Overview of the national laws on electronic health records in the EU Member States and their interaction with the provision of cross-border eHealth services

Contract 2013 63 02

Overview of the national laws on electronic health records in the EU Member States

National Report for Denmark

time.lex

milieu
Law & Policy Consulting

1 March 2014

This Report has been prepared by Milieu Ltd and Time.lex under Contract 2013 63 02.

This report was completed by Professor, LL.D. PhD Mette Hartlev. The views expressed herein are those of the consultants alone and do not necessarily represent the official views of the Executive Agency for Health and Consumers

Milieu Ltd. (Belgium), rue Blanche 15, B-1050 Brussels, tel: +32 2 506 1000; fax: +32 2 514 3603; florent.pelsy@milieu.be; web address: www.milieu.be

Executive Summary

1. Stage of development of EHRs in Denmark

The Danish health care authorities highlight Denmark's role as one of the forerunners in the use or ICT in the health care sector.[1] Although the use of EHRs is widespread, the current stage of development in the Danish health care sector could best be characterised as fragmentary. This is partly due to the fact that the architecture of the ICT landscape has developed bit by bit during the last twenty years. EHRs have been widely used among General Practitioners for many years whereas the development in the hospital sector has been more challenging. There has been a continuous political and administrative focus on ensuring more coherence through stronger collaborations between the different actors (regions, municipalities, hospitals, individual health care providers, centralised health care authorities etc). So far this has been successful in some areas. The work of MedCom and the development of Sundhed.dk and the Shared Medication Record could be mentioned as successful examples. In other areas, there are still room for improvements.

2. Summary of legal requirements applying to EHRs

There is no special and comprehensive regulation on EHRs in Danish law. Consequently, the general regulation on processing of personal data[2] together with regulation on patients rights[3] and health care professional's duties and obligations[4] apply both for paper based health records and EHRs.

There is, however, a few specific rules targeting EHRs in the general regulation of health care services, health care professionals obligations and patients' rights. The special rules are concerned with health care professionals access to EHRs and patients' right to self-determination in this regard, and with storage of information in and access to the Shared Medication Record.

In general, there are very few *requirements on the institutions hosting* EHRs. The general data protection rules apply, and according to the Act on Processing of Personal Data (APPD), it is easy to set up EHRs in both the public and the private health care services.[5] Rules are generally stricter in the public health care services, than among private health care providers. In the private health care sector, private hospitals are subject to stricter rules than individual practising health care practitioners.

Patients' right to self-determination is an important principle in Danish health care legislation[6]. However, in regards to creating health records and storing, updating and having access to information in records, the legislation takes a balanced approach based on a combination of professional obligations and presumed patient consent. Keeping and updating health records is a mandatory obligation for all licensed health care professionals in Denmark, and patient consent is irrelevant in this respect.[7] In regards to access to and disclosure of data, the principle of confidentiality applies, and, as a rule, consent from the patient is required. However, the legislation strives at the same time to facilitate provision of care, and to ensure good quality and patient safety. Hence, it takes a rather sophisticated approach distinguishing between access by other health care professionals involved in

[1] See e.g. , "eHealth in Denmark. – eHealth as part of a coherent Danish health care system", Ministry of Health, April 2012. Available at http://www.medcom.dk/dwn5350 (last accessed February 2014).
[2] Act No. 429 of 31 May 2000 on Processing of Personal Data.
[3] There is no special patients' rights act, but a special section in the Health Act (Consolidating Act no. 913 of 13 July 2010 – Health Act). is dedicated to patients' rights.
[4] Consolidating Act no. 877 of 4 August 2011 on Authorisation of Health Care Professionals and on Health Care Services.
[5] Act No. 429 of 31 May 2000 on Processing of Personal Data, Art. 43-51 supplemented by Executive Order no. 528 of 15 June 2000 on Security Measures for the Protection of Personal Data Processed for Public Authorities.
[6] Patients' right to self-determination is stipulated in Consolidating Act no. 913 of 13 July 2010 – Health Act, Art. 16-17.
[7] Rules on patients records are laid down in Consolidating Act no. 877 of 4 August 2011 on Authorisation of Health Care Professionals and on Health Care Services. Art. 22- 25, and in Executive Order no. 3 of 2 January 2013 on Licensed Health Care Professionals' Patient Records.

the treatment, access by health professionals not directly involved in the particular treatment and access by other persons (health administrators, insurance companies, social services etc).[8] In general, the law relies on patients implied acceptance of health professionals getting access to health records whenever this is necessary for provision of treatment and care. It is expected that the patient's consent to treatment also implies consent for involved health professionals to access or disclose health data necessary for the actual treatment. As a consequence of the assumption of implied acceptance, it is recognised that patients are entitled to prohibit access to health records in these situations. Instead of demanding a specific consent, the patient is instead allowed to refuse processing of health data. In a few situations, patient consent is not needed, and patients are not allowed to refuse access to their health records. This is normally the case in situations where important societal interests or interests of other individuals take precedence over the patients right to self-determination.

The development of an eHealth architecture has enforced *patients' right to access health data.* It has been legally acknowledged that if patients should profit from the opportunities provided by the technological development, previous rules, which allowed health care professionals to refuse access to patients in special situations, had to be abandoned. In the current legislation there are no restrictions on patients' right to access his/her health data. This may be one of the major practical achievements of the establishment of sundhed.dk and the digital platforms hosted by sundhed.dk (Sundhedsjournalen (the Health record), E-journalen (E-record), P-journalen (P-record) and Shared Medication Record (SMR).

