Proposed Privacy Patterns for Privacy Preserving Healthcare Systems in Accord with Nova Scotia's Personal Health Information Act

Maha Aljohani[1(✉)], Kirstie Hawkey[1], and James Blustein[1,2]

[1] Faculty of Computer Science, Dalhousie University, Halifax, Canada
mh578194@dal.ca, {hawkey,jamie}@cs.dal.ca
[2] School of Information Management, Dalhousie University, Halifax, Canada

Abstract. We propose privacy design patterns in the context of healthcare systems. These patterns are designed to support the Privacy-By-Design concept through the software lifecycle, focusing on the early design phase and mitigating privacy risks. As a departure point, we used Personal Health Information Act (PHIA) in Nova Scotia to derive the following five proposed privacy patterns: 1-request an access 2-request a correction 3-request not to disclose Personal Health Information 4-being notified if the PHI is lost, stolen or subject to unauthorized access 5-request a review. The patterns provide a guide to designers and developers in designing privacy-preserving systems in healthcare.

Keywords: Privacy patterns · Personal Health Information Act (PHIA) · Privacy-by-Design · Privacy Enhancing Technologies (PETs) · Personal information · ISO 29100 · Privacy-by-Policy

1 Introduction

In 2013, Nova Scotia's Personal Health Information Act (PHIA) came into effect to cover additional rules on top of the Personal Information Protection and Electronic Documents Act (PIPEDA) [1].

Laws and regulations alone do not prevent individuals from giving personal information nor prevent anyone from gaining access to someone else's personal information without permission. Privacy patterns are privacy design guidelines that can be used early in design lifecycles. The concept of Privacy-By-Design (PbD) is essential because it integrates concern for privacy from the first design steps and maintains such care throughout the design lifecycle [2]. Therefore, design privacy patterns are proposed to protect personal information by design and default. Proposing privacy patterns is motivated by the need to bridge the gap between laws and application. At the same time, another motivation is to maintain levels of privacy as hard copies are transferred into digital artefacts requires PbD.

Our overall objective is to provide Information Technology (IT) designers and developers a solid framework of privacy patterns that covers the privacy rights according to Personal Health Information Act (PHIA). A secondary goal is to validate the proposed

T. Tryfonas (Ed.): HAS 2016, LNCS 9750, pp. 91–102, 2016.
DOI: 10.1007/978-3-319-39381-0_9

patterns by comparing them to the principles of ISO29100 Privacy Framework and to identify the properties that are guaranteed when the system design follows the patterns. The proposed patterns will be used as an input to the prototype of a privacy portal to Electronic Health Records (EHRs) as future work.

2 Background and Related Work

In human-computer interaction, privacy is defined as the right of individuals to have control over the personal data shared online [3, 4]. Researchers have been studying privacy from different perspectives including privacy-preserving technologies, organizational approaches to serve the ultimate goal, which manages and protects personal information [5]. Privacy engineering can be defined as the effort made to design models, tools, methodologies and technologies embedded in system designs where they guarantee privacy protection depending on applicable laws [6]. The Freedom of Information and Protection of Privacy Act (1990) defines personal information as any recorded information that defines an individual when is disclosed [7].

2.1 Privacy-by-Design and Privacy Enhancing Technologies (PETs)

The International Privacy Commissioners and Data Protection Authorities, Ontario, Canada approved the Privacy-By-Design concept in October 2010 as an "essential component of fundamental privacy protection" [2, 8]. To support the concept of PbD, the proposed privacy patterns should help designers and developers to integrate privacy from the design phase and throughout the development cycle.

Borking [11] defined a PET as a "system of ICT [Information and Communication Technology] measures protecting informational privacy by eliminating or minimizing personal data thereby preventing unnecessary or unwanted processing of personal data, without the loss of the functionality of the information system." The European Commission adopted the same definition in 2007.

