Journal of Diabetes Science and Technology
2017, Vol. 11(6) 1234–1239

DOI: 10.1177/1932296817709797
journals.sagepub.com/home/dst
SAGE

Shared Electronic Health Record Systems: Key Legal and Security Challenges

Ellen K. Christiansen, Cand.Jur[1], Eva Skipenes, MSc[1,2], Marie F. Hausken, RN[3], Svein Skeie, PhD, MD[3], Truls Østbye, PhD, MD[4], and Marjolein M. Iversen, PhD, RN[3,5]

Abstract

Use of shared electronic health records opens a whole range of new possibilities for flexible and fruitful cooperation among health personnel in different health institutions, to the benefit of the patients. There are, however, unsolved legal and security challenges. The overall aim of this article is to highlight legal and security challenges that should be considered before using shared electronic cooperation platforms and health record systems to avoid legal and security "surprises" subsequent to the implementation. Practical lessons learned from the use of a web-based ulcer record system involving patients, community nurses, GPs, and hospital nurses and doctors in specialist health care are used to illustrate challenges we faced. Discussion of possible legal and security challenges is critical for successful implementation of shared electronic collaboration systems. Key challenges include (1) allocation of responsibility, (2) documentation routines, (3) and integrated or federated access control. We discuss and suggest how challenges of legal and security aspects can be handled. This discussion may be useful for both current and future users, as well as policy makers.

Keywords

data security, legal aspects, privacy, shared electronic health record (EHR) systems, telemedicine, telehealth, ulcer treatment

Use of shared telemedicine solutions in general, and, as is the case in our study, a shared electronic health record system (EHR system) combined with an electronic cooperation platform for health staff opens up a whole range of new possibilities. It facilitates flexible and fruitful cooperation among health personnel in different institutions, to the benefit of the patients. The shared electronic health record is suitable to support integrated care in the health sector.[1] However, there are legal and security challenges that need to be resolved before it can be integrated on a permanent basis into the health care system. Nevertheless, a systematic review pertaining to telemedicine security concluded that most of the reviewed articles only identified security problems, but did not address what the solutions to these problems might be.[2] It is also of great interest, especially for future users and policy makers, to understand how legal requirements related to allocation of responsibility, documentation, and secure access can be organized for shared EHR systems and, hence, how the requirements for responsible conduct can be fulfilled.

The aim of this article is to highlight and discuss some legal and security challenges related to shared electronic health record systems, which also serve as a tool for cooperation between involved health personnel, and thus are expected to increase the focus on integrated care. This is illustrated by our experiences from an evaluation project (DiaFOTo). The project evaluates a telemedicine follow-up intervention for patients with diabetes-related foot ulcers supported by the use of a web-based ulcer record, Pleie.net (Dansk Telemedicine AS, Copenhagen, Denmark). Use of Pleie.net involves health personnel in different health institutions.[3] The key ingredient in the intervention is the close integration between health care levels.

Discussion of possible legal and security challenges is critical for successful implementation of telemedicine. Key challenges include (1) allocation of responsibility, (2) documentation routines, and (3) integrated or federated access control. We discuss and suggest how challenges of legal and security aspects can be handled. This discussion

[1]Norwegian Centre for Integrated Care and Telemedicine, University Hospital of North Norway (UNN), Tromsø, Norway
[2]Helse Nord IKT HF, Tromsø, Norway
[3]Department of Medicine, Section of Endocrinology, Stavanger University Hospital, Stavanger, Norway
[4]Duke Global Health Institute, Duke University, Durham, NC, USA
[5]Centre for Evidence-Based Practice, Western Norway University of Applied Sciences, Bergen, Norway

Corresponding Author:
Marjolein M. Iversen, PhD, RN, Centre for Evidence-Based Practice, Bergen University College, PO Box 7030, N-5020 Bergen, Norway.
Email: miv@hvl.no

may be useful for both current and future users, as well as policy makers.

General Legal and Regulatory Background for Health Care by Use of Telemedicine

There is no specific legislation for telemedicine in most countries, including Norway. This implies that use of telemedicine services is governed by current general legislation; primarily health legislation and legislation concerning privacy protection in general, and protection of health data in particular. Health legislation and legislation concerning protection of privacy are intertwined. If, as an example, patient information goes astray due to the use of systems with insufficient security, this might be considered as breach of professional secrecy and therefore not in accordance with the requirements to professional responsibility and diligent care for health personnel in the health legislation.

