Information Accountability for Online Healthcare Social Networks

Randike Gajanayake[1], Renato Iannella[2] and Tony Sahama[3]

Queensland University of Technology, Australia[1,3]
Semantic Identity, Australia[2]
gajanaya@qut.edu.au[1]
ri@semanticidentity.com[2]
t.sahama@qut.edu.au[3]
Corresponding Author: gajanaya@qut.edu.au

Abstract

Online social networking has become one of the most popular Internet applications in the modern era. They have given the Internet users, access to information that other Internet based applications are unable to. Although many of the popular online social networking web sites are focused towards entertainment purposes, sharing information can benefit the healthcare industry in terms of both efficiency and effectiveness. But the capability to share personal information; the factor which has made online social networks so popular, is itself a major obstacle when considering information security and privacy aspects. Healthcare can benefit from online social networking if they are implemented such that sensitive patient information can be safeguarded from ill exposure. But in an industry such as healthcare where the availability of information is crucial for better decision making, information must be made available to the appropriate parties when they require it. Hence the traditional mechanisms for information security and privacy protection may not be suitable for healthcare. In this paper we propose a solution to privacy enhancement in online healthcare social networks through the use of an information accountability mechanism.

Keywords: Information accountability, online social networks, healthcare, online healthcare social networks, information sharing, privacy

1. Introduction

It has come to the point where the popularity of the Internet can be measured by the activity on online social networks which have become one of the most widely used internet applications. For example, taking into account some of the most popular social networks; Facebook has over 640 million registered users, Flickr has more than 30 million users, MySpace with over 100 million users and LinkedIn has over 100 million users; as of May 2011. They can range from general purpose to business and professional networking. The primary goal of social networks was to give Internet users the capability to share information be it personal or otherwise with other users of the same social network. But with time this has evolved to an extent where users demand more diverse functionality and better privacy protection from the developers of these technologies. When personal information is available on the Internet the aspects of information security and privacy take in a whole new perspective. The control over the information in current social networks is done by a separate body which sustains the social web even with user preferences for information visibility.

With this increasing popularity and the diverse functionality, online social networks are stepping towards applications in healthcare despite being slow. The foreseeable benefits of using online social networks in healthcare have obscured the potential privacy risks of disclosing sensitive health information in online social networks. But that does not mean that health information can be managed the same way current online social networks manage information.

In this paper we will investigate the concept of online social networks and their role in healthcare. We will try to identify the benefits and risks involved when bringing such a technology into domain that is driven by such sensitive information that safeguarding them is a vital aspect in the success of such systems. We propose a solution to the potential risks of disclosing sensitive health information in online social networks that will benefit both the information owners (patients) and the users (both patients and health professionals) by introducing an information accountability mechanism for online healthcare social networks (OHSN).

2. Online social networks

2.1 Introduction

“Web 2.0” is a concept of participatory information sharing, interoperability, user centred design and collaboration on the World Wide Web (Wikipedia 2011). This concept is the basis for all online social networks allowing users increased levels of participation which was absent in the initial architecture of static content from owner to the reader. Web 2.0 allows the users to easily generate and publish content on the Web.

The most attractive aspects of Web 2.0 architectures are those found in online social networking web sites. When users register on an online social networking web site they create a profile containing personal information. Once this profile is complete, the user can begin to construct a social network, by creating relationships with other users in the same online social network. A distinct feature of the modern online social networks is that they make the relationships between users precise and visible to others. Online social networks can be found that have been developed for various purposes.

An online social network can be defined as web-based services that allow individuals to construct a public or semi-public profile within a bounded system, articulate a list of other users with whom they share a connection, and view and traverse their list of connections and those made by others within the system (Boyd & Ellison, 2008). This means that the connections made by each user will allow them to view and share each other's information within the social network. The purpose of which they share information may vary from network to network.

