EPiC Series in Computing

Volume 58, 2019, Pages 210–218

Proceedings of 34th International Conference on Computers and Their Applications

Implementation of Security and Privacy Aspects in a Healthcare Social Network

Kasi Periyasamy and Saleh Alsyefi

University of Wisconsin-La Crosse, La Crosse, Wisconsin, U.S.A.
(kperiyasamy, alsyefi.saleh)@uwlax.edu

Abstract

A recent medical survey indicates that healthcare social networks are very helpful in promoting awareness of health issues, discussing related health problems with other patients and healthcare providers, and finding quick solutions for some of the health problems[12]. Social media and advances in mobile technology make healthcare information accessible to many patients. Healthcare providers are also able to gain more benefits from healthcare networks by exchanging information with other providers and disseminating valuable health related information. The two major problems in using healthcare networks as reported in the literature are security of information stored and passed through the network, and privacy of patients' health information. This paper describes the design and implementation of a healthcare network focusing on the two aspects - security and privacy. The authors chose Nephrology, the study of kidney diseases, for illustration. However, the design and implementation of the network has been made sufficiently generic so that it can be used for other health domains such as gynecology and psychiatry.

1 Introduction

Social networks are extremely powerful media for sharing and seeking information. With the advent of mobile technology, accessing information through social networks is made easier for anyone who has a mobile device. As reported in Oxford Research Encyclopedia [10], 37% of world's population used social media in 2017. There is a ten-fold increase in the use of social media by Americans during the time 2005-2015. A similar trend is also seen in the United Kingdom in 2016 where more than six in 10 adults use social media. While a social media is a channel to disseminate information, a social network, on the other hand, also provides mechanisms for interactions.

Healthcare domain also uses both social media and social networks extensively; in particular, the latter is used to seek, query, comment, share and exchange healthcare information. Some healthcare networks are available to only healthcare providers (Sermo[5], Doximity[1], and QuantiaMD[4], to name a few). These networks provide a forum for providers to discuss specific cases or problems, and exchange diagnostic and medical information. Some healthcare networks are available for both groups - patients and healthcare providers (PatientsLikeMe[3], Mercy Health Network[2], and Triad Healthcare Network[6] to name a few). Griffiths and others[7]

have discussed the advantages of using healthcare networks and how they support both patients and healthcare providers. In particular, they argue that "social networking has the potential to change patterns of health inequalities and access to healthcare, alter the stability of healthcare provision and lead to a reformulation of the role of health professionals." Moorhead[10] describes a wide range of activities that are supported by healthcare networks which include providing answers to medical questions, facilitating dialogues between patients, and between patients and healthcare professionals. In addition, some healthcare networks also provide facilities for online consultations. The authors of this paper are highly motivated by the benefits of using a healthcare network as described by Moorhead. These include increased interactions among patients, interactions between patients and healthcare professionals, more available, shared, and tailored information, and increased peer, social and emotional support.

When comes to healthcare information, privacy and security of information posted and shared are most important[10, 9]. Social networks such as *Facebook* and *Twitter* are used for general purpose in the sense that any topic can be posted or discussed in these networks. As a result, anyone can join these networks and exchange any information. Though there are some security controls available in these networks, they are not sufficiently strict. Li pointed out that openness in virtual communication and the growing trend of using technology for sharing healthcare information create increased opportunities for misuse of healthcare data. Even though the Health Information Portability and Accountability Act (HIPPA) of 1996 in the United States protects people from unauthorized access of healthcare information, HIPPA does not protect the privacy of an individual when the individual himself or herself posts his/her healthcare related information on a social network[9]. Many users of general healthcare media such as *Facebook* and *Twitter* are not aware of this openness in communication and the huge audience behind it. Because of the sensitivity of healthcare information, the designer of healthcare networks should focus on additional mechanisms by which a patient's healthcare information is not leaked accidentally or inadvertently. Security of a healthcare network (in fact, any computer network) mostly depends on the design of such network. The design involves several factors including the types of users, type or sensitivity of information to be maintained and/or to be shared, the resources available, and potential threats known or published in the literature.

This manuscript describes the design and implementation of a social network called *Nephro Net*. Though the current implementation of Nephro Net was created for patients with kidney problems and professionals in Nephrology (a study of Kidney Diseases), the network can be easily adapted to other domains as well. Section 2 describes an overview of Nephro Net, followed by discussions on some design decisions of Nephro Net in section 3 and its operations in section 4. The final section includes concluding remarks, challenges and future work.

