therefore, security must not interfere with this process but be present, nevertheless. Ideally, users should be part of the solution and become more involved in the design of secure and usable systems (Ferreira, 2010). In fact, this design can many times raise issues that cannot be met with existing human computer interaction (HCI) knowledge and methods (Kainda, 2010), but must integrate interdisciplinary knowledge such as from socio-technical systems research, safety critical systems design and social psychology (Whitten, 1999), (Sasse, 2003).

According to healthcare legislation, both the North American Health Insurance Portability and Accountability Act (HIPAA) (Break Glass, 2012) and the United Kingdom National Health Service (NHS) documentation (NHS, 2012) specify the need for Break-The-Glass (BTG) or overriding situations (*break the seal*) as described in (Break Glass, 2004). BTG is required when static access controls are insufficient and there is the need to override those controls in emergency and/or unexpected situations. BTG permits the use of a more flexible and dynamic access control policy, which can be adapted to the users' needs at the point of care.

In terms of BTG auditing, an email alert (or another type of alert such an SMS or a phone call) can be sent to a responsible party when the glass is broken (e.g. when a user overrides access control permissions) and this party or another entity can further investigate whether this access was justified (Ferreira, 2006).

The BTG users' interaction logs can provide regular monitoring and auditing functions (which are rarely used unless a serious breach needs investigation) but can also gather a rich amount of information concerning both security and usability behaviours (Iglesias, 2012).

The main goal of this paper is to raise security usability awareness by identifying some security and/or usability problems regarding human-computer interaction behaviour, with the analysis of users' interaction logs of a BTG feature in healthcare. The identified problems can then be further explored and mitigated with the most appropriate methodologies.

This paper is organised as follows: the next section presents background information; Section 3 describes the use-case scenario where this research has been applied, together with the methods used for log acquisition and analysis; Section 4 presents the obtained results while Section 5 discusses and analyses those results; Section 6 presents some future work and Section 7 concludes the paper.

2 BACKGROUND

2.1 Security Usability

An information system is usable when its users can perform the tasks they need in a fast and easy manner and routinely/automatically apply correct protection mechanisms (Saltzer, 1975). This points out that: (1) usability focuses on users; (2) people use products to be productive; (3) users are busy people trying to accomplish tasks; and (4) users decide when a product is easy to use (Redish, 1999).

With this in mind, there seems to be an implicit assumption that technologies that are widely used are, by definition, usable. However, examples such as passwords and email security show that technologies that worked well enough when introduced can evolve into usability disasters with extended use (Sasse, 2003).

Different approaches need to be applied regarding not only, authentication mechanisms (Kuo, 2006), (Brostoff, 2000) email encryption (Whitten, 1999), access control (Ferreira, 2011a), security tools and privacy (ZIshuang, 2005), but also issues that are aimed at achieving users' goals, which may not be directly related with security, but have an element of security in them (Cranor, 2005).

Security usability's main goal is then to improve the usability of information system's security features or even other features not directly related with security. In the later scenario, this must be done without compromising system's security.

2.2 Log Analysis

Non-repudiation is also a very important security goal (Harris, 2012) and so auditability measures are commonly put into place usually for when something goes wrong and a thorough investigation is needed. Most of the times, the only way to do this is to recur to the registration of all activities performed within a system. This log of activities includes all accesses and interactions that programs, processes, and most importantly, users have with that system.

So besides its most common usages, logs can integrate a wide and rich set of interaction data whose analysis can be used for other purposes rather than auditing. Users' interaction logs can help improving data quality and integrity by allowing, for instance, the detection of healthcare information errors and inconsistencies (Cruz-Correia, 2011). Although logs may need pre-processing to allow a useful analysis they can be very valuable to study user modelling, improve activity analysis, monitoring and security (Xhafa, 2012). There are also cases where logs can be used to provide a better knowledge of users' behaviour with the main goal to assist them in performing their tasks (Iglesias, 2012), (Shun-Hua, 2010), as well as identify usability problems (Palanque, 2011).

3 USE-CASE & METHODS

3.1 Legislation Compliance

Many healthcare institutions developed their healthcare processes and subsequent healthcare information systems. Legislation is usually generic and abstract enough to allow this type of diversity. However, this also allows for systems' heterogeneity and, commonly, difficult communication and integration (Cruz-Correia, 2007).

