Privacy Management in Consumer e-Health

Arnab Chowdhury, Pradeep Ray
School of Information Systems Technology and Management
University of New South Wales
Sydney, Australia
arnab.chowdhury@student.unsw.edu.au
p.ray@unsw.edu.au

***Abstract*—Healthcare organizations are moving towards more diversified channels to provide the healthcare services. The increasing dependency on the Internet to provide the healthcare services opens up a whole gamut of privacy concerns of consumers and providers. The misuse of personally identifiable information could drag the patient to vulnerability, humiliation, discrimination, economic hardship. There is a need for tools to improve transparency and awareness of information security practices in the context of Internet based consumer e-Health systems. This paper presents a cooperative management methodology for the development of Privacy solutions for consumer e-Health.**

Keywords-Privacy, privacy policies, policy enforcement, CoMENS, security, social and legal issues, P3P, policy enforcement, eHealth.

I. INTRODUCTION

E-Health involves all aspects of healthcare supported by the web based Internet technologies that have now pervaded all sectors of the business and services including healthcare. The future success of e-Health is likely to depend on how ordinary citizens can access their health and obtain health-related information over the web in a secure manner. However, these sites also require to store and share substantial amount of consumer personal information, ostensibly for "research" purposes or to deliver health services. The question of informed consent and privacy are some of the primary needs of the consumers and it is hard for consumers to trust the web site with so much of personal (often sensitive) information. That's why the electronic health care websites of the future need to satisfy consumers on how the privacy of their personal information will be protected.

Generally privacy points to the tools used for controlling disclosure based on techniques, such as cryptography. On the other hand information privacy tools could be also seen as means of improving transparency and awareness of information security practices. In this paper we refer to privacy according to the later definition. The term transparency is used widely to mean that public oversight bodies are informed on the practice of the organisation or website. But, if such privacy platform is implemented over the internet it would serve three purposes. Firstly, it would provide notice to the user and create awareness. Secondly, it would provide information to the externally controlling bodies and thirdly, internal department would develop greater awareness of how much information is disclosed to the other business partner. So, the awareness of risk and transparency is as important as other information security measures. [1]

If the privacy awareness in mapped to the consumer heath arena which is mostly internet dependent the problem could be delineated from the consumers or patients point of view. [2] The personal medical information that the patient provides could potentially reveal information which may make the patient vulnerable to humiliation, discrimination and economic hardships. It could also cause a loss of a job or insurance coverage, and other emotional and physical harms.

Since healthcare services involve the cooperation of a number of groups of people and organisations (e.g., hospitals, clinics, pathologists, radiologists etc.), any methodology for privacy management must support cooperation within and across organizations – hence we call it "cooperative management". The paper starts with a brief description of a cooperative management methodology for privacy which is followed by an illustration of the methodology in the consumer e-Health problem. The following sections present the different stages of this methodology leading to the development of architectural framework for privacy management solutions in consumer e-Health. This methodology is based on Ray's Cooperative management Methodology for Enterprise Networks and Services (CoMENS). [3].

II. RELATED WORK

The health industry tries to assure that the easy access to medical information is not hampered so that efficient service to the patients assured and to minimize the intricacy of getting patient consent on the flip side legislation allows patients to impose penalties if and when unauthorized disclosures occur.

There are international legislative and technological bodies already have been working in this area. World Wide Web Consortium (W3C) has a recommendation of Platform for

1-4244-0942-X/07/$25.00 ©2007 IEEE.

Privacy Protection (P3P) which notifies and publicizes the websites policy in the machine readable format, in the form of a Protocol and XML schema. And to the user side, user sets his privacy preferences in the Agent that is used in tandem with the browser and while the user visits a website the agent matches the website's security policy with the users own privacy preference. [4] Enterprise Privacy Authorization Language(EPAL) a formal language developed by for writing enterprise privacy policies to govern data handling practices in IT systems according to fine-grained positive and negative authorization rights. [5]. XACML (eXtensible Access Control Markup Language) , a standard ratified by OASIS , is a general purpose access control policy language which is defined using XML. [24]

The legislation and standards like the HHS security rule, Health Insurance Portability and Accountability Act (HIPAA) has clauses to recommendation for implementation of machine readable privacy policies that such policies should be embodied with the websites that deal with health information. Also, the fair information practice principal specified in Health Insurance The Health Insurance Portability and Accountability Act (HIPAA) of 1996, Children's Online privacy Protection Act (COPPA), AS/NZS 7799.2, National Privacy Principles of Australia (NPP), The E-Government Act of 2002 requires that user must be provided with notice and awareness, given choice and consent, allowed access and participation, have information security and integrity, enforcement of security. [6][7][8][9][18]