2 Nephro Net - A healthcare social network

Recent advances in healthcare is moving towards patient-centric networks in which patients have more control in entering and releasing personal healthcare information[8]. A recent survey published by the Massachusetts Medical Society [12] indicates that 52% (out of 601 responses) indicated that patient-to-patient support will be very useful; 85% considered that social healthcare networks are useful for chronic disease management; and 75% mentioned that disease specific patient support groups will be the most effective. These statistics along with the notion of patient-centric design motivated the authors to develop a healthcare social network Nephro Net, specifically designed for patients who have kidney problems and healthcare providers in Nephrology. The aim of this network is to provide a forum for patients to search, post and

discuss kidney related healthcare problems. Professionals in Nephrology can also join the network to disseminate specific information to patients (such as an optimal dosage of a medication for dialysis patients with diabetes), to answer questions posted by other users (both patients and professionals) in the system and engage in private consultation with a patient. Nephro Net ensures that privacy and security of information passing through the network are strictly enforced. The major advantages of Nephro Net are listed below:

- Patients having kidney problems will be able to discuss their problems, treatments and consequences with other patients. If two or more people have similar problems and treatments but different results, the inadequacy in the treatments or the reasons for differences in the results may be identified. Age groups, gender and other health conditions such as diabetes play major roles in this type of discussion. Notice that personal information such as age and gender of a patient will not generally be revealed to other users; it is up to the patient who can disclose personal information in a discussion. For example, a patient may say "I am 65 years old male, and I have . . . I appreciate if anyone of my age or closer can help me in identifying whether the medication . . . will work correctly for me."

- Patients will be able to identify and choose better health care facilities and services by exchanging their problems, solutions and ideas. Cost of treatment, location of treatment, availability of drugs and a list of healthcare providers are some of the factors generally discussed in this category. Nephro Net does not store any of these discussion parameters in its database; these parameters will be part of the messages exchanged between patients.

- A patient can choose a physician and engage in a private consultation with that physician. They may both exchange any sort of information including the patient's personal healthcare information. Nephro Net provides extra level of security to ensure that other users of the network cannot access such information.

- Physicians will be able to answer medical questions posted by patients. They will also be able to post educational information for patients. For example, a nephrologist may post a warning message on using a particular drug for patients with diabetes.

- Physicians will also use this forum to discuss multiple cases with other healthcare professionals and educate themselves. It is quite common among healthcare providers discussing common problems, their treatments and results. Medical forums, journals and conferences are all created specifically for this purpose. While these interactions are quite formal, their interactions through Nephro Net are quite informal, short and can be focused to specific cases.

- All users' registrations are strictly verified by a group of administrators. The administrators have the rights to view, block and/or remove most of the information posted on the network. However, administrators will not be able to view passwords, personal profiles of the users if they are set to be private, and will not be able to see any part of a private consultation between a patient and a physician.

- Privacy of information is completely left to the users who create, post and/or exchange information.

- Security of information is provided by appropriate protection through passwords, encryption/decryption mechanisms and session controls.

3 Design decisions made in implementing Nephro Net

As stated earlier, privacy and security of information were given utmost importance in the design of Nephro Net. This section elaborates the important design decisions considered in the implementation of Nephro Net.

Registration Every user who wants to join Nephro Net must register with the system by filling up relevant information in a registration form. Appropriate validation checks have been implemented to ensure that all required fields are duly filled in by the registrant. All communication from and to the system will use the email address provided in the registration form. Upon completion, an administrator will evaluate and approve (or deny) the request. If approved, an account will be created for the user and an email is sent to the user with system-created username and an initial password. The user is required to change the password when logging in for the first time.

Current implementation is expected to be launched within a healthcare organization such as a hospital or clinic. Every user of Nephro Net is expected to be a registered member of the healthcare organization so that when new users register with Nephro Net, the information provided during registration will be verified against the database of the organization. The verification process uses the unique ID given to the user in the organization to retrieve information from the organization's database. As an example, if someone steals the ID number of a patient in the organization and uses that ID to register with Nephro Net, most likely the information provided by the hacker will be different from that stored in the organization's database and hence the hacker will not be able to get an account in Nephro Net. As another example, if a user tries to get another account with a different name, it will be flagged as an error during the verification process. Once verified, some personal information of a new user will be extracted from the organization's database in order to create a short profile of the new user. This short profile will be used to identify the user by other users of Nephro Net.