New privacy enhancing technologies are introduced to protect the privacy of users and at the same time allow them to share and communicate electronically, e.g. using the Internet. Examples of PETs are: (1) anonymizers[1] (which remove all personal information to preserve users' privacy thus providing users with the ability to browse the Internet without their identity being disclosed [12]); (2) Crowds (which aggregate users into diverse groups to hide personal information [13]). (3) Platform for Privacy Preferences (P3P) (which was designed in a way that helps users understand how their personal information is used by websites; it compares a website privacy policy and a user's privacy policy [14]). Other examples of PETs are 'cut-and-choose' techniques [15], 'onion routing' [16], and Privacy Incorporated Software Agent (PISA)[2].

[1] https://www.anonymizer.com.
[2] http://www.tno.nl/instit/fel/pisa.

2.2 Privacy Patterns

PETs are not the same as privacy patterns. PETs solve only one specific privacy problem in already implemented software such as TOR, that applies Onion Routing protocol, which uses many routers to encrypt the requests and process it in many layers, while privacy patterns are considered to be design frameworks and guidelines that can be used in similar contexts [9, 27]. Privacy patterns are structured to state a problem and propose solutions followed by known uses and related or similar patterns. Examples of already existing patterns are described in the sections that follow:

2.2.1 Informed Consent

Informed Consent for Web-Based Transaction Pattern was developed by Romanosky et al. [10]. When collecting personal information, websites often employ so-called cookies. Users are concerned that their personal information would be collected and used without their consent or not want to share their personal information. The problem rests on how designers can have a balance between the reasons for using the PHI and the users' concerns about how their PHI is used. To solve the problem, the web designer has to provide the user with the following elements: disclosure, agreement, comprehension, voluntariness, competence, and minimal distraction.

The pattern has been used in many well-known websites, such as Yahoo!, Google and ehealthinsurance.com during the filling of the registration form. Similar patterns include: informed consent [17, 18], need-to-know [18] and obtaining explicit consent pattern by Porekar et al. [19].

2.2.2 Minimization

A masked online traffic pattern by Romanosky et al. [10] focuses on solving the problem of minimizing the amount of personal information shared over a public network. The pattern uses the following techniques:

- Anonymity Techniques–to help the user to communicate but still be unidentified. Two types of systems can be used: Anonymizing systems, which help users to be completely anonymized to parties, and pseudonymous systems, which help users to not be identified as individuals
- Blocked Requests-to use software tools that block cookies and web bugs that are used to track users

The pattern is used by PET applications to insure anonymity such as Anonymizer (www.anonymizer.com) and Privoxy (www.privoxy.com). Related pattern is minimal Information Asymmetry by Romanosky et al. [10].

2.2.3 Access Data

Porekar et al. [19] designed the Access Control to Sensitive Data Based on Purpose to solve the problem of allowing individuals to be informed of the purpose of collecting

information. The user should have the ability to decide which aspect or piece of information a third party should be allowed to have access to. The pattern applies the *Need-to-know*[3] mechanism to limit the amount of sensitive information transmitted to third parties. The pattern provides access to only what the user give permission to be accessed. P3P is well-known use of the pattern [14].

2.2.4 Feedback

Ambient notice by [21] solves the problem when the users' location information is used as a repeated model dialog with or without the users' permission. How can users get notice about every time a service is pulling location information? An ambient notice that appears instantly when location information is retrieved.is considered to be the solution. The notice should provide an opportunity for interaction in terms of permissions. Known uses of the pattern is the location-based service icons used in Mac OS/X where is it shown as a compass arrow that appears in the taskbar every time a software program is used identify the user's location.

Other patterns include outsourcing and non-repudiation by [18], data abstraction by [20] privacy dashboards, private link by [21], and instant user interface for information about personal identification information by [20].

3 Methodology Model

Nova Scotia's Personal Health Information Act (PHIA) was used as a departure point. This is to minimize the gap between the provincial laws and to modalize the laws as there is a gap between laws and technology. We believe this is going to provide more practical and easier understanding of privacy requirements in the very early design stages at a higher level of abstraction.

The process of deriving the proposed privacy patterns relied on both the currently available patterns and the investigation of the legal framework of PHIA to cover individuals' rights. Then, the proposed patterns were analyzed against the principles of ISO29100 Privacy Framework and to be used as design guidelines in the prototype of a privacy web-based EHRs portal.