Specific Norwegian Regulations

The obligation to document the treatment of the patient is the duty of the provider of the health care service.[4,5] This implies responsibility on two levels: each health personnel providing health care is legally obliged to document the medical treatment as enshrined in the legislation. In addition, the health institution is required by law to organize a documentation system allowing the staff to follow up their statutory obligations in this field. In Norway, most documentation systems in the health care sector are electronic, and it is expected that all such systems will be electronic before very long.

In a Norwegian circular about telemedicine and responsibility, it is implicit that medical treatment can be delivered without face-to-face contact between patient and doctor.[6] As an example, this implies that a specialist can be responsible for medical treatment based on a patient consultation via video conference if it is deemed responsible under the circumstances. This is not the case in all European countries, such as for example Poland, Malta, and Austria.[7] It is, however, up to the specialist to judge whether the information received is sufficient and the quality satisfactory for a reasonable evaluation of the patient. When a specialist uses video conferencing (or other telemedicine means) for patient consultations, she or he is obliged to maintain the patient's health record. This is not the case when the specialist is merely asked to give advice to other health professionals. The main point is that when telemedicine is used, the premises and responsibility conditions must be clarified among the cooperating staff from the outset. It is a key principle that distribution of responsibility in a medical consultation is not altered when telemedicine is applied.[6]

There have recently been changes in the legislation concerning EHR systems in Norway in general, and shared EHR systems in particular. The former Norwegian Personal Health Data Filing System Act from 2001[8] prohibited shared EHR systems. Each institution was obliged to have its own internal EHR system to which only the institution's own employees could legally be granted access. This restriction was altered in 2015 when Act on Medical Records[9] and a new Personal Health Data Filing System Act[10] were passed and replaced the law from 2001. Since then, shared EHR systems have been legal. The goal is to facilitate cooperation and coherence, and increase the quality of medical treatment and care when such care involves more than one health entity. However, it is emphasized by the legislator that documentation in shared EHR systems shall *replace* documentation in internal EHR systems. In other words, dual documentation is prohibited.[11] The reason for this is among others to avoid inconsistent documentation in different systems if the documentation is updated in one of the systems and not in the others. Updating of copies in external systems represents a big challenge.

Accordingly, the legislators wanted to enable legal use of shared EHR systems such as the web-based ulcer record system used in our evaluation project (DiaFOTo). This system is, among others, highlighted as a good example several times in the preparatory works of the Act on Medical Records.[11] It is in particular pointed out as a tool to facilitate cooperation between primary health care and specialist health care services.

Shared health record systems can include the entire health record, parts of it, or consist of documentation concerning one specific ailment, according to the Act on Medical Records of 2015. As dual documentation is prohibited, it is mandatory that medical treatment shall only be documented in one system. When primary health care and specialist health care services use a shared web-based ulcer record system for collaboration, both cooperating parties shall document their treatment of the ulcer in that system, and not in their respective internal health record systems. This represents dilemmas for the use of shared EHR systems and cooperation platforms, except when the patient's entire health record is shared. In that case, all documentation will be in the shared system and potentially available for all employees in the institutions sharing the system.

Methods

As there is little or no case law to illustrate the legal aspects related to shared EHR systems specifically, our considerations are mainly based on other sources. These include relevant current legislation, literature studies, lessons learned through use of telemedicine in general, and our experience with the web-based ulcer record in particular.[3]

The web-based ulcer record, Pleie.net (www.Pleie.net and www.Pleje.net), developed by Dansk Telemedicin AS, is an example of a technical solution, suitable to support

