A software platform to analyse the ethical issues of electronic patient privacy policy: the S3P example

M A Mizani, N Baykal

J Med Ethics 2007;**33**:695–698. doi: 10.1136/jme.2006.018473

Paper-based privacy policies fail to resolve the new changes posed by electronic healthcare. Protecting patient privacy through electronic systems has become a serious concern and is the subject of several recent studies. The shift towards an electronic privacy policy introduces new ethical challenges that cannot be solved merely by technical measures. Structured Patient Privacy Policy (S3P) is a software tool assuming an automated electronic privacy policy in an electronic healthcare setting. It is designed to simulate different access levels and rights of various professionals involved in healthcare in order to assess the emerging ethical problems. The authors discuss ethical issues concerning electronic patient privacy policies that have become apparent during the development and application of S3P.

provision of services by teams rather than by individual physicians³, compound the problems of enforcing a privacy policy. Even when flawless privacy protection is claimed to be in effect, enforceable, automated policies are still needed to make such protection compatible with the procedural requirements of electronic healthcare. Enforcing privacy policies and relying on machines to control them bring forth new challenges. First, there are inadequate standards in practice to protect patients' privacy. Furthermore, unintentional abuses are possible because of flaws and conflicts in the existing policy and the lack of awareness of privacy issues. Therefore, HCOs should make plans to create standardised, formulated, automated privacy policies in order to minimise the ethical problems due to privacy violations. Enforcing and automating the privacy policy through software tools will enable privacy protection efforts compatible with the procedural needs of electronic healthcare.

The development of information technology has had a significant impact on modern healthcare. Shared care, telemedicine and electronic health records (EHRs) are some of the important changes. However, new methods create new challenges; therefore, health care organisations (HCOs) need to adopt new solutions to overcome the problems posed by the electronic environment. "The emergence and evolution of a new technology gives us a chance to test old tools and, as necessary, to invent new ones in order to get better moral leverage on the problems at hand. Such tools will inform our decisions, guide our actions and prepare us for future challenges".¹

Shifting to electronic healthcare is a complex procedure in HCOs, since there are parties with different interests and moral values, so it is difficult to attain a consensus on the standards for medical practices. Furthermore, security threats can have life-threatening consequences if they target EHRs, for instance by preventing access to vital patient information. In such a realm, measures to manage and mitigate risk become more intricate, because it is impossible to quantitate the risks and the cost of impact in terms of human life.² The need to manage and mitigate the risks to provide a high quality of healthcare requires that HCOs implement various policies, of which electronic privacy policy is the focus of this paper.

A privacy policy is a formal statement describing the legitimate uses and disclosures of health information. It is concerned with protecting patients' privacy and preserving their safety by regulating the actions of the agents of healthcare. New aspects of modern healthcare, such as

Regardless of the progress in electronic healthcare, there is no standard software tool capable of enforcing privacy policies. To fill this gap and to address and resolve the resulting problems, we have developed a computer program called the Structured Patient Privacy Policy (S3P).⁴ This tool is designed to test and compare privacy policies in the electronic healthcare environment. S3P provides authentication, authorisation and auditing services that are the basis for any information security and privacy efforts. During its development and application, we have encountered many ethical challenges. Some of them are inherited by the existing privacy policies and some have emerged during their enforcement.

Here we try to identify and scrutinise ethical issues encountered during the development and application of S3P rather than studying them from a theoretical perspective. We think that this experiential knowledge might be helpful to bridge the theoretical and the practical, thus enabling us to present ethically sound policies as we move from paper-based policies to electronic ones. Although we have come up with some preliminary solutions, solving ethical problems of electronic healthcare and computerised policies is a sophisticated task and needs a collaborative effort by experts from different professional backgrounds, such as physicians, sociologists, ethicists, lawyers and epidemiologists. S3P can serve this purpose by

See end of article for authors' affiliations

Correspondence to: Mehrdad A Mizani, Informatics Institute, MM Building, METU, Inonu Blvd, Ankara, Turkey 06531; mehrdad@ii.metu.edu.tr

Received 14 July 2006
Revised 14 October 2006
Accepted 16 October 2006

Abbreviations: EHR, electronic health record; HCO, health care organisation; S3P, Structured Patient Privacy Policy

providing a software platform for testing various healthcare scenarios and privacy policies.