We believe that the proposed patterns cover all aspects of the PHIA and provide a useful guide that should be implemented by any healthcare privacy-preserving system in Nova Scotia even before the design phase and throughout the design lifecycle. The rights according to PHIA are as follows: request an access, request a correction, request not to disclose Personal Health Information (PHI), being notified if the PHI is lost, stolen or subject to unauthorized access, request a review of company's decision for access or correction and make a complaint if the custodian did not follow the rules of PHIA. The design of the privacy patterns was implemented in the following sequence; designing one privacy pattern for each right; designing privacy patterns for rights that do not have matching or somehow matching patterns; discussing each pattern by explaining the context, problem, proposed solution, and related patterns.

[3] Provide users with feedback on collected information [18].

The template we followed in forming the proposed privacy patterns was derived from the Pattern-Oriented Software Architecture (POSA2) outline as a simplified version, which was developed by Bushman et al. [25]. In the following patterns, the term individual refers to the person whose personal health information is the subject of interest, and the term user refers to the professionals who gain access to that information.

4 Results and Discussion

Five privacy patterns are proposed to cover the individuals' rights based on PHIA. Keywords used in the description include: *Custodians:* Health care professionals, Eastern Health, Western Health, Central Health and Labrador-Grenfell Health, Provincial government departments when engaged in health care activities, the Public Health Laboratory, the Newfoundland and Labrador Centre for Health Information, and the Workplace Health and Safety Compensation Commission [22] *Data Subject:* Individuals, *Data Controller/Processor:* Organizations, their agents or both, *Data holder*: Organizations or a third party. The proposed patterns are as following:

4.1 Request an Access

The right assures individuals that they can view or receive a copy of their personal health information and some fees might be applied depending on the organization [1]. The Proposed Privacy Pattern is shown in Fig. 1.

Context: Personal Health Information, according to PHIA, offers individuals the access to information about them that is held by health sector organizations and providers.

Problem: Individuals want to use private healthcare systems that help them access their personal health information. Every individual has the right to have a level of control over the information by gaining access to the information and perform some tasks such as receiving or downloading a copy. Individuals have the right of access to the privacy policy of the organization or the third party that hosts the information.

Factors: Data Subject (DS) and Data Controller (DC).

Solution: To design an efficient privacy pattern, we need to provide transparency where DS can access the PHI. PHI is stored within organizations or on external servers. Users will be able to access the PHI and before that, they need to agree on what is saved on these servers according to their rights provided by the PHIA. As soon as they request access to the information, they need to deal with the consent once and another time after viewing the information to confirm that the information is up-to-date and/or correct. Viewing or delivering a copy of PHI should be limited to what the organization can view or deliver to DS based on the time the data was collected.

Agreement: The user must obtain consent in three situations: for access to the individual's sensitive information (PHI) regardless of where the information is stored; when the individual is being asked to agree to the initial or updated privacy policy of third parties who may host the information; and individuals have to agree on the information

stored once individuals gain access. The individual whose PHI is the subject of the requests for consent has the right to opt-out at any time without any consequences.