2.2 Online Healthcare Social Networks (OHSN)

Health 2.0 is the result of the reliance of the Internet as a source of health information. It leverages social software to promote collaboration among patients, caregivers, medical professionals and other health stakeholders (Sarasohn-Kahn, 2008). As a result of Health 2.0 participatory medicine has become the attention of many researchers and many argue between the benefits and the potential concerns of health information security, privacy and trust. Personal health records (PHR) are the basis for Information Technology use in healthcare (Ferreira et al., 2003). Of all the health information technology in current use, PHRs has the most wide-ranging capabilities and thus the greatest potential for improving quality (Miller & Sim 2004). PHRs allow patients to keep a permanent record of their health information which can be used to create a personal health profile in an online social network.

Ball and Lillis (2001) claim that today the Internet facilitates crucial components of healthcare delivery, including consumer education, disease management, clinical decision support, physician/consumer communication and administrative efficiencies. The word 'patient' is slowly transformed into 'consumer' because of the Internet and the demand for a more active role in their own care. Deloitte and Touche as stated by Ball and Lillis (2001), patients do not receive literature about their medications. They, therefore, take the education to their own hands. In 1999, 74% of US Internet users searched for online medical information. This number has since increased rapidly. The reasons for patient to search the Internet for medialc data range from simple searches about disease or symptoms to attempt self treatment (Elkin 2008). This has resulted in a change in the physician/patient relationship (Xie et al., 2006). This change can be made to the benefit both patient and the caregiver if it is managed properly. Online healthcare social networks can be one way that this can be done.

Sharing information through a social network and allowing patients to control the flow of their health information could prove to be very effective in future healthcare needs. According to Domingo (2010), at the moment, healthcare social networks provide an attractive platform for sharing ideas, discussing symptoms and debating treatment options. By allowing medical professionals to access PHRs of their patients, this can be taken to the next level and healthcare can be made more efficient and more effective.

Online social networks for better healthcare needs have to be different from the basic architecture of online social networks. Since the main goal of these is to allow the patient and the caregivers to share information in an efficient and secure manner. But these capabilities are limited by several issues such as information security, privacy, data accuracy and trust. There need to be tasks that a user can perform as well as the content that user can view depending on the role they play in the social network. The first idea is to categorise the roles a user can play in the social network. The tasks can be defined according to the user roles in the social network. We will discuss this further later in this document.

2.3 Existing Online Healthcare Social Networks

Online healthcare social networks can be categorised into two; physician centered and Patient centered.

Online physician social networks provide an infrastructure for doctors to share clinical cases and medical knowledge with peers. This gives them the opportunity to help investigate particular clinical cases which literature cannot give answers to. Small or private physicians can also benefit from these social networks without the need for physically contacting other doctors. Rural based practioners will have a readily available source of information and peer guidance for more efficient care delivery. But the accuracy and correctness of the information shared in such social networks has to be genuine. The physicians that join the networks may be asked to verify their credentials or invitations can be sent to physicians by other already registered in the network to increase trust and confidence of network users. Sermo, Ozmosis and DoctorNetworking are some of the popular online physician social networking sites.

Online patient social networks focus on increasing awareness about diseases and help stay healthy while living with a medical condition. Users will benefit from direct patient support and can share medical information with other users with similar health conditions. Patients can benefit from a 24/7 knowledge base and a supportive environment rather than treatment for acute events. However, posting personal information, be it health information or other, poses the risk of privacy infringement for the information owners. For example PatientsLikeMe (www.patientslikeme.com), a popular online patient social network warns users before they join that their information will be visible to others in the network and also that insurance and drug companies can pay to access the information. The patients however are more concerned about their health conditions than online privacy and hope that the information exchange will help them improve their medical conditions (Domingo, 2010). But

privacy could be of greater concern later. PatientsLikeMe, Disaboom, Inspire, CureTogether and HeartPatients are some of the popular online patient social networks.