Authentication A two-factor authentication mechanism has been implemented to gain access into Nephro Net, even for administrators. That is, in addition to username and password, a user is required to answer to a security question to login into Nephro Net. A user is required to choose three security questions and set up answers for them when logging in for the first time. Thereafter, every time when the user logs in, one security question at a time from the pool of three selected questions by the user will be randomly selected and displayed. If the user answers incorrectly to all the three security questions, the user's account will be blocked. Only an administrator can restore the account. This requires negotiation with the administrator after showing proofs or evidences of valid access requests. This two-factor authentication process is a step forward towards tightening security as expected for a healthcare network. Use of biometric sensors could be another option to consider; however, additional devices and processes are required to implement biometric sensors which will limit the use of Nephro Net by potential users.

Password encryption Passwords in Nephro Net are all hashed using SHA-256 hashing algorithm. Hashing occurs right after a user enters a password for the first time and then the hashed password is stored in the database. By this way, every password is protected even when it is sent to the database.

Sessions In addition to sessions that are normally used in web-based application to ensure security, Nephro Net also uses an additional sessions token that is generated every time

when a user accesses the system. This token is stored in the system and is used to compare the session data when a user navigates to a different page. The use of additional token thus increases the level of security in Nephro Net.

Health records Nephro Net provides interactions between kidney patients and healthcare professionals. There will be several messages containing some health details of patients that are exchanged by the users of this system. For example, a patient may post a message asking a question about a particular syndrome he/she has. However, Nephro Net does not access the health record of any patient; nor it reveals/displays any health-related information of a patient without the patient himself/herself revealing that information as part of a message. Thus the users of Nephro Net have control over their personal information.

User profile Every user of the system, particularly a patient, has the option of creating a personal profile. This profile is under complete control of the user who created it. No other user in the system has access to another user's profile. The system may internally use this profile to suggest some messages or disseminate some information relevant for this user. It does so by scanning for some keywords within the profile and compares them against posted messages. Since this activity is performed internally by the system, no other user will be aware of even the existence of the profile. In addition, the profile may be password protected. That is, the creator of the profile has the option to set a password at the time of creating the profile. Thereafter, every access to the profile, even by the same user, requires authentication using the profile's password. If the user forgets the profile password, the profile can never be accessed. The creator has the option to let other users access his/her profile by giving the profile password. However, such actions are highly discouraged in order to ensure tight security of the system. The user profile itself is encrypted using AES-256 encryption algorithm.

Consultation messages A patient has the option of exchanging private messages with a physician. These messages are called "consultation messages". Such a private conversation is meant to provide personalized service by a physician to a patient. Consequently, Nephro Net ensures that the messages exchanged during consultations are encrypted using AES-256 encryption algorithm and are not visible or accessible by any other user of the system, including administrators.

4 Operations of Nephro Net

The primary focus of Nephro Net is to provide a forum to exchange information between patients and healthcare professionals in the domain of Nephrology. The authors made Nephro Net only for exchanging information regarding kidney related problems. Consequently, every message posted on the network will be monitored by administrators. Though it is a time consuming task, the authors strongly believe that a focused healthcare network will serve the community much better and will be easier to manage and administer, than a general purpose healthcare network such as PatientsLikeMe [3]. This belief is also justified by a recent survey conducted by Massachusetts Medical Society[12].

Users of Nephro Net can post messages by creating and/or participating in one of the three types of postings - *dissemination*, *discussion* and *consultation*. A posting refers to a structure that contains a type, a topic, the creator's identification and one or more messages (ordered on date/time of creation of these messages). A topic includes a title (user for listing and searching

purposes) and a description (explaining the purpose of the topic and what is expected from the messages posted under this topic). Each topic has a unique internal identifier which is not visible to the users. Hence, a user may see the same title for different topics but they are differentiated by the creator, and the date and time of creation of the topic. A typical example of a posting is the following:

> Type: Dissemination
> Creator: John Doe
> Time stamp: Oct 20, 2018 12:34 P.M.
> Topic: Hepatitis C and CKD
> Description: Impact of Hepatitis C on CKD patients
> Message: "NEW!! ©goKDIGO Clinical Practice Guideline Update on Hepatitis C in CKD now available - posted on September 23, 2018 6:20 AM."

