Security and privacy legislation guidelines for developing Personal Health Records

Jelena Mirkovic, PhD
Center for Shared Decision Making and Collaborative Care Research,
Oslo University Hospital
Oslo, Norway
Jelena.Mirkovic@rr-research.no

Eva Skipenes, Ellen K. Christiansen
Norwegian Center for Integrated Care and Telemedicine,
Tromsø, Norway
eva.skipenes@telemed.no,
ellen.christiansen@telemed.no

Haakon Bryhni, PhD
Department of Informatics
University of Oslo
Oslo, Norway
haakon@bryhni.com

***Abstract*—Personal Health Records (PHR) open new opportunities for enhancing delivery of standard health care services and health information to general population and supporting individuals to take more active role in health management and decision making processes. However, while utilization of PHR as part of a health management process brings much more flexibility, and advanced options to individuals, it also introduces questions related to responsibility and authority for creation, processing, maintenance and ensuring privacy and security of personal health related data. This paper summarizes the issues related to EU legal-regulatory requirements for developing PHR that enable storage, sharing and management of health data between different stakeholders (patient and healthcare institutions on different levels of care). We present a list of guidelines that outline which security and privacy issues must be taken into consideration and be addressed when developing PHR, and discuss them in the context of one European country (Norway). In the discussion we raise the issues that are not addressed in the existing regulations, but play an important role in developing secure PHR systems. We also propose a direction for further development of policies and legislations in Europe to facilitate further development and utilization of PHR systems.**

Keywords—Security; Privacy; eHealth; Legal aspects; Personal Health Records; Human factors; Interoperability

I. INTRODUCTION

A Personal Health Record (PHR) is a health record that contains health data and information related to the care and is managed by the patient [1]. PHR gives the patients options to access, manage and share information regarding their health [2]. A PHR system can be implemented as a stand-alone application without connection to any other system, where patients can access, enter and manage data in their private system or device [3]. However, the full potential PHR systems can provide if they are integrated with Electronic Healthcare Records (EHR) systems that are used and managed by the clinicians and/or health care institutions. In this type of PHR patients can obtain a more thorough overview of their health related data from multiple sources (including both healthcare facilities and individual managed sources), actively contribute and participate in personal health management and decision making processes, and involve different stakeholders in the process. It is shown that this type of PHR systems can result in empowering patients to take a more active role in their own health and increase the patients' self-efficacy, decrease symptom distress and depression, and improve communication between patients and healthcare providers [4-6]. In the rest of the paper the term PHR will be used for PHR integrated with EHR.

Besides the advantages a PHR system can provide, it also introduces potential risks to the privacy and security of health data, especially when data is shared between different organizations and persons. In this type of distributed systems it is very important that ethical, legal, and social responsibilities and constraints are clarified and addressed so that all involved parties (e.g. patients, health professionals and the business community) are aware of their rights, obligations, and legal responsibilities regarding preserving privacy and security of personal health data [7]. However, most of the privacy policies of PHR systems in use today do not include detailed description of policies implementation, and the compliance with existing regulations and standards is still very low [8].

In the presented work our goal is to summarize and outline the list of guidelines that could be used during planning, evaluation and implementation of PHR systems in Europe, and in that way facilitate development of systems that comply with legal, regulatory, and security requirements. The guidelines presented are based on EU regulations and directives, while the specific context of Norway is used as a use case and demonstration of implementation of guidelines.

II. METHODS

The study is performed in 4 steps: (1) Laws and regulations related to protection of sensitive health data are identified and evaluated (both on EU level and specific context of Norway), (2) It is identified how these laws and regulations address privacy and security issues for providing healthcare information services in PHR, (3) How they support participation and cooperation between different stakeholders (e.g. patients, healthcare providers from different healthcare institutions at different levels of care) and (4) Distribution of responsibilities.

III. RESULTS

Based on identified and evaluated laws and regulations we outlined the set of guidelines that could be used to inform planning and development of PHR systems in Europe and ensure compliance with existing rules and regulations. The guidelines are shown in Table 1, and a more detailed discussion is given in the continuation of this chapter.

TABLE I. LIST OF SECURITY GUIDELINES

#	***Security guideline***
1	Define type of data, type of service and legal basis for processing
2	Define legal responsibility for processing of personal data
3	Define, document and monitor purpose of the processing
4	Define general condition(s) for processing data
5	Planning and performing systematic actions to protect data security and privacy
6	Enabling access to health information
7	Social network features
8	Notifying the Data Protection Authority that personal data will be processed and applying for licensing