THE NEED FOR AN ENFORCEABLE ELECTRONIC PATIENT PRIVACY POLICY IN ELECTRONIC HEALTHCARE

Although there are existing policies in HCOs, they are not capable of protecting privacy in electronic healthcare. “Having extensive privacy policies in an enterprise does not directly ensure privacy protection if there are no effective means of consistent policy enforcement across multiple applications and across enterprise boundaries”.³ Enforcement of privacy policy is essential to ensure that personal information is accessed, used and disclosed in accordance with ethical norms, so privacy policies should be represented electronically and be managed through software tools capable of detecting the underlying hidden errors. This approach will enable HCOs to enforce a policy while sharing information with other HCOs. The most important aspects of electronic healthcare relating to privacy policies are summarised here.

Decision-making

In modern, electronic-based HCOs, individuals from diverse professional backgrounds work collaboratively in decision-making processes concerning patients’ health, and patients have the right to influence these processes. Winkler states that an organisation-wide policy that covers all individuals in an HCO and deals with both standard and morally controversial medical practices ensures autonomy, quality, fairness and efficiency of decision-making processes.³ The privacy policies of many developing countries, which mainly assume a traditional physician–patient decision-making approach, fall short of fulfilling such goals.

Shared care

In addition to the collaborative efforts of various individuals in providing healthcare within an HCO, several HCOs may cooperate by sharing parts of the patient information. In this situation, a difference between privacy protection measures in the referring and referred HCOs may endanger patient privacy or safety. A lax privacy policy in the referred HCO can lead to abuses of privacy, whereas an overly restrictive one may lead to denial of access to vital information.

Therefore, checking the adequacy of privacy protection is important for faultless sharing of information between HCOs. An example of such adequacy checking is the Safe Harbor, which assures the adequacy of privacy protection as defined by the European Directive on Data Protection with regard to data shared with nations outside the European Union.⁶

Conflict resolution and ethical checks

Since electronic healthcare introduces changes such as division of labour and more comprehensive health records, electronic privacy policies are more sophisticated than the traditional ones. Consequently, unforeseen conflicts and errors can materialise that are difficult and costly to resolve with the traditional forms of privacy policies. However, an electronic policy can be controlled and revised using sophisticated software to ensure validation and verification of its contents and to make it compatible with ethical values.

Use of the electronic health record

The most significant aspect of electronic healthcare is the EHR that is going to replace paper-based records entirely in HCOs. The EHR contains personal, confidential, vital information, such as information about chronic diseases, drug interactions or HIV status. HCO agents need differing levels of access to the EHR, according to the tasks they have to perform. Lax access

rights can endanger information confidentiality, introduce inconsistencies in the EHR and adversely affect the course of treatment, whereas highly restrictive privacy policies can lead to the denial of access to vital information. An electronic privacy policy can be enforced to adjust the access limits of HCO agents. However, implementation of such a policy will lead to emergence of many ethical issues that need to be considered. S3P provides insight on the problematic nature of the points of connection between ethics and technology.

STRUCTURED PATIENT PRIVACY POLICY (S3P), A SOFTWARE TOOL FOR AN ENFORCEABLE ELECTRONIC PRIVACY POLICY

Structured Patient Privacy Policy (S3P) is a computer program written in JAVA. It is structured using eXtensible Access Control Markup Language (XACML), which is a standard describing both a policy language and an access control decision request/response language.⁷ Basically, S3P is an automated, enforceable electronic replacement of paper-based patient privacy policies. It has authentication, authorisation and auditing services in order to access the EHR. These services are necessary to protect the confidentiality, integrity and accessibility of information and minimise technically oriented privacy violations. However, they are not effective in preventing the violations caused by deficiencies in privacy policies. S3P primarily aims to provide a software platform to define, test and compare privacy policies in order to reveal errors or inefficiencies. It provides flexibility and dynamism, since it enables policy-makers to detect problems and revise policies. S3P can also be used as an educational tool to highlight and assess the privacy issues of electronic healthcare and related ethical challenges. The intended audiences are individuals from different professional backgrounds, especially policy-makers of HCOs, who can use S3P to assess new aspects of privacy policy management in electronic healthcare. To facilitate this assessment, S3P provides means to define paradigmatic healthcare scenarios and test the effect of privacy policies on healthcare processes so the policy-makers can verify that the information is accessible to the right people and spot any defects in privacy policies.

