# Physician’s awareness of e-prescribing security risks

**Authors Names**: Hugo Rodrigues, Luis Filipe C. Antunes, Cristina Santos, Manuel Eduardo Correia, Tiago Miguel Pinho, Hilário Gil Magalhães
***Author Affiliations****: Faculdade de Ciências da Universidade do Porto, Faculdade de Medicina da Universidade do Porto, Portugal*
***Contact E-mail****: hugoamrodrigues@gmail.com*

## Abstract

*New governmental legislation introduced e-prescription as mandatory in the Portuguese health system. This changes consequences were not properly considered, which caused security problems related to patient and prescriber's data, such as digital identity fraud or access to prescriptions history to build clinical profiles. In order to evaluate the e-prescribing software users awareness to those risks, a survey took place, and the results revealed ignorance of certain obligations and procedures of the e-prescribing process. A significant part of doctors are not conscious about where the patient's data is stored neither about the risks related with prescription’s information.*

## 1. Introduction

Electronic prescribing as become mandatory in Portugal from August 1st, 2011, accordingly with law decree 198/2011 [1] in order to reduce costs and start to dematerialize the prescribing processes. It’s also believed that logging and tracking prescription activities will help in fraud prevention [2].

Public awareness of the potential for violation of personal privacy in clinical information systems is increasing. [3] Besides this aspect, Francis France wrote some articles about this thematic where he considers the Heath care environment physically very open, vulnerable to theft, damage and unauthorized access. [4] Comparing to other kind of data, clinical informations are required to be accessible in any time and it’s storage is also retained for a long time [5].

Portuguese government stimulated software houses to develop software and services that would send data from public and private institutions directly to the Health Services Central Administration (ACSS). Consequently, many software houses developed numerous sets of e-prescribing software and webservices that were submitted for ACSS to approval, resulting in a variety of applications available on the market [6].

From the authors’ point of view: some details are missing from the contracts made by those companies; too much personal information is required from the prescribing physicians; data stored on provider’s servers what can be very dangerous due the data sensibility. Patients’ medications history represents very valuable information for many organizations like insurance companies, banks or laboratories.

This problem has been very discussed by public organisms such as ARS (Regional Health Administrations), Medical Association and social media [7].

The National Health Data Protection (CNPD) support that doctors don’t have enough technological skills to be aware about the consequences of this kind of prescribing that is necessary to inform them. Also advise that the relationship between doctors and patients became weaker due the existence of an intermediary in the prescription process [8].

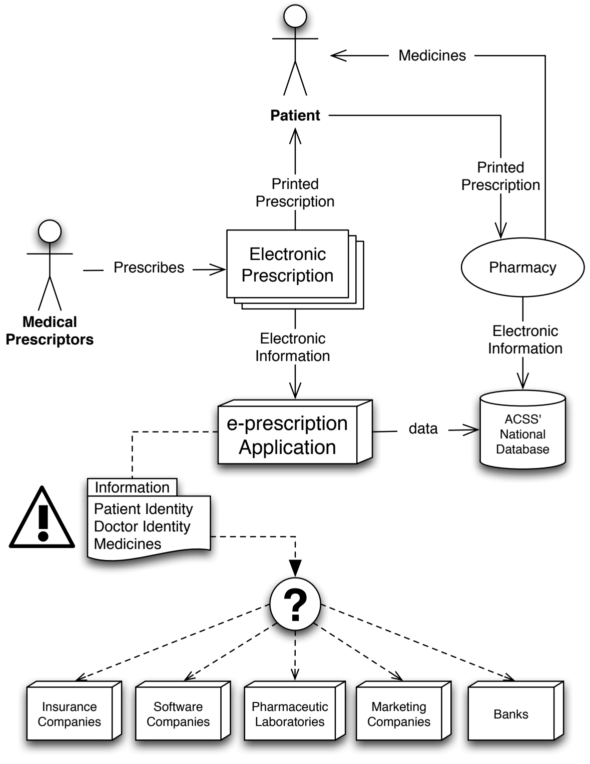

**Figure 1: E-Prescription process and its intervenients with the hypothesis of data leak**

978-1-4799-1053-3/13/$31.00 ©2013 IEEE

Figure 1 represents e-prescribing stakeholders and their roles. Physicians are responsible for prescription filling and delivering to patients in a printed format. At the same time, that information is transmitted to ACSS National Database through the e-prescription application. The patient withdraws the drugs at the pharmacy and is confirmed at ACSS. The prescription's data is valuable for the organizations mentioned before, what turns them stakeholders too.