Internet-based PHR systems that allow patients to maintain online records of their health information are also in common use. The most prominent of these are Google Health and Microsoft HealthVault. Google Health is an online tool that helps the patients take control of their health information. Google Health allows the users to create online health profiles, manage them, and share health profiles with others including family and caregivers. It also allows the users to download medical records from doctors and other care giving organisations. Information sharing is done with the use of invitations sent to the recipient via emails (Google Health).

Microsoft HealthVault itself is not an application but a platform which vendors can create PHR systems. Once a HealthVault record is created it can be accessed through a HealthVault account. Microsoft HealthVault uses an access control scheme that allows the owners of the health profiles select what information another account can access. These access control schemes are implemented in the vendor applications with the explicit consent of the owner (Microsoft HeathVault).

There is the possibility of further increasing the functionality of online healthcare social networks to give them close to the same user friendly capabilities as regular online social networks but with better security measures and privacy protection mechanisms

3. Privacy

Although a difficult term to define, privacy can be justified when coupled with information security. When security is breached there is a risk of disclosure of personal information. In other words is security is breached you lose control over your personal information. So we can argue that when one loses control over the personal information their privacy has been violated. In this section we will discuss the concept of privacy in terms of disclosing health information on the Internet.

3.1 Privacy risks of Online Social Networks in Healthcare

Information security and privacy are main issues that arise when manipulating health information. When using sensitive information about patients through the Internet, the danger of the security of information being compromised is increased. According to Kind and Silber (2004), because of the open architecture of the Internet, organisational policies and procedures are needed to guarantee the privacy of and integrity of applications that manage the information. Security and privacy problems must be addressed in a timely and organised manner when health information is used in online applications.

In a domain such as healthcare these issues should be eliminated to the best possible extent. As Goldman and Hudson (Goldman & Hudson 2000) state, without trusting that their most sensitive health information will be safeguarded, patients are reticent to fully and

honestly disclose their personal information and may avoid seeking care altogether. This indicates that the trust (Matysiewicz & Smyczek 2009) of the patients would be tainted. This obviously is a major issue when it comes to giving the proper treatment to the patients.

Privacy management in modern online social networking web sites is done through rigid access restrictions for unauthorised users. But these policies are not always properly understood by the users and often their information is publicly available. Even though users have great concern of privacy of their personal information, they are less concerned about safeguarding it (Awad & Krishnan 2006). This creates more complications for the developers of online social network forcing them to enforce better mechanisms for privacy protection. Online social networks are already being accused for their poor privacy policies and mechanisms. If such a social network was used to manage sensitive health information the outcome would be catastrophic. In their study of two popular online social networking sites Dwyer et al. (2007), has come to the conclusion that trust and privacy concerns in social networking sites are not yet understood to a sufficient degree to allow accurate modeling of behaviour and activity. Therefore, better means of protecting privacy in social networks has to be defined to enable heath information from being disclosed to unwanted entities. Such a mechanism is to use information accountability in OHSNs.

4. Information accountability (IA)

4.1 Introduction to IA

What is accountability? Accountability is when someone is held answerable for their actions and their outcomes. Eriksen (2002) also agrees with this definition of accountability. According to Emanuel et al. (1996) “Accountability entails the procedures and processes by which one party justifies and takes responsibility for its activities”. When focusing on information accountability, users of the information are held liable to explain, justify or answer for their use of information, when requested by the party to whom the information belongs to.

Information is widely available and the use of that information needs to be controlled. Rather than enforcing rigid up-front control over the use of information, there is a need to accommodate fair use. The control over the use of information is imperfect and exceptions are possible, but violators can be identified and held accountable (Weitzner et al., 2008)

It is appropriate to define IA contextually in healthcare since we are focused on information use in healthcare. To define Information accountability in healthcare we must identify and define the components of information accountability; Who, What and How. In other words, the parties that are held accountable or can hold someone accountable, what are they held accountable for and how they are held accountable. In any given scenario in healthcare we can identify four types of participants (Figure 2):

1. health Professionals

2. non-health professionals
3. consumers
4. organizations

These become the roles that a participant can play in a healthcare scenario. The tasks they perform in the scenario can be categorised by the type of role itself or according to specific health care scenarios. The mechanisms for holding accountable for inappropriate misuse can be defined according to the tasks they perform and the type of information that has been misused. The owners of the information need to have the visibility of the processes (or the processes need to be transparent (Weitzner et al., 2006) to the owner of the information) their information is going through in order to enforce the IA functionality.