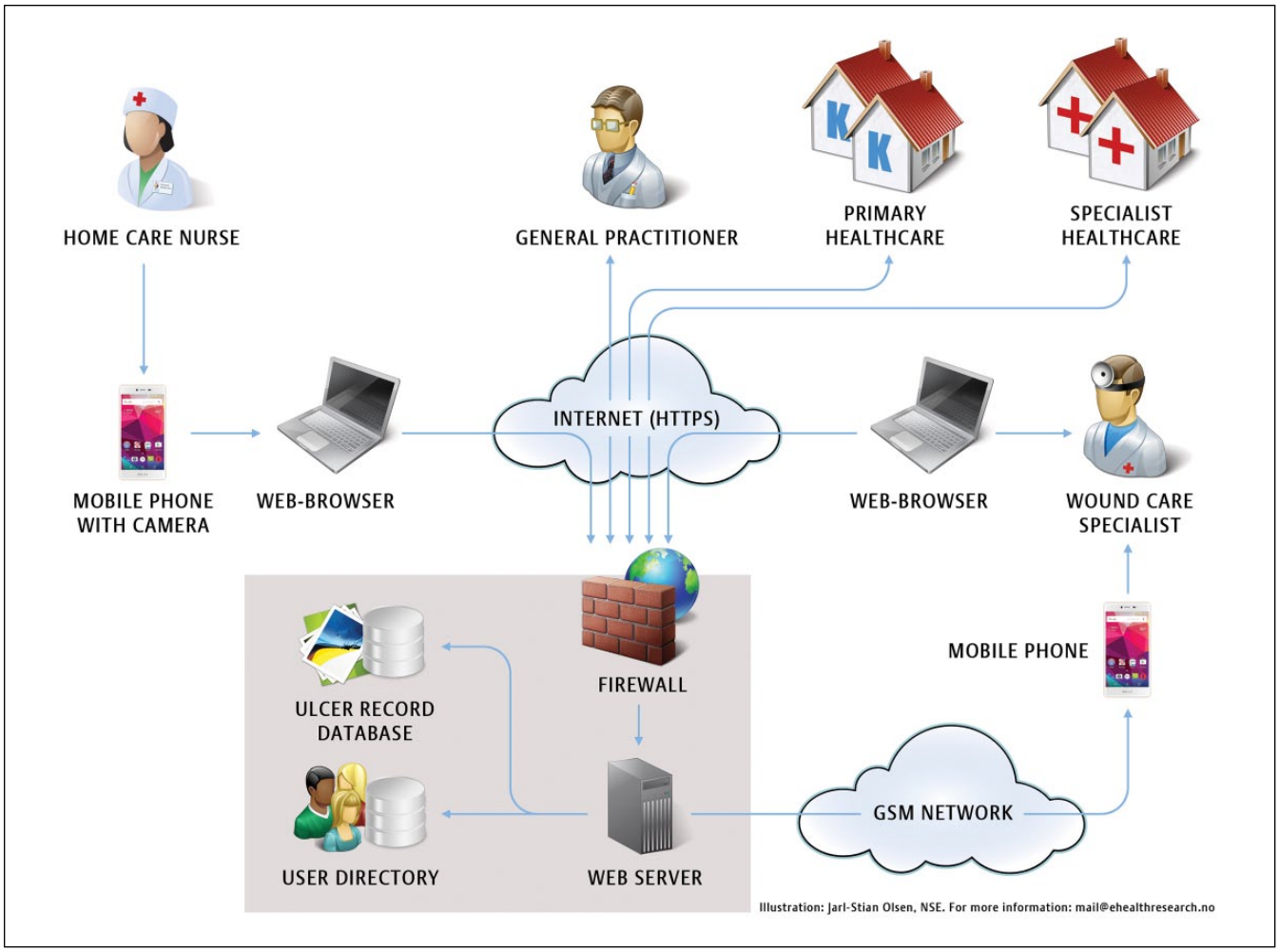

Figure 1. Diagram illustrating the general use of the web-based ulcer record.

integrated care in the health care sector (Figure 1)[3]. It is an electronic system comprising communication and cooperation facilities for health care personnel in different health institutions. It also serves as the legally required documentation system for the treatment they cooperate on. The web-based ulcer record system is accessible from mobile devices and computers via the Internet. The system makes it possible to register relevant data regarding the ulcers, digital images of the ulcers and measurements that can be compared over time to visualize the healing process of the ulcer, describe the situation and possible problems, and ask for and give advice. This allows all involved staff to contribute, even though some of them will not necessarily be situated in the vicinity of the patient. The system has functionality for documentation related to ulcer treatment at a far higher level than standard EHRs in use in Norway. And, unlike traditional EHR systems, this system is also customized for collaboration, discussions, and advice regarding the treatment between cooperating medical staff in different health care institutions. The discussions and advice given will be included as a substantial part of the documentation of the treatment. The institutions using Pleie.net emphasize that the main reason for using the web-based ulcer record system is the collaboration functionality that enables integrated care across different levels in the health care sector.

