FROM LEGISLATION TO PRACTICE
A Case Study of Break the Glass in Healthcare

P. Farinha, R. Cruz-Correia
CINTESIS – Centre for Research in Health Technologies and Information Systems, Faculty of Medicine, Porto, Portugal

L. Antunes
Instituto de Telecomunicações, Faculty of Science, Porto, Portugal

Filipe Almeida
Comissão de Ética para a Saúde, Hospital S. João, Porto, Portugal

A. Ferreira
CINTESIS – Centre for Research in Health Technologies and Information Systems, Faculty of Medicine, Porto, Portugal

Keywords: Healthcare legislation, Access control, Break the glass.

Abstract: Recommendations and regulations are available in healthcare to protect sensitive medical information. These regulations tend to be generic and orient attitudes within the medical practice and are usually not straightforward to be translated into practice. The main objective of this paper is to present the implementation of the Break the Glass (BTG) concept in a real healthcare setting in order to enforce the legislation for genetic information and evaluate the process of translating legislation into the healthcare practice. The user logs were analysed to assess if the BTG system was working as expected, providing genetic information confidentiality, as well as if the legislation was being enforced in a controlled and responsible manner. Results show that the process to translate legislation into practice could be faster and more efficient. User logs show that in terms of confidentiality the BTG features prevent more non authorised people from accessing genetic reports. We expect the tendency to be that only users who really need to access the reports will go through with the process of BTG. Enhancements to the system include the implementation of the access control management infrastructure within a more robust access control platform to perform the authentication and authorization processes.

1 INTRODUCTION

Recommendations and regulations are available in healthcare to protect sensitive medical information and to guarantee that this type of information is only accessed and used in specific and justified contexts (CdMaÉ, 1997) (CoE-Co. 2004). These regulations tend to be generic and orient attitudes within the medical practice. However, is not straightforward to translate these orientations into practice. Many times this is not even possible. Research shows that excessive regulation can actually create a barrier that physicians have to surmount when treating patients (Ross-Lee et al, 2004). Nevertheless, means need to be put into place to make that translation possible so that confidentiality of medical information – prevention of unauthorized access – is provided.

As an important support tool for consultation, diagnosis and integration of heterogeneous information from different places, the Electronic Medical Record (EMR) (Waegemann, 2003) (Cruz-Correia et al, 2005) stresses even more the need for confidentiality and access control. However, security must not constitute a barrier for a successful use and integration of EMR into the medical practice but allow for a controlled yet transparent way of doing it. With this in view, an EMR was developed and is in use since 2004 at the 2nd biggest hospital in

Farinha P., Cruz-Correia R., Antunes L., Almeida F. and Ferreira A. (2010).
FROM LEGISLATION TO PRACTICE - A Case Study of Break the Glass in Healthcare.
In *Proceedings of the Third International Conference on Health Informatics*, pages 114-120
DOI: 10.5220/0002748201140120

Portugal – the Hospital S. João (HSJ) - (Cruz-Correia et al, 2005) (Ferreira et al, 2004). As there was also the need to provide for an access control management platform for the EMR, the *webcare* platform was developed for this purpose (Farinha et al, 2006). This platform is based on the role-based access control model - RBAC (Ferraiolo et al, 2001) and helps to perform, in an easy and flexible way, the most basic administrative access control actions.

However, this is not enough in such a hectic environment. More flexible access control policies are required not only to improve EMR efficiency but also to enforce the legislation related to genetic information (Lei, 2005). This is a Portuguese legislation and defines how genetic information must be protected, and what and how healthcare professionals are authorized to access it during the course of their work.

In order to do this in a flexible way the information is restricted to an authorized group of healthcare professionals previously defined. However, this access is not entirely denied to all the other healthcare professionals that may need to access this information in emergency situations, but in a controlled way (Rissanen et al, 2004) (Povey, 2000) (Ferreira et al, 2006) (Break-Glass, 2004). We designated this access by *Break the Glass* (BTG). The idea is that healthcare professionals are warned they are not authorized to access that information, but if it is an emergency, they can still access it knowing that they will have to justify and face the consequences later.