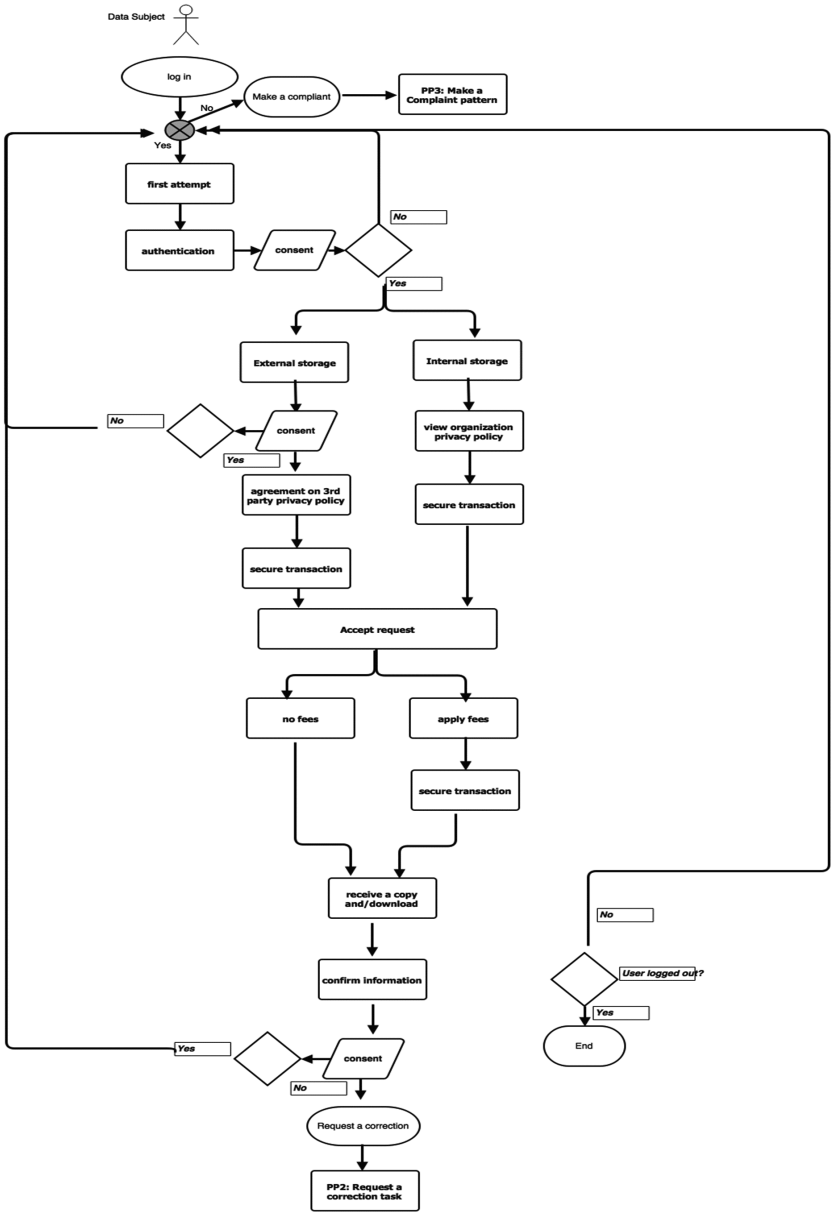

Fig. 1. Request an access proposed privacy pattern

Access Control: the user has to clarify the purpose of accessing the information and security measures have to be applied to download the copy, or they can view the document online (i.e., security patterns). Such controls should allow individuals to have a level of control over the information stored about them.

Feedback: the feedback feature should be applied in every pattern to inform and notify individuals of the ongoing changes either in privacy policies or the changes on the PHI.

Consequences: The proposed pattern applies Need-to-know and Informed Consent to complete the request. We are assuming that the authentication technique is reliable from the security requirements aspect.

Related Patterns: Access control to sensitive data based on purpose by [19] privacy pattern matches the right in one aspect in which the individual has the right to have a level of control over the collected information by providing access to the information. The privacy pattern known as Instant User Interface Pattern by [20] was designed to allow individuals to understand reasons for collecting the information by providing feedback and access to the information collected.

4.2 Request a Correction

Individuals have the right to ask to correct their health information. According to PHIA, the request should be formally written. If a company rejects the request, the individual has the right to file and submit a complaint to the review officer. It is important to transform the hard copies practices into digital forms to serve the ultimate goal of performing privacy patterns that can be considered as guidelines for designing health private system. It is considered as a subtask or follow-up task after requesting access to the PHI. The proposed Privacy Pattern is shown in Fig. 2.

Context: PHIA provides individuals the ability to request corrections if the information they gained access to are not up to date or not correct.

Problem: Individuals have the right to be able to correct the PHI they have on the system.

Solution: The request should be processed through many steps. The individual is asked to confirm a consent form that the entered information is correct. Health providers should review the information before approving it and saving it in the database.