III. Co-operative Methodology for Privacy Management

In this paper we use CSCW techniques, analysis and practical scenario based on concepts, such as roles, interactions, artifacts, and tools in a real application environment. [10]. The Cooperative management Methodology for Enterprise Network (CoMEN) has been used in the development of privacy management solution.[11] The CoMENS methodology is adopted of due to the analogous nature of Privacy Management Problem with Network Management Problem. CoMENS has two parts.

Scenario Analysis: Provides a method for the definition and analysis of scenarios of a cooperative management environment. This level includes requirement study and analysis and is based on soft system methodology.[3]

System Design: This part is based on a design formalism of distributed systems, CSCW and network management. This level includes design implementation and evaluation of cooperative application design. [3].

The following subsections illustrate the use of CoMENS for the development of a cooperative management solution for privacy in consumer e-Health.

IV. Privacy Requirement Analysis

For the purpose of developing the privacy solution the following steps could be identified. As the main threat underlies in the Consumer Health sector is, Information being misused without the owner's specific consent or knowledge.

For the above privacy thereat the following risks could be identified that could be considered to be mitigated,

1. Non-compliance with the Industry best practices from the information owner and information receiver.

2. Deviation in service quality standard – on e-service issues proper privacy policy should be there in compliance with the legislation, ethics and standards, deviation from which would mean that the breach of legal agreement and dispute must be resolved to cover losses due to this. When the service provider fails to meet the privacy policy statement the provider may accrue fine to cover the losses incurred by the client.

3. Usually, the privacy clauses may not be properly understood by the user or user may agree without reading too technically written privacy policy.

If we interpret this abstract business requirement to technical requirement which could be interpreted as the user's private information should be safeguarded based on,

Choices—options users should have on using their voluntary and mandatory collected data (opt-in or opt-out)

Access—Disclosure of who has access to data and if users to the website can access or correct their own data

Usage—for what business purpose collected data is used and disclosed

Sharing—with whom data is shared and why and whether sharing is optional.

Expiration—how long information is retained. [12]

The widely adopted and discussed mitigation technique for privacy threat is Machine readable Policy, According to HHS, Public citizens, private sector, and public sector organizations interacting with HHS must be informed of website privacy practices on the following. While clients understand his acceptable preference for disclosing privacy preference it could allow a software agent to go through the privacy policy of the website and accept or reject according to the user's privacy preferences. [13]

A. Scenario Analysis

Scenario Analysis is an important technique in the analysis of CSCW application. We have looked in the privacy in Consumer health sector from a more social perspective. Existing privacy management platforms does not unequivocally safeguards security of PII (Personally Identifiable Information). The issues on the existing practices could be isolated based on the analysis. And a model could be

developed that would verify, validate and enforce the privacy policies publicized by the website.

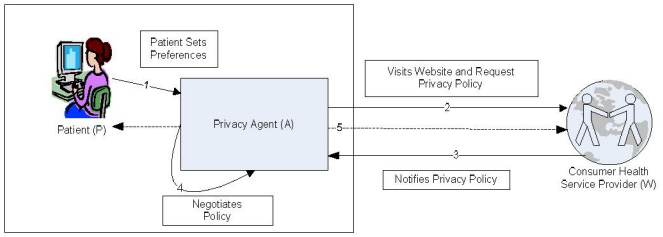

Figure 1. Interaction Scenario

The above figures the typical process scenario of Privacy management when a patient visits a consumer health site for services. The Interactions in the above numbered interactions in the diagram could be described as follows,

Patient (P) is the user interacting with the e-health service providing website.

Privacy Agent (A) is the software agent that interprets user's privacy preferences.

Consumer Health Service Provider (W) provides the health services in the Internet.

