Strengthening Privacy in Healthcare Social Networks

Bertsima Maria[1], Iraklis Varlamis[1], Panagiotis Rizomiliotis[1,2]

itp13307@hua.gr, prizomil@aegean.gr, varlamis@hua.gr

[1]Harokopio University of Athens , Department of Informatics and Telematics

[2]University of the Aegean , Department of Information and Communication Systems Engineering

Abstract

The purpose of this chapter is to present a comprehensive approach to the problem of privacy protection in healthcare social networks, to summarize threats and suggest emerging technological solutions to protect users. For this purpose we start with a definition of the term "privacy" and how it evolved through time. We continue within the context of social networks and highlight the main privacy issues and threats for network members. On the other side, we summarize the privacy requirements and provide suggestions that may enhance privacy in online healthcare networks.

1. Introduction

Privacy as a concept has been studied in depth by researchers from different disciplines such as philosophy, social sciences and law, but yet has not a commonly accepted definition. The American judges Warren and Brandeis (1890) in their article entitled "The Right to Privacy" provided one of the oldest and most popular definitions of privacy as a person’s “right to be left alone". Alan Westin in his "Privacy and Freedom" book (1967) gave the following more comprehensive definition of privacy: "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."

Originally the term *privacy* was coined to the protection of the home and in general the physical space surrounding a person. When mail first appeared as a means of communication, the first mail privacy violation phenomena were recorded as early as 1624. The advent of mass media in the dawn of 1900, in conjunction with inventions such as photography and telephone resulted in the first incidents of breaches in private life and phone conversations. In the second half of the 20th century, the appearance of personal computers and computer networks gave a rise to concerns about privacy issues and turned focus to data collection and processing (Holvast, 2009). It becomes obvious that depending on the data communication, collection, storage and processing methods that existed in every era, respective mechanisms have been developed for violating the privacy of individuals. Thus, the need for privacy has created the need for legislative mechanisms for protection.

Privacy has been included in the Universal Declaration of Human Rights issued by the United Nations in 1948. According to Article 12 of the Declaration:

> *"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."*

Finally, according to Articles 7 and 8 of the Charter of Fundamental EU rights:

"*Everyone has the right to respect for his or her private and family life, home and communications*" and "*the right to the protection of personal data concerning him or her*". "*Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified*". "*Compliance with these rules shall be subject to control by an independent authority*".

Although privacy cannot be restricted only to personal data, since it refers to the general "right to solitude and withdrawal" (Mitrou, 2010), the prevention from "unauthorized use or disclosure of data" (Dies, 2010) became the main objective of privacy protection devotees. A healthcare network allows its members such as doctors, patients and caregivers to communicate and collaborate in order to virtually manage the illnesses and improve the quality of patients' life. The virtual environment removes distance and time barriers, enables patients to submit online requests for advice and share problems and solutions with other patients and facilitates doctors to cooperate with each other and supervise their patients. However, in order for the healthcare network to thrive, its members need to share their personal and sensitive data with other members and, thus, must be confident for the secure, reliable and lawful operation of the network.

The aim of this chapter is to define the limits of privacy in health focused social networks, highlight the privacy issues that arise in such networks and the potential threats for their members. Through this study, we aim to summarize the privacy requirements and provide some hints that may enhance privacy in health related social networks.

In Section 2, we provide a brief introduction to online social networks and focus on health focused online networks. Section 3 gives a background on privacy and highlights the main privacy issues and threats for online healthcare networks and applications. In Section 4, we summarize the privacy requirements and in Section 5, we provide suggestions that may enhance privacy in online healthcare networks. Finally, Section 6 contains references to specific healthcare social networks and applications and discusses their current status in terms of privacy preservation.

2. Social Networks

The term social network was invented in 1954 by LSE's Professor JA Barnes (Barnes 1954) who examines social relationships in a Norwegian fishing village, concluding that the entire social life of the village could be represented as "a set of points, some of which are connected by lines", to finally form a "comprehensive network" of relations.

2.1. Online Social Networks

Recently, the advent of the so-called social networking sites attracted a large number of users and brought the concept of “online social networks” in light. The definition given by Boyd and Ellison (2008), clearly defines the assets of a user that joins an online social network:

> *“social network sites are web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system.”*

As a result, when users join an online social network, such as Facebook, Twitter, LinkedIn, Google+ etc. to mention some of them, they are invited to fill their profile page by providing a range of personal information, then encouraged to create digital relationships with other members of the network who either already know or want to know and finally, are asked to maintain these relationships. As a result, they agree to share profile and connections with other (selected) users.

In a broader definition, given by the European Agency for Information Systems Security (ENISA) (Hogben, 2009), online social networks are defined as federated identity management spaces, where users: a) store and manage personal data, b) control access to them based on credentials, c) are able to find out who has accessed their personal data.