Agreement: Individuals have to sign a consent regarding the changes they will make over the stored information. The changes include correcting the currently existing information or adding more information. The consent will save the individuals' rights and record who made the changes and when.

Review the Changes: It is the healthcare organization's responsibility to review the changes, confirm them and notify the individual's of the result of the review.

Feedback: the feedback feature should be applied in every pattern to inform and notify individuals of the ongoing changes on their PHI.

Consequences: The proposed pattern applies feedback, access control, and informed consent to be able to complete the request.

Related Patterns: Consent to access sensitive data by [19].

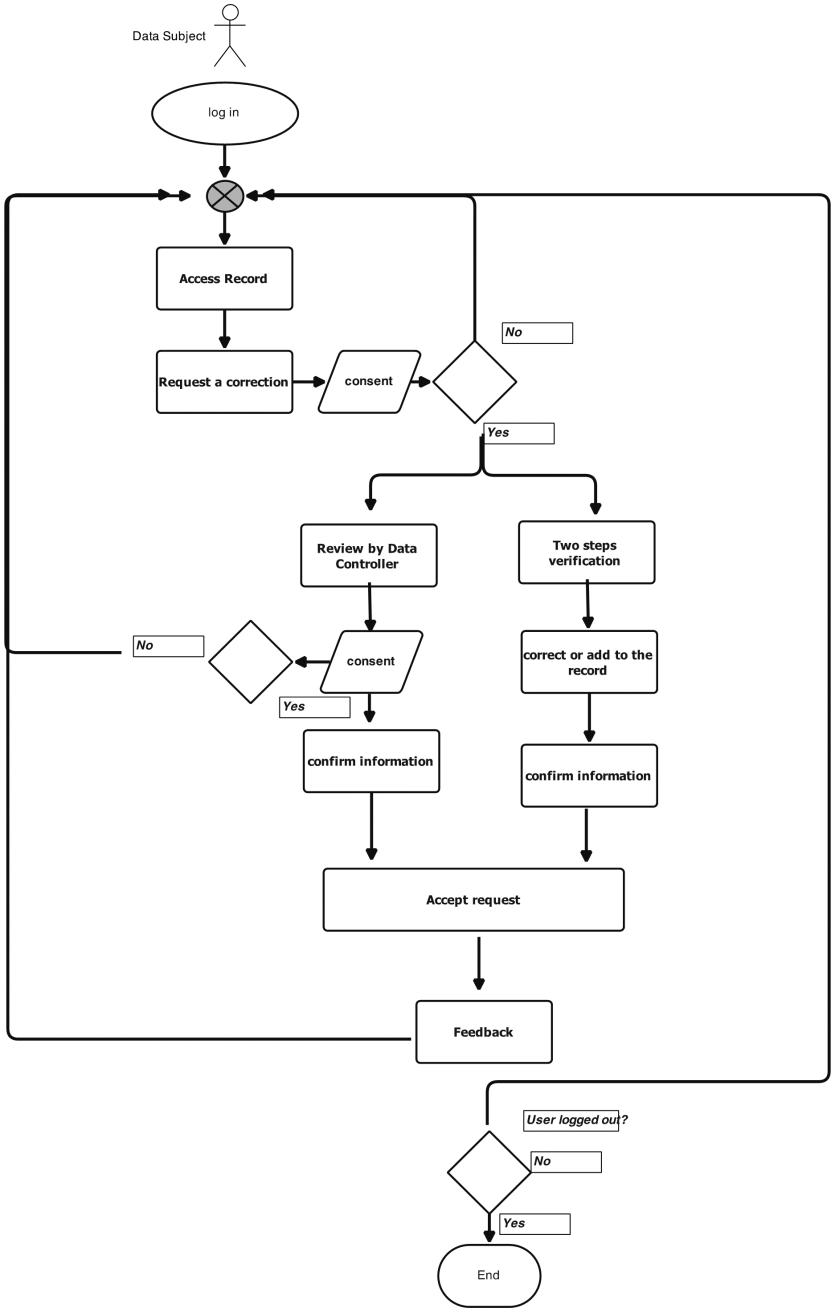

Fig. 2. Request a correction privacy pattern

4.3 Request not to Disclose Personal Health Information (PHI)

Individuals have the rights to request a record of activities in the form of a list of health agents or providers who accessed the online records and minimized access to the information. Therefore, the individual has the right to access, have a list of who accesses the information, and perform a task to limit individuals who can access the information and/or request not to disclose. The proposed Privacy Pattern as shown in Fig. 3.