The main objective of this paper is to present the implementation of the BTG concept in a real healthcare setting in order to enforce the legislation for genetic information. Further, we evaluate in generic terms the process of translating legislation into the healthcare practice and the impact of BTG use within the same practice.

2 BACKGROUND

The core of the EMR system is composed by three modules (VIZ – Viewing modules, MAID - Multi-Agent system for Integration of Data and CRep – Central repository) which are presented in Figure 1. MAID collects clinical reports from various hospital departments (e.g. DIS A and DIS B), and stores them on a central repository (CRep) consisting of a database holding references to these resports. After searching the database, the users can access the integrated data of a particular patient through a web-based interface (VIZ). When selecting a specific report, its content is downloaded from the central repository file system to the browser.

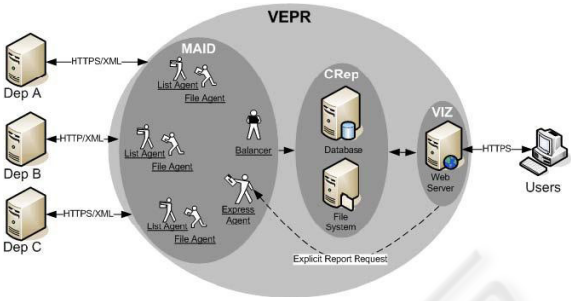

Figure 1: Architecture of the EMR system showing the MAID, the VIZ and the CRep modules.

In order for the access control management platform, the *webcare*, to be implemented it is necessary an authentication procedure where the user is uniquely identified and associated with his profile according to the role or groups where he belongs (i.e. privileges and permissions).

To associate this profile to the user, an infrastructure to model the relationships between all the identities that integrate the RBAC model, including exceptions (accesses with more or less privileges that are related to specific users and not only their roles or groups), was created (see Fig. 2).

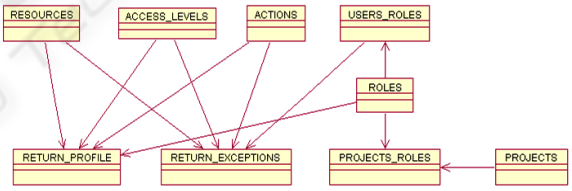

Figure 2: Entity-relation model for the access control platform.

This infrastructure includes entities such as users, roles (which can include subroles), resources, access levels, actions, projects, the entity that includes the privileges and connects all of them (return_profile), and also the entity that does the same for the exception rules (return_exceptions). This model implements all the necessary structure as well as the exceptions needed to generate the profile for a specific user at the time he/she authenticates to the system. To retrieve all this information there is a centralized feature, a procedure, to search the whole structure and collect all the privileges associated to the user.