A. Define type of data, type of service and legal basis for processing

First step when planning, developing and evaluating security and privacy policies of any system is to define and categorize the data stored and processed by the system, and identify the laws and regulations that apply. By EU regulations every organization that provides services that process personal data, is responsible for ensuring that personal data is handled in accordance with the existing directives. The EU Directive on the protection of processing of personal data (also known as Directive 95/46/EC) is a directive adopted by the European Union designed to protect the privacy and protection of all personal data collected for or about citizens of the EU [9]. Directive 2002/58/EC on privacy and electronic communication complements Directive 95/46/EC and addresses additional issues related to the protection of privacy when processing personal data using new telecommunication technologies [10]. In addition to following the rules outlined in the EU directives, the organization must ensure that national legislation that implement the EU directives are followed. For example, Norway used Directive 95/46/EC and Directive 2002/58/EC as a central framework for developing and establishing the Norwegian regulatory policy in this field. The directives are implemented mainly by the Personal Data Act [11], Regulations on the processing of personal data [12], a new law regulating all processing of health information necessary for giving, administrating or assure the quality of health care to individuals [13], and Act on personal health data filling system and the processing of health data [14].

The EU directives do not focus specifically on security and privacy of health related data, but rather introduces broad data-protection and privacy laws and more general categories of personal and sensitive personal data. The personal data are defined as "any information relating to an identified or identifiable natural person" [9]. Additionally, there is the category of sensitive personal data (e.g. data relating to racial, or ethnic origin, or political opinions, philosophical or religious beliefs, criminal acts, health, sex life, or trade-union membership), which can require additional restrictions for processing. Since PHR contains health related information the data is by default categorized as sensitive data.

If the service is processing any personal data, the regulations for protecting private personal data apply. However, if the data are anonymised before processing i.e. so they cannot be related to any identified or identifiable person, the regulations will not apply. By anonymisation is meant removing the information that can be used to directly link personal information to individuals (such as names, ID numbers), but also removing information that indirectly might lead to identification of a person (e.g. phone number, IP address). Additionally, if the processing is performed for exclusively personal or other private purposes, the regulations will not apply. For this reason it is highly relevant to define the role of the user of the system and make a clear distinction between private and professional processing of personal data.

If data are defined as personal data, it must be identified if they are processed as part of a personal data filing system ('filing system'). A filing system is defined as "any structured set of personal data which are accessible according to specific criteria" [9]. In the case the personal data are part of a filing system, additional laws and regulations may apply. Regulations in Norway additionally define personal health data filing systems as "filing systems or records where health data are systematically stored so that information concerning a natural person may be retrieved" [14]. This definition applies for both EHR and PHR systems.

Besides deciding upon the type of data that is processed, it must be considered how the service that is provided could be additionally categorized and if that will additionally influence which rules and regulations that must be applied. In Norway for example, if the service is categorized as health care, specific regulations apply. The term health care means "any act that has a preventive, diagnostic, therapeutic, health-preserving or rehabilitative objective and that is performed by health personnel" [15]. The distinction between health care and other types of services are important, partly because it determines whether the general regulations related to health services is applicable or not. This will have further consequences, for example, to distribution of responsibility between involved parties and requirements for notification and/or authorization from the Norwegian Data Protection Authority. Additionally, if the health data filing system is used by health care personnel, and the administration of such data for the purpose of providing a health care services, the filling system is defined as health data filing system established for therapeutic purposes [14]. An example of this type of system is a Electronic Healthcare Record (EHR) system in a healthcare organization.

B. Define legal responsibility for processing of personal data

Before the organization can start planning systematic actions for establishing and maintaining satisfactory information privacy and security systems, legal responsibility for processing of sensitive personal data must be clarified. First it must be defined who has the role as data controller. The

Directive 95/46/EC defines data controller as the "entity which alone or jointly with others determines the purposes and means of the processing of personal data" and defines which means are to be used for the processing [9]. The day-to-day responsibility is usually given to the general manager of the data controller organization, but individual tasks can also be delegated to employees or transferred to external organizations, called data processors. If data processors are involved in processing data, a written agreement must be signed, that specify among other things how security and privacy shall be ensured and which security measures shall be implemented. Independent of involvement of external organizations, the legal responsibility for security and privacy of the data remains with the data controller.

The data controller is not the owner of the data, but will need to be in control of the data based on the guidelines defined through legislation. Also, it is not always the case that just one single organization has the role of data controller and is in charge of defining the purpose of the processing of the data alone (Directive 95/46/EC, Article 2(d)) [9]. For example, the legislation in Norway allows different organizations to establish joint health data filling system and state in the written agreement how they will secure the private information and deal with the data controller's responsibilities [13].

As part of the data controller's obligation to implement appropriate organizational measures to protect personal data against security and privacy threats, the data controller organization is responsible for informing its employees of the scope of their responsibilities related to all health and personal data. The data controller must inform its employees about other information relevant to information security, and enable them to conduct their work in a proper manner [15]. Allocation of responsibility must be documented and described by the data controller and made known within the organization [11].