There isn't enough information about Physician awareness of clinical data security, yet a questionnaire aimed to 66 forensic physicians in United Kingdom expressed the need for information, education and training in data security [9].

For all those reasons, we aim to measure the prescribing systems' responsible of private healthcare institutions awareness about the security levels in the electronic prescription software.

## 2. Definitions

Dale G. O'Brien and William A. Yasnoff, defined the term privacy "as the right of individuals to hold information about themselves in secret, free from the knowledge of others", while their notion of confidentiality bases itself in the presupposition that information about any identifiable individual must never be revealed without the subject's consent, excluding any cases which this act will be allowed by law [10]. The eventual release of information without the person's authorization constitutes an act of privacy invasion. The same authors also describe security "as the mechanisms by which privacy and confidentiality policies are implemented in computer and telecommunication systems." One can deduce that when privacy and confidentiality of information is assured the security is granted [11].

## 3. Methods

A survey took place between 24th January 2012 and 22nd February 2012. A tool was developed to access the Portuguese Health Regulation Authority website and take advantage of their sequential data structure to collect contacts from the responsible of private sector healthcare institutions. The survey is made of 17 questions of closed answers, which 4 of them are for sample characterization endings, supported by the Medquest Platform [12]. From the initial number of 9444, some institutions were excluded for several reasons, as invalid email addresses or not using e-prescribing software. In the remaining 7768 institutions some responsible of private sector healthcare institutions were not physicians, however for this study only physicians' answers were analyzed. Statistics analysis was performed with SPSS software.

## 4. Sample characterization

From the 7768 institutions questioned only 836 (11%) valid answers were obtained. In 674 (81%) the responsible of private sector healthcare was physician.

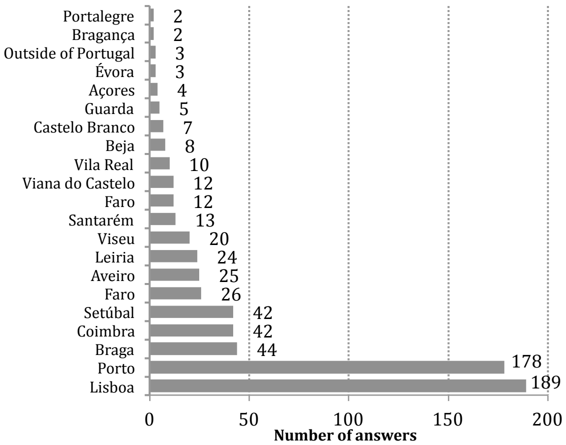

**Figure 2: Geographical sample distribution**

From these 674, 465 (69%) were male, and the average age is 52 years old. The geographical distribution of the respondents is shown on Figure 2, where is notable a high predominance of citizens from Oporto and Lisbon (the largest cities of Portugal).

All the respondents hold a college degree, where 512 are BSc, 94 MSc and the 58 left are PhD.

Table I describe the answers of questions about security and privacy and table II the mean age of respondents per answer of questions about security and privacy. The respondents who are not sure about the answer of questions about security and privacy had more age in average.

**Table I: Results of answers about security and privacy**

| Question | Yes | | No | | Not sure | |
|---|---|---|---|---|---|---|
| | n | (%) | n | (%) | n | (%) |
| Your access credentials are known just for you? | 538 | (80) | 82 | (12) | 54 | (8) |
| Is it possible for an unauthorized third-party to prescribe in your name? | 142 | (21) | 336 | (50) | 196 | (29) |
| You gave too much personal information to conclude the contract with the company for electronic prescribing? | 203 | (30) | 373 | (55) | 98 | (15) |
| The personal information transferred, empowers fraudulent use of your digital identity, if compromised? | 357 | (53) | 139 | (21) | 178 | (26) |
| Do you trust in private companies to store your patient's prescription data? | 348 | (52) | 326 | (48) | — | — |

Most of respondents (n=538) affirm to not share their passwords, however, 232 (43%) of those prescribers (that do not share passwords) don't deny the possibility of somebody to use their identity to prescribe.