In regards to *liability* issues there are no specific rules in Danish law addressing liability in connection with the creation, updating, storage and use of information in EHRs. However, general liability measures apply which involves both disciplinary and penal liability. Keeping health records is part of licensed health care professionals obligation, and non-compliance can lead to disciplinary sanctions. Likewise, confidentiality is also a professional obligation for which violations can be met with both disciplinary and penal sanctions. Finally, violation of the data protection legislation may also result in economic liability or penal sanctions.

According to the general rules on health records, EHRs must as a main rule be stored for a period of ten years after the last recording of data. However, for some health care professionals the archiving period is only five years. There is no legal obligation to delete the data after the mandatory archiving period has expired, but the data protection legislation generally requires that data are not kept longer than necessary for the purpose for which they were collected.

Data in EHRs can be used for *secondary purposes* (e.g. research and quality control) in accordance with the general health regulation and the APPD. In general, data can be used for quality control, research and statistics without the patient's consent, provided there is compliance with the APPD. In some situations a notification and/or approval from the Data Protection Agency is necessary (e.g. research or quality control carried out in the public sector), whereas this is not the case in other situations (e.g. research carried out in the private sector). Normally, patient consent is not necessary, and research on health data does not need approval from a research ethics committee.

The Danish EHR-system is a national solution, which is not designed to interact with similar systems in other countries. In fact, ensuring national interoperability has turned out to be challenging in itself. Some Danish EHRs are centralised in one database at a national level. This is the case for the SMR and the E-journal and P-journal. In regards to the SMR, the HA, Article157 and Article157a clearly presupposes that registration of prescribed medicine and vaccinations will take place in one centralised database. Furthermore, the HA, Article 193a authorises the Minister of Health with power to issue executive orders to ensure applications of standards, and Article 193b has the aim to ensure the establishment of a National Patient Index. Although the initial ideas and visions regarding the National Patient Index has turned out to be too ambitious, the development of the national E- and P-journal rely

[8] Access to EHRs and patient consent is regulated in Consolidating Act no. 913 of 13 July 2010 – Health Act, Art. 42a-42c and Art. 157-157a

on this legal basis.

The Danish ePrescription system and the SMR are closely linked but are not dependent of each other. This means that patients with a manual prescription will have data about prescribed medicine registered in the SMR, and that patients without a SMR (e.g. a person visiting Denmark as a tourist) in principle can make use of ePrescriptions. However, when ePrescriptions are used, it facilitates the pharmacies procedure in keeping the SMR updated. Pilot testing of cross border use of electronic prescriptions is currently taking place within the framework of the epSOS collaboration.

3. Good practices

Even though the Danish legislation on access to EHRs is complex, it seems that using a "need to know" principle as basis for regulation of access to various health care professionals is operating quite well. In addition, relying on implied patient consent to access and use data in situations, where patients are undergoing treatment, is also mentioned in the interviews as a clear advantage for health care professionals. It diminish bureaucratic barriers while at the same time acknowledging the patient's right to self-determination

4. Legal barriers

There are very few legal barriers for the deployment of EHRs in Denmark. As the Danish legislation is quite pragmatic in regards to formal requirements (patient consent, approval of health institutions or individuals using EHRs etc), there are not many bureaucratic obstacles for creating and making use of EHRs. In one of the interview it was, however, mentioned, that emergency doctors, monitoring patient care off-hours, don't have access to the EHR kept by the patient's normal GP. Even though the emergency doctor has access to the patient's EHRs available at sundhed.dk, these do not contain the same comprehensive information as the GP's EHR. According to information provided in another interview, this situation may not be a result of legal but rather technical barriers.

Another obstacle concerns access to EHRs for patients under the age of 15 years. In case of children under the age of 15 years, direct online access to EHRs is not possible. In order to ensure the interests of minor patients' right to privacy and to protect the best interest of the child, the health legislation allows health care professionals to limit parents' access to health information concerning their child. As this cannot be monitored technically in the EHRs, it has been necessary to exclude on-line access to HER's of this group of patients.

Interestingly, it was also mentioned in one of the interviews, that the Danish legislation in some ways is too permissive in allowing many groups of health professionals to have widespread access to patient records. This could undermine confidentiality and trust between the patient and the primary caregiver (e.g. the GP) and thus be an impediment for providing the best possible care. The widespread access to the SMR together with an obligation for GP's to provide patient data to the regions for planning purposes was mentioned as examples of rules, which could potentially hamper confidentiality in the doctor – patient relationship.

Contents

List of abbreviations

EHRs	Electronic Health Records
AOA	Act on Autorisation of Health Care Professionals and on Health Care Services: Consolidating Act no. 877 of 4 August 2011 (lovbekendtgørelse nr. 877 af 4.august 2011 om authorisations af sundhedspersoner og om sundhedsfaglig virksomhed)
APPD	Act on Processing of Personal Data: Act No. 429 of 31 May 2000 (lov nr. 429 af 31. Maj 2000 om behandling af personoplysninger)
HA	Health Act, Consolidating Act no. 913 of 13 July 2010 (lovbekendtgørelse nr. 913 af 13. Juli 2010. Sundhedsloven)
SMR	Shared Medication Record (Fælles medicinkort)

1. General context

1.1. EHR systems in place

There is no universal Danish EHR-system. The EHR-system is build of various blocks operating at local, regional and national level. Historically, the General Practitioners were the frontrunners in using EHRs and also in developing a common standard for EHRs. In the hospital sector the use of EHRs is also widespread. However, despite many years' attempts to create a uniform national standard for EHRs within the hospital sector, it seems to be very difficult, and the hospitals still rely on various regional and local solutions[9]. Consequently, most basic information in various parts of the health care sector has been digitalised, but (unfortunately) a number of different EHR-systems are operating.