International and national regulations and codes of ethics (e.g International Medical Informatics Association Code of Ethics for Health Professionals [16]) set additional responsibilities of health professionals for preserving confidentiality and privacy of private health data they are using in their everyday work. In Norway all health personnel are subject to a duty of secrecy, which "includes both a passive obligation to remain silent and an obligation to actively prevent unauthorized persons gaining knowledge of confidential data" [15]. Additionally, the healthcare personnel have the general requirement to perform their work in accordance with professional responsibility and diligent care for both general practice services [15] and specialist service [17]. Further distribution and scope of responsibilities could be resolved based on type of the data that is processed and type of service (introduced in *Security Guideline 1*).

The patients must be fully informed about the collection and processing of their personal data, including all the circumstances of the collection (e.g. purpose of processing, categories of data, identity of data controller) (Directive 95/46/EC, Article 11) [9]. Also they have to be informed about their responsibilities and rights to access and rectify the data concerning themselves. This information is usually provided as part of the procedure for obtaining user consent (more detailed description in *Security Guideline 4*).

C. Define, document and monitor purpose of the processing

The organization must define the purpose of the processing of health personal data and make sure that the data collected and processed are adequate, relevant and not excessive in relation to the purpose. The data controller must ensure that the purpose defined is explicit and legitimate and that the data is not processed for any other purposes than specified, that the data is accurate and complete, and that it is not stored longer than necessary (Directive 95/46/EC Article 6)[9]. For example, in Norway the main purpose behind processing of personal data in the health and care services sector is to provide proper medical assistance and care services (including healthcare services to individual health care users where the organization follows the provisions of the Health and Care Services Act, provide education, conduct research, or perform government-mandated reporting) [18].

Defining some specific purposes of the processing can result in requirements to apply additional regulations that are defined to protect information security and privacy for specific types of services. In the case of Norway, if the purpose of processing of data is research, the Act on medical and health research should also be applied [19]. The act introduces some additional requirements, such as that the research project must be approved in advance by the regional committee for medical and health research ethics instead of applying for authorization to the Data Protection Authority (see *Security Guideline 8*). The committee presupposes that all relevant and statutory security measures are in place. All research projects must entitle a person or body that is responsible for the research and project management.

D. Define general condition(s) for processing data

The general rule is that personal data may be processed only if one or more predefined criteria are fulfilled (Directive 95/46/EC, Article 7) [9]. Some of the criteria are: consent from data subject, fulfilling legal obligations of the data controller, protecting the vital interests of the data subject. Additionally, member states can define their own processing conditions.

If the general condition is consent from the data subject (or patient in this case), the consent must contain information such as: name and address of the data controller, purpose of data processing, description of recording and processing procedures of sensitive data, description that the service is voluntary, if and which information is to be shared with other entities and which ones, categories and sources of data processed, what are the rights of the user (e.g. inspecting access logs, correct, delete, block access to some content). The user consent is not required to contain detailed description of implementation of security mechanisms. Protection of security and privacy are requirements set by underlying laws and regulations, and it is the responsibility of data controller and data processor to define and implement appropriate security mechanisms (see *Security Guideline 5*). However, the data controller must establish procedures for obtaining consent from users and establish procedures for complying with any users reservations related to limiting access rights, processing, and/or rectifications of deficient personal data [11, 18].

E. Planning and performing systematic actions to protect data security and privacy

The data controller and the data processors should ensure satisfactory data security with regard to confidentiality, integrity and accessibility by planning and performing systematic measures (Directive 95/46/EC, Section VIII) [9]. The data controller should define security objectives that describe the purpose behind the processing of data and how information technology is used and integrated in organization's operation to provide security and privacy protection. A security strategy should also be set to describe choices and priorities of security activities and specify how work regarding security should be organized and performed. All security measures should be documented, archived in a secure storage and made known and available to the employees of the controller and the processor or other entities on demand (e.g. the Data Protection Authority, Privacy Appeals Board). Additionally, the data controller should ensure that all external parties that have access to the personal data fulfill these defined requirements.

Existing regulations impose extensive requirements on the organizations (e.g. defining how privacy of data should be protected, how this should be documented and what security procedures to be established). However, the regulations do not specify what specific actions and security measures should be implemented to accomplish these requirements. Before selecting and implementing specific security mechanisms, it is up to the data controller to conduct a risk assessment to determine the probability and consequences of possible security breaches regarding confidentiality, accessibility and integrity of personal data. The results of the risk assessment are afterwards assessed against the previously established criteria for acceptable risk level. If the expected risk level is higher than the acceptable risk level, the organization will need to put into effect additional security measures to reduce the risk to an acceptable level.