The following is an example of privacy policy definition and testing in S3P.

- **Labelling the EHR:** The policy-maker labels different parts of the EHR according to their sensitivity—for example, the patient’s identity can be labelled as “personal identifiable”, mental health notes can be labelled as “private to physician” and HIV status can be labelled as “highly confidential”.
- **Role definition and assignment:** The policy-maker then defines several roles in healthcare. A role represents a collection of agents, and an agent can be assigned to multiple roles⁸, according to duty and position. Examples of roles are general practitioner, specialist, nurse, hospital administrator and insurance representative. Agents are then assigned to one or more roles—for example, a podiatrist may have a role of “specialist” and “hospital staff” at the same time.
- **Definition of access for the roles in treatment-based uses:** The policy-maker then specifies the parts of the EHR that should be accessible to each role, along with the permissible actions. Examples of possible actions are viewing, changing, removing and printing the contents of the EHR. For instance, a scenario may define that “Medical students do not have access to personal-identifiable parts. Specialists have the right to view private-to-physician parts. Nurses do not have the right to modify the highly confidential parts.” Consequently, an agent who enters the system as a nurse can view confidential information, such as HIV status, but cannot make any changes.

- **Access definition for disclosure:** The EHR should be de-identified for secondary uses such as research. De-identification refers to removing the personal, identifiable parts of the EHR to prevent identification of the patients. Policy-makers should decide on the parts of EHR that should be concealed before disclosure.
- **Testing and comparing the policy:** Testing the policies in S3P and comparing different policies help the policy-makers to spot any unnecessary restrictions or errors.
- **Policy refinement:** After the testing process, policy-makers can make refinements to achieve ethically sound privacy policies.

ETHICAL QUESTIONS FOR DISCUSSION IN STRUCTURING AND COMPUTERISING PRIVACY POLICIES

During the development of S3P, we have been confronted with several ethical dilemmas. Below are some of the themes that we have compiled from our experience with S3P and the questions relating to them. The typology of the questions was inspired by Anderson and Goodman.¹

Restrictions

The main purpose of the access control policy is to limit access to the right people according to the privacy policy and patient consent. Members of each role need to know a minimum subset of the EHR to accomplish their task. Highly restrictive policies are helpful in protecting privacy but may affect patient safety adversely.

- What is the minimum need-to-know information for each role?
- What happens if restrictions imposed by the policy prevent access to vital information?
- What happens if authorised users with sufficient access rights to information are not available during an emergency?
- If it is reasonable to over-ride policy restrictions to provide care, who should initiate such over-rides? Should it be done by staff on duty or by a dedicated, authorised staff in the HCO?
- Should patients be allowed to request customised restrictions on their EHR? For example, should they be allowed to hide their HIV status from medical staff?

Recommendation: The access to vital information can be analysed using the software in order to spot any unnecessary restrictions imposed by the privacy policy.

Shared care and granted access

In electronic healthcare, various HCOs may participate in the treatment of patients by sharing parts of their health information. Additionally, physicians may need to grant access to other physicians for consultation purposes, a feature called “granted access” in S3P.

- What is the minimum necessary information for each case?
- What should be done if the policy of the referred HCO is laxer than the policy consented to by the patient in the referring HCO?
- What should be done if the policy standards used by referring and referred entities are incompatible? What should be done if there is not a ready-to-use interface for checking policy protection?
- Should the HCO delay treatment to inform patients about differences in policies? If sharing is done without informing the patient, who is responsible for possible privacy violations?