In order to have a more coordinated and efficient development, the Danish Government and the Danish Regions (association for the five Danish regions) reached an agreement in 2010 on a number of changes in the organisational setup of the eHealth structure. Among other things this has recently resulted in efforts focusing on integration and streamlining of data sharing and access across the health system to profit from existing e-ressources and make all relevant patient data more accessible when needed. A special public authority – the National eHealth Authority – has been set up by the Ministry of Health with the task of ensuring a more coherent and standardised framework for EHS's. Another result of the agreement between the two parties, was the launch of a major project on the development of a National Patient Index which should be a comprehensive digital platform allowing all health care professionals access to and overview of all existing data on patients stored in all parts of the health care sector. The project was, however, put on hold in 2013, when it turned out not to be economically and technically feasible.

At a national level the EHR-structure consist primarily of the following elements:

- E-Journalen (E-record), which is a centralised database, collecting information from hospitals in all the five Danish regions. E-journalen is supplemented by P-journalen (P-record), which is a centralised data base collecting patient data from GP's and other private practising health care professionals. Information in E-Journalen and P-Journalen is accessible for all health care professionals as well as for the patient by using NemID (easy-ID – a national digital signature platform)
- Fælles Medicinkort (Shared Medication Record (SMR)), which store information about patient's prescribed medication (the medication module of the SMR) and information about vaccinations (the vaccination module of the SMR). Both health care professionals and patients can access this information by using NemID.
- Sundhed.dk is a digital platform set up by the Ministry of Health in collaboration with Danish Regions and Local Government Denmark (association of the 98 municipalities). Sundhed.dk is hosting E-journalen, P-journalen, SMR and other databases with relevant patient information (e.g. registry on advance directives). Together these information tools constitute the Sundhedsjournal (Health Record). Sundhed.dk also provides general information to patients and health care professionals.

In addition to these centralised platforms EHRs are used regionally/locally by municipalities, individual health care professionals as well as hospitals.

In general, the use of EHRs is not restricted to certain health professionals, institutions or types of

[9] In 2007 there were 27 different EHR-solution operating in the five Danish regions. The aim has been to reduce this to give coherent EHR-landscapes by the end of 2013 – one for each of the five regions, cf. Ministry of Health, "eHealth in Denmark. – eHealth as part of a coherent Danish health care system", Ministry of Health, April 2012. Available at http://www.medcom.dk/dwn5350 (last accessed February 2014)

patients. There may be certain restrictions on access to EHRs, which is normally based on an assessment of "need to know" in order to provide due care.

1.2. Institutional setting

The main responsibility for implementing eHealth policies has for many years been shared among the Ministry of Health, the National Board on Health and Medicine, the five regions and the 98 municipalities. The Danish Data Protection Agency (Datatilsynet) is also an important actor. In addition, some actors have been assigned special tasks and authority to develop comprehensive and robust eHealth architecture.

- The Ministry of Health (Ministeriet for forebyggelse of sundhed)

The Ministry has the overall responsibility for public health and for the organisation of the health care sector. In regards to EHRs, the Ministry is responsible for overall development and national coordination and prioritization, and has legislative power and legislative responsibility in regards to the development of eHealth systems. The Ministry has set up the National eHealth Authority (see below)

- Regions

The five Danish regions are responsible for the hospital sector and provision of care by GP's, specialists and other private practising health care professionals. In regards to EHRs, the regions are responsible for investments in and the implementation of specific eHealth solutions. The five regions have an association – Danish Regions – which represents them in various settings.

- Municipalities

The 98 municipalities are responsible for primary care at citizens home, in schools etc. Development of eHealth-solution for primary care is an integrated part of the Danish eHealth system, and there are developed special EHR-solutions for home care. Likewise, health care professionals working at municipality level can access some of the EHRs available at sundhed.dk.

- Danish Data Protection Agency

The Danish Data Protection Agency (Datatilsynet) is the administrative authority assigned with the task to ensure compliance with the Act on Processing of Personal Data. This Agency provides guidance and advice to authorities, companies and citizens. In areas where this is legally required, it receives notifications of applications for authorization of processing of personal data. When receiving such notifications and applications the Agency can give its opinion and stipulate binding criteria for processing of data. As EHRs involves processing of sensitive personal information, the Agency is an important actor in this field. The Agency receives complaints and can perform audits, and it can give its general opinion on e.g. proposal for new laws and regulation.

- The National Board on E-health

As a part of an agreement reached between the Danish Government and Danish Regions in 2010 (see above), a board has been established to advise the Minister of Health. The advisory board consists of three representatives from the government, three representatives from the regions and one representative from the municipalities. The role of the board is to advice relevant ministers on the overall strategy and development within eHealth, and to ensure coordination and follow up regarding progress and benefits realization.

- National eHealth Authority

The National eHealth Authority has recently been established and located administratively at Statens Serum Institute. The Authority is assigned with the task of developing national standards for eHealth to ensure coherent data and ICT architecture for the Danish healthcare sector. One of the major projects was the development of a National Patient Index which should be a comprehensive digital platform allowing for compilation and exchange of health data. However, the project was cancelled in 2013, when it turned out that the project was not economically and technically feasible.