On the other hand, there is also specific legislation available which focus on special parts of

healthcare data protection that needs compliance. This is the case of the Portuguese law for genetic healthcare related information that defines how genetic information must be protected and how and what healthcare professionals are authorized to access it during the course of their work (Assembleia, 2005). The law states that only a pre-defined group of healthcare professionals, whose speciality is directly related with genetics' study and treatment, can access data containing this type of information. Section 3.2 describes how this law was enforced using the BTG feature.

3.2 Healthcare Scenario

In May 2003, the Department of Biostatistics and Medical Informatics (currently CIDES - Departamento de Ciências da Informação e da Decisão em Saúde) at Porto Faculty of Medicine implemented a Virtual Electronic Patient Record (VEPR) (Cruz-Correia, 2005) at the São João Hospital Center, which is the second biggest hospital in Portugal, where more than 5300 patients are attended every day. This VEPR is a subset of an EHR and integrates clinical reports from 14 hospital departments, Diagnosis Related Groups and hospital administrative databases. Around 452 healthcare professionals access the system on a daily basis (there is a total of 2300 active users) and visualize 1525 reports in 1674 daily sessions (there are more than 9.000.000 stored patient reports but usually around 3.000.000 are available for access).

The authentication mechanisms used for this VEPR are login and password and the authorisation platform is based on the RBAC (Role-Based Access Control) standard (Ferraiolo, 2001). Once the user authenticates successfully to the system his/her access control profile is selected and activated in a transparent way. This profile includes permissions and resources that can be accessed by that user and associated role(s). A web based platform (*webcare*) was developed to administer the access control policy for all VEPR users (Farinha, 2010).

The described VEPR integrates reports which contain patients' genetic information. In order to comply with the legislation described in Section 3.1, only a predefined group of healthcare professionals has direct access to this type of patient reports. The Hospital's Ethical Commission and the board of directors have defined the group of authorised users. However, if needed, other healthcare professionals can access these reports if they perform BTG by overriding the stated access control policy and abide to its subsequent conditions and/or consequences. BTG was implemented to control policy override and block immediate access to the reports that contain genetic information to unauthorised users. When the users try to access a genetic report and do not belong to the authorization group, a popup window appears, alerting them of the BTG procedure, the legislation it enforces and possible consequences.

The user needs to decide if the reason to perform BTG is strong enough to still perform this access. He/she is obliged to select a reason to execute BTG. Two of the reasons are fixed and are: [reason **R1** - "I belong or should belong to the authorised group"] and [reason **R2** - "I have urgency to see this report even though I have no permission, at this moment, to do it"]. A third option is also available where the users can [reason **R3** - write his/her own reason/justification].

3.3 Log Acquisition and Analysis

For the presented VEPR (Section 3.2) users' log interactions are registered within a separate instance of a relational database system solely for this purpose. All records are stored in a structured manner in database tables where is easier and faster to search and retrieve them.

Users' interaction logs have been collected since November 2004 but the data analyzed within this paper were collected from November 2007 until December 2012. Genetic reports started to be identified on collection in November 2007 so data are presented according to these figures. May 2009 was the date when the BTG feature started to be used. The log analysis focused on the comparison of the period before and after using BTG features and verifies if these specific access control mechanisms can reveal how users interact and/or change behavior over long periods of time. As a means to easily and quickly reveal usability and security problems, the analysis presented in this study is mainly about summarizing the main user interaction behaviour. So analysis is made regarding data frequencies from search queries applied directly to the audit log database. It is possible to make deeper analysis using several data mining tools (Iglesias, 2012) to find more complex behavioural patterns but this is not the main purpose of this research.

The search queries that were applied to the audit database for this study included: (1) the total number of identified genetic reports; (2) the total number of accesses to genetic reports by all users (authorised and unauthorised) before and after BTG implementation; (3) how many users performed BTG and how many gave up once warned about its

consequences; (4) the reasons chosen to perform BTG and the most common inserted reason **R3**; (5) if there was any suspicious individual behaviour amongst the users who most perform BTG and also give up doing it; (6) and if there was a specific time of the year where usage patterns were very different from other periods of time.