Group Interaction and communication Mechanism

1. Patient sets privacy preferences. (Role P → Role A)
2. *When user visits the health service providers website, agent requests providers privacy policy. (Role A → Role W)
3. *Website notifies the machine readable privacy policy to the Agent. (Role W → Role A)
4. Agent negotiates privacy policy with the user's preferences and if unsuccessful notifies user of the potential risk of sharing PII. (Role A→ Role A)
5. User exchanges data to the website. (Role P → Role W)

As explained in the above diagram, the P3P agent informs or alerts the user to takes a decision based on the preferences set by the user, on what and how information would be exchanged with the website. Thus the user or the P3P agent negotiates with the website according to the notice advertised by the website. The steps in the scenario highlighted with '*' identifies the privacy gaps in interactions which could be further improved. To expand the scenario further, the service provider further shares the information with other specialized organization or business partners for example insurance agency and pharmaceutical company.

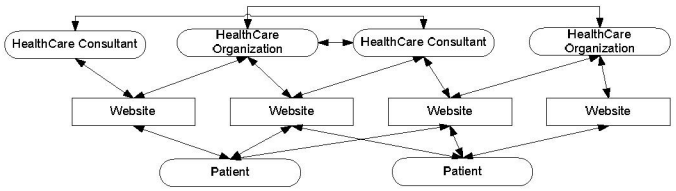

Figure 2. world web information Exchange

If we compare conventional healthcare scenario with E-healthcare, in E-Health care scenario, the same exchange of information takes place on the internet but, an extra layer is added in the middle which is the website. Our research comes into relevance while defining the privacy practices of the websites bound by the legalities and technologies. As described in figure 2, the patient and the healthcare service provider interact with the website for their specialized requirement. Each Website is represented by a specific service provider or its competitor for e.g., a pharmaceutical website, Diabetic management website, Medical Insurance management website.

Issues that became evident as the result of analysis,

1. There will be no assurance to users that the web sites will follow published policies: If the websites do not follow the web based privacy policies the step for implementing privacy policy would be refuted and would further complicate the users trust on disclosing privacy information.

2. No valid independent audit of sites privacy practices: No valid standard independent audit is available for web sites privacy practices.

3. No strong legislation, requiring adherence to standard privacy practices on the collection, processing, access to and sharing/disclosure of personal identifiable information. : If strong privacy legislation is not present, health care consumers on the Internet will not totally trust Web as a secure medium for disclosing personally Identifiable Information. [12]

B. System Design

The idea of improving trust on the web could be achieved by following the real life social phenomena of trust. [17] As it is commonly observed in most general business scenario, the authenticity of the interacting partner is validated or verified with a trusted third party or a reference, which greatly improves the trust relationship between the interacting parties [14].

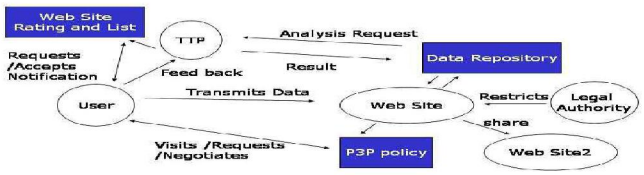

Figure 3. Role Interaction Diagram

In the above scenario described in Figure 3, an analysis of role interaction [15] executed. The roles are User or agent, Website representing Health care service provider, Website2 representing partner website for Healthcare service provider, Legal Authority, Trusted Third party. Artefacts are, P3P Policy, Data held in the website, Website rating.

User agent negotiates with the Website on sharing PII (Personally Identifiable Information) based on the P3P policy sent by the Website. In the P3P policy, the interacting website takes up the responsibility of the privacy practice of website2 with whom information is shared for providing services. And, Healthcare Service provider and websites remains transparent to Legal authority by disclosing information handling practice.

Website maintains a log, history and checkpoints based on the rules notified in the privacy policy. A software policy enforcement agent would generate messages to notify incident on identified anomalies.

Trusted third party is a commonly accepted authority by the users and the healthcare service provider, which maintains a privacy rating list on different websites privacy practices. The user agent on behalf of the user would have the capability to generate a request to the trusted third party on the privacy practice of the website and alert the user while negotiating with the website.

The architecture is user focused as it provides the user control over his PII. It provides additional functions to the P3P agent to accommodate more intelligent decision. The adoption of data repository or privacy logs assures accountability by keeping records of the negotiation of contracts and keeping audit trail on the usage of private data.

C. *Validation of the Design*

The following discussion validates our design using role-interaction modelling, a technique used earlier for understanding gaps in the cooperation of roles in a sample privacy management scenario.

1) *Roles and Tasks*

User, U: Patient or entity requiring disclosing information.