For guiding the risk assessment process different sources can be utilized. For example, the ISO/IEC 27005:2011 standard describes the generic methodology for performing information security management [21]. The ISO/IEC 27799:2008 standard [20], formulated to provide guidance for managing the security of information in health information services and environments, outlines in Annex A a list of 25 types of threats that must be addressed by the organization when assessing risks of confidentiality, integrity and availability of health information and health information services. Additionally, some of the related scientific literature work investigates and further categorizes threat categories in health information systems (e.g. [21, 22]). In Norway, the Data Protection Authority has outlined the general security guidelines that can be applied for planning and implementing protection of confidentiality, availability, and integrity of personal data [23].

F. Enabling access to health information

The EU Directive state that the data subject (patient in our case) has the right to obtain the information about the data that is processed and logic behind processing, and should be able to require rectification, erasure or blocking due to incomplete and inaccurate nature of data (Directive 95/46/EC, Article 12) [9]. Since PHR systems enable sharing of personal data between different stakeholders (patients, different healthcare providers and healthcare organizations) the issue of privacy and security when enabling interoperability of personal data is of high importance. The term legal interoperability is used to cover "the broader environment of laws, policies, procedures and cooperation agreements needed to allow the seamless exchange of information between different organizations, regions and countries" [24]. The EU directives state that Member states may determine circumstances and use cases in which personal data may be used and shared with a third party organizations (Directive 95/46/EC, Article 7) [11]. Member states are obliged to specify the conditions that must be fulfilled before sharing the data and also to provide necessary information to the data subjects and give them the right to oppose to this sharing.

In Norway, the regulations state that disclosure of health information to health personnel from other organizations should be in accordance with statutory rules regarding professional secrecy, and procedures must be defined to satisfy the requirements of confidentiality, integrity and availability [18]. Regarding health information in EHRs regulations state that two organizations can sign an agreement to enable reading access to structured health information in each other's health record systems if the goal of the action is to provide health care services to the patient at hand, and both organizations provide required security protection of personal health information [13]. In addition, multi-organizational records can be implemented for certain areas of collaboration between health institutions as a supplement to the organization's internal EHR or instead of the different EHRs [13]. Data should only be registered in one of the systems, i.e. either in the supplementary system or in the organizations' internal systems in order to avoid dual recording.

Norwegian regulations state that access to the personal health data should be provided to healthcare personnel only if: it is necessary for the work of the individual, it is based on an official need and it is handled under the duty of secrecy [13]. User authentication procedures should be implemented based on the role the person has in the organization and conditions of employment. Selection of satisfactory authentication mechanisms should be performed in accordance with the performed risk evaluation (see *Security Guideline 5*). For example, the laws specify that for a person to be given access to the health data filing system established for therapeutic purposes he/she must be authenticated in such a way that it uniquely identifies the person, and that it can be used as an evidence in court.

One of the responsibilities of the data controller related to ensuring legal interoperability is granting, managing and reviewing authorizations for access to personal sensitive data. More specifically the data controller is responsible for: creation of an authorization register that documents access rights and its relation to user roles, delegation of authorization authority to individual person/responsible manager, establishing procedures for granting and managing access privileges [18]. Besides implementing and managing user authentication and authorization systems, the data controller must ensure secure physical access to equipment used for processing personal data, implement control of security measures and perform regular follow-up reviews of access control mechanisms [18].

G. Social networks features

The EU directives do not address privacy and security issues in social media specifically, but rather outlines general rules in relation to processing personal and sensitive data. The Article 29 Working party (an independent European advisory body on data protection and privacy set up under Article 29 of directive 95/46/EC) delivered an opinion on online social networking [25]. The document states that Social Network Service (SNS) providers are considered to have the role of data controller under Directive 95/46/EC, since they provide the means for processing the data, user management services, and define the purpose of use of the personal data. However, it is also given some exceptions where the application provider or even the end service users might be considered to take some of the responsibilities of a data controller. For example, if an application provider develops an application, which in addition to its basic functionalities integrates social network functionality of an SNS provider, the application provider is considered to be data controller. Also, if an individual user processes his/hers personal data for some activities that are not considered as "purely personal or household activities" (e.g. acts on behalf of the company or association) he/she could take some of the responsibilities of the data controller. Deciding when this is the case is often difficult.

The document additionally addresses issues such as concern over dissemination and use of information available on the SNS to unintended purposes, robust security and privacy-friendly default settings, and processing of sensitive data and images. At the end the Advice outline the key recommendations with the list of obligations for SNS providers to comply with the Directive 95/46/EC and to uphold and strengthen the rights of the user. The main requirements set for SNS providers are: inform users of their identity and all purposes for processing personal data at this SNS, offer privacy-friendly default settings, provide warnings and information about privacy risks, inform users that use of pictures or information about other individuals require their consent. Also, the SNS users retain all the rights outlined in the Directive 95/46/EC Article 10-14 [9] and additionally have a right to use pseudonym to protect his/her privacy and have access to an easy-to-use complaint handling procedure.