Results are presented in Section 4 and their subsequent discussion is introduced in Section 5.

4 RESULTS

Before the implementation of the BTG feature (November 2007 – April 2009), 2875 genetic reports were stored within the database. A total of 7774 genetic reports were available afterwards (May 2009 - December 2012).

Table 1 compares the accesses to genetic reports from authorised and unauthorised users, before and after the BTG implementation. Before BTG, all accesses (n=842) by unauthorised users to genetic reports were successful. After the BTG implementation and from the unauthorised users' attempts (n=5608), 3071 (55%) BTG accesses were successful while 2537 (45%) were unsuccessful as users gave up performing BTG after being warned (waivers). From these waivers, 2366 (93%) closed the browser while 171 (7%) preferred to select the "I don't want to see this report" button.

Table 1: Frequencies (percentages) of attempts (total of 7176) to access genetic reports from authorized (n=726) and unauthorised users (n=6450), before and after the Break The Glass (BTG) implementation and use.

	Attempts *before* BTG (Nov 2007 – Apr 2009) (n=1001)	Attempts *after* BTG (May 2009 - Dec 2012) (n=6175)	
	successful accesses n (%)	successful accesses n (%)	unsuccessful accesses n (%)
Authorised users	159 (16)	567 (9)	0 (0)
Unauthorised users	842 (84)	3071 (50)	2537* (41)

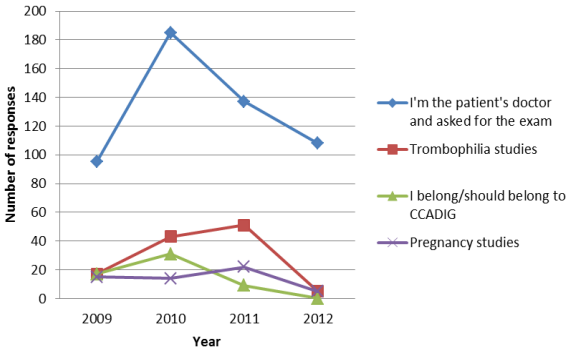
* From the 2537 unsuccessful accesses, which correspond to 45% of the total of 5608 access attempts from unauthorised users after BTG use, 171 (7%) of these users pressed the button "I don't want to see this report" while 2366 (93%) closed the browser.

For the three reasons that could be selected by the users who performed a BTG access, Table 2 presents the total number of selections that were made, together with the four most common reasons that the users inserted before "breaking the glass". Figure 1 presents the yearly distribution of these four reasons. Moreover, there were also 6 empty answers (the users are obliged to insert a reason) and one user that refers that the system is wrong.

Table 2: Frequencies (percentages) of pre-selected (R1 and R2) and stated reasons (R3a to R3d) chosen by unauthorised users who performed BTG within their 3071 accesses to genetic reports.

Type of pre-selected or stated reasons	Total number of selections n (%)
R1 – I belong to the authorised group	834 (27)
R2 – I have urgency to see this report	1229 (40)
R3 – I write another justification:	1008 (33)
R3a - "I'm the patient's doctor and requested the exam"	525 (52)
R3b - "Thrombophilia studies"	116 (12)
R3c - "I belong to the authorised group"	57 (6)
R3d - "Pregnancy/infertility studies"	56 (6)

Figure 1: Four most common reasons introduced by the users to justify their BTG accesses (yearly distribution).



Focusing now on individual accesses, the top three BTG users were identified. Table 3 compares the total of BTG accesses and waivers to patient genetic reports regarding these three users. This comparison is performed between two moments in time: 2009-2010 and 2011-2012. Table 4 presents in more detail the number and types of reasons selected by the three users that performed most BTG accesses.

Table 3: Frequencies (percentages) of BTG accesses and waivers (unsuccessful accesses) regarding the total number of attempts to access genetic reports by the three unauthorised users who mostly performed BTG (u_A, u_B, u_C), in two consecutive periods.