Privacy Agent, A: Software Agent acts on behalf of User based on the privacy preferences set by the user. It parses the XML based P3P policy which is an enhancement to the existing available P3P agents with additional functionality to communicate with the Trusted Third Party.

Web Site along with Web Application and Databases, W: Receiver of user information logs and provides the user a requested service.

Independent Trusted Third Party and Automatic Privacy Rating System, I: Independent software management system that would reside with on the commonly accepted body on the Internet. Have an independent database of related P3P enabled healthcare websites and Privacy Practice rating.

Privacy Enforcement Agent, EA: A proactive agent which will be residing in W and produce and communicate the policy enforcement with the state and practice with I. This could be automated or have a questionnaire based system and would require periodical inputs from the privacy designated enforcers of the website.

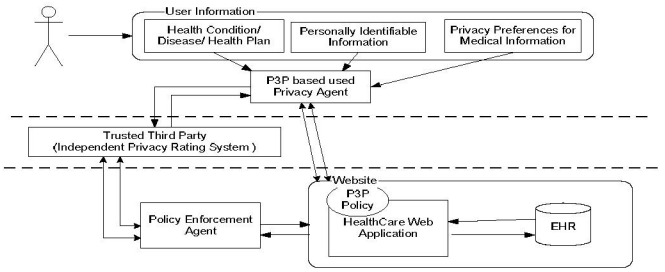

Figure 4. Diagram for enforcement of User Privacy

2) *Role Interaction*

1. U → A, User sets the privacy preferences based on the particular consumer healthcare sector.

2. A→ W, 'A' requests P3P Based policy, Negotiate the P3P privacy policy with its own set of privacy preferences and accept or reject information disclosure requirement.

3. A→I, The user may opt in to pre check with the Privacy practice of W with C and request a trust assurance.

4. I→A Provide a Privacy practice rating (i.e. 'I' may caution 'A' if 'W' is Black Listed)

5. EA→I, Validate the Policy enforcement and 'I' collects messages from EA and update the database for privacy rating of the Website.

6. EA→W, Collect enforcement status from the Web Site. [22]

The initial prototype development is undertaken based on the use of P3P, implementation of Web Services and development of application on Microsoft Platform. XACML is undertaken for lower level policy enforcement based on the policy expressed in P3P. Trusted Third Party has a log of violation which is rated again based on a set of rules and the violation is communicated to User agent accordingly. The implementation and evaluation of the prototype is not discussed due to the space constraint. Also, from the CoMENS point of view, the group communication scenario is not relevant in this particular scenario as all the interaction takes place over the internet.

V. CONCLUSION

eHealth (Healthcare service over the internet) is seen as a potential strategy to reach patients in remote areas where patients have inadequate access to specialists. But, as the spectrum of e-health services over the internet grows the

concern of privacy would grow proportionately, especially in the context of diagnosis over the Internet. Standards, such as W3C's P3P allows users to have some control over privacy policies with respect to web based services. However, these measures only provide user control over stated privacy policies at web sites. They do not provide any means for privacy enforcement. Such a solution would require the cooperation of a number of human and organisation roles in the context of an e-Health service.

This paper has proposed a cooperative management methodology for the development of privacy management. The methodology (CoMENS) involves the analysis of a typical consumer health privacy management scenario using role-interaction modelling that shows the gaps in cooperation support in web-based privacy management for e-Health. This is followed by the design of a cooperative privacy management solution. Finally, the design is validated with respect to the same privacy management scenario that was analysed earlier. This methodology provides an approach to the development of consumer e-healthcare security and privacy solutions in the context of future web-based electronic policies and their compliance.

REFERENCES

[1] Annie I. Antón, Privacy Matters, National Science Foundation CISE Distinguished Lecture Series, Washington, DC, North Carolina State University, 2 Mar 2005, Available online at <http://www.theprivacyplace.org/presentations/nsfCISE_dls_aia_mar05.pdf>

[2] Wimalasiri, Jaminda S; Ray, Pradeep; Wilson, C. S.(2005), Security of Electronic Health Records Based on Web Services, Proceedings of the IEEE HealthCom2005.