2.2. Healthcare Social Networks

In a general context, we could say that social networks can take different forms, depending on the purpose they serve. Although general purpose social networks are the most popular among them, we can also find professional (business) networks, network that relate to health (healthcare), and others that are designed with ethnic, religious or political criteria (Zilpelwar et al., 2012). Healthcare professionals use traditional social media networks to connect with others, but also 1 out of 3 joins social networks which are exclusively focused on healthcare[1].

Gunther Eysenbach used the terms "infodemiology" and "infoveillance", in order to describe a new emerging approach for public health (Eysenbach, 2011), based on large-scale monitoring and data mining of information published in (health and general purpose) social networks. Health focused social networks allow their members such as doctors, patients and caregivers to communicate and collaborate in order to manage the illnesses and improve the quality of patients' life. The online environment removes distance and time barriers, enables patients to submit online requests for advice and share problems and solutions with other patients and facilitates doctors to cooperate with each other and supervise their patients. In analogy to social networks, users in online healthcare networks must be ready to share their personal data, which in this case are sensitive health data, with other network members.

In order for the healthcare network to thrive, members need to trust each other and be confident for the secure, reliable and lawful operation of the network (Chryssanthou et al 2011). Online healthcare networks have some unique characteristics, which make the aforementioned targets hard to accomplish. They cross national borders and operate in a continuous basis; they are responsible for securing members' medical data and are entrusted to preserve members' anonymity. At the same time, they must guarantee the reliability of both participating members and submitted content. Under these circumstances, the smooth operation of such social networks is a heavy duty for moderators and administrators.

The concept of privacy is strongly connected to the (social and technological) trust of users to the network and the application provider. Users are willing to upload their data to the online healthcare application, only when they are completely confident about the correct use of their data, from the authorized people and for the appropriate purpose. According to the study of Damschroder et al (2007) patients are positive in sharing their medical data with experts only when they trust that they will be kept private and confidential in a way that patients can see and understand; when clear and

[1] Infographic provided by MEdTech Media at: http://www.medtechmedia.com/files/medtech_images/Infographic_SOCIAL_MEDIA_SURVEY_AMN_HEALTHCARE.jpg

consistent consequences exist for privacy violations and when the computerized systems are proven to be highly secure.

3. Privacy

3.1 Privacy - Background

Nowadays, the use of Internet has enabled the instant diffusion of information and has transformed the online social networks to repositories, where personal data is collected, enriched, modified, shared and reused continuously (Robinson et al., 2009). Consequently, the concept of privacy has been transformed from one’s "right to be left alone" to the ability of social network users “to control and protect personal information” (Stuart, 2007).

According to Rosenberg (1992) privacy can be: a) territorial, when it refers to the physical space of an individual, b) personal, when it protects the individual from unwanted interventions, c) informational privacy, when it defines how personal data are collected, stored and processed and who can gain or grant access to.

A more recent approach by Finn et al (2013) distinguishes 7 types of privacy:

1. The privacy of the person
2. The privacy of behavior and action
3. The privacy of data and image
4. The privacy of communication
5. The privacy of thought and feelings
6. The privacy of space and location
7. The privacy of association and group privacy

In the case of online healthcare networks, users share their medical records in order to receive medical advices from experts, to monitor the progress of their health etc. In this context, users reveal their data to specific users (e.g. their doctors) and hide them from others (for example for insurance companies or their employers). Revealing medical data could also reveal medical or psychological conditions, treatments or other details about personal life. Privacy in healthcare networks may comprise control over personal information (informational privacy), physical restriction to data accessibility (physical security) and the respect of the doctor to patients' beliefs, thoughts, values and feelings (psychological security - confidentiality) (Serenko & Fan, 2013).

Personal and sensitive data

"Personal data" and "sensitive data" are the two main assets of HSN users, which must be protected or controlled within a privacy context.

According to the European Data Protection Supervisor (EDPS) Glossary and Article 2 (a) of Regulation (EC) No 45/2001 the term "***personal data***" may refer to "*any information relating to an identified or identifiable natural person (referred to as "data subject"), in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity*".

The name and the social security number are two examples of personal data which relate directly to a person. But the definition also extends further and also encompasses for instance e-mail addresses and the office phone number of an employee. Other examples of personal data can be physical characteristics, education, labor, economic status, interests, activities, habits or any other information found in the medical records of a patient or in the evaluation report of an employee.

The term "***sensitive data***" is coined with "information that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, membership of a trade union, health status, social welfare, erotic life preferences, prosecutions and convictions etc. (Article 10 of Regulation 45/2001; Article 8 of Directive 95/46/EC). Usually, sensitive personal data are legally protected by more stringent regulations than simple personal data. The processing of such information is in principle prohibited, except in specific circumstances. It is possible to process sensitive data for instance if the processing is necessary for the purpose of medical diagnosis, or with specific safeguards in the field of employment law, or with explicit consent of the data subject.