Context: The individual under this right is able to gain access to a list of activities carried out on the information (have a list of who accessed the information) and be able to request not to disclose information (choose from the list). The individual agrees on sharing the information with some health agents and organizations but wants to limit the access to a well-identified list of agents.

Problem: The individual wants to balance between what is shared and who can gain access. The second use of information shared between organizations without consent concerns individuals.

Solution: The privacy pattern protects individuals' health information by reducing the agents/organization that can access the PHI. This limits the PHI shared over organizations.

Access Control: DS requests a record of activities that have been done on the PHI regarding the list of agents who accessed the information. The DC retrieves the information either from a third party, which should be gained from an earlier agreement or from the organization server. The DS has the ability to; agree on the list or; limit the list by choosing from the list (blocking some), and request not to disclose at all to any of them.

Authentication: The system applies two-steps identity clarification technique to lock out unauthorized access and/or modification as a security measures we assume that they are applied in the system or through security patterns[4].

Consent: Individuals has to sign a consent form on the responsibilities associated with the task (not to disclose). The DC has to confirm changes and provide feedback. *Feedback:* the feedback feature should be applied in every pattern to inform and notify individuals of the ongoing changes on the new settings.

Consequences: The privacy pattern applies consent and feedback. It is part of the access pattern as the individual has to request access to be able to make the changes provided by this pattern.

Related Patterns: Masked online traffic pattern by [10] allows users to control what information to reveal and minimize the amount of personal health information shared.

Suggestion added to the proposed privacy pattern: Individuals would be able to choose the information that they decide they would like to reveal and mask the rest by providing levels of disclosure. The data abstraction pattern [20] allows individuals to control whom to reveal the information and provide feedback on who has access to the information. Individuals would be able to choose from a list of agents/health providers and control or decide who can access what. Private link pattern [21] works in limiting who can see the personal health information. Instant user Interface by [20] allows individuals to opt in or opt out.

[4] Security patterns and measures are out of the scope of this phase of the project.