A user may be able to browse through the postings and read the messages under a selected topic. The three types of postings are described in detail below:

Dissemination A dissemination can be created by a patient or a physician. The purpose of a dissemination posting is to share an information that deemed to be useful for other users. It is similar to posting something on a message board in a work place. Every dissemination posting, when created, needs to be approved by an administrator before it is actually posted on Nephro Net. Since no further response is expected for a dissemination posting, there is only one message posted under its topic.

Discussion A discussion posting can be created by a patient or a physician. It is meant for exchanging information among several users of Nephro Net, discussing a particular issue or problem. For example, a patient may want to discuss the side effects of one of the medications that he/she takes. So this patient opens up a discussion posting under a topic "Side effects of non-steroidal anti-inflammatory drugs for patients on hemodialysis." Like dissemination posting, a discussion posting must also be approved by an administrator before it is visible to other users. Once approved, any user of Nephro Net can search for the topic of discussion and can also join the discussion by posting messages under the same topic. However, every message in a discussion must be approved by an administrator.

Messages may also include images. It is expected that the users participating in a discussion will only post messages that are relevant to the topic and are useful to other users. If any message seems to be irrelevant to the current topic of discussion, any user can send a complaint on that particular message. Several users may complain about the same irrelevant message. An administrator, after reviewing the complaint(s), will decide whether to keep or remove that message.

During a discussion, the creator of a message can remove the message at any time; an administrator also has the freedom to remove a message.

Only administrators have the ability to terminate a discussion. A discussion, after termination, is still accessible by other users when they search for the topic. However, no new messages can be added to that topic. An administrator may decide to remove the discussion at any time after the discussion is terminated. Administrators will archive removed discussions at their own convenience. If a user asks for that discussion, an administrator can reload the discussion again so that the corresponding topic and its associated messages will appear when searching.

Consultation Nephro net also provides a mechanism for personal consultation between a patient and a healthcare professional. A consultation is similar in structure to a discussion but is restricted to only two participants. To start with, a patient who wishes to consult with a physician must create a consultation posting (just like creating a new discussion, but must indicate the intention for private consultation.) The posting will already include the identification of both the patient and the physician. An administrator should approve the topic and the consultation. Once approved, both participants will post messages through Nephro Net, just like in any other discussion. However, neither the consultation topic nor its associated messages will be visible to any other user of Nephro Net. Administrators may be able to view the topic of a consultation, but will not be able to view its messages. These messages will be encrypted to ensure privacy. The patient who created the consultation is the only user who can terminate the consultation. After termination, either one of the participants can search for the topic and/or the messages of the consultation at any time later but will not be able to post any new messages.

4.1 Short and Complete Profiles

In order to ensure close monitoring of messages, Nephro Net is expected to be launched within an organization (such as a hospital or clinic) instead of making it available for general public. A user of Nephro Net may be able to find the credibility of another user by reviewing the short profile of that user. For example, a patient may want to check the credibility of a physician before launching a consultation with the physician. A short profile of a user will contain name(s), demographic information and some additional information (e.g., specialty of a physician) of that user. The information for short profile will be extracted from the organization's database during registration. Consequently, a new user, while registering with Nephro Net, is expected to provide his/her identification in the organization's database using which Nephro Net will extract information for short profile.

A user can also create a (separate) complete profile. For a patient, this complete profile may include personal and health related information. The complete profile of a physician may include the current cases he/she is working on, places where he/she worked before and interests of the physician. A complete profile is password protected. That is, when a user creates a complete profile, Nephro Net asks the user to set a password which will be stored along with the profile. This password may be different from the user's login password, but it is encrypted and stored in the same way as the login password. If a password is set for a complete profile, then every access to the profile, even for the creator, requires authentication using this password.

In order to ensure privacy, it is highly recommended that Nephro Net users handle complete profiles very carefully and give access to other users only when it is absolutely necessary. For example, a patient may give access to his/her complete profile during a consultation with a physician. It is recommended that the patient changes the password for the profile after the consultation is terminated.

4.2 Administrative tasks

There can be one or more administrators in Nephro Net. When installed for the first time, Nephro Net will come up with a default administrator account. Thereafter, new administrator accounts can be created through the same registration process as any other user (patient or physician). An administrator is also required to use the three-piece authentication process to login into Nephro Net, described earlier. The following is a list of tasks that an administrator could perform in Nephro Net:

- Approve/deny new user registration.
- Approve/deny creation of new posting.
- Approve/deny a message posted under discussion. The only one message under dissemination posting is approved along with the approval of the posting itself.
- Review complaints against a posted message in a discussion.
- Remove an irrelevant message posted under a discussion.
- Terminate a discussion.
- Remove a discussion and archive it.
- Reload a discussion.