Privacy and personal data

Privacy is a broader concept than personal data protection since the former includes also "the right to be left alone, out of public view, and in control of information about oneself”. However, personal data protection arises as a necessity to ensure privacy and therefore constitutes a part of the privacy concept. As a result, personal data protection is a prerequisite for guaranteeing privacy against potential technological threats.

3.3. Privacy Issues in HSNs

The practices used by social networking sites like Facebook, Twitter or Instagram and the various stories concerning privacy violations in such networks, make health social network members skeptical about sharing personal data, or even posting questions. However, they are prone to share data on specialized sites, with a transparent security and privacy policy and healthcare professionals that they can trust.

The protection from unauthorized access is the only action that assists in personal data protection. However, more principles must be guaranteed in order to achieve govern the protection of personal data. In this context, the Organisation for Economic Co-operation and Development (OECD) defined in 1980 the principles that must govern privacy protection and personal data exchange across countries. These principles are:

- Collection Limitation Principle: The collection of personal data should be made using fair and lawful means, and - where possible - with the consent f the data subject.
- Data Quality Principle: Personal data should be relevant to the purpose for which they are to be used and depending on the extent necessary for this purpose should be complete, accurate and updated.
- Purpose Specification Principle: The purposes for which personal data are collected should be specified before data collection and any subsequent use must be limited to the fulfillment of those objectives or some fully compatible objectives.

- Use Limitation Principle: Personal data will not be communicated and made available to third parties or used for purposes other than specified, unless the data subject agrees or the law authorizes such changes.
- Security Safeguards Principle: Personal data should be protected using appropriate mechanisms against risks such as unauthorized access, destruction, use, modification or disclosure to third party entities.
- Openness Principle: There should be a general openness policy regarding the practices that relate to the collection and processing of personal data and the identity of the body performing the collection and processing.
- Individual Participation Principle: Each person should have the right to:

  a. Receive a confirmation from the data controller administrator that person related data are in the data controller's possession.

  b. Receive information on the data that is of interest to him/her in a reasonable time limit, in an understandable manner and low price (if any).

  c. Be informed for the reasons that he/she cannot have a and b above and argue, question and further claim these rights.

  d. Correct or delete personal data.
- Accountability Principle: Any personal data controller should be accountable regarding the implementation of those measures that promote the aforementioned principles, which should govern the protection of personal data.

It is worth noting that the definition of the above principles was a first step towards establishing rules for the management of personal data and has influenced the legislation that currently governs the protection of personal data. The above principles highlight the strong connection between the concepts of privacy and protection of personal data.

3.2. Privacy Threats

According to ENISA (Hogben, 2007) the risks for social network users can be categorized as follows: a) privacy related threats, b) traditional risks of internet embrace the environment of social networks (SNS variants of traditional network and information security threats), c) risks associated with the user ID (Identity related threats) and d) social risks (social threats).

The most important threats for privacy, under the prism of healthcare social networks are discussed in detail in the following.

Digital Dossier Aggregation

Online social networks are an ideal source for user profile information. Modern technology enables the automated aggregation of user profiles data and the storage of all traces in order to create a digital user dossier. Such data can be used for purposes other than those for which the user intended, or may take different meaning outside the initial social network context. More specifically, users publish to healthcare social networks information, which is intended for a specific audience and may prove embarrassing for them when it goes outside this audience.

Difficulty of Complete Account Deletion

When a user leaves the social network, he/she usually wants to delete the profile data and any other digital traces or to be able to take them offline. However, network providers cannot always guarantee that all traces are completely erased (Hogben, 2007). For example, even when data are delete from the user profile, other data such as messages or comments exchanged with other users is not removed from the pages of those users. In general, there is ambiguity about whether indeed the user information in social networks is permanently deleted or if copies of user data are kept in storage. Social networking companies are interested in collecting such information, because it enables them to create data warehouses from which they can derive significant economic benefits.

Secondary Data Collection

In secondary data collection, the attacker collects information about users of a social networking site using secondary sources rather than the network itself. Specifically, the attacker uses sources (e.g. search engines) outside the social network for the collection of data on a user and then linking these data with the profile of that user. In this way, the attacker is able to gather the maximum information about the user by any available Internet sources. Such techniques can be applied in cases where users keep their profiles private. Then through secondary data collection, the person concerned can collect all possible information from other internet sources (Cutillo, 2012).

De-Anonymization Attacks

In many social networking sites, especially in health focused sites, users want to protect their privacy and their anonymity by using virtual identities. At the same time, they upload personal data, which if are properly collected, analysed and combined with information from other sites (Krishnamurthy & Wills, 2009) may reveal the true user identity. De-anonymization attacks aim to reveal user identities and expose them to the members of the network or to the public. The ideas of Rowe & Ciravegna (2008) for identity disambiguation can be easily reversely used by an attacker in order to match user's profiles across different networks and construct a complete user profile. A weak point that attackers exploit in order to connect information from different networks and reveal user's identity are bugs in the browser monitoring mechanisms, such as cookies and history. Malicious sites, with simple Javascript code can easily retrieve history information from popular browsers (history-sniffing) when a user visits them (Eckersley, 2010). In their research, Wondracek et al. (2010) used a similar history stealing technique from the user's browser and managed to de-anonymize correctly 42% (unique fingerprint) of the targeted users, when a social network user visits a malicious website.

Inference Attacks

Under the umbrella of identity exposure, we can also put the inference attacks. These attacks employ data mining techniques and data from within and outside the network in order to infer and consequently reveal parts of a user identity (e.g. sex, age, habits, preferences, etc.).

Identity Theft

Through identity theft, an attacker can gain access to user accounts and profiles and consequently to their contacts and communications (Zilpelwar et al., 2012). This can possibly harm the reputation or credibility of the real owner's profile while he/she is unaware of the attack. The attacker can simply pretend that he/she is the owner of the profile and use it to communicate with potential "victims" (e.g. pretend to be a doctor and give false advices to patients). The identity theft is rarely due to technical reasons and is mainly due to user ignorance about security precautions (Cutillo, 2012). A similar threat to Identity Theft is Profile Cloning, where a user clones the profile and mimics another user in order to gain access to his/her social connections.

Phishing

The "phishing" is an act of deception, where the attacker impersonates a trusted entity, to acquire personal information such as sensitive private data and codes. Recently, such attacks on social networks have grown rapidly. According to Microsoft Security Intelligence an 84.5% of all phishing attacks target social networks users (Fire et al., 2014).
The latest development in phishing techniques is the technique and spear phishing is a highly targeted attack "phishing". The huge amount of personal information available on social networks allows the perpetrator of such an attack to collect reliable information on his victims and then to

cheat by sending them an e-mail, which appears to come from someone other. Experiment conducted by the Indiana University showed that phishing attacks via e-mail and by collecting data from social networks have been successful in 72% of cases (Hogben, 2007).

Communication Tracking

In the past, health care was managed mainly via interpersonal communication between the caregiver and the patient, while today, social media offers different modes of interaction. Recent studies in Internet-delivered therapy, especially for issues such as anxiety and depression show that online communication is more effective in alleviating mild to moderate symptoms than other methods of searching for health advice online (Glozier et al, 2013). This is expected to further increase the amount of doctor-patient communication data in the near future.

Communication tracking is a privacy threat that targets mainly the information that users exchange in their everyday communication within the network. By monitoring users' communications the attacker manages to collect much more information than is available in their profile. This attack can also be performed by automatically traversing all user comments in a social network.

Information Leakage

Social network members exchange information with their friends and other network members and frequently voluntarily share sensitive data. In a survey with 166 participants, Torabi and Beznosov (2013) observed that 95.8% of users had shared some health data through their personal accounts on social networks. Such practices by users of social networks can result in the leakage of sensitive personal data.

Dossia, Microsoft HealthVault and Google Health in the past, provide personal health record management services, and allowed users to store medical information as well as personal information on their central servers. Although they publish a privacy policy, these policies do not include confidentiality towards the provider and they do not allow patients to check whether the provider complies with their privacy policy. Information leakage incidents may due to several reasons:

a. improper and incomplete privacy settings by the data owner. In several cases, it becomes very complicated for the user to define his/her own privacy settings, and the predefined privacy policies set by the application provider are not adequate to cover all issues.
b. unauthorised access by third-party applications. Especially, when multiple applications in the cloud can gain access to a user profile or settings, there is always a risk for these applications to ask for more privileges than necessary, or to take advantage of their privileges for wrong purpose.

In order to conclude this long list of privacy threats for the users of social networks, we must add the results of an ENISA report on the top rising risks for social networks. According to this report the top risks comprise: malicious software, information leakage, phishing, spam, identity theft.

4. Privacy Requirements for HSNs

The Evolution of Privacy in Healthcare

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) recognized the possible threat to privacy from the electronic data exchange in healthcare. HIPAA mandated the U.S. Department of Health and Human Services (HHS) to develop regulations that protect privacy and security of electronically-transmitted health information. In 2000, HHS created a set of rules known as the Privacy Rule, which sets a framework for handling medical records and other sensitive personal health information. Privacy Rule defines safeguards, uses and disclosures and patient authorizations and provides patients with certain rights over their health information. In order to be properly applied, the Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of sensitive electronic health information. However, both HIPAA Privacy and Security Rules are the designed to establish minimum standards for the purpose of setting the “legal floor.”

Privacy as system requirement

In order to transform privacy from a general concept to a technical requirement included in information systems development, we need of a set of specific requirements which are known as privacy requirements (Kalloniatis et al, 2014). According to the Common Criteria for Information Technology Security Evaluation standard (CC) these requirements are:

- Anonymity: the state of a subject being non-identifiable within a set of subjects,
- Pseudonymity: the state of using a pseudonym as ID.
- Unlinkability: defined for two or more items, unlinkability assumes that within the system, these items are no more and no less related than they are related concerning the a priori knowledge.
- Unobservability: the state of an item of interest being indistinguishable from any other item of interest.

With all the aforementioned requirements in mind, which are formally defined in (Pfitzmann & Hansen, 2010), privacy can be defined as a set of technical requirements which prevent the disclosure of the identity of a user (Yanes, 2014). Additional requirements may comprise:

- Authentication
- Authorization
- Identification
- Data Protection

5. Enhancing Privacy in OSNs & HSNs

Privacy enhancing technologies, comprise the tools, applications and devices designed to protect personal data and assist Internet users in maintaining their privacy and anonymity. They can also be considered as a series of measures that protect privacy by eliminating or minimizing, unnecessary or undesirable processing personal data without loss of functionality of the information system (Van Blarkom et al, 2003). In particular, privacy enhancing technologies provide the following options:

- They allow to minimize or eliminate disclosure, and collection of personal data or user identification data.
- They give users the possibility to carry out transactions without disclosing their identity.
- They allow users to exercise control over their personal data.
- They assist companies and organizations to implement policies and practices for privacy protection.

Privacy enhancing technologies have been categorised in the past using different classification schemes. The criteria for categorizing PETs can be the purpose they serve (e.g. minimization of disclosure and collection of personal data) or the technology they use to protect privacy (e.g. anonymisation, encryption, etc.).

According to ***FIDIS*** (Future of Identity in the Information Society) project classification PET tools are divided to ***transparency*** and ***opacity tools*** (Fritsch, 2007). The former aim at increasing users' awareness of the processes and practices that are followed when their personal data are processed and at helping them understand the potential consequences of data processing. Database audit interfaces, audit agents and log files are some example of transparency tools. Opacity tools aim at concealing the identity of users or to prevent linkage between users and data. Examples are MixMaster anonymous e-mail, TOR anonymizing web surfing, Pseudonyms etc.

The ***Meta Group survey*** (2005) performed on behalf of the Danish government divides PETs into two main categories. The first category concerns privacy protection and the second privacy management. More specifically, the first category includes tools and technologies directly are involved in the protection of privacy by concealing information or eliminating the need for personalization of information, while the second includes tools that support the management of privacy rules.

According to the same survey, the purpose of PETs is to cover the four main requirements for privacy mentioned in Section 4 (i.e. unobservability, unlinkability, anonymity and pseudonymity). In addition, they provide secondary tools (e.g. tools for addressing spam, undesired Web content or even unauthorized programs such as spyware, virus) and informational tools which assists users in understanding privacy issues. The long list of such tools comprises amongst others:

- Privacy Protection tools such as: Pseudonymizer Tools, Anonymizer Products and Services, Encryption Tools, Filters and Blockers, Track and Evidence Erasers.
- Privacy Management tools such as: Information and Administrative Tools.

In a classification provided by Koom et al (2004) in the book “Privacy Enhancing Technologies - White Paper for Decision Makers" PETs are grouped into:

- General: includes encryption tools, logical access, biometrics etc
- Separation of data: separates the processing of data that identify a person from all other data, in order to avoid cross linking,
- Anonymization tools: e.g. MIX routers, Onion routers, cookie management tools etc
- Privacy management systems: automatic enforcement of security policies and compliance control tools, such as P3P (Platform for Privacy Preferences Project).

Finally, the technical report of Shen and Pearson (2011) classifies PETs into five categories as follows:

- PETs for anonymization
- PETs to protect network invasion
- PETs for identity management
- PETs for data processing
- Policy-checking PETs

Privacy enhancement solutions comprise data filtering and minimization, anonymization, adding noise to disclose information etc. In metadata approaches, privacy policies are injected in the form of privacy rules that control access to data from different applications. HL7 is working on a flexible standard that applies privacy and security labels to segments of user personal data (HL7, 2010).

According to a white-paper issued by the Healthcare Information and Management Systems Society (HIMSS) about Privacy & Security Considerations from the use of Social Media in Healthcare (HIMSS, 2013), privacy in health related social media and social networks is achieved through a multi-step approach which comprises the following actions:

- Perform a social media risk assessment
- Develop an overarching, risk-based social media strategy consistent with organizational goals and objectives
- Define a strategy to protect the organization's online reputation and brand from harm
- Develop social media policies and procedures
- Educate staff and volunteers
- Minimize regulatory and other legal/liability risks
- Proactively monitor social media for compliance

Yeratziotis et al (2012) claim that security and privacy do not come alone in healthcare social networks. According to the authors, it is vital that the development of security and privacy features for applications and websites are assessed for their usability, which will consequently increase the continuous and effective utilisation of the provided services. Authors propose a framework that consists of three components: a three-phase process, a validation tool and a usable security heuristic evaluation and propose a list of items that must be checked to ensure usable security and privacy. The list comprises user awareness about security and privacy issues, user control on the privacy and security restrictions and different levels of configuration details depending on the user expertise.

In this line, the concept of Privacy by Design is gaining attention in the design of HSNs. It is a systems engineering approach that it was developed by the former Information and Privacy Commissioner of Ontario, Dr. Ann Cavoukian, back in the 90's and it aims to encourage system designers to take privacy into account throughout the whole engineering process.

Privacy by Design was initially expressed by deploying PETs. However, after several years of unsuccessful experimentation, it is clear that a more substantial approach is required. Privacy cannot and must not be an add-on, but it must be embedded into the design of the HSN.

Ann Cavoukian has indentified 7 Foundational Principles that must be practiced in order to achieve the Privacy by Design objectives and that the architects and operators of HSN must follow. Namely,

1. Proactive not Reactive; Preventative not Remedial: Privacy by Design anticipates and prevents privacy-invasive events before they happen. It aims to prevent them from occurring.
2. Privacy as the Default Setting: Privacy must be the default state of the system. No action must be required on the part of the individual.
3. Privacy Embedded into Design: Privacy is not an add-on. It must be embedded into the design and architecture of IT systems.
4. Full Functionality – Positive-Sum, not Zero-Sum: Privacy by Design avoids trade-offs between design goals. For instance it demonstrates that both privacy and security are possible.
5. End-to-End Security – Full Lifecycle Protection: Privacy by Design seeks to protect data throughout their entire lifecycle of the data, i.e. at the end of the process, all data are securely destroyed.
6. Visibility and Transparency – Keep it Open: Privacy by Design gives the opportunity to verify the efficiency of the privacy protection mechanism through transparency.
7. Respect for User Privacy – Keep it User-Centric: Privacy by Design requires the system designers to keep the interests of the user uppermost.

6. Online Social Networks in the Healthcare Domain

Health focused social networks and user communities can be build on top of existing social networking applications or on new platforms, which are designed on purpose. The survey work of Grajales et al. (2014) provides a good summary of social networking applications that host health focused networks. More specifically, authors analyse different categories of social media which have been used by healthcare professionals, patients and researchers, such as: (1) blogs (e.g. WordPress), (2) microblogs (e.g. Twitter), (3) social networking sites (e.g. Facebook), (4) professional networking sites (e.g. LinkedIn), (5) wikis (e.g. Wikipedia), (6) collaborative filtering sites (e.g. Digg), (7) media sharing sites (e.g. YouTube, Slideshare), and (8) 3-D virtual worlds (e.g. SecondLife). They also examine thematic networking sites (e.g. 23andMe) and application mashups (e.g. HealthMap).

Healthcare requires privacy and anonymity, making traditional social media sites such as Facebook and Twitter inadequate in sharing health data or personal health experiences. This is where platforms designed specifically for supporting health related social networks come in to the scene.

Advice seeking networks

Patients, on the other side, access specialized social networks which focus on healthcare subjects - especially on specific diseases, research and support around them. In such networks, they are encouraged to connect with other patients, share their stories, and get informed about their disease.

CureDiva[2], is a social network and online e-shop, targeting breast cancer patients. It has a privacy mechanism, which allows members to choose their preferred level of privacy on personal content. The network creates a personalized experience for its members in order to increase their comfort.

MedHelp[3] is a social media site that aims in consumer health engagement. It has 13 million active monthly users, over 200 condition-specific communities and provides expert forums for the health professionals to answer the questions from health consumers directly. It offers community forums and expert blogs and a data platform for consumers to gather data from mobile apps, web apps, and health devices.

E-couch[4] is an online communication tool, which provides several self-help interactive programs that allows patients with depression, generalised anxiety & worry, social anxiety, relationship breakdown, and loss & grief to contact experts and ask for their support.

Patient communities

[2] https://www.curediva.com/

[3] http://MedHelp.org

[4] https://ecouch.anu.edu.au

ConnectedLiving[5] is a private social network, which interconnects residents of nursing homes, assisted living complexes, and other senior housing centers and aim in creating a community of seniors, which are currently the most disconnected part of the population. Network-members form friendship bonds with their real-world friends within the social network and in the same time can grant access to external social networks contents such as the members' profile in Instagram of Facebook.

The popularity of smartphones and the emerge of mobile health gave rise to data intensive applications and networks where patients perform self-tracking and share their data with doctors and the community. Self-trackers are using applications to monitor sleep, food intake, exercise, blood sugar and other physiological states and behaviors. Patients use the data in order to receive alerts for their health, physicians suggest these solutions to patients so that they can have real-time feedback on the results of a treatment and be able to adjust therapies faster (Swan, 2009). ***PatientsLikeMe***[6]***, Smart Patients***[7]***, FacetoFaceHealth***[8] are a few out of many online social networks where patients share their experience using patient-reported outcomes, find other patients like them matched on demographic and clinical characteristics, and learn from others to improve their way of living. The goal of such websites is to help patients answer the question: "Given my status, what is the best outcome I can hope to achieve, and how do I get there?" (Wicks et al 2010).

Professional networks

Sermo[9] is the most popular social network for doctors, which however, limits its membership to US-based doctors. ***NurseTogether***[10] is a similar professional networking community for nurses. ***Doximity***[11] is a professional social network for doctors only, founded in 2010, which resembles more

[5] http://www.connectedliving.com/

[6] https://www.patientslikeme.com/

[7] https://www.smartpatients.com/

[8] www.facetofacehealth.com

[9] http://sermo.com/

[10] http://www.nursetogether.com/

[11] https://www.doximity.com/

to LinkedIn than Facebook. In contrast to Sermo that allows anonymous postings, Doximity insists on real names. Membership is validated by DEA number, which guarantees the true identity of a member. The two networks have very different styles, since Sermo focuses more on discussion forums, while Doximity emphasizes professional networking and private messaging. In this direction, Doximity members have the ability to selectively share contact information (e.g. cellphone number) with other members.

Each network type poses different challenges in terms of meeting the privacy requirements. A comprehensive study of the controls needed in order to achieve each requirement for such network types must follow in order to ensure privacy for all types of networks. One of the main challenges that need to be further addressed is the conflict between legal restrictions, human privacy restrictions and the need for immediate access to a patient's data when his health is in danger.

7. Conclusions

The use of Social networks and social media from patients and doctors, for health related issues hides several privacy threats and risks, which must be properly addressed due to the sensitive nature of patient information.
Indicative types of social networks for health include professional networks, advice seeking applications and patient communities. This work, presented privacy risks, requirements and available solutions and made a first step towards a best practice guide, which will outline both the technical and procedural countermeasures required in order to maintain privacy, taking into account modern technology environments.

References

Barnes, J. A. (1954). Class and committees in a Norwegian island parish. Plenum.

Boyd D. M., Ellison N. B. (2008). "Social network sites: Definition, history, and scholarship". Journal of Computer Mediated Communication, 13 (1) (2008), pp. 210–230.

Chryssanthou, A., Varlamis, I., & Latsiou, C. (2011). A risk management model for securing virtual healthcare communities. International journal of electronic healthcare, 6(2), 95-116.

Cutillo, L. A., Manulis, M., & Strufe, T. (2010). Security and privacy in online social networks. In Handbook of Social Network Technologies and Applications(pp. 497-522). Springer US.

Damschroder, L. J., Pritts, J. L., Neblo, M. A., Kalarickal, R. J., Creswell, J. W., & Hayward, R. A. (2007). Patients, privacy and trust: patients' willingness to allow researchers to access their medical records. Social science & medicine, 64(1), 223-235.

Eckersley, P. (2010). How unique is your web browser?. In Privacy Enhancing Technologies (pp. 1-18). Springer Berlin Heidelberg.

Eysenbach, G. (2011). Infodemiology and infoveillance: tracking online health information and cyberbehavior for public health. American journal of preventive medicine, 40(5), S154-S158.

Finn, R. L., Wright, D., & Friedewald, M. (2013). Seven types of privacy. InEuropean data protection: coming of age (pp. 3-32). Springer Netherlands.

Fire M., Goldschmidt R. & Elovici Y. (2014). "Online Social Networks: Threats and Solutions". Communications Surveys & Tutorials, IEEE. Article in Press.

Fritsch L. (2007): "State of the Art of Privacy-enhancing Technology (PET) - Deliverable D2.1 of the PET web project". In Norsk Regnesentral Report 1013, ISBN 978-82-53-90523-5, Oslo, Norway.

Glozier, N., Christensen, H., Naismith, S., Cockayne, N., Donkin, L., Neal, B., ... & Hickie, I. (2013). Internet-delivered cognitive behavioural therapy for adults with mild to moderate depression and high cardiovascular disease risks: a randomised attention-controlled trial. PloS one, 8(3), e59139.

Grajales III, F. J., Sheps, S., Ho, K., Novak-Lauscher, H., & Eysenbach, G. (2014). Social media: a review and tutorial of applications in medicine and health care. Journal of medic

Healthcare Information and Management Systems Society (2013). Social Media in Healthcare: Privacy and Security Considerations. HIMSS White Paper. Available for download from: http://himss.files.cms-plus.com/HIMSSorg/Content/files/Social_Media_Healthcare_WP_Final.pdf

HL7 International, Inc. (2010). HL7 Privacy, Access and Security Services (PASS) Specification. Ann Arbor, MI, USA: HL 7 International. Available for download from: http://wiki.siframework.org/file/view/PASS+Access+Control+Conceptual+Model+Release+1.0.pdf

Hogben, G. (2007). Security issues and recommendations for online social networks. ENISA position paper, 1, 1-36.

Hogben, G. (2009). Security issues in the future of social networking, in W3C Workshop on the Future of Social Networking.

Holvast J. (2009). "History of Privacy". IFPI Advances in Information and Communication Technology, Vol. 298, pp.13-42.

Kalloniatis, C., Mouratidis, H., Vassilis, M., Islam, S., Gritzalis, S., & Kavakli, E. (2014). Towards the design of secure and privacy-oriented information systems in the cloud: Identifying the major concepts. Computer Standards & Interfaces, 36(4), 759-775.

Koorn, R., van Gils, H., ter Hart, J., Overbeek, P., Tellegen, R., & Borking, J. (2004). Privacy Enhancing Technologies, White paper for Decision Makers.Ministry of the Interior and Kingdom Relations, the Netherlands.

Krishnamurthy, B., & Wills, C. E. (2009). On the leakage of personally identifiable information via online social networks. In Proceedings of the 2nd ACM workshop on Online social networks (pp. 7-12). ACM.

META Group (2005). "Privacy Enhancing Technologies – META Group Report v 1.1". [Online]. Available for download from: https://danskprivacynet.files.wordpress.com/2008/07/rapportvedrprivacyenhancingtechlologies.pdf

Pfitzmann, A., & Hansen, M. (2010). A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management.

Robinson, N., Graux, H., Botterman, M., & Valeri, L. (2009). Review of the European data protection directive.Technical report No TR-710-ICO. RAND Corporation

Rosenberg R. (1992). "The Social Impact of Computers". San Diego: Academic Press.

Rowe, M., & Ciravegna, F. (2008). Disambiguating identity through social circles and social data.

Serenko, N., & Fan, L. (2013). Patients' perceptions of privacy and their outcomes in healthcare. International Journal of Behavioural and Healthcare Research, 4(2), 101-122.

Shen Y., Pearson S. (2011). "Privacy Enhancing Technologies: A Review". Tech. rep., HP Laboratories.

Stuart, A. H. (2007). Online Privacy Policies: Contracting Away Control Over Personal Information?. Penn State Law Review, 111(3).

Swan, M. (2009). Emerging patient-driven health care models: an examination of health social networks, consumer personalized medicine and quantified self-tracking. International journal of environmental research and public health, 6(2), 492-525.

Theoharidou, M., Tsalis, N., & Gritzalis, D. (2014). Smart Home Solutions for Healthcare: Privacy in Ubiquitous Computing Infrastructures. Handbook of Smart Homes, Health Care and Well-Being.

Van Blarkom, G. W., Borking, J. J., & Olk, J. G. E. (2003). Handbook of privacy and privacy-enhancing technologies. Privacy Incorporated Software Agent (PISA) Consortium, The Hague.

Warren S. D., & Brandeis L. D. (1890). "The Right to Privacy". Harvard Law Review, Vol. 4, No. 5, pp. 193-220.

Westin A. F. (1968). "Privacy And Freedom". Washington and Lee Law Review, Vol. 25, Iss. 1, Article 20.

Wicks, P., Massagli, M., Frost, J., Brownstein, C., Okun, S., Vaughan, T., ... & Heywood, J. (2010). Sharing health data for better outcomes on PatientsLikeMe. Journal of medical Internet research, 12(2).

Wondracek, G., Holz, T., Kirda, E., & Kruegel, C. (2010). A practical attack to de-anonymize social network users. In Security and Privacy (SP), 2010 IEEE Symposium on (pp. 223-238). IEEE.

Yanes, A. (2014). Privacy and Anonymity. arXiv preprint arXiv:1407.0423.

Yeratziotis, A., Van Greunen, D., & Pottas, D. (2012). A Framework for Evaluating Usable Security: The Case of Online Health Social Networks. InHAISA (pp. 97-107).

Zilpelwar, R. A., Bedi, R. K., & Wadhai, V. M. (2012). An Overview of Privacy and Security in SNS. International Journal of P2P Network Trends and Technology, 2(1).