**Table II: Mean age and standard deviation (std) per answer about security and privacy**

| Question | Yes | No | Not sure | p |
|---|---|---|---|---|
| | Mean (std) | Mean (std) | Mean (std) | |
| Your access credentials are known just for you? | 52 (12) | 51 (11) | 53 (10) | 0.578 |
| Is it possible for an unauthorized third-party to prescribe in your name? | 51 (11) | 52 (12) | 52 (11) | 0.681 |
| You gave too much personal information to conclude the contract with the company for electronic prescribing? | 50 (11) | 52 (11) | 54 (13) | **0.009** |
| The personal information transferred, empowers fraudulent use of your digital identity, if compromised? | 50 (12) | 53 (12) | 54 (11) | **0.003** |
| Do you trust in private companies to store your patient's prescription data? | 51 (11) | 53 (12) | - - | **0.024** |

Half of the respondents (50%) claim to know that it is the health care professionals duty to notify the patient about this procedure. The other half of the respondents, divide their answers either attributing this responsibility to the companies which developed the software (22%) or to none at all, which means that more than a quarter of the respondents (28%) believe that the patients don´t need to be informed at all. Still related with data protection, 76% of the physicians believe that the company is responsible for inform the CNPD about the use of the prescription software; 18% assumed it was their responsibility and 6% denial this procedure. We tried to analyze the physician's awareness about possible stakeholders of the prescription data (Figure 3), using the mean of answers scaled in a four level scale (from none interest to highly interested).

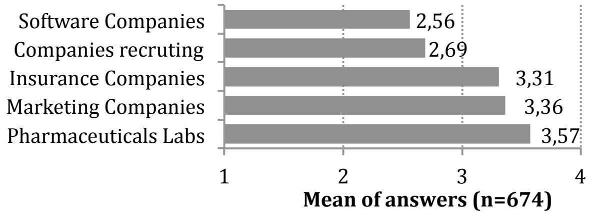

**Figure 3: Mean of answers, about possible interests in prescription data (range 1-4)**

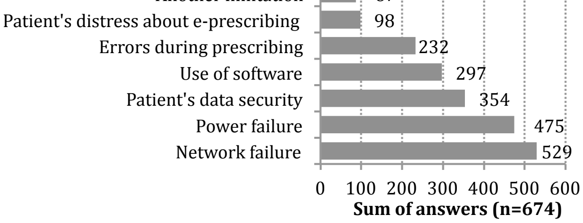

**Figure 4: Sum of answers, about e-prescription disadvantages (multiple answers)**

Multiple questions focused on the electronic prescription disadvantages from the physician's point of view (Figure 4) and the awareness about clinical data location (Figure 5) and were analyzed by summing all the answers in order to detect the more prevalent choices.

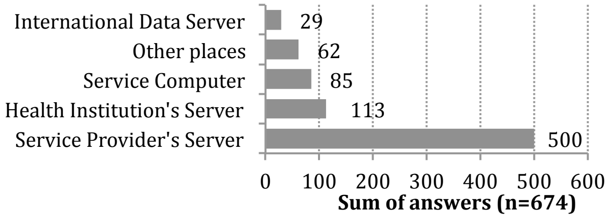

**Figure 5: Sum of answers about location of electronic data's storage (multiple answers)**

## 5. Discussion

Literature highlights the fact of on hospital environment "... passwords and logon sessions and passwords may be shared among providers and because the use of information technology in health care is still relatively new and not yet ubiquitous, there is generally too little awareness of the risks conjured by such actions" [10]. In many cases login information is written and posted on monitors, or they are so simple that they're easily minded. Regarding this point, 20% of respondents admitted to share passwords, or admitted not to be sure about it. This value is high enough to concern because granted access to a health information system by an unauthorized entity risks data privacy, integrity and confidentiality. Even in the respondents who affirm to not share their passwords, almost half don't deny the possibility of somebody to use their identity to prescribe. Others prescribers believe that with a password kept in secret they are safe, what is not necessarily true.

Half of the respondents do not exclude the hypotheses of someone use their digital identity to prescribe in their name and only 48% of the physicians admitted to not trust on private enterprises do store their patient's prescriptions data.

When celebrating a contract between healthcare providers (institutions or singulars) and software houses, lots of information is asked (professional certificate number, belonging order, specialty, etc.). In case of this information being somehow compromised, the risk of digital identity robbery, motivating prescribing fraud is highly increased. Unfortunately, only half of the respondents are conscientious of this possibility (Table I).

The youngest physicians seem more suspicious about the contract's information demand, and the possibility of fraudulent use of digital identity empowering; the youngest also trust more in private companies to store your patient's prescription data.

Another interesting subject to discuss in the matter of electronic prescription methods is the responsibility to inform the patient that his clinical data will be transferred to a remote location through the internet: only 50% of the respondents claim to know that it is the health care professionals duty to notify the patient about this procedure. This value suggests a serious problem in the informed consents with the patients.