5 Conclusion and Future Work

This manuscript describes the design and implementation of a healthcare network called Nephro Net with more emphasis on its security and privacy aspects. As indicated by the survey published by Massachusetts Medical Society[12], the authors were motivated to create a healthcare network for a specific purpose (in this case, Nephrology).

Though Nephro Net has been designed for patients and physicians in the domain of Nephrology, the design is somewhat generic so that it can be easily tailored to other health domains such as Family Medicine, Psychiatry, Gynecology and so on. Current design of Nephro Net enforces strict monitoring of messages by administrators so that every message floating around the network should be approved by an administrator. In order to ease posting of messages and faster responses in discussion postings, this restriction could be relaxed. However, such relaxation can make Nephro Net like any other social network. An alternate solution for this problem is to automate the approval of a message by the administrators. The authors have planned this as one of the immediate future work of Nephro Net. Administrators can still monitor messages and remove them if they deemed irrelevant. Verification of credibility of a user by an administrator depends on the data collected during the registration process.

As with any social network, Nephro Net also expects its users hold ethical responsibilities of proper usage of the network. For example, a patient can reveal his/her complete profile to another user by giving the password associated with the profile. Sometimes patients may do this during consultation. However, care must be taken by the patient himself/herself to reset the password after it was viewed by another user. Similarly, a physician is expected not to misuse a patient's personal and/or health information obtained during consultation. Raus and others[11] discusses such ethical responsibilities, particularly by patients when using healthcare networks.

Currently, Nephro Net supports three types of users - patients, physicians, administrators. The type 'Physician' can be generalized into 'Healthcare providers' to accommodate other types of healthcare service providers such as nurses and physician assistants. However, in practice, the roles of these healthcare providers vary and hence additional features need to be implemented to guarantee adequate security and privacy of healthcare information.

Generally, security aspects involve Confidentiality, Integrity and Availability. It is also known as the CIA triad. This paper focuses more on confidentiality of information. Due to lack of time, the other two security aspects have not been addressed. Future versions of Nephro Net will address those aspects as well.

6 Acknowledgments

The authors wish to express their sincere thanks to Dr. Venkateshwaran Iyer, M.D., Nephrology, Mayo Clinic, La Crosse, Wisconsin for his valuable guidance to this project. Almost all information related to Nephrology reported in this manuscript was discussed with him. He also provided help in identifying HIPAA regulations during the implementation.

References

[1] Doximity - a healthcare network. https://www.doximity.com, 2018. Online; accessed on Oct 10, 2018.

[2] Mercy health network. https://www.mercyhealthnetwork.com, 2018. Online; accessed on Oct 10, 2018.

[3] Patients like me - a healthcare network. https://www.patientslikeme.com, 2018. Online; accessed on October 01, 2018.

[4] Quantiamd. https://en.wikipedia.org/wiki/QuantiaMD, 2018. Online; accessed on Oct 10, 2018.

[5] Sermo - talk real world medicine. https://www.sermo.com, 2018. Online; accessed on Oct 10, 2018.

[6] Triad healthcare network. https://www.triadhealthcarenetwork.com, 2018. Online; accessed on Oct 10, 2018.

[7] Frances Griffiths et al. Social networks - the future for health care delivery. *Social Science & Medicine*, 75:2233 – 2241, 2012.

[8] L. Fass. Patient-centric healthcare. In *3rd IET International Conference on Medical Electrical Devices and Technology (MEDTECH 2007)*, pages 77–109, London, UK, 2-3 October 2007.

[9] Jingquan Li. Privacy policies for health social networking sites. *Journal of the American Medical Informatics Association*, 20:704–707, 2013.

[10] S. Anne Moorhead. Social media for healthcare communication. *Oxford Research Encyclopedia of Communication*, August 2017.

[11] Kasper Raus, Eric Mortier, and Kristof Eeckloo. The patient perspective in health care networks. 19, 2018.

[12] Kevin G. Volpp and Namita S. Mohta. Patient engagement survey: Social networks to improve patient health. *NEJM Catalyst*, November 2017.