All relevant ulcer data are stored in a *shared* database, accessible to medical staff that are involved in the treatment of the patient *and* registered in the user directory of the system, regardless of which institution they are employed by. The system has been in use in Denmark for several years, and, to a limited extent, in Norway since 2007.[2,3]

This system makes it possible for specialists to transfer parts of the medical treatment of the ulcers to home care services. The specialists can supervise home care nurses by using Pleie.net, when needed. Ulcer documentation and treatment plans will be available for all involved staff, and they can communicate by text and/or digital images in the shared system. Without such a system, the patient would usually have to visit the hospital much more frequently to receive treatment of the same quality.

Results: Legal and Security Challenges in the Future

Telemedicine and Distribution of Responsibility Among Involved Staff

When health services are offered in a traditional way, definition of roles, responsibility, and liability of the involved staff, at any time, may be approached by defining physical boundaries. The main rule is that when the patient is situated in his or her home municipality and receives services from local health staff, the GP is liable for the treatment. When the patient is referred to the hospital for further examination and treatment, the hospital takes over the responsibility until the treatment is finished there. When the patient is treated in parallel by health staff from different levels or institutions in the health care service, each level is responsible for their part of the treatment and must document this in their respective health record systems.

When health care staff in different institutions communicate by means of the web-based ulcer record system or other telemedicine solutions, the physical borders are less clear. It may not be obvious who is responsible for what at the outset. The involved staff must discuss and clarify from the beginning who is responsible for the treatment of the patient, since that role is accompanied by a variety of work tasks and duties established in the health legislation. This is essential for safeguarding the patients' rights. Patients need to know whom to approach when they need to talk to someone responsible for the medical treatment.

Lack of Integration With the Internal EHR System—Challenges

The web-based ulcer record system described in this publication is a free-standing system, not integrated into the internal hospital or community EHR systems of the collaborating partners. There are several reasons for this. First, the main EHR systems in use in Norway do not have sufficient functionality for documentation of ulcer related data, digital images or visualization of the evolution/healing of the ulcer. Second, the current EHR systems in use in Norway do not support access for personnel from external institutions. Third, there is no satisfactory solution for integration between different EHR systems in Norway yet. Thus, the web-based ulcer record system has to have its own user directory and dedicated access control system. These issues cause some challenges. Both documentation and access control become complicated. To date, there are few, if any, external systems that have been integrated in a user-friendly way with the internal EHR systems in the health care service in Norway.

Availability of Documentation. The lack of integration with internal EHR systems and the prohibition against dual documentation cause interesting challenges. Since dual documentation is prohibited by law, patient information about the ulcer treatment documented in the shared EHR system will be available only for those who are involved in this treatment and, therefore, are given explicit access to the shared EHR. Remaining health care personnel in the collaborating institutions will not be given access to these ulcer treatment data. Information stored in the web-based ulcer record might be relevant and important, but not available, for health personnel treating the same patients in emergency-situations and for other diseases, such as for example kidney problems or pneumonia. As the legislators have pointed out, there is undoubtedly a need for shared health record systems. However, to make extensive use of such systems possible, challenges related to access control integration must be solved as discussed below. Then the use of integrated shared health record systems can be far more widespread than today.

Lack of Access Control Integration Between Systems. Since the users of the shared EHR systems work in different health institutions, they are registered as users in user directories owned and managed by separate institutions. In addition, they need to be members of the user directory of the shared EHR system to get access to the health records of that system. These different user access solutions are not integrated in any way for the time being, but suppliers of EHR systems and national health authorities in Norway recognize the importance of such integration.