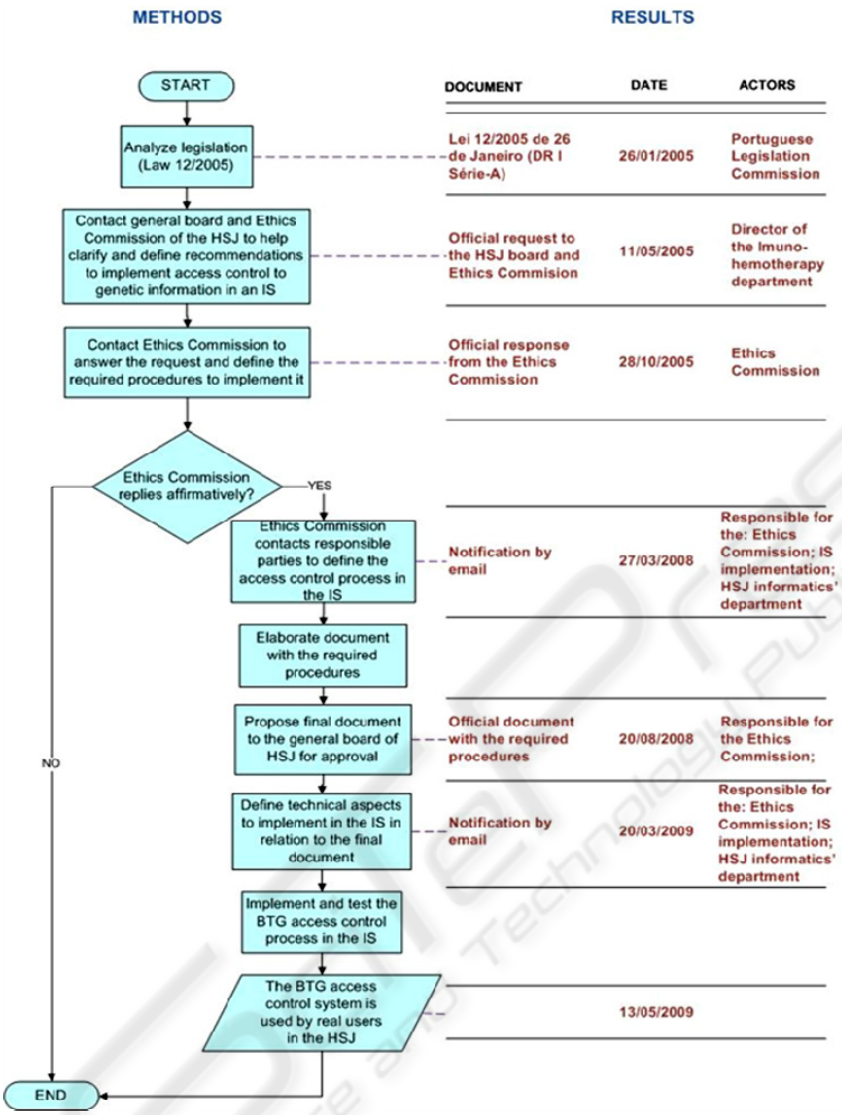

Figure 3: Methods and results from legislation to practice.

All accesses are registered in a specific database structure, separate from the one above. It registers the user, date and time and also the errors that may occur during this process. This is easy to do because the procedure itself can generate exceptions and insert error information according to the failed action.

Figure 4: Access control management platform.

As this platform does not handle BTG accesses some changes needed to be made. These changes are presented in Section 4.

3 METHODS

Figure 3 presents the methodology used to define and implement the BTG access control engine from legislation to practice.

After the implementation the user logs were analysed so that we could assess if the BTG system was working as expected and if legislation was being enforced in a controlled and responsible manner. We also wanted to evaluate the impact that

the BTG systems had on the protection of confidentiality of patient genetic information.

We did this by analysing logs where users tried to access patient reports that contained genetic information. Similar time periods were compared: the 3 months of BTG access control features usage, by real users, on a real setting with the same period of time on the previous year, where no BTG features were available.

4 RESULTS

4.1 From Legislation to Practice

The necessary steps for a user to perform BTG within the presented EMR system are the following (see Figure 5):

1. The healthcare professional tries to access a patient report within the EMR application and that report contains genetic information.
2. The webcare platform validates the healthcare professionals' credentials.
3. The webcare platform checks within the database if the pair login/password is correct.

(In the case where the authentication fails, a reject message is sent from the application to the user and the request terminates here; if the user is privileged and can access directly the required report than the process is done normally)

Figure 3 presents the results from each step of the applied methodology described in the previous section.

4.2 BTG Implementation

4. The webcare platform sends back the user profile that states if the user can BTG or not to the EMR application.
5. The EMR application asks the healthcare professional if he/she wants to BTG on that report, warning about the consequences of doing that (see Figure 6).
6. If the user chooses to BTG (giving a reason for it) he/she just needs to press the appropriate button within the shown interface (see Figure 6).
7. The EMR application makes the requested operation to get the report.
8. The report is given to the EMR application.
9. The EMR application shows the report to the healthcare professional.