- Should authorised physicians be allowed to transfer access rights to other physicians for consultation or collaborative provision of care?
- Should the access rights of the referred individual be less than the rights of referring parties?

Disclosure, de-identification and re-identification

For secondary uses, such as research, disclosed information should be de-identified by removing personal, identifiable parts of the EHR.

- What is the minimum necessary⁹ subset of the EHR for research?
- Removing parts of the EHR may affect the accuracy of research. How do we balance protection of patient privacy by de-identification versus accuracy of research?
- The patient’s residence should be hidden to prevent patient identification. What should be done if the residence information is necessary for epidemiological research?
- When can the EHR be disclosed without informing the patients? Should patients be informed later about such disclosures?
- Is it ethical to disclose patient information for public benefit despite their non-consent, as in cases of domestic violence?
- Should non-consent disclosures be audited?

To prevent the duplication of records and for the accuracy of research, disclosed records should be uniquely identified without making the record owners known to others. Duplications may occur because the patients may have records in several hospitals. Additionally, de-identification should be reversible (a process we call re-identification)—for instance, to inform the patient about a rare disease diagnosed during research.

- What is the impact of duplication on the accuracy of research?
- In what situations should disclosed information be re-identified?

Informed consent

Informed consent is used to inform patients about the uses and disclosures of their records. It also provides the opportunity for patients to specify the privacy protection level by opt-in and opt-out choices applied on policy rules. By opting in, patients can include their records in any information gathering and usage activity, and by opting out, they can exclude their records from such activities.

- Is it ethical to delay patient care if informed consent is not present?
- What happens if the patient-customised consent restricts access to vital information?
- Which option of patient consent is more suitable for electronic healthcare: opt-in, opt-out, or both?

Deficiencies in privacy policy

Policies may contain errors or conflicts that can lead to privacy violations or unavailability of necessary information. Conflicts may arise due to diversity of roles and the membership of individuals in possibly multiple roles.

- Should patients be informed of any abuses encountered in the policy?
- Does informing of deficiencies result in patients’ mistrust in the HCO?

- Who is responsible for privacy protection: policy-makers? applications developers? hospitals?
- How do we balance protection of privacy versus timely availability of information?

Recommendation: Privacy policies can be analysed using the software to reveal conflicts in assigning access rights to different roles.

Unique health identifier

Patient records should be uniquely identified in order to prevent medical errors. Using a social security number as a health identifier is one choice. However, it is subject to abuse and can endanger patient privacy by linking EHRs to other records, such as financial ones.¹⁰

- What is the best choice for a unique health identifier?
- How do we balance ease of use versus privacy protection?

Recommendation: An alternative identifier model is used in S3P to identify disclosed records uniquely and to re-identify them if needed.

Patient empowerment

Patients can have access and control over their health records; this is called "patient empowerment".¹¹

- Which parts of the EHR should be viewed by patients?
- Should patients be allowed to modify their HER, and who is responsible if patient safety is endangered?
- Should changes made by patients be reviewed by HCOs?

Hiding

In Turkey, patients have the right to have a copy of their medical records according to the statute of patient rights¹² (as cited in Aydin, 2004¹³). However, some parts of the EHR, such as mental health information, may be concealed from patients for their own safety.

- Is it ethical to conceal some parts of the health records from patients? Does that guarantee the safety of patients?
- Is it ethical to conceal the condition of patients upon the request of relatives?
- Should patients be given a right to opt out of concealment?

Telemedicine

Telemedicine is the "use of telecommunication technologies to deliver medical information and services to locations at a distance from the care giver or educator".¹⁴ High-speed connections and low-cost storage devices enable the recording of all physician-patient conversations.

- Which conversations should be recorded during the provision of telemedical care?
- Is it ethical to use recorded conversations against the patient in any litigation?
- Does recording physician-patient conversations make patient privacy more vulnerable in telemedicine than in other types of care provision?

Audits

All activities carried out on an EHR can be audited for later quality analyses or for possible litigation.

- How comprehensive should auditing be?
- How long should the audits be stored?
- Should the audits be removed when the patient dies?

- Who should have access to audit trails?