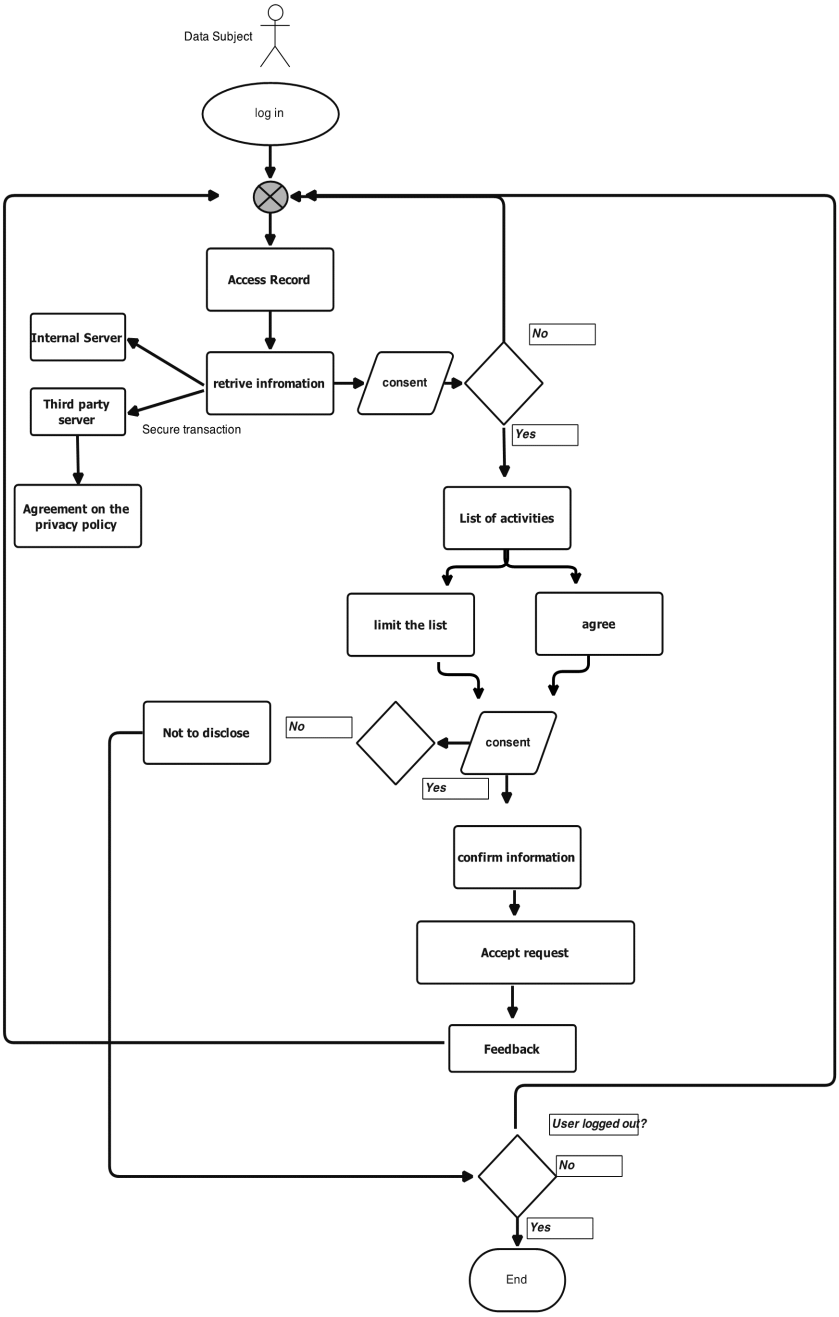

Fig. 3. Request not to disclose health information privacy pattern

The patterns *Being Notified* and *Request a Review* along with the detailed diagrams are in the full tech report [26].

5 Conclusion and Future Work

Six privacy patterns are proposed to cover the individuals' rights. We evaluated the proposed privacy patterns according to ISO29100. We believe that the principles can be mapped to our patterns.

Because the there is a lack of methods to validate privacy patterns and the lack of extensive work on privacy patterns, we will evaluate the proposed privacy patterns according to ISO29100 and the Process Oriented Strategies. To validate our privacy patterns, we compare each pattern to the ISO 29100 privacy framework [24] The ISO 29100 privacy Framework principles include consent and choice, purpose legitimacy and specification, collection limitation, data minimization, use, retention and disclosure limitation, accuracy and quality, openness, transparency and notice, individual participation and access, accountability, information security, privacy compliance.

For further research, these patterns along with design guidelines for the electronic health records portals are going to be used to create the portal's prototype as a second step of the project. The prototype will be tested for its usability and health customers' 'patients' behavior toward the implementation of rights and the level of acceptance.

We have used PHIA as a departure point and focused on the individuals' rights for this stage of the project. The proposed privacy patterns cover these rights and support the Privacy-by-Design concept by providing these privacy design guidelines from the first step of the system lifestyle.

Acknowledgments. This research was supported and funded by the Saudi Cultural Bureau in Ottawa-Saudi Royal Embassy.