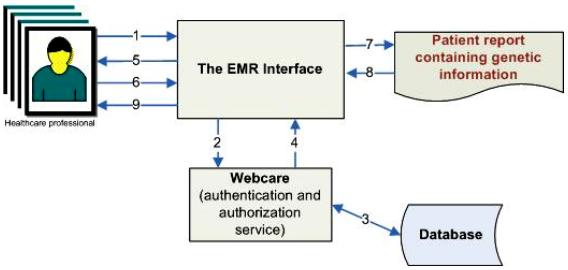

Figure 5: BTG steps.

Once the user chooses a report that contains genetic information, several actions are registered so that the user is accountable for it afterwards. The system registers if the user just made a mistake, whether he/she carries on the BTG procedure or not, and if so, registering the reason he/she gives to do it.

Several procedures were altered within the webcare platform in order to do this. These included:

- The creation of a new group of users (11 medical doctors) that comprise the healthcare professionals that are authorized to access patient reports that contain genetic information, according to the Ethics Commission official document;
- The creation of a new table within the database (BTG audit table) in order to register information about who is trying to access patient reports that contain genetic information (Table 1);

Table 1: Database table to audit user actions regarding BTG accesses.

Campo	Tipo	Descricao
Id	Number	Unique identifier (primary key)
Timestamp	Date	Date & time the BTG popup warning occurred
Id_sessao	Number	Session identifier
Id_relatorio	Number	Report identifier the user tried to Access while BTG
Resposta	Number	The final option chosen by the user (BTG or not)
Motivo_opc	Number	The reason that was chosen for BTG
Motivo	String	Reason described by the user for BTG when the option "Other" is chosen

Besides Table 1, a new attribute was created within another table that stores all the patient reports within the database. This new attribute is a Boolean and is named as "genetics". It states whether the patient report contains genetic information or not. This information is registered automatically from the moment the patient report is collected and stored in the database.

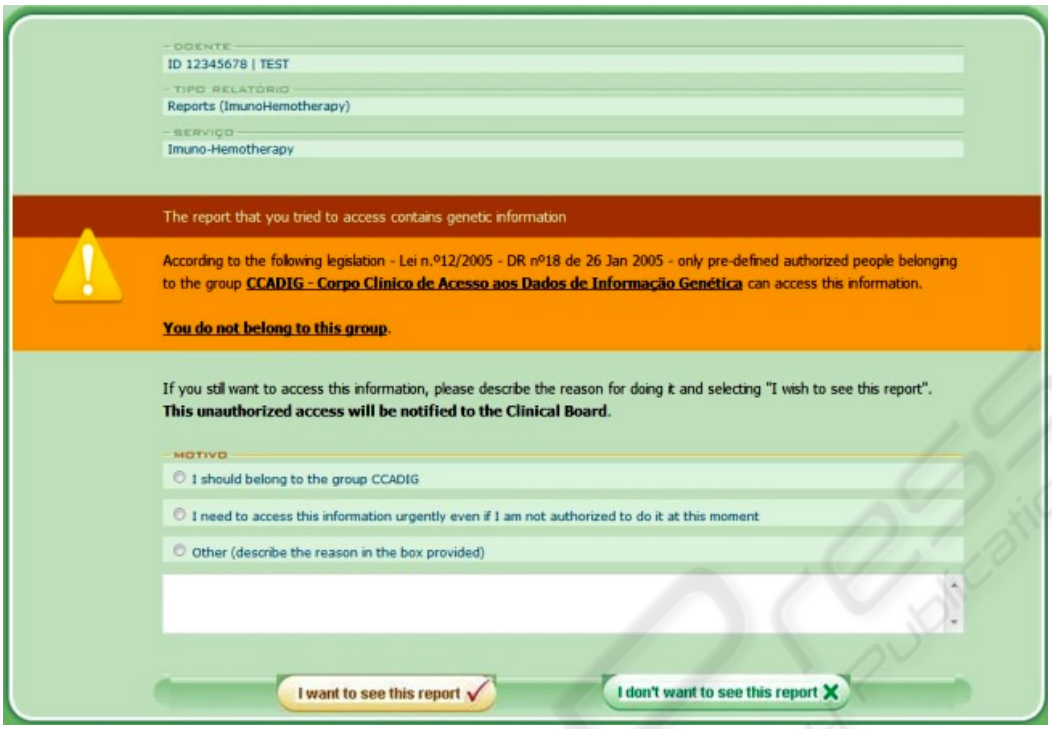

Figure 6: BTG Interface.