The amount of doctors who answer correctly and assumed their responsibility to communicate the use of software or other source of storage of clinical data is very low (18%) and it suggests a stronger intervention in the medical community to spread informations about data security and data protection procedures.

Accordingly with physician's point of view, the Pharmacological Labs are probably the most interested entities about patients prescribing data (Figure 3). With this data, prescribing trends could be close followed by Labs, increasing competition between drugs producers and pressing prescribers to choose a brand over the others. For similar reasons, advertising and marketing enterprises (placed in second) would be able to accurate marketing campaigns targets, if in possession of which drugs each doctor prefers to prescribe. A clinical profile is easily conceived through a prescription history and insurance companies would appreciate to be aware of their customer's clinical profile before selling them insurance.

The question related about the disadvantages of e-prescribing (Figure 4) showed that the situation that would concern most of the physicians was the impossibility of prescribing in case of connection failure, followed by the impossibility of prescribing in case of power failure. Obviously these situations are predicted in law and manual prescribing is allowed in this cases [13]. Security issues were the third concern to the healthcare professionals

One limitation of this study is related with the computerized questionnaire self-administration and the method (e-mail) used to distribute it. Actually, the low survey response rate (11%) obtained can be explained by the methods used to administrate and distribute the questionnaire, and a high response rate would be desired to help to ensure that survey results are representative of the target population.

## 6. Conclusion

Is known that to prescribe electronically is not an option, however, doctors and patients should be enlightened about the invisible part of the process. Since the administered questionnaire was oriented to the physicians who were responsible by an institution's prescription software (and therefore with some base knowledge), it is expected that the results for all doctors would be even worse.

The results showed that the Portuguese medical doctors aren't aware of the totality of risks behind the current electronic prescription's system, which it's a young system and it must grow and get mature.

The best way to improve this situation would be:

- Aware the prescribers of these dangers;
- Ensure they proceed correctly and according the CNPD rules;
- Fix the contracts and certifications to ensure the quality of the services provided in the health system;
- Encrypt the data flux;
- Check the companies and their resources, system and processes before certificate them and organize periodically reviews.

## Acknowledgments

This work is supported by the Master Degree in Medical Informatics of the University of Porto (http://mim.med.up.pt)."

## References

[1] Diário da República, nº 139, 21/07/2011. http://dre.pt/pdf2sdip/2011/07/139000000/3031730317.pdf

[2] Diário da República, nº 96, 18/05/2011. http://dre.pt/pdf1sdip/2011/05/09600/0279202796.pdf

[3] J. W. Bowen, J. C. Klimczak, M. Ruiz, and M. Barnes, "Design of access control methods for protecting the confidentiality of patient information in networked systems," Proc AMIA Annu Fall Symp, pp. 46-50, 1997.

[4] F. H. France and P. N. Gaunt, "The need for security - a clinical view," Int J Biomed Comput, vol. 35 Suppl, pp. 189-94, Feb 1994.

[5] Roger France FH. Gaunt PN, "Control and use of health information: a doctor's perspective", Inf J Biomed Comput, 43 (1996) 19-25.

[6] Software para prescrição electrónica de medicamentos. www.acss.min-saude.pt/Portals/0/Emp_sw_certificado_2012-01-09.pdf

[7] RCMPharma News, 18/01/2012. www.rcmpharma.com/actualidade/politica-de-saude/18-01-12/bastonario-dos-medicos-alerta-para-falta-de-seguranca-da-pres

[8] RCMPharma News, 13/04/2012. www.rcmpharma.com/actualidade/politica-de-saude/13-04-12/receitas-electronicas-nao-garantem-proteccao-dos-dados-dos-ci

[9] I. McLean and C. M. Anderson, "The security of patient identifiable information in doctors' homes" J Clin Forensic Med, vol. 11, pp. 198-201, Aug 2004.

[10] R. C. Barrows, Jr. and P.D. Clayton, "Privacy, confidentiality, and electronic medical records. J Am Med Inform Assoc, 1996. 3(2): p. 139-48.

[11] Science Direct News. www.sciencedirect.com/science/article/pii/S0749379799000240

[12] Medquest Website. http://newdbserver.med.up.pt/projext/medquest/verprod

[13] Diário da República, nº 96, 26/10/1998. http://dre.pt/pdf1sdip/1998/10/247A00/55365546.pdf