4.2 IA for OHSN

As discussed earlier there are two types of online healthcare social networks. Even though these technologies greatly enhance healthcare management, if the two categories are linked together the benefits to care delivery could be further improved. Since patients are the consumers of healthcare the networks must be centered towards the patients more than the physicians or health professionals. An online healthcare social networking environment where all types of network users can share health information could prove to be much more advantageous than keeping the domains separate. The health professionals can share patient information with other medical professionals to make better decisions towards the wellbeing of the patients. But since there is a transition of information between the two domains, there need to be a mechanism to control the use of information by different users. Information accountability can be use as a mechanism for controlling this use of information to identify misuse of information and to hold users accountable for unintentional misuse.

By allowing patients control over their personal health information, information privacy can be achieved (Cavoukian et al., 2010). Information accountability can assure the user of secure information sharing and the proper use of information in healthcare. The way information is used has to be monitored and patients should be informed of how their information is being used and by whom. This will allow them to hold people accountable for inappropriate use.

The public will own their health records and be responsible for the control of their health profiles in the social network. They will be given the opportunity to grant access to the health information to specialists that they feel are suitable for a specific task. The specialists will make further linkages with other medical professionals that will support the ultimate goal of sharing of information, which leads to better healthcare delivery.

The users of an online social network with IA capabilities can be categorised in the following manner.

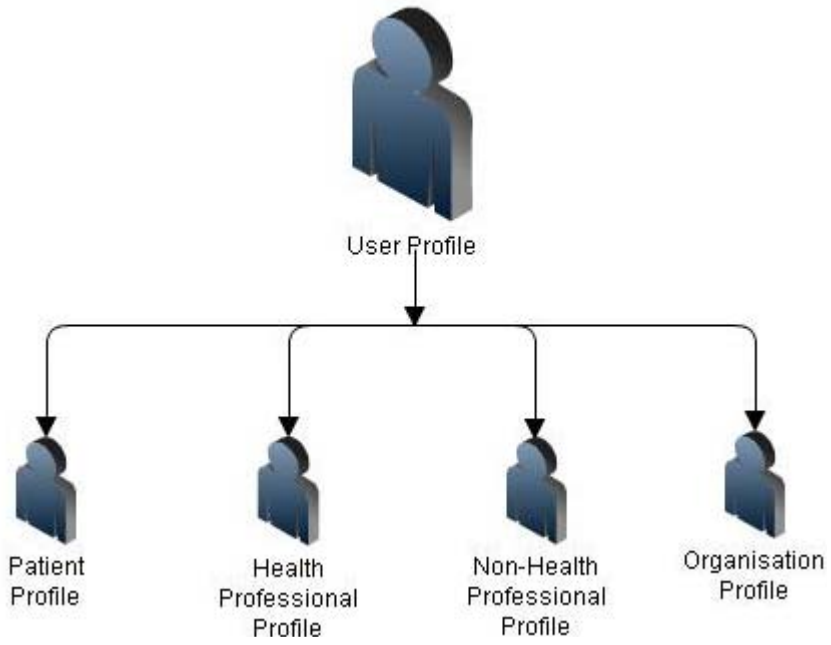

Figure 2: Types of users

Figure 03 illustrates how and IA process can be incorporated in to the current architecture of an online healthcare social network. The “User Profile” in the figure includes all categories of users of the healthcare social network. This means that patients are able to access health profiles of other patients (e.g. friends, family members).