Also, on a coding level, there was only the need to introduce a condition that would check for each user's request of a report if that report contains genetic information and if that user is a member of the group of healthcare professionals that is authorized to access these kind of reports. Each time one of these reports is requested to be seen by the healthcare professionals, a new record is inserted within the BTG audit table with identifiers of the report and the healthcare professional. All this is registered whether the healthcare professional chooses to go back, or if the user answers no or yes to BTG.

All this information is summarized and sent to the hierarchical superior of those users by email on a weekly basis. This makes sure that proper justification or any other disciplinary action can be taken afterwards. It guarantees that BTG accesses are properly controlled and taken responsibility for.

4.3 Results Before and After BTG Implementation

The comparison period comprised 15 weeks of BTG access control features usage on a real setting (between the 13th of May 2009 and 26th of August 2009) with the same period of time on the previous year, where no BTG features were available (between the 13th May 2008 and 26th of August 2008).

The patient reports started to be tagged with a genetic label (so that they could be identified) on the 27/11/2007, so we can only analyse the obtained results based on the reports that were stored from this day onwards. The number of genetic reports that were marked at the date of 26/08/2008 is 1093, while on the 26/08/2009 this number had risen to 3274 (2181 more in a year). To this same date the total number of distinct users of the EMR system is 906.

Table 2: The percentage of accesses to reports containing genetic information according to the total number of genetic reports that was available before and after the BTG system implementation, as well as the number of distinct users that performed those accesses.

Accesses to reports containing genetic information		
	Before BTG	**After BTG**
Total of collected genetic reports	**1093**	**3274**
% of accesses	**21**	**14**
Within authorization group	4	3
Not within authorization group	17	11
No of distinct users accessing	**76**	**135**
Within authorization group	4	5
Not within authorization group	72	130

After the BTG features started to be used (between 13/05/2009 and 26/08/2009) the total number of tries to access genetic reports was 471, being 86 from within the authorisation group while 385 from users that are not normally authorized to access them. Table 3 shows within this last number the actions the users took once they were alerted they were not authorised to access the report they requested.

Table 3: Number of BTG accesses made to patient reports containing genetic information (from the users NOT within the authorisation group).

BTG accesses to reports with genetic information		
	BTG	NO BTG
No of accesses	208 (54%)	177 (46%)
No of distinct users	83	98

Within the 177 users that did not do BTG after choosing to access a genetic report, 156 selected NO to BTG while 21 closed the browser without further action. From the 208 users that selected to perform BTG, Table 4 describes the most common reasons the users gave to justify their access.

Table 4: Most common reasons given by the users to perform BTG (n=208).

Reasons to perform BTG	%
I have urgency in seeing the requested information although I'm not normally allowed to do it	50%
Write own reason	32%
I should belong to the group that can access genetic information	18%

5 DISCUSSION

The healthcare legislation for genetic information was published in January 2005 and its implementation in practice took, on the whole, 4 years and 4 months (see Figure 7). The process took more time in phases 3 & 4, which include the definition of the regulatory (2 years and 5 months) and technical specifications (1 year and 1 month). Figure 7 presents the main phases of this process. In all of the phases we believe is possible to fasten the process.

Phases 1 & 2 are more logistic intensive and therefore should be accomplished in a swifter fashion.