HOW DOES S3P HELP IN SOLVING ETHICAL PROBLEMS OF COMPUTERISED PRIVACY POLICIES?

Only a minority of the problems we have confronted during the development of S3P could be solved technically. Most are due to administrative, organisational and social aspects of privacy policy, eventually leading to complex ethical questions. The routes to solution are complex and require the contributions of experts with various professional backgrounds. S3P provides a means for policy-makers to define healthcare scenarios and apply privacy policies on a sample EHR to assess the effectiveness of existing policies. S3P can also be used to inform experts about ethical problems in healthcare and the new challenges posed by moving towards electronic healthcare and computerised privacy policies.

CONCLUSIONS

Herein we present S3P, a prototype computer program that simulates enforceable electronic privacy policies in an electronic healthcare setting. It is a tool for testing medical scenarios and assessing the effect of computerised privacy policies on healthcare processes. We have observed several ethical challenges during the development and application of the software. S3P can help to highlight these problems and assist policy-makers in fine-tuning and perfecting the patient privacy guidelines in the electronic healthcare setting. This task will lead to design of ethically sound privacy policies appropriate for electronic healthcare.

ACKNOWLEDGEMENTS

Many thanks to Dr Atac Baykal and Dr Arda Arıkan for their helpful comments and generous support in editing the drafts of this paper.

Authors' affiliations

M A Mizani, N Baykal, Informatics Institute, Middle East Technical University, Ankara, Turkey

Competing interests: There are no competing interests related to this paper.

REFERENCES

- 1 Anderson JG, Goodman KW. Ethics and information technology: a case-based approach to a health care system in transition. In: Anderson JG, Goodman KW. *Introduction: case studies in ethics and health informatics*. New York: Springer-Verlag, 2002:1.
- 2 Smith E, Eloff JHP. Security in health-care information systems—current trends. *Int J Med Inform* 1999;**54**:39–54.
- 3 Winkler EC. The ethics of policy writing: how should hospitals deal with moral disagreement about controversial medical practices? *J Med Ethics* 2005;**31**:559–66.
- 4 Mizani MA. *An XACML based framework for Structured Patient Privacy Policy (S3P)* [thesis]. Ankara, Middle East Technical University, 2006.
- 5 Reed A. What privacy? *DigitalIDWorld* 2005:68–70,72.
- 6 *Safe Harbor*. Washington, DC: US Department of Commerce, Introduction, <http://www.export.gov/safeHarbor/index.html> (accessed 13 Sep 2007).
- 7 Sun's XACML implementation, programmer's guide for version 1.2. sunxacml.sourceforge.net/guide.html (accessed 13 Sep 2007).
- 8 Ferraiolo DF, Kuhn DR, Chandramouli R. Role based access control. In: *Core RBAC features*. Boston: Artech House, 2003:53.
- 9 **HIPAA—Minimum necessary**. Oregon Association of Hospitals and Health Systems. http://www.oahhs.org/issues/legal/minimum_necessary.php (accessed 20 Sep 2007).
- 10 **HIPAA FAQ: unique identifiers**. HIPAAAction. http://www.hipaadvisory.com/action/faqs/FAQ_Identifier.htm (accessed 13 Sep 2007).
- 11 Munir S, Boaden R. Patient empowerment and the electronic health record. *Medinfo* 2001;**10**:663–5.
- 12 **Hasta haklari yonetmeliği**. [Statute on patient rights] *Official Gazette* 1 August 1998 (no23420) *Hasta haklari yonetmeliği*. http://www.tbmm.gov.tr/komisyon/insanhak/orta/um_hastahaklari.pdf (accessed 20 Sep 2007).
- 13 Aydin E. Rights of patients in developing countries: the case of Turkey. *J Med Ethics* 2004;**30**:555–7.
- 14 **Nutrition education for the public**. Discussion papers of the FAO Expert Consultation (Rome, Italy, 18–22 September 1995)—FAO Food and Nutrition Paper 62. Glossary. <http://www.fao.org/docrep/W3733E/w3733e08.htm> (accessed 13 Sep 2007).