[3] P. Ray, "Cooperative management of enterprise Network", Kluwer Academic/Plenum Publishers, New York, 2000, ISBN 0-306-46276-1

[4] Platform for Privacy Preferences (P3P) Project, Copyright 1994-2003 W3C (MIT, ERCIM, Keio), Available online at <http://www.w3.org/P3P/>

[5] EPAL : Ashley P; Hada, S; Karjoth, G; Powers, C and Schunter, M; "Enterprise Privacy Authorization Language (EPAL)", available online at <http://domino.watson.ibm.com/library/cyberdig.nsf/papers/8342B6EDF4D8C09485256CDF0050482C/$File/rz3485.pdf>

[6] AS/NZS 17799:2001 Information Technology - Code of practice for information security management

[7] AS/NZS 7799.2:2003 Information security management - Specification for information security management systems

[8] Health Information Security Management Implementation Guide to AS/NZS 7799.2, Deloitte Touche Tohmatsu

[9] The Office of Federal Privacy Commissioner, Available online at <http://www.privacy.gov.au/publications/npps01.html>

[10] Hawryszkiewycz, I; "A Generalized Model for CSCW systems", Proceedings of 5th International Conference on Database and Expert Systems, Athens 1994

[11] P. Ray, G Weerakkody, Case Study: CSCW based systems Development Methodology for Health-Care Information Systems , 2003

[12] Mills, Darrell M.(2002); P3P –A Case of Privacy Smoke and Mirrors, March 31, 2002, GSEC Version 1.3, © SANS Institute 2000 – 2002, available online at: <http://www.giac.org/certified_professionals/practicals/gsec/1858.php>

[13] Secure One HHS:Machine-Readable Privacy Policy Guide, 6 Apr 2005, US Department of Health and Human Services, page 3-8, Available online at:<csrc.nist.gov/fasp/FASPDocs/program-mgmt/050425-Machine_Readable_Priv_Policy_Guide_FINAL.doc

[14] Chowdhury A, Ray P, "A Model for the Enforcement of Privacy Protection in Consumer Healthcare, Smart Homes and Beyond, ICOST 2006: 4th International Conference on Smart Homes and Health Telematics, IOS Press, Netherlands, 2006, ISBN 1-58603-623-8

[15] Ray, Pradeep Kumar, Integrated Management from E-Business Perspective: Concepts, Architectures, Methodologies, Kluwer Academic/Plenum Publishers, New York, 2003, ISBN 0-306-47485-9

[16] Linn, John(2005); Technology and Web User Data Privacy-A Survey of Risks and Countermeasures, IEEE SECURITY & PRIVACY, JANUARY/FEBRUARY 2005, Available online at : <http://ieeexplore.ieee.org >

[17] Jutla, Dawn; Bodorik, P(2005), Sociotechnical Architecture for Online Privacy, IEEE SECURITY & PRIVACY, MARCH/APRIL 2005, Available online at < http://ieeexplore.ieee.org >

[18] Hirsch, Reece (2003); The HIPAA Security Rule, Healthcare Informatics, April 2003, Available online at <http://www.healthcare-informatics.com/issues/2003/04_03/hipaa.htm>

[19] Teltzrow, Maximilian; Preibusch, Sören; Berendt, Bettina (2004) ; SIMT - A Privacy Preserving Web Metrics Tool, Proceedings of the IEEE International Conference on E-Commerce Technology, © 2004 IEEE, Available online at <http://ieeexplore.ieee.org >

[20] Antón, Annie I.; Earp, Julia B.; Reese, Angela (2002); Analyzing Website Privacy Requirements Using a Privacy Goal Taxonomy, Proceedings of the IEEE Joint International Conference on Requirements Engineering, © 2002 IEEE, Available online at <http://ieeexplore.ieee.org >

[21] Karjoth, G¨unter; Schunter, Matthias; Herreweghen , Els Van, Waidner, Michael (2003); Amending P3P for Clearer Privacy Promises, IBM Research Zurich Research Laboratory, Proceedings of the 14th International Workshop on Database and Expert Systems Applications, © 2003 IEEE, Available online at <http://ieeexplore.ieee.org >

[22] First Gov for Consumer, Last Updated: Thursday, December 15, 2005, Available online at <http://www.consumer.gov/health.htm>

[23] United States Department of Health and Human Service, AHRQ Agency for health case research and quality, <http://www.ahrq.gov/consumer/>

[24] Lorch Markus; Proctor Seth, Lepro Rebekah, Kafura Dennis, Shah Sumit (2003), First Experience Using XACML for Access Control in Distributed Systems, ACM workshop on XML Security, October 31, 2003, Fairfax, VA, USA, Copyright © Sun Microsystems inc and Association for Computing Machinary 2003.