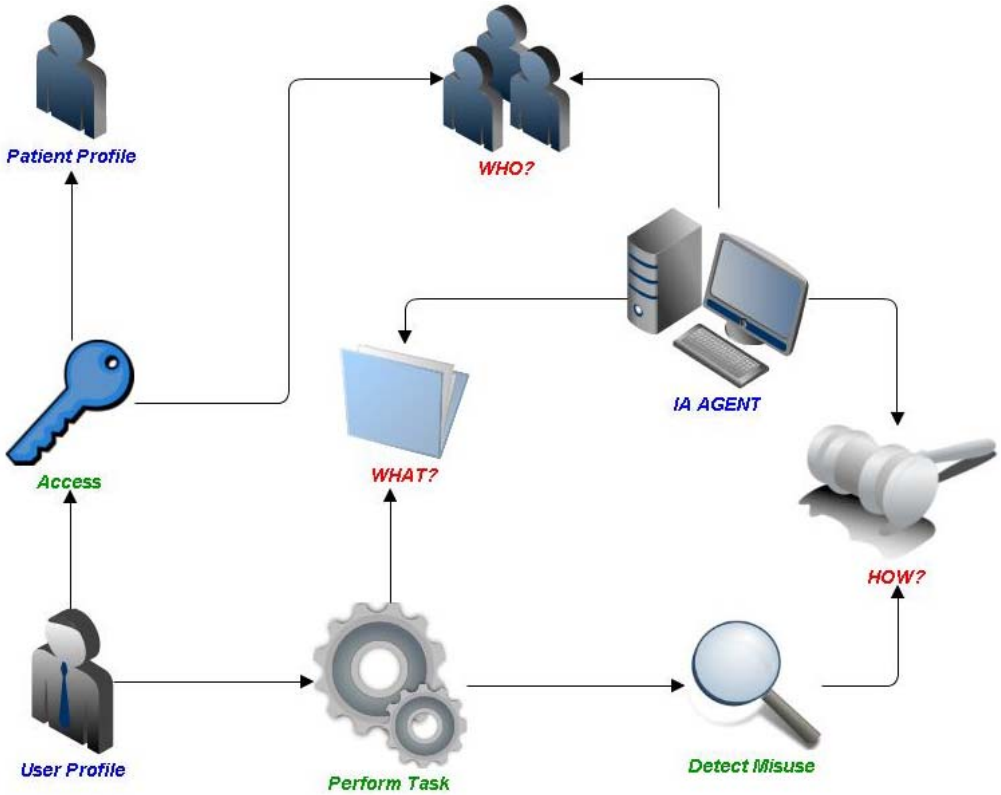

Figure 3: IA mechanisms for an Online Healthcare Social Network

In current online social networks these mechanisms are not present. By having the information accountability mechanisms in place will provide the patients a way of monitoring the use of information by the different participants and give them the ability to act upon inappropriate misuse of their health information in a more informed manner. The “IA Agent” will be responsible for all message handling, monitoring of profile access, notifications and alerts. The owners of the information will be notifies of the use of their information. The users will be alerted or warned when they try to access information of other patients about what they are about to access and the consequences of misuse of patient information. With this mechanism in place health professionals will be capable of sharing patient information with other health professionals to make better decisions.

Rigid access (Weitzner et al., 2008) restrictions in any healthcare information system tend to delay the task at hand which is care delivery. With the use of the IA capability access restrictions can be somewhat moderately implemented to allow quick access to information or example in emergencies where gaining patient consent is not always feasible.

5. Discussion and conclusion

In this paper we have investigated online social networks in order to identify their role in modern healthcare. We have identified two types of healthcare social networks; physician centered and patient centred. Even though these technologies provide the users a high degree of capabilities, the drawback that are present in terms of privacy concerns and trust, the traditional social network structure may not be appropriate for an industry that deals with very sensitive information. A combination of these two types of healthcare social networks that allow both physicians and patients to share health related information will benefit the healthcare systems in a much more effective and efficient manner. But sharing health related information means that patient privacy infringement is even more prominent. This means that better measures for privacy protection must be incorporated to online healthcare social networks that allow sharing of patient health information. This will ensure the end users that their sensitive information will not be disclosed to unwanted parties.