In Norway, the Agency for Public Management and eGovernment (Difi) issued guidelines for managing social media services in public organizations [26]. The guidelines outline that due to difficulty of ensuring users' confidentiality in social media the government should not engage in offering administrative procedures over this type of communication channels. Since public sector has the responsibility to protect personal information, it should not use nor facilitate services where citizens' privacy and security of personal information could be compromised.

Additional guidelines are published by The Norwegian Directorate of Health to address security and privacy issues relevant to social media in healthcare services specifically [27]. The document includes an overview of the issues that must be considered, templates for policies and guidelines for staff and patients and their families. In the guidelines it is stated that the organization has no responsibility for how users (e.g. patients and their family members) use social media features, due to the basic right of freedom of expression. However, the organization that provides the social media service is expected to create recommendations and guidelines for use of social media services provided by this organization. The guidelines do not imply the transfer of the responsibilities to the organization, but the organization is required to provide physical and organizational mechanisms to protect the privacy and security of the users' personal data while users are responsible for generating and publishing user-contributed content.

H. Notifying the Data Protection Authority that personal data will be processed and applying for licensing

The data controller must notify the supervisory authority before carrying out processing of personal data (Directive 95/46/EC, Article 18) [9]. Additionally, the Directive outlines the right of Member states to provide exception of notification in some specific cases (e.g. processing is affecting the rights and freedoms of data subjects, appointment of personal data protection officer that ensure application of the national regulations) and specifies the minimum set of information that should be contained in the notification.

In Norway the general rule is that processing of personal data in general requires sending notification to the Data Protection Authority, while processing sensitive personal data requires license from the Data Protection Authority [11]. In addition, the Data Protection Authority may decide that data that is not declared as sensitive could be subject to licensing in some cases. When developing and establishing a PHR system, the requirement for providing notification and/or obtaining license from Data Protection Authority must be reviewed based on type of data and type of processing that is performed. In the notification the organization is just informing the Data Protection Authority that the processing is going to be performed. The notification must be sent before processing of data begins and does not have to be answered. If the organization must obtain a license from the Data Protection Authority this must be obtained before processing of the data starts. During processing of the request the Data Protection Authority will evaluate if all conditions and requirements are fulfilled. An obtained license gives the organization permission to process sensitive data.

IV. Discussion

In this section we will discuss some of the issues regarding security and privacy that are not full addressed in the outlined guidelines but play an important role in PHR systems.

A. Sharing data between different stakeholders

One of the main goals of the PHR system is to support more effective collaboration between and among patients and healthcare providers by enabling shared access to patient's health information in diverse contextual purposes within and across organizations. To ensure security and privacy only the subset of health data that is necessary to provide the best quality of care should be made available to each healthcare provider. However, even though the technological solutions to support implementation of granular and limited access control exist (e.g. Role Based Control can be used to implement and

manage a wide range of access control policies to support complex nature of data access for diverse purposes [28]), utilization of these solutions in PHR and EHR system and their operationalization remains a major challenge [29-31]. For example, one of the issues is how to know which data are relevant and which should be shared to support healthcare providers to provide best quality of care without receiving too much and irrelevant information [30]. And what happens and who is responsible if the required data is not shared. This problem is present in all types of eHealth systems, but its importance is even more highlighted in the context of PHRs where multiple stakeholders are involved and physical contact between the healthcare provider and patient is usually absent. Additionally, implementation of access control management mechanisms is not just about applying a technical solution, but requires consideration of multiple additional factors, such as work process, organizational structure and culture to provide the right level of information security and privacy protection [29].

If the PHR system should include data from EHR systems belonging to different organizations, and is managed by the patient and accessible by employees from these different organizations, who is actually responsible for ensuring the privacy and the security of the data? Who should decide about the sensitivity of the information, and how to find the right balance between transparency and privacy protection [30]? The regulations state that the data controller is the one who decides on these issues. Is it possible for the patient to be the data controller for a PHR and have the responsibility to decide on who should get access to which information? And if information is not shared with healthcare professionals, how should this risk be measured? Should the patient be allowed to hide information from health care professionals at the risk of being treated sub-optimally? Or even if the patient is the data controller, are the health professionals then obliged to use the data in the PHR or not and who can decide on that? Also, from the other side maybe the patient cannot be the data controller since the data controller is responsible for implementing and providing the PHR service. And if that is the case, who actually then decides on the issues of sharing data and enabling access to different parties?

The legislation in Norway states that the patients have the right to decide who will be given access to their personal health information, but in the same time he/she must accept the risks that come with these decisions [15]. Also, circular letter I-12/2001 regarding Telemedicine and distribution of responsibility discusses the challenges for ensuring responsible conduct of healthcare providers in situations where data are shared electronically and patients are not physically present in the same place as the healthcare providers [32]. In general, healthcare personnel are responsible for providing treatment and decisions based on the information that is received and shared. The focus is on the quality of the information received, rather than on the manner in which the information is received (face-to-face meeting with patient, video, images, text or audio). The healthcare provider is responsible for the quality of the provided services, and must ask for additional information if it is required for performing responsible conduct. If that is not sufficient, it might be necessary to arrange a face-to-face consultation.