	During 2009 and 2010			During 2011 and 2012		
	Total n	BTG accesses n (%)	Waivers n (%)	Total n	BTG accesses n (%)	Waivers n (%)
u_A	81	47 (58)	34 (42)	155	90 (58)	65 (42)
u_B	134	67 (50)	67 (50)	125	64 (51)	61 (49)
u_C	95	73 (77)	22 (23)	72	53 (74)	19 (26)

Table 4: Number and types of reasons selected by the three unauthorised users who most performed BTG (u_A, u_B, u_C).

	During 2009 and 2010			During 2011 and 2012		
	R1	R2	R3	R1	R2	R3
u_A	1	45	1	0	89	1
u_B	67	0	0	64	0	0
u_C	1	0	72	1	0	52

Users u_A and u_B hardly selected reason **R3** to justify their BTG accesses. User u_A mainly selects reason **R2** and chooses reason **R3** to justify only two accesses (i.e., 1 trombophilia study and 1 I asked the patient's exam). This user also mistakenly inserts reason **R2** together with reason **R3** at one time, and again gives "thrombophilia study" as the justification. User u_B only selects reason **R1**. User u_C mainly selects reason **R3** to justify the BTG accesses and writes "I asked the patient's exam" 124 times in total. This user also mistakenly inserts two times the reason **R1** with that same justification in reason **R3**.

5 DISCUSSION

This section discusses the results presented in Section 4 and gives some recommendations on what security and usability issues need further investigation, and what are the most appropriate methodologies to better understand and resolve those issues.

Regarding Table 1, before implementing the BTG features , 84% of all accesses were unauthorised, but successful accesses.

After BTG implementation, from all the access attempts and with 3 times more patient genetic reports available, 55% of those attempts from unauthorised users were successful and used BTG, with the most varied reasons presented in Table 2. Still, in total, 45% of unauthorised accesses (that would not normally be detected) were prevented, after BTG implementation. However, 91% of all access attempts were made from unauthorized users, so only 1 in every 9 attempts is made from authorised users.

During the course of 4 years there has been an increase of almost 200% of access attempts. Before BTG features there were around 55 access attempts per month (in this case all successful) while after BTG features this number increased to 144 access attempts per month (71 from unauthorised users). Further investigation with qualitative studies such as focus groups is needed to make sure daily processes match the users' daily needs regarding data access. Why the number of unauthorised access attempts has increased so much? Do unauthorised users need to access genetic reports this often? If so, why? (the legislation may not match real healthcare processes). If not, better monitoring and feedback needs to be made to avoid most unauthorised accesses.

Also important to note from Table 1 is the fact that, in percentage, accesses from the authorised group were reduced to half. Does this mean that users belonging to the authorised group need to be re-checked? Maybe some users have already left the hospital and some unauthorised users should belong to the authorised group instead. Either way, the access control policy to genetic reports needs to be reviewed and updated. In order to do this, the responsible parties and board of direction, as well as the Hospital Ethical Committee need to be consulted.

Finally, from users who give up performing BTG and are warned of the consequences, only 7% select the provided button. The other 93% simply closed the window. Further investigation needs to be done to find out why users do not select the "I don't want to see this report" button. Do they think is a mistake and close the window to restart the browser? More specific individual user log analysis can be done to exploit this question (Table 3 gives evidence that some users can do that). If users do not need to see the requested genetic report, do they think that just by closing the window their access attempt is not registered as if it would be by actively pressing a button? Again, focus groups can be performed to better understanding the later question.

Analysing now the results regarding the three reasons that users choose to perform BTG (Table 2), the most selected reason is the one that states that they have urgency to see the report (40 %). This in itself does not say much. There can be

many different types of urgencies and some more "urgent" than others. The text which appears on the BTG warning interface may need revision and the reasons to perform BTG need to be clarified. Further, open interviews can be applied to the users to better understand what types and degrees of urgencies can commonly appear. Maybe one suggestion could be to have only one reason where users could introduce their justification and no other options as, for example, even with a fixed option reason **R1** – "I belong or should belong to the authorised group" available (with 27% of selections), users still use reason **R3** to state that they belong to the authorised group (6%).

For the previous suggestion, there are also some issues to be further explored. The most common BTG justification inserted by the users include the fact that they are the healthcare professionals treating the patient and asked for that exam (52%) or that they requested it in order to perform studies relating to specific medical specialities (i.e., thrombophilia and pregnancy studies) (18%).