References

1. Government Nova Scotia. Personal Health Information Act (2013). http://novascotia.ca/dhw/phia/public.asp
2. Cavoukian, A.: Privacy by design: leadership, methods, and results. In: European Data Protection: Coming of Age, pp. 175–202. Springer, Netherlands (2013)
3. National Research Council: Who goes there? Authentication through the lens of privacy. National Academies Press, Washington, D.C. (2003)
4. OECD: OECD guidelines on the protection of privacy and transborder flows of personal data (1980). http://www.oecd.org/home/
5. Brodie, C., Karat, C.M., Karat, J., Feng, J.: Usable security and privacy: a case study of developing privacy management tools. In: Proceedings of the 2005 Symposium on Usable Privacy and Security, pp. 35–43. ACM, July 2005
6. Guarda, P., Zannone, N.: Towards the development of privacy-aware systems. Inf. Softw. Technol. **51**(2), 337–350 (2009)
7. Office of the Information & privacy commissioner in Nova Scotia (2015). http://foipop.ns.ca
8. http://privacybydesign.ca

9. Chung, E.S., Hong, J.I., Lin, J., Prabaker, M.K., Landay, J.A., Liu, A.L.: Development and evaluation of emerging design patterns for ubiquitous computing. In: Proceedings of the 5th Conference on Designing Interactive Systems: Processes, Practices, Methods, and Techniques, pp. 233–242. ACM, August 2004
10. Romanosky, S., Acquisti, A., Hong, J., Cranor, L.F., Friedman, B.: Privacy patterns for online interactions. In: Proceedings of the 2006 Conference on Pattern Languages Of Programs, p. 12. ACM, October 2006
11. Borking, J.: Deridentity-protector. Datenschutz und Datensicherheit **20**(11), 654–658 (1996)
12. Seničar, V., Jerman-Blažič, B., Klobučar, T.: Privacy-enhancing technologies—approaches and development. Comput. Stan. Interfaces **25**(2), 147–158 (2003)
13. Damiani, M.L.: Privacy enhancing techniques for the protection of mobility patterns in LBS: research issues and trends. In: European Data Protection: Coming of Age, pp. 223–239. Springer Netherlands (2013)
14. W3C, Platform for Privacy Preferences, P3P 1.0 (2002). http://www.w3.org/P3P/
15. Chaum, D., Fiat, A., Naor, M.: Untraceable electronic cash. In: Goldwasser, S. (ed.) CRYPTO 1988. LNCS, vol. 403, pp. 319–327. Springer, Heidelberg (1990)
16. Communication COM (2007) 228: from the Commission to the European Parliament and the Council. On Promoting Data Protection by Privacy Enhancing Technologies (PETs) (2007)
17. Fischer-Hübnner, S., Köffel, C., Pettersson, J.-S., Wolkerstorfer, P., Graf, C., Holtz, L.E., König, U., Hedbom, H., Kellermann, B.: Prime Life (2010). http://primelife.ercim.eu/images/stories/deliverables/d4.1.3-hci_pattern_collection_v2-public.pdf
18. Compagna, L., El Khoury, P., Krausová, A., Massacci, F., Zannone, N.: How to integrate legal requirements into a requirements engineering methodology for the development of security and privacy patterns. Artif. Intell. Law **17**(1), 1–30 (2009)
19. Porekar, J., Jerman-Blazic, A., Klobucar, T.: Towards organizational privacy patterns. In: 2008 Second International Conference on the Digital Society, pp. 15–19. IEEE, February 2008
20. Bier, C., Krempel, E.: Common privacy patterns in video surveillance and smart energy. In: 2012 7th International Conference on Computing and Convergence Technology (ICCCT), pp. 610–615. IEEE, December 2012
21. Privacypatterns.org, accessed 2015. http://privacypatterns.org/patterns/
22. Department of Health and Community Services (2015). http://www.health.gov.nl.ca/health/phia/
23. Personal Health Information Act, Department of Health and Community Services (2014). http://assembly.nl.ca/Legislation/sr/statutes/p07-01.htm
24. ISO/IEC 29100. Information technology–Security techniques–Privacy framework. Technical report, ISO JTC 1/SC 27
25. Buschmann, F., Meunier, R., Rohnert, H., Sommerlad, P., Stal, M.: Pattern-Oriented Software Architecture. John Wiley, Chichester (1996)
26. The tech report is named CS-2016-01 and available at: https://www.cs.dal.ca/research/techreports/cs-2016-01
27. Dingledine, R., Mathewson, N., Syverson, P.: Tor: the second-generation onion router. In: Proceedings of the 13th USENIX Security Symposium (2004)