One way of solving the challenges related to the lack of integration of access control between different EHR systems, gradually, could be to establish a standardized and secure solution for federation of authentication credentials between all EHR systems, for example, in a given region or country. The Norwegian Directorate of eHealth (NDE) has initiated a project for establishing a national secure authentication service for the health care sector. This includes a provisioning service (SPS) with a "trust anchor." It provides a security token service that can forward authentication information for a user from one system to another. When using an SPS, a security token including a unique user ID and trusted information about the security level used for authentication of the user in the internal system, is sent via the "central trust anchor" to the external system, to apply for access. Such a system consists of both technical solutions and organizational agreements to achieve the necessary level of trust between the institutions responsible for the systems. The Norwegian project mentioned has completed a pilot phase for the technical part of the national authentication service. Planning and implementation of a permanent national solution will be started in 2017. In addition, each organization wanting to use the solution must implement necessary functionality in their own infrastructure.

Discussion

We have highlighted some crucial legal and security challenges for successful implementation of shared EHR

systems. Key issues include (1) allocation of responsibility, (2) documentation routines, and (3) integrated or federated access control. We provide insights into legal and security aspects when telemedicine in general, and shared electronic health records in particular, is used.

The allocation of responsibility among involved staff is a key issue. Distribution of responsibility in medical consultations is not altered due to adoption of telemedicine tools. In our opinion, it is of vital importance that these matters have been elaborated at the outset, and that all involved personnel are aware of and have approved the premises for the cooperation. Distribution of work tasks and responsibility must of course in practice be in accordance with the conclusions.

Lack of integration, in our example, of the ulcer treatment EHR system in the internal health record system has consequences for documentation and availability of necessary information about the treatment of the patients. For obvious reasons, one must ensure that all health care personnel in the collaborating institutions have access to necessary and relevant information about the patients' ulcer treatment when needed. Given that the documentation of the ulcer treatment in the shared EHR is not integrated in the internal health record system, a reasonable solution could be to document essential information from the shared EHR in the internal EHR system of each of the collaborating institutions as well. That is, however, prohibited by law in Norway. On one hand, duplicate documentation might be desirable with regard to patient safety, on the other hand it is prohibited. Besides, dual documentation implies challenges: If the information is updated in one of the systems, how do we guarantee that it is also updated in the other systems? Availability of necessary information for health personnel treating the patient is required according to the Act on Medical Records, section 1 (a) (cf section 22).[9] An improvised, provisional solution could be to avoid dual documentation by a note in the patient's internal EHR stating that the patient in addition has a web-based ulcer record somewhere else. It should also be spelled out how access to this information can be obtained when it is necessary and relevant for the current treatment. This improvised solution is, however, not really a flexible and user-friendly arrangement and not fit for use in emergency situations. If use of telemedicine systems like the web-based ulcer record, leads to lack of vital patient information among health staff, this will not be in accordance with the requirements for responsible conduct. In our opinion remedial measures are possible, for example, by developing solutions for integrating the access control between different EHR systems. In our opinion, this is mainly a question of the national health authorities' willingness to develop standardized solutions for such integrations, and to allocate the required resources needed to do this. We assume that challenges related to lack of integration of different EHR systems are not only technical and related to confidentiality, but also economical in nature.

Further work to establish standardized routines and other necessary activities to achieve the necessary level of trust between the organizations involved, has not been given prioritization by Norwegian governments currently. These standardized routines and agreements are a prerequisite for widespread use of the solution. There must be an automated way to decide whether a request for access to a system for a given user should be granted or not, and this decision must be based on predetermined conditions. The conditions must in some way reflect the context of the user, if regarded as necessary for access. How to achieve these conditions is not yet investigated thoroughly. If an SPS solution of this kind was implemented, access control for personnel who need and is authorized for access to the patient's shared EHR, could be solved without prior registration of their user credentials in the shared EHR system's user directory.

It is also a possibility that the internal EHR system of one of the collaborating institutions could serve as the collaboration tool for integrated care related to ulcer treatment instead of an external system. A precondition for this is that the necessary functionality for ulcer treatment and electronic collaboration, and the access control integration challenge is solved. However, the use of the internal EHR system of one of the collaborating institutions could lead to other challenges. If the collaboration came to an end, only the institution who owned the internal EHR system in use would have the documentation of the ulcer treatment, unless remedial actions are established.

Conclusions

Experiences with implementation and use of a web-based ulcer record system so far has proven that despite the new Norwegian legislation and the legal authorities' wish to facilitate use of shared EHRs, there are still challenges to handle. The fact that we now have documented the main improvement areas by using the web-based ulcer record system makes it easier to approach and solve them. We regard this as a good starting point for establishing shared EHR systems in the health care sector in due course.