All these issues can be related to how the access control policy is defined. Firstly, there is not yet the possibility for the patient to define or control what healthcare professionals can/should access which parts of his/her medical record, as stated within the European legislation. This is an issue outside the scope of this research but which needs to be urgently addressed in a near future as also interferes with healthcare access control policy definition (Santos-Pereira, 2012). Secondly, focus groups need to be performed with the users to find out if the most common inserted reasons are/can be justified. If they are, the access control policy needs to be reviewed and updated by the responsible parties.

Within the mentioned focus group study, another issue must be raised. Why have the reasons inserted decreased so much during 2012? In this year, the BTG accesses by users that selected reason **R3** have decreased almost 60% when compared with the two previous years. Are users performing BTG only when they really need now? Do they select mainly the other two fixed reasons? Or have they access to this type of information from other means (i.e., other applications, paper documents), bypassing this way BTG features so that their accesses are not so closely monitored and registered? Has the background justification process become more active or effective? Is there any technical problem with the BTG features? Are they working as expected? To help answering these questions, qualitative observation and focus group studies should be performed with the users, as well as meeting with responsible parties to analyse the BTG background justification (is it being done? How? When? By Whom?). Quantitative users' interaction log analysis, together with testing and validating the technical aspects of the interface, must also be performed.

One more issue that can be directly related with the interface and technical implementation is the fact that there were at least two situations detected where a user was able to perform BTG without having to insert a reason to justify it. Maybe the user just filled the space provided with space characters, if this is allowed. It should be compulsory to select or insert a non-empty reason to perform BTG. Technical measures need to be corrected so that empty answers are avoided.

Focusing now on the analysis of BTG accesses from individual users (Table 3), further investigation is required to understand why these users need to perform BTG more often than the others. In more detail, user u_A has increased by almost 100% his BTG accesses and attempts in the last two years (2011 and 2012). The other two users (u_B, u_C) have slightly decreased their BTG accesses but still remain high. Further research needs to be made to confirm if these users are just maliciously or negligently accessing the genetic reports or if they should be part of the authorised group and access control policy needs, once more, reviewing and updating.

Individual users' interaction logs seem to reflect what was also identified by the generic analysis of those same logs. It is also possible to identify in Table 3 that the users who most perform BTG also give up doing it a very high number of times. So maybe the issue of trying several times before actually succeeding when they see there is no other option but to press the "I want to see this report" button, may be happening. Observation studies and more detailed analysis of interaction logs can be performed to confirm this.

Finally, regarding Table 4 results, the most common reasons to perform BTG which were inserted mostly by user u_A are in tune with the ones presented in Table 2. Also, the three identified users tend to choose the same reason every time they try to access a genetic report. Their behaviour regarding BTG does not change over 4 years of use. However, separately, they choose very different reasons to justify BTG accesses. Furthermore, these users choose a few times both a fixed reason (**R1** or **R2**) with reason **R3** to describe a BTG access**.** This must be corrected in the interface. Users must only be able to select one reason at a time.

In summary, and as a preliminary analysis of the obtained results, several technical, usability, security and even social issues were raised for further investigation. In order to fasten this investigation, each study to be performed should include the biggest number of issues to study. For example, if focus groups are employed, all the issues raised here that require this type of method can be explored at the same time. Is it also important to state that these studies should not be used to control or survey users' actions to further punish them. The main goal is to improve BTG's HCI, security, usability and its usefulness, and allow users to perform their daily tasks in a safe/efficient manner.

However, a very important question remains: why were some users accessing genetic reports before BTG implementation, if they did not access those reports so often once BTG features were available? It may not be easy to find out why this was happening with the proposed research methods but maybe by correcting some of the other problems raised in the discussion, this type of unauthorised accesses can be avoided in the future.

6 FUTURE WORK

Future work includes further investigation of the previously identified security usability issues, but also the analysis of other issues that arose during this research, including if there are (recommendations on what type of studies could be used to further explore these issues are in square brackets): (a) accesses made simultaneously by the same login at different locations with different sessions [quantitative log analysis]; (b) many waiting sessions or automatic session locks [quantitative log analysis]; (c) any suspicious behavior relating with the number of times a user authenticates daily [quantitative log analysis & qualitative observations]; (d) any suspicious behavior relating with how many times a computer is used and for how many different people on a daily basis [qualitative observations & interviews]; (e) any common authentication errors, mostly login or password problems [quantitative log analysis & qualitative interviews].