B. Usability of security systems and human factors

One of the biggest challenges and barriers to patients accepting and using PHR systems is lack of system's usability, especially due to the fact that they often do not possess high technical skills, have limited health and eHealth literacy, and even physical limitations [33, 34]. Lack of usability can also greatly influence and decrease security and privacy of the system. For example, if patients do not understand how security and privacy mechanisms should be used and managed and what the requirements and consequences related to safeguarding the private information are, it can significantly endanger the security and privacy of their data. For example, research has shown that if patients have problems understanding how to access and use the system, they often share their personal credentials with others to get technical assistance [35].

These issues are even more relevant for PHR systems where patients play an important role in preserving security and privacy of their health information, and it is of high importance to present security and privacy information and security and access control mechanisms on a very understandable, user-friendly, and usable manner. Implementing security and privacy management methods that are not clear and understandable for users can jeopardize both accessibility of the system and security of sensitive information. For example, providing users security and privacy notices can be highly challenging since they often overlook them, or even worse, misinterpret them. One way to address this issue is proposed by Cranor, that developed a framework that supports creating security warnings that users can effectively notice, understand, evaluate the options of, and take actions with respect to [36]. This framework is also proposed by some related research to lead the design of mechanisms for obtaining informed consent from users [37].

These are just some of the examples of why it is highly important to strike the right balance between security and usability in PHR systems. Usability of security mechanisms is not raised as a specific requirement in the existing legislation and directives, even though it could be an important factor that largely influences the privacy and security. Providing user-friendly and meaningful information and guidelines for managing security and privacy issues, without disturbing and confusing the user, is highly important in order to support users in taking a bigger and more responsible role in security and privacy management. Human factors are usually considered and addressed indirectly as part of performing a system's risk assessment, where they are considered as specific aspects of the security and privacy management process.

C. Social networking

New technology developments are changing the way (health) information services are delivered, used, and shared between individuals. Emerging technologies such as social media can support users' needs for self-expression, participation in self-defined communities and contributing to discussions and cooperation with similar patients groups by utilizing and sharing previous experience and knowledge [38].

They differ from traditional information services by allowing more interactivity and many-to-many communication. However, one of the main challenges when integrating social media features is that the content provider role is shifted from one centralized service provider (e.g. healthcare organization) to service users (e.g. patients). Due to this shift, new issues related to preserving information security and privacy emerge. For example, the data ownership in this new context is often very unclear resulting in undefined responsibilities between users and service provider, and it is unclear what is regarded as responsible conduct and relationship with the service users. Hence, it is important that (health) service providers implementing social media features, respect the user's rights and freedom, and make sure that the data disclosed and shared are processed in accordance with global and national data protection and privacy legislations.

Williams and Weber-Jahnke in their work [39] summarize security and privacy issues of social networking applications in eHealth systems in 8 main categories: (1) complex usage scenarios that makes it difficult for users to assess risks associated with sharing data, (2) expansibility of networks are often misjudged by users, (3) trust issue, (4) use of accumulated information for different purposes, (5) no control over retention period, (6) leaking information to third party servers, (7) location of servers is not often clear, (8) cost of switching from one to another social networking provider are exceedingly high. As we discussed before, in Norway regulations state that the data controller is responsible for providing physical and organizational mechanisms to protect privacy and security of users' personal data (such as to protect use of data for any other purposes than defined in the user consent, or leaking data to another server), but has no responsibility of how users (patients and their family members) use social media features, due to the basic right of freedom of expression. However, even though the patient will have the main responsibility over content he/she shares, the data controller has to provide guidelines and recommendations to users that will help users to assess security and privacy threats in the system (such as understanding complex usage scenarios and/or expansibility of social networks) and decide upon their behavior and actions in order to minimize the difference between achieved and desired privacy levels.

D. New legislation

The existing EU legislation and directives have known limitations. For example, the rules outlined in the Directive 95/46/EC have been implemented by the 27 EU Member States differently, resulting in divergences in enforcement. Different states have had different opinions on interpreting the Directive rules and as a result not all legal requirements are transported in a harmonized way [40]. Due to this, in 2012, the European Commission proposed a major reform of the EU legal framework on the protection of personal data [41]. The goal with the new proposed regulation is to modernize the current principles, to strengthen individual privacy and rights and to introduce a new single regulation (General Data Protection Regulation) that will be directly applicable in all EU countries. In that way the EU privacy protection legislation will be identical in all EU states.