It is also our experience that use of the web-based ulcer record and other telemedicine systems apparently require clarification of responsibility and roles for involved health personnel. However, distribution of responsibility in medical consultations should not be altered due to adoption of telemedicine. This is a matter of great significance, and relatively easy to handle by means of good cooperation routines.

Lack of integration solutions for different EHR systems might reduce user-friendliness and user willingness. It is important to establish user-friendly systems. Systems that require additional login will likely increase complexity in a busy daily life. This might cause the enthusiasm and the willingness to use such shared systems to vanish, regardless of the quality and the benefit of the systems. Lack of integration will also prevent availability to patient information concerning the treatment documented in the shared EHR for health providers without a user account in the shared EHR system, when needed. Even when the providers are not involved in the

current treatment, they might need access to the information documented there, for example, in emergency cases. Therefore, development of standardized solutions for integrated access control between the different EHR systems is essential. This implies the need of an infrastructure/technological environment suited for this kind of telemedicine solutions.

Both standardized solutions for integration of access control between different EHR systems, and an acceptable level of trust among the institutions in the health care sector, are necessary. These goals can be achieved if they are prioritized by national and regional health authorities. Engagement and cooperation from all organizational levels of the health care sector and from clinicians, IT management, and IT system and service providers are also required to achieve efficient and secure solutions.

Commitment at all levels is required. Identification of and attention to legal and security challenges are of fundamental importance for further development and use of electronic collaboration and documentation systems for integrated care.

Abbreviations

EHR, electronic health record; NDE, Norwegian Directorate of eHealth; SPS, Secure Provisioning Service.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work is funded by a grant from the Norwegian Research Council (project number 221065), the Norwegian Directorate of Health, the Western Norway Regional Health Authority (911716), the Norwegian Diabetes Association, and Bergen University College.

References

1. Ekeland AG, Skipenes E, Nyheim B, Christiansen EK. Making a web based ulcer record work by aligning architecture, legislation and users—a formative evaluation study. *Stud Health Technol Inform*. 2011;169:417-421.
2. Garg V1, Brewer J. Telemedicine security: a systematic review. *J Diabetes Sci Technol*. 2011;5(3):768-777.
3. Iversen MM, Espehaug B, Hausken MF, et al. Telemedicine versus standard follow-up care for diabetes-related foot ulcers: protocol for a cluster randomized controlled noninferiority trial (DiaFOTo). *JMIR Res Protoc*. 2016;5(3):e148.
4. Act of 2 July 1999 No. 61 relating to Specialist Health Services [The Specialist Health Services Act]. (In Norwegian only).
5. Act of 2 July 1999 No. 64 relating to Health Personnel etc. [The Health Personnel Act].
6. Ministry of Health and Care Services. Circular I-12/2001, Telemedisin og ansvarsforhold (In Norwegian only, content in English: Telemedicine and responsibility). Oslo. 2001. Available at: https://www.regjeringen.no/nb/dokumenter/i-122001/id108946/. Accessed April 19, 2016.
7. Stroetmann KA, Artmann J, Dumortier J, Verhenneman G. United in diversity: legal challenges on the road towards interoperable eHealth solutions in Europe. EJBI. 2012;8(2):3-10.
8. Norwegian Government 24/2001. Act on personal health data filing systems and the processing of personal health data [in Norwegian only, content in English]. Personal Health Data Filing System Act. Oslo; 2001.
9. Norwegian Government 42/2014. Act on processing of health information when health care services are delivered [in Norwegian only, content in English]. Act on Medical Records [this law does not yet have an official English name]. Oslo; 2014.
10. Norwegian Government 43/2014. Act on Personal Health Data Filing System [in Norwegian only, content in English]. Act on Personal Health Data Filing Systems and the Processing of Personal Health Data. Oslo; 2014.
11. Norwegian Government Prop.72 L Pasientjournalloven og helseregisterloven (2013-2014). Proposisjon til Stortinget (forslag til lovvedtak) [Consultation Paper Proposing a New Medical Records Act and New Personal Health Data Filing Systems Act]. Oslo; 2014.