Other usability issues that also be analysed include if: (a) there could be any suspicious behavior relating with password sharing [quantitative log analysis] (Ferreira, 2011b); (b) there are any common paths to search for information inside the system [quantitative log analysis & qualitative observations]; (c) there are many backward flows within the searches performed by the users [quantitative log analysis].

7 CONCLUSIONS

Users' interaction logs can be a helpful tool to studying *user-system* interaction but other exploratory studies are needed to focus on *user-user* interaction, in which *context* the user is interacting with the system and which *characteristics* and *individual knowledge* the user has and uses to perform those interactions (Xhafa, 2012).

This paper presented an analysis of users' interaction logs in order to study HCI security and usability issues. Logs generate a great amount of data that can be useful as to unveil both those issues. Users' interaction log analysis can be used not only in healthcare to analyse users' behaviour regarding BTG accesses but also in other scenarios where confidentiality is very important (i.e., home banking, online shopping, etc). However, logs are not enough to change unsecure, erroneous or even malicious users' behaviour. Other methods and techniques need to be used to further explore how this can/should be done.

Finally, as much as users' interaction logs can be a promising tool to be used to study and improve HCI and security usability problems, bad quality logs (many times they do not even exist), will certainly not be helpful in pursuing these tasks and so it is recommended that logs should be taken more seriously and be adequately and securely implemented and maintained.

ACKNOWLEDGEMENTS

This work was supported by the Fonds National de la Recherche Luxembourg – FNR-CORE project [1183245] – "Socio-Technical Analysis of Security and Trust" (STAST)" and by the Portuguese FCT, through the research project "Optimizing Information Systems for healthcare: improving Graphical User Interface and Storage Management through Machine Learning techniques on user logs data" [PTDC/EIA-EIA/099920/2008].

REFERENCES

Assembleia da República, 2005. *Lei n. 12/2005 de 26 de Janeiro*. DIÁRIO DA REPÚBLICA — I SÉRIE-A.

Break-glass, 2004. *An approach to granting emergency access to healthcare systems*. White paper, Joint – NEMA/COCIR/JIRA Security and Privacy Committee (SPC).

Break Glass, 2012. *Granting Emergency Access to Critical ePHI Systems – HIPAA Security*. Accessed at: http://hipaa.yale.edu/security/breakglass.html. Accessed on the 13th December 2012.

Brostoff, S., Sasse, A., 2000. Are passfaces more usable than password? A field trial investigation. People and Computers XIV-Usability of else. *Proceedings of HCI 2000*. S. McDonald Springer, 405-424.

Cranor & Garfinkel, 2005. *Security and usability: designing secure systems that people can use*. O'Reilly.

Cruz-Correia, R., Lapão, L., Rodrigues, P., 2011. *Traceability of patient records usage: barriers and opportunities for improving user interface design and data management*. Studies in Health Technologies and Informatics, vol. 169, pp. 275-279.

Cruz-Correia, R., Vieira-Marques, P., Costa, P., Ferreira, A., Oliveira-Palhares, E., Araújo, F., Costa-Pereira, A., 2005. Integration of Hospital data using Agent Technologies – a case study. *AICommunications special issue of ECAI*, 18(3):191-200.

Cruz-Correia, R., Vieira-Marques, P., Ferreira, A., Almeida, F., Wyatt, J., Costa-Pereira, A., 2007. Reviewing the integration of patient data: how systems are evolving in practice to meet patient needs. *BMC Medical Informatics and Decision Making*, 7(14).

Farinha, P., Cruz-Correia, R., Antunes, L., Almeida, F., Ferreira, A., 2010. From legislation to practice: a case study of break the glass in healthcare. *Proceedings of the International Conference on Health Informatics*, 114-120.

Ferraiolo, D., Sandhu, R., Gavrila, S., Kuhn, R., Chandramouli, R., 2001. Proposed NIST Standard for Role-based Access Control. *ACM Transactions on Information and systems security*, 4(3): 224-274.