We believe that with the integration of information accountability aspects in to the online social network structure will overcome most privacy concerns that impede current online social networks. This will enable the health professionals to share information and make better decisions about a patient’s health more efficiently and by keeping the patients a part of the process of the information use by allowing them the required visibility the care process will be more effective.

References

Awad, N. F. & Krishnan, M. S. (2006). The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingeness to be Profiled Online for Personalization. *MIS Quarterly*, *30*(1), 13-28.

Ball, M. J., & Lillis, J. (2001). E-health: Transforming the physician/patient relationship. *International Journal of Medical Informatics*, *61*(1), 1-10.

Boyd, D. M., & Ellison, N. B. (2008). Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication*, *13*(1), 210-230.

Cavoukian, A., Fisher,A., Killen,S. & Hoffman, D. (2010). "Remote home health care technologies: how to ensure privacy? Build it in:Privacy by Design." Identity in the Information Society **3**(2): 363-378.

Domingo, M. C. (2010). "Managing Healthcare through Social Networks." Computer **43**(7): 20-25.

Dwyer, C., Hiltz,S. & Passerini, K. (2007). Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. Proceedings of the Thirteenth Americas Conference on Information Systems, Keystone, CO, USA.

Elkin, N. (2008). How America Searches: Health and Wellness, iCrossing.

Emanuel, E. J. & Emanuel, L. L., (1996). "What Is Accountability in Health Care?" Annals of Internal Medicine **124**(2): 229-239.

Eriksen, S. (2002). Designing for accountability. Proceedings of the second Nordic conference on Human-computer interaction. Aarhus, Denmark, ACM**:** 177-186.

Ferreira, A., Shiu, S. & Baldwin, A. (2003). Towards accountability for Electronic Patient Records. Computer-Based Medical Systems, 2003. Proceedings. 16th IEEE Symposium.

Goldman, J. & Hudson, Z. (2000). "Virtually exposed: Privacy and e-health." Health Affairs **19**(6): 140.

Google Health. "About Google Health." Retrieved 01 March 2011, from http://www.google.com/intl/en_us/health/about/index.html.

Kind, T. & Silber, T. J. (2004). "Ethical Issues in Pediatric E-Health." Clinical Pediatrics **43**(7): 593.

Matysiewicz, J. & Smyczek, S. (2009). Consumer Trust - Challenge for E-healthcare. Cooperation and Promotion of Information Resources in Science and Technology, 2009. COINFO '09. Fourth International Conference on.

Microsoft HeathVault. "Learn About Microsoft HealthVault." Retrieved 01 March 2011, from http://www.healthvault.com/personal/websites-overview.aspx.

Miller, R. H. & Sim, I. (2004). "Physicians' Use Of Electronic Medical Records: Barriers And Solutions." Health Affairs **23**(2): 116-126.

Sarasohn-Kahn, J. (2008). The Wisdom of Patients: Health Care Meets Online Social Media, California Healthcare Foundation; www. chcf.org/topics/chronicdisease/index.cfm?itemID=133631.

Weitzner D. J., Abelson, H., Berners-Lee, T., Feigenbaum, J., Hendler, J. & Sussman, G. J. (2008). "Information accountability." Commun. ACM **51**(6): 82-87.

Weitzner, D. J., Abelson, H., Berners-lee, T., Hanson, C., Hendler, J., Kagal, L., Mcguinness, D. L., Sussman, G. J. & Waterman, K. K. (2006). Transparent accountable data mining: New strategies for privacy protection.

Wikipedia. (2011). "Web 2.0." Retrieved 05 May 2011, from http://en.wikipedia.org/wiki/Web_2.0.

Xie, B., Dilts, D.M. & Shor, M. (2006). The physician-patient relationship: the impact of patient-obtained medical information, Health Economics. **51**(8): 813-833.