Although being the hardest to do, we think that phase 3 is the one that needs more attention. It should be possible to fasten the process of translating legislation into regulations that can be

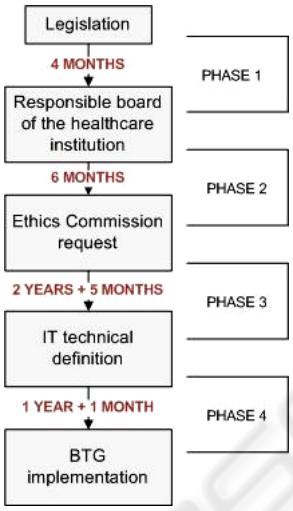

Figure 7: Timeframe of the methodology from legislation to practice.

implemented in an EMR. In addition, the definition of what to implement can be faster if the meetings with the technical people are made earlier in the process. 4 years to enforce legislation is, in our view, a long time. The institutions and systems must be ready to do this in an easier and more efficient way. We believe that the whole process could have taken place in possibly half the time. This study helped in identifying where the major problems can be located and where improvements can be made.

Regarding the technical implementation of the BTG concept, this was an easy and fast process because it was integrated within an EMR platform that was already in use in the healthcare practice and was implemented in a modular and flexible way. Only a few changes were needed to adopt the BTG concept and this allowed for the long period spent in defining the procedural regulations to be enforced, to be shortened at this stage.

The results of implementing and using the BTG features showed that there is a significant decrease in the percentage of accesses to genetic reports when the BTG features are available, even when the number of genetic reports available are much higher (almost triple). There is a similar decrease in non authorized people accessing those reports. Further, from the unauthorized users that tried to access genetic reports, almost half of them decide not to go through with it. This means that the BTG features can filter these non authorized accesses that would normally not be prevented. We expect that the tendency will be that only users who really need to access the reports will go through with the process of BTG.

The most common reason given by the users that perform BTG is that they have urgency to do it. This reason needs to be more detailed. Also, the justification process that happens afterwards needs to complement the reasons given in an efficient and coherent way.

Limitations for this study include the few data that was available as the system had only been in use in a real setting since May 2009 and the fact that genetic reports were only identified from November 2007, when the EMR system has been in use since October 2004. Moreover, the users of the system still need to get familiar with this feature because in the beginning they may think it is an application error that does not let them access what they normally did, and try it several times in a row. Also to take into account is the fact that, at the moment, only medical doctors are using the EMR system. Its use will need to be more scrutinised when other healthcare professionals will start accessing it as well.

Future research to continue the improvement of this BTG system includes a thorough analysis of the justification process, to make sure accountability really works. Another enhancement to this system will be the implementation of the access control model within a more robust access control platform and not only the usage of a database to perform the authentication and authorization process. Further, we want to implement the BTG system into similar domains that require BTG features to conform to legislation, or any other regulations and needs, in order to enhance the process from legislation to practice.

REFERENCES

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

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

Farinha P., Ferreira A., Cruz-Correia R., 2006. Gestão de acessos e recursos para estudos clínicos multicêntricos on-line. *Actas da 1ª Conferência Ibérica de sistemas e Tecnologia de Informação*. 1: 631-640.

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., Cruz-Correia R., Costa-Pereira A., 2004. Securing a Web-based EPR: An approach to secure a centralized EPR within a hospital. *Proceedings of the 6th International Conference on Enterprise Information Systems*. 3: 54-9.

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.

Lei nº 12/2005. Informação genética pessoal de saúde.

Membres CdMaÉ, 1997. *Protection des Données Médicales*. Recommendation n° R (97) 5.

Ministers CoE-Co. 2004. *On the impact of information technologies on health care – the patient and Internet.* Recommendation Rec (2004) 17.

Povey D., 2000. Optimistic security: a new access control paradigm. *Proceedings of the 1999 workshop on New security paradigms*. ACM Press. 40-45.

Rissanen E., Firozabadi S., Sergot M., 2004. Towards a Mechanism for Discretionary Overriding of Access Control. *Proceedings of the 12th International Workshop on Security Protocols, Cambridge.*

Ross-Lee B., Weiser M., 1994. Healthcare Regulation: Past, present and future. *JAOA – Healthcare policy*. 94(1):74-84.

Waegemann C., 2003. EHR vs. CPR vs. EMR. *Healthcare Informatics online*.