Even though most of the security guidelines outlined in this work will be applicable in the new context, the new regulations will bring some adaptations and changes to how they should be applied, and we will discuss some of the issue here. The new regulation includes the subject's right to data portability that ensures the right of the data subject to obtain a copy of data from the data controller and to further use this data without hindrance from the data controller. This right will support patients in gathering and sharing their data in a PHR, but also in the same time raise further issues that are not addressed in the new regulation – e.g. who is responsible for preserving security and privacy of this new copy of the data and how should multiple copies of the same data set be managed? Also, Article 25 of the regulation introduce the term *Joint controllers* that enables one organization to determine the purposes, conditions and means of processing personal data together with another organization and determine and share responsibilities. This concept is similar to the statutory provision in the new Norwegian act concerning patients health records that allows different health institutions to establish joint health record systems (described in *Security Guideline 2)*. Additionally, from the new EU regulation, every data controller should appoint the Data Protection Officer that is in charge to ensure and manage security of personal data. This requirement is introduced as a surrogate of a notification requirement, giving the increased responsibility and accountability for the organizations processing personal data and removing unnecessary administrative requirements. This new requirement should result in adaptation of the *Security Guideline 8* from this article to reflect a new requirement of the Data Protection Officer instead of notification of Data Protection Authority.

V. Conclusion and Future Work

Due to the sensitivity of data that PHR systems process and the involvement of different stakeholders it is highly important to address all relevant legislation rules and requirements during the design and development phases of such a system. The paper outlines and organizes a complex list of security, privacy and confidentiality issues, which can be used as a checklist during design and development of PHR systems in Europe. Additionally, as part of the discussion we outlined issues that are still not fully addressed by the current legislations (e.g. enabling and managing access rights and shared records between parties, usability and human factors, managing security and privacy issues in social network features). We found that these issues play an important role in protecting and preserving security and confidentiality of sensitive data, and that further work is required to define more clear and concise security and privacy policies and guidelines to overcome potential security breaches and threats.

We can conclude that implementation of PHR systems, besides benefits it provide to patients, also introduces new significant risks to patients' privacy and confidentiality. Additionally, patients themselves play an important role in protecting privacy and confidentiality of their own health information and they should have the right and responsibility to decide on how information about them is shared and exchanged between different stakeholders. For this reason, we think that legislation should put more focus on patients' responsibilities in preserving security, and provide a base and

support for development of secure systems that will help patients fulfilling this new role (for example by focusing on privacy by design). This is the main requirement for development of future PHR systems that will provide a more active role of patients, not just in health care management and decision making processes but also in managing security and privacy issues while sharing their health information between different healthcare providers to receive timely and more efficient health services.

REFERENCES

[1] P. C. Tang, J. S. Ash, D. W. Bates, J. M. Overhage, and D. Z. Sands, "Personal health records: definitions, benefits, and strategies for overcoming barriers to adoption," J Am Med Inform Assoc, vol. 13, pp. 121-6, Mar-Apr 2006.

[2] Markle Foundation, "Personal Health Working Group Final Report," 2003.

[3] F. L. Maloney and A. Wright, "USB-based Personal Health Records: An analysis of features and functionality," International Journal of Medical Informatics, vol. 79, pp. 97-111, 2010.

[4] N. Archer, U. Fevrier-Thomas, C. Lokker, K. A. McKibbon, and S. E. Straus, "Personal health records: a scoping review," J Am Med Inform Assoc, vol. 18, pp. 515-22, Jul-Aug 2011.

[5] C. M. Ruland, T. Andersen, A. Jeneson, S. Moore, G. H. Grimsbo, E. Borosund, et al., "Effects of an internet support system to assist cancer patients in reducing symptom distress: a randomized controlled trial," Cancer Nurs, vol. 36, pp. 6-17, Jan-Feb 2013.

[6] G. H. Grimsbo, G. H. Engelsrud, C. M. Ruland, and A. Finset, "Cancer patients' experiences of using an Interactive Health Communication Application (IHCA)," Int J Qual Stud Health Well-being, vol. 7, 2012.

[7] N. Ferraud-Ciandet, "Privacy and data protection in eHealth: A comparative approach between South African and French legal systems," in IST-Africa, 2010, 2010, pp. 1-10.

[8] I. Carrion Senor, J. L. Fernandez-Aleman, and A. Toval, "Are personal health records safe? A review of free web-accessible personal health record privacy policies," J Med Internet Res, vol. 14, p. e114, 2012.

[9] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. European Parliament and of the Council, 1995.

[10] Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) European Parliament and of the Council, 2002.

[11] Personal Data Act, Mininstry of Justice and Public Security, 2000.

[12] Regulations on the processing of personal data, Mininstry of Labour and Government, 2003.

[13] LOV-2014-06-20-42 Lov om behandling av helseopplysninger ved ytelse av helsehjelp (pasientjournalloven), Helse- og omsorgsdepartementet, 2015.

[14] LOV-2014-06-20-43 Act on personal health data filing systems and the processing of personal health data (Personal Health Data Filing System Act), Helse- og omsorgsdepartementet, 2015.