- MedCom

MedCom has since 1994 been a strong actor in the area of eHealth development. It is a public funded, non-profit cooperation financed and owned by The Ministry of Health, Danish Regions and Local Government Denmark (association of the 98 municipalities). MedCom has among other things participated in the development of E-journalen (the E-record) and P-journalen (the P-record) and is hosting The Danish Healthcare Data Network (SDN) and video hub (VDX).

1.3. Legal setting and future legal development

There is no special and comprehensive regulation on EHRs in Danish law. Consequently, the general regulation on processing of personal data[10] together with regulation on patients rights[11] and health care professional's duties and obligations[12] apply both for paper based health records and EHRs. In regards to EHRs, the provisions in the AOA on patient records and health care professionals duty of providing due care, is of special importance together with regulation of access to and disclosure of health data laid down in the HA. APPD is also of importance, as it supplements the rules on processing of personal data in the general health legislation.

In addition to the general legal framework, there are also a few rules in the HA specifically targeting EHRs. The special rules are concerned with health care professionals access to EHRs and patients' right to self-determination in this regard (HA, Art. 42a-42c), and with registration of information and access to the Shared Medication Record (Art. 157-157a).

The legislation relevant for EHRs has developed gradually. A new scheme for regulating access to and sharing of health data was introduced with the Patients' Rights Act (1998). The provisions in this act were, however, to a large degree relying on a paper based patient record system. It was e.g. unclear whether "direct access" to health data in EHRs was covered by the regulation, which was exclusively concerned with "disclosure" of information from health care professionals. When a new comprehensive Act on Health came into force in 2005, the provisions from the Patients Rights Act was transferred without any changes. It was first in 2007 that the Health Act was amended with special provisions (Art. 42a-42f) specifically addressing access to EHRs[13]. Initially widespread access was restricted to doctors and dentists. Other health care professionals had only more limited access. A later amendment in 2011 has granted widespread access to a wider group of health care professionals.

A separate legislative initiative to set up an electronic Personal Medicine Profile was taken in 2003[14]. The profile provides an electronic overview of the purchase of prescribed pharmaceuticals. All purchases are registered automatically on the citizens' individual personal profile. Registration is mandatory. Initially, access to the profile was restricted to doctors, but in later amendments access has been granted to a wide group of health care professionals and also to other persons working in social institutions, prisons etc. The Personal Medical Profile is now part of the Shared Medication Record

[10] Act No. 429 of 31 May 2000 on Processing of Personal Data.
[11] There is no special patients' rights act, but a special section in the Health Act (Consolidating Act no. 913 of 13 July 2010 – Health Act). is dedicated to patients' rights
[12] Consolidating Act no. 877 of 4 August 2011 on Authorisation of Health Care Professionals and on Health Care Services.
[13] Act no. 431 of 8 May 2007.
[14] Act no. 378 of 28 May 2003.

and regulated by HA, Art. 157[15]. An electronic Vaccination Register was set up in 2010 with an amendment to the Health Act (Art. 157a)[16]. The main purpose was to keep a register on all HPV-vaccines, but the register stores data about all vaccinations. It is the other component of the Shared Medication Record.

Since February 2007 the Personal Medicine Profile has been supplemented by a Prescription Server. All electronic prescriptions are transferred to the Prescription Server, which is connected to the Personal Medicine Profile. The pharmacies have access to the Prescription Server, and can deliver pharmaceuticals to patients on the basis of the prescription. The patient can obtain the medicine at any pharmacy and does not need to decide in advance which pharmacy to use. The prescriptions is stored in the server which means that the patient does not need him or herself to keep the prescription in situations where the prescriptions covers several dispenses of medicine. Pilot testing of cross border use of electronic prescriptions is currently taking place within the framework of the epSOS collaboration. ePrescriptions are covered by the same regulation as other prescriptions[17].

Main legislation relevant for the use of EHRs in Denmark:

Penal Code: Consolidating Act no 1028 of 22 August 2013 (lovbekendtgørelse nr. 1028 af 22. august 2013 – Straffeloven.

Act on Complaints and Compensation within the Health Care Services: Consolidating Act no. 1113 of 7 November 2011 (lovbekendtgørelse nr. 1113 af 7. november 2011 om klage og erstatning inden for sundhedsvæsenet)

Act on Authorisation of Health Care Professionals and on Health Care Services: Consolidating Act no. 877 of 4 August 2011 (lovbekendtgørelse nr. 877 af 4.august 2011 om autorisation af sundhedspersoner og om sundhedsfaglig virksomhed)

Act on Research Ethics Review of Health Research Projects: Act no. 593 of 14 June 2011 (lov nr. 593 af 14. Juni 2011 om videnskabsetisk behandling af sundhedsvidenskabelige forskningsprojekter)

Health Act: Consolidating Act no. 913 of 13 July 2010 (lovbekendtgørelse nr. 913 af 13. Juli 2010. Sundhedsloven). There are 25 amendments to the Act of which the following are of particular relevance:

- Act no 605 of 14 November 2011 (extended access to public registers and electronic health records etc)
- Act no 603 of 18 June 2012 (revision regarding planning, collaboration, IT, quality and financing of the health care sector etc)
- Act 1638 of 26 December 2013 (implementation of part of directive 2011/24/EU on the application of patients' rights in cross border health care etc)

Act on Processing of Personal Data: Act No. 429 of 31 May 2000 (lov nr. 429 af 31. Maj 2000 om behandling af personoplysninger)

Executive Order no. 1671 of 12 December 2013 on Prescriptons (bekendtgørelse nr. 1671 af 12. December 2013 om recepter (receptbekendtgørelsen).

[15] The Ministry of Health has issued a Executive Order with specific rules about the content, registration and access to the Personal Medical Profile (Executive Order no. 436 of 11 May 2011 regarding the Danish Health and Medicine Authority's Electronic Registration of Information regarding Individual Citizens' Medicine)
[16] The Ministry of Health has issued a Executive Order with specific rules about the content, registration and access to the Vaccination Register (Executive Order no. 1017 of 25 August 2010 on Statens Serum Institut's Electronic Registration of Individual Citizens' Vaccinations and Related Information).
[17] Executive Order no. 1671 of 12 December 2013 on Prescriptions

Executive Order no. 160 of 12 February 2013 on Standards for use of IT in the Health Care Services (Bekendtgørelse nr. 160 af 12. Februar 2013 om standarder for IT-anvendelsen i sundhedsvæsenet)

Executive Order no. 3 of 2 January 2013 on Licensed Health Care Professionals' Patient Records (Bekendtgørelse nr. 3 af 2. Januar 2013 om autoriseret sundhedspersoners patientjournaler (journalføring, opbevaring, videregivelse og overdragelse m.v.))

Executive Order no. 436 of 11 May 2011 regarding the Danish Health and Medicine Authority's Electronic Registration of Information regarding Individual Citizens' Medicine (Bekendtgørelse nr. 436 af 11. Maj 2011 om Lægemiddelstyrelsens elektroniske registering af de enkelte borgeres medicinoplysninger)

Executive Order no. 1017 of 25 August 2010 on Statens Serum Institut's Electronic Registration of Individual Citizens' Vaccinations and Related Information (Bekendtgørelse nr. 1017 af 25. August 2010 om Statens Serum Instituts elektroniske registrering af de enkelte borgeres vaccinationer og hertil knyttede oplysninger)

Executive Order no. 528 of 15 June 2000 on Security Measures for the Protection of Personal Data Processed for Public Authorities (Bekendtgørelse nr. 528 af 15. Juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, der behandles for den offentlige forvaltning)

2. Legal requirements applying to EHRs in Denmark

2.1. Health data to be included in EHRs

2.1.1. Main findings

Danish law does not have special rules regarding the content of EHRs. The general rules in the health legislation regarding data to be included in patient records apply. These rules are laid down in the AOA and further detailed in Executive Order no. 3 of 2 January 2013 on Licensed Health Care Professionals' Patient Records. A patient record can both be a paper record and an EHR. The Executive Order provides a rather comprehensive list of data, which – provided it is relevant – must be filed in the record. These data include general patient information as well as information related to the specific decisions and services provided to the patient in the health care sector (examinations, analysis, diagnosis, prescribed medicine, surgeries etc). Other relevant information such as X-rays, CT- and MR scans, laboratory analysis etc, must also be included in the patient record. Although the rules are rather detailed, they still allow for some professional discretion of whether it is relevant to record data or not.

There are no special rules for special types of data (e.g. blood tests etc). The rules also allow for recording of non-purely medical information, and in practise it is normal to record information of a more socio-economic character. In one of the interviews it was also mentioned that the increased focus on prevention of life style diseases in the Danish health care sector, encourages health care professionals to discuss life style issues with patients and record observations from these conversations.

In addition to the general rules on health records there are separate regulation of the content of SMR's issued in Executive Order no. 1017 of 25 August 2010 on Statens Serum Institut's Electronic Registration of Individual Citizens' Vaccinations and Related Information and in Executive Order no. 436 of 11 May 2011 regarding the Danish Health and Medicine Authority's Electronic Registration of Information regarding Individual Citizens' Medicine. These rules are more precise and leaves less discretion to the health care professional compared with the general rules on health records.

2.1.2. Table on health data

Questions	Legal reference	Detailed description
Are there specific rules on the content of EHRs? (or regional provisions, agreements, plans?)	AOA articles 22-25. Executive Order no. 3 of 2 January 2013 on Licensed Health Care Professionals' Patient Records. HA, Art. 157-157a. Executive Order no. 1017 of 25 August 2010 on Statens Serum Institut's Electronic Registration of Individual Citizens' Vaccinations and Related Information. Executive Order no. 436 of 11 May 2011 regarding the Danish Health and Medicine Authority's Electronic Registration of Information regarding Individual Citizens' Medicine	There are not special rules for EHRs, but the general rules regarding patient records applies to both manual and electronic health records. According to Act on Authorisation of Health Care Professionals and on Health Care (AOA), Art. 22, there must be an individual patient record, which according to Art. 23 of the Act may both be a manual and an electronic record. The content of the record is stipulated in Executive Order no. 3 of 2 January 2013 on Licensed Health Care Professionals' Patient Records, which does not distinguish between manual and electronic health records. According to Art. 2.1 of Executive order no. 3 of 2 January 2013 on Licensed Health Care Professionals' Patient Records a patient record is registered information regarding a patient's medical condition and the planed and performed treatment, including which information was given in advance to the patient and the patient's decisions based on this information. The general aim of the patient record is according to Art. 2.4 of the Order to serve as a means of communication and documentation about the patient and the treatment provided in order to ensure good patient safety, continuity of care and provide for audit and quality control. Art. 10 of the Order specify in details the specific content of the patients' health record. According to Art. 10.1 all health records must list the name and the personal identification number of the patient. According to Art. 10.2 the record must in addition – and provided it is relevant – include the following information: ▪ General patient information (address, contact details of relatives, identity of proxy if patient is unable to give consent, allergies, other health care providers involved in the treatment, information about advance directives) ▪ Information regarding specific patient contacts (including the purpose of the contact, description of the medical history and current health status, observations and medical examinations and analysis, results of such examinations and analysis (including

Questions	Legal reference	Detailed description
		description of analysis of tissues samples, X-rays, CT and MR scans etc), indication for examinations and analysis, treatment and care provided including detailed information about prescribed medicine (name, doses, period etc) and vaccinations, information about side effects and complications (including incidents of malpractice), information about referrals to or advice obtained from other health care providers, content of discharge letters, control and follow-up settlements, information, instructions and advice given to patient) ▪ Other relevant information and material (X-rays, clinical photos, descriptions of CT and MR scans laboratory results, information about anesthesia and other important clinical information) ▪ Other information (including name of health care professionals involved in the treatment, decisions made regarding analysis and treatments, plan for follow up, information regarding medical implants and information about side effects and complications as well as incidents of medical malpractice) In regards to the SMR's there are special rules in the Health Act (HA), Art. 157-157a regarding registration of data on medicine and vaccinations, and powers to issue executive orders, specifying which data should be registered, is delegated to the Minister of Health. The Minister has issued two separate orders regarding registration of individual citizens' vaccinations and medicine consumption. As this information is focused on particular medical "events" (provision of vaccination and prescribed medicine) the rules regarding the content of the SMR's are simpler compared to the rules governing health records in general. SMR's must contain name and date of the vaccination, name and indication of prescription of medicine as well as the doses, and the dates of prescription etc.
Are these data restricted to purely medical information (e.g. physical or mental health, well-being)?		The general rules on patient records in Executive Order no. 3 of 2 January 2013 on Licensed Health Care Professionals' Patient Records stipulates that the name of patient's relatives must be specified. Furthermore, information regarding instructions of the patient must also be provided.

Questions	Legal reference	Detailed description
		This may include non-purely medical information. In general, the order presupposes that other information about the patient will be part of the record as it stipulates in Art. 2.1 that supplementary private and confidential information, which is registered, is considered to be part of the official patient record. In general, patient records normally contains general observation and description of patient which has a more social / socio-economic character.[18] Obligation to register such information is, however, not specified in the legal rules, and health care professionals must ensure compliance with the Act on Protection of Personal Data when registering such supplementary data. Executive Order no. 1017 of 25 August 2010 on Statens Serum Institut's Electronic Registration of Individual Citizens' Vaccinations and Related Information and Executive Order no. 436 of 11 May 2011 regarding the Danish Health and Medicine Authority's Electronic Registration of Information regarding Individual Citizens' Medicine provides for "free text" relevant for e.g. handing over, administration of, and consumption of medicine and regarding vaccination. This free text may include other information than purely medical information, and as stressed above, health care professionals must ensure compliance with the Act on Protection of Personal Data when registering such supplementary data.
Is there a definition of EHR or patient's summary provided in the national legislation?	Executive Order no. 3 of 2 January 2013 on Licensed Health Care Professionals' Patient Records, Art. 2.1	There is no definition of EHR provided in the legislation, and as there are so many different types of the EHRs it may be difficult is to agree on a unique definition. However, there is a legal definition of patient records in Art. 2.1 of Executive Order no. 3 of 2 January 2013 on Licensed Health Care Professionals' Patient Records. According to this definition a patient record is registered information regarding a patient's medical condition and the planed and performed treatment, including which information was given in advance to the patient and the patient's decisions based on this information. It is also stipulated that additional/supplementary private and confidential information registered, is also considered to be part of the official patient record.

[18] Information provided in interview with MD Malene Mohr, former chairperson of Lægeansvarsudvalget (Medical Responsibility Board) at the Danish Medical Association.

Questions	Legal reference	Detailed description
Are there any requirements on the content of EHRs (e.g. detailed requirements on specific health data or general reference to health data)?	AOA Art. 22-25. Executive order no. 3 of 2 January 2013 on licensed health care professionals' patient records. HA articles 157-157a. Executive order no. 1017 of 25 August 2010 on Statens Serum Institut's Electronic Registration of Individual Citizens' Vaccinations an Related Information. Executive order no. 436 of 11 May 2011 regarding the Danish Health and Medicine Authority's Electronic Registration of Information regarding Individual Citizens' Medicine	There are no special legal requirements on the content of EHRs, but the general rules regarding patient records applies to EHRs. The specific requirement regarding the information, which must be included in all patient records, is stipulated in Executive Order no. 3 of 2 January 2013 on Licensed Health Care Professionals' Patient Records (see answer above for more details) In regards to SMR's there are specific requirements regarding registration of information related to vaccinations stipulated in Executive order no. 1017 of 25 August 2010 on Statens Serum Institut's Electronic Registration of Individual Citizens' Vaccinations an Related Information, and also specific requirement regarding registration of information on medicine stipulated in Executive order no. 436 of 11 May 2011 regarding the Danish Health and Medicine Authority's Electronic Registration of Information regarding Individual Citizens' Medicine (see answer above for more details)
Are there any specific rules on the use of a common terminology or coding system to identify diseases, disorders,	(Executive order no. 436 of 11 May 2011 regarding the Danish	The National eHealth Authority at Statens Serum Institute is the responsible organisation in regards to monitoring and developing the

Questions	Legal reference	Detailed description
symptoms and others?	Health and Medicine Authority's Electronic Registration of Information regarding Individual Citizens' Medicine	Danish e-health architecture. This also includes the task of developing uniform standards / coding systems based on international standards.[19] Currently there are rules stipulating the mandatory use of coding system in regards to indication and dose of medicine (Executive order no. 436 of 11 May 2011 regarding the Danish Health and Medicine Authority's Electronic Registration of Information regarding Individual Citizens' Medicine) and use of medical devises (Executive Order no. 3 of 2 January 2013 on Licensed Health Care Professionals' Patient Records). Apart from this, there are no legal rules stipulating mandatory use of common terminology. Among General Practitioners a uniform national coding system on diagnosis and services seems to be widely used.[20] In the hospital sector the WHO ICD-10 codes are used.[21]
Are EHRs divided into separate categories of health data with different levels of confidentiality (e.g. data related to blood type is less confidential than data related to sexual diseases)?	Executive Order no. 3 of 2 January 2013 on Licensed Health Care Professionals' Patient Records	According to the general rules laid down in Executive Order no. 3 of 2 January 2013 on Licensed Health Care Professionals' Patient Records, the patient must only have one record at each health care facility. However, it is possible at hospitals to have a psychiatric record separated from the somatic patient record.
Are there any specific rules on identification of patients in EHRs?		There are no specific rules on identification of patients in EHRs. In general, the regulation regarding patient records stipulates the mandatory use of the patient's personal identification number (the CPR number). In Denmark this is a unique identifier used in all parts of the health care services and in general by all public authorities. It is also widely used in the private sector.
Is there is a specific identification number for eHealth purposes?		There is no specific identification number for eHealth purposes. The personal identification number is used as unique identifier in all contacts between the citizens and public authorities (including the public part of the health care services), and it is mandatory to use the number in the private part of the health care services as well (article 10.1 of Executive Order no. 3 of 2 January 2013 on Licensed Health Care Professionals' Patient

[19] Executive Order no. 160 of 12 February 2013 on Standards for use of IT in the Health Care Services. Information about the work of Statens Serum Institute in this area is available at this link http://www.ssi.dk/English/HealthdataandICT/The%20National%20eHealth%20Authority/Terminology.aspx (last accessed February 2014)
[20] Information provided in interview with MD, GP, Ole Noerskov, Chairperson of Lægeansvarsudvalget (The Medical Responsibility Board), Danish Medical Association
[21] Information provided in interview with MD, Chief Physician, Martin Hulgaard, Kolding Hospital

Questions	Legal reference	Detailed description
		Records).

2.2. Requirements on the institution hosting EHRs data

2.2.1. Main findings

Danish law does not contain specific rules on institution hosting EHRs data (e.g. prior authorisation of institutions hosting EHRs data). The general rules on processing of personal data laid down in the APPD applies and in terms of formalities APPD distinguish between hosting of EHRs in the public and the private sector.

Generally, the rules are stricter in the public than in the private sector. Hence, hosting and processing of data from EHRs in the *public* health care sector requires both notification to and prior opinion of the Data Protection Agency (Datatilsynet) before any processing of data is allowed (APPD, Art. 45). Furthermore, it is required that the data controller has a security system in place, which ensures that personal data can only be accessed and processed by persons when this is necessary for the performance of professional tasks and based on individual authorisation (Art. 10-11 of Executive Order no. 528 of 15 June 2000 on Security Measures for the Protection of Personal Data Processed for Public Authorities).

In contrast, EHRs in the *private* health sector are subject to less formalistic rules; especially in regards to practising, licensed health care professionals. They are exempted from the normal requirement of obtaining authorisation from the Data Protection Agency, provided processing is necessary to perform his/her professional activities. Accordingly, hosting and processing of EHRs among private practitioners must be notified to the Data protection Agency, but no authorisation is needed. If, however, EHRs are hosted and data processed by a private hospital, it is mandatory both to notify and get an authorisation from the Agency.

When it comes to *data security* there is also a formal difference between the public and the private sector. Data security in the public sector is regulated in Executive Order no. 528 of 15 June 2000 on Security Measures for the Protection of Personal Data Processed for Public Authorities, which stipulates a number of rules for public sector EHRs. There are no similar explicit rules regulating EHRs in the private health care sector. However, all data controllers must comply with general security rules laid down in APPD, and the Data Protection Agency recommends that data controllers in the private sector take notice of and follow relevant rules laid down in Executive Order no. 528 of 15 June 2000 on Security Measures for the Protection of Personal Data Processed for Public Authorities.

2.2.2. Table on requirements on the institutions hosting EHRs data

Questions	Legal reference	Detailed description
Are there specific national rules about the hosting and management of data from EHRs?		There are no specific rules about hosting and management of data from EHRs. The general rules on processing of personal data laid down in the APPD apply (see below for details)
Is there a need for a specific authorisation or licence to host and process data from EHRs?	Act No. 429 of 31 May 2000 on Processing of Personal Data (APPD) Executive Order no. 528 of 15 June 2000 on Security Measures for the Protection of Personal Data Processed for Public Authorities	In regards to hosting and processing of data from EHRs in the *public* health care sector APPD, Art. 45, requires notification to and prior opinion of the Data Protection Agency (Datatilsynet) to allow processing of data. Furthermore, the data controller must have a system, which ensures that personal data can only be accessed and processed by persons for the performance of professional tasks and based on individual authorisation (Art. 10-11 of Executive Order no. 528 of 15 June 2000 on Security Measures for the Protection of Personal Data Processed for Public Authorities). Normally, authorisation from the Data Protection Agency is necessary for private actors processing sensitive personal data. However, according to APPD, Art. 49, such authorisations is not needed if the processing is carried out by a licensed health care professional and provided the processing is necessary to perform his/her professional activities. Accordingly, hosting and processing of EHRs among private practitioners must be notified to the Data protection Agency, but no authorisation is needed. If, however, EHRs are hosted and data processed by a private hospital, it is mandatory both to notify and get an authorisation from the Agency.
Are there specific obligations that apply to institutions hosting and managing data from EHRs (e.g. capacity, qualified staff, or technical tools/policies on security confidentiality)?	APPD Executive Order no. 528 of 15 June 2000 on Security Measures for the Protection of Personal Data Processed for Public Authorities	In general, persons or institutions processing personal data must comply with the rules laid down in APPD and the administrative orders issued based on delegated powers laid down in APPD. In regards to security measures APPD, Art. 41.3, stipulates that the data controller shall implement appropriate technical and organizational security measures to protect data against accidental or unlawful destruction, loss or alteration and against unauthorized disclosure, abuse or other processing in violation of the provisions laid down in APPD. Individuals, companies' etc.

Questions	Legal reference	Detailed description
		performing work for the data controller and who have access to data may, according to APPD, Art. 41.1, process these only on instructions from the controller unless otherwise provided by law or regulations. More detailed rules regarding security of data within the *public* sector is laid down in Executive Order no. 528 of 15 June 2000 on Security Measures for the Protection of Personal Data Processed for Public Authorities. These rules include an obligation for the data controller to issue internal security rules and also to have a system of authorisation of persons who have access to personal data (see above). It is furthermore required to register all rejected attempts to access personal data and to keep a log file on all processing of personal data. This is also applicable to processing of data from EHRs within the public health care sector. The Data Protection Agency may also stipulate special conditions in its opinion to public data controllers when it is notified about processing of sensitive personal data in EHRs. In regards to the use of Sundhedsjournalen (the Health Record) the Data Protection Agency has stipulated a number of conditions.[22] Similar specific rules are not generally applicable for data controllers in the private sector, but all data controllers are under an obligation to comply with the general data security rules laid down in APPD and are advised to follow the same standard as in the public sector. In addition special conditions may be laid down in the authorisation issued by the Data Protection Agency to the data controller. In practise, such conditions will only apply to private hospitals, as individual health care practitioners in the private sector don't need an authorisation (see above).
In particular, is there any obligation to have the information included in EHRs encrypted?		In general, it is the data controller's responsibility to ensure a sufficient level of security. Hence, there is no general obligation laid down in the regulation to have information included in EHRs encrypted. However, the Data Protection Agency requires transmission of sensitive personal data on

[22] See decision from the Data Protection Agency of 10. May 2012, journalnummer 2011-082-0234 on Sundhedsjournalen og det Nationale Patient Indeks (NPI). The decision is available at this link http://www.datatilsynet.dk/afgoerelser/arkiv-over-afgoerelser/artikel/vedroerende-sundhedsjournalen-og-det-nationale-patient-indeks-npi/ (last accessed February 2014).

Questions	Legal reference	Detailed description
		websites to be encrypted, and it furthermore recommends encryption when sensitive personal data are send by e-mails on the internet.
Are there any specific auditing requirements for institutions hosting and processing EHRs?		There is no specific audit requirement for institutions hosting and processing EHRs, but the Data Protection Agency has legal authority to supervise processing of personal data (APPD, Art. 58) and is entitled to have access to premises to make inspections (APPD, Art. 62)

2.3. Patient consent

2.3.1. Main findings

Patients' right to self-determination is an important principle in Danish health legislation[23]. However, in regards to creating health records the Danish legislation perceives this as a professional obligation of the health care professionals. Hence, keeping and updating health records is a mandatory obligation for all licensed health care professionals in Denmark. Patient consent to the creation of health records is not needed, and patients are not allowed to refuse registration of data in health records provided the registration of these data are based on the health care professionals legal duty to store information in the health record.

In regards to access to and sharing of data, the principle of confidentiality applies, and, as a rule, consent from the patient is required. However, the legislation strives at the same time to facilitate provision of care without too many bureaucratic obstacles and thereby ensure both quality and patient safety. Hence, it takes a rather sophisticated approach distinguishing between access by other health care professionals involved in the treatment, access by health professionals not directly involved in the particular treatment and access by other persons (health administrators, insurance companies, social services etc).[24] In general, the law relies on patients "implied acceptance" of health professionals getting access to health records whenever this is necessary for provision of treatment and care. It is expected that the patient's consent to the treatment also implies consent for health care professionals being part of the "treatment relation" to access or disclose health data necessary for the actual treatment. As a consequence of the assumption of "implied acceptance", it is recognised that patients are entitled to prohibit access to health records in these situations (a kind of opt-out scheme). In a few situations, patient consent is not needed, and patients are not allowed to refuse access to their health records. This is normally the case in situations where important societal interests or interests of other individuals take precedence over the patients right to self-determination.

Interestingly, the patient's right to self-determination is less respected in regards to SMR's where the patient is not allowed to refuse access to this particular health record in situations similar to those where refusal is accepted for other EHRs (see above).

[23] Patients' right to self-determination is stipulated in Consolidating Act no. 913 of 13 July 2010 – Health Act, Art. 15-16.
[24] Access to EHRs and patient consent is regulated in Consolidating Act no. 913 of 13 July 2010 – Health Act, Art. 42a-42c and Art. 157-157a

2.3.2. Table on patient consent

Questions	Legal reference	Detailed description
Are there specific national rules on consent from the patient to set-up EHRs?	AOA Art. 22-25	There are no specific national rules on patient consent for setting up EHRs. According to the general rules on patient records laid down in Consolidating Act no. 877 of 4 August 2011 on Authorisation of Health Care Professionals and on Health Care Services, licensed health care