Ferreira, A., Antunes, L., Chadwick, D., Cruz-Correia, R., 2010. Grounding Information Security in Healthcare. *International Journal of Medical Informatics*, 79(4): 268-283.

Ferreira, A., Correia-Cruz, R., Antunes, L., 2011a. Usability of authentication and access control: a case study in healthcare. *IEEE International Carnahan Conference on Security Technology*, 1-7.

Ferreira, A., Cruz-Correia, R., Chadwick, D., Santos, H., Gomes, R., Reis, D., Antunes, L., 2011b. *Password sharing and how to reduce it*. Certification and Security in Health-Related Web Applications: Concepts and Solutions, 243-263.

Ferreira, A., Cruz-Correia, R., Antunes, L., Farinha, P., Oliveira-Palhares, E., Chadwick, D. W., Costa-Pereira, A., 2006. How to break access control in a controlled manner? *Proceedings of the 19th IEEE Symposium on Computer-Based Medical Systems*, 847-851.

Harris, S., 2012. *CISSP All-in-one Exam Guide*. McGraw-Hill Osborne Media. 6th Edition.

Iglesias, J., Angelov, P., Ledezma, A., Sanchis, A., 2012. Creating evolving user behavior profiles automatically. *IEEE Trasactions on Knowledge and data engineering*, 24(5): 854-867.

Kainda, R., Flechais, I., Roscoe, A.W., 2010. Security and usability: analysis and evaluation. *International conference on Availability, Reliability and Security*, 275 – 282.

Kuo, C., Romanosky, S., Cranor, L., 2006. Human Selection of Mnemonic Phrase-Based Passwords. *Symposium on usable privacy and security (SOUPS)*, 67-78.

Lehoux, P., Sicotte, C., Denis, J., 1999. Assessment of a computerized medical record system: disclosing scripts of use. *Evaluation and Program Planning*, 22(4): 439-53.

NHS care records service, 2012. NHS Connecting for Health. *Sealing Overview*. Accessed at: http://www.connectingforhealth.nhs.uk/elearning/scr/scr2008b/modules/scr07_sealing/t1/scr07t1p1.htm. Accessed on the 13th December 2012.

Palanque, P., Barboni, E., Martinie, C., Navare, D., Winckler, M., 2011. *Proceedings of the 3rd ACM SIGCHI symposium on Engineering interactive computing systems*, 21-30.

Redish, J., Dumas, J., 1999. *A Practical Guide to Usability Testing*. Intellect Ltd.

Saltzer, J., Schroeder, M., 1975. The protection of Information in Computer Systems. *Proceedings of the IEEE*, 63(9): 1278-1308.

Santos-Pereira, Cátia., Augusto, Alexandre., Correia, Manuel., Ferreira, Ana., Cruz-Correia, Ricardo., 2012. A Mobile Based Authorization Mechanism for Patient Managed Role Based Access Control. *Information Technology in Bio and Medical Informatics*. Lecture Notes in Computer Science, 7451: 54-68.

Sasse A., 2003. Computer Security: Anatomy of a Usability Disaster and a Plan for Recovery. *Proceedings of CHI2003 Workshop on Human-Computer Interaction and Security Systems*.

Schneier, B., 2000. *Secrets and Lies: digital security in a networked world*. 1st ed.: John Wiley &Sons

Shun-Hua, T., Miao, C., Guo-Hai, Y., 2010. User behavior mining on large scale web log data. *International Conference on Apperceiving Computing and Intelligence Analysis*, 60-63.

Whitten, A., Tygar, J., 1999. Why Johnny can't encrypt: a usability evaluation of PGP 5.0. *Proceedings of 8th USENIX Security Symposium*, 169-183.

Xhafa, F., Ruiz, J., Caballe, S., Spaho, E., Barolli, L., Miho, R., 2012. Massive Processing of Activity Logs of a Virtual Campus. *Third International Conference on Emerging Intelligent Data and Web Technologies*, 104-110.

ZIshuang, Ye., Smith, S., 2005. Trusted Paths for Browsers. *ACM transactions in information systems security*, 8(2): 153-186.