[15] The Health Personnel Act, Ministry of Health and Care Services, 2002.

[16] International Medical Informatics Association (2011). IMIA Code of Ethics for Health Information Professionals. Available: http://www.imia-medinfo.org/new2/pubdocs/Ethics_Eng.pdf

[17] Lov om spesialisthelsetjenesten m.m. (spesialisthelsetjenesteloven), Ministry of Health and Care Services, 1999.

[18] The Norwegian Directorate of Health, "Code of conduct for information security for healthcare and care services sector," The Norwegian Directorate of Health 2014.

[19] Act on medical and health research (the Health Research Act), Ministry of Health and Care Services, 2009.

[20] ISO/IEC, "ISO 27799:2008 Health informatics -- Information security management in health using ISO/IEC 27002," ed, 2008.

[21] G. Narayana Samy, R. Ahmad, and Z. Ismail, "Security threats categories in healthcare information systems," Health Informatics Journal, vol. 16, pp. 201-209, September 1, 2010.

[22] S. Katsikas, "Security of the Electronic Medical Record," in Handbook of Medical and Healthcare Technologies, B. Furht and A. Agarwal, Eds., ed: Springer New York, 2013, pp. 401-416.

[23] Data Inspectorate, "Sikkerhetsbestemmelsene i personopplysningsforskriften med kommentarer " 2000.

[24] eHealth Governance Initiative, "Discussion paper on semantic and technical interoperability " 2012.

[25] Opinion 5/2009 on online social networking, The Article 29 Working Party, 2009.

[26] R. O. Amdam, S. K. Hoel, A. Kalleberg, D. Solumsmoen, I. Stranger-Thorsen, and M. Strøm, "Social media in goverment," The Agency for Public Management and eGovernment 2012:2, 2012.

[27] The Norwegian Directorate of Health, "Guidelines for use of social media in healthcare services (in norwegeian)," 2012.

[28] D. Ferraiolo, D. R. Kuhn, and R. Chandramouli, Role-based Access Control: Artech House, 2003.

[29] A. Appari and M. E. Johnson, "Information security and privacy in healthcare: current state of research," International Journal of Internet and Enterprise Management, vol. 6, pp. 279-314, 01/01/ 2010.

[30] R. Cushman, A. M. Froomkin, A. Cava, P. Abril, and K. W. Goodman, "Ethical, legal and social issues for personal health records and applications," Journal of Biomedical Informatics, vol. 43, pp. S51-S55, 10// 2010.

[31] L. Rostad and O. Edsberg, "A Study of Access Control Requirements for Healthcare Systems Based on Audit Trails from Access Logs," in Computer Security Applications Conference, 2006. ACSAC '06. 22nd Annual, 2006, pp. 175-186.

[32] Helse og Omsorsdepartementet, "Telemedisin og ansvarsforhold," 2001.

[33] V. N. Patel, E. Abramson, A. M. Edwards, M. A. Cheung, R. V. Dhopeshwarkar, and R. Kaushal, "Consumer attitudes toward personal health records in a beacon community," Am J Manag Care, vol. 17, pp. e104-20, Apr 2011.

[34] S. Emani, C. K. Yamin, E. Peters, A. S. Karson, S. R. Lipsitz, J. S. Wald, et al., "Patient perceptions of a personal health record: a test of the diffusion of innovation model," J Med Internet Res, vol. 14, p. e150, 2012.

[35] J. Robison, L. Bai, D. S. Mastrogiannis, C. C. Tan, and W. Jie, "A survey on PHR technology," in e-Health Networking, Applications and Services (Healthcom), 2012 IEEE 14th International Conference on, 2012, pp. 184-189.

[36] L. F. Cranor, "A framework for reasoning about the human in the loop," presented at the Proceedings of the 1st Conference on Usability, Psychology, and Security, San Francisco, California, 2008.

[37] S. Avancha, A. Baxi, and D. Kotz, "Privacy in mobile technology for personal healthcare," ACM Comput. Surv., vol. 45, pp. 1-54, 2012.

[38] D. M. Zulman, K. M. Nazi, C. L. Turvey, T. H. Wagner, S. S. Woods, and L. C. An, "Patient interest in sharing personal health record information: a web-based survey," Ann Intern Med, vol. 155, pp. 805-10, Dec 20 2011.

[39] J. B. Williams and J. H. Weber-Jahnke, "Social networks for health care: Addressing regulatory gaps with privacy-by-design," in Privacy Security and Trust (PST), 2010 Eighth Annual International Conference on, 2010, pp. 134-143.

[40] M. Verschuuren, G. Badeyan, J. Carnicero, M. Gissler, R. P. Asciak, L. Sakkeus, et al., "The European data protection legislation and its consequences for public health monitoring: a plea for action," Eur J Public Health, vol. 18, pp. 550-1, Dec 2008.

[41] European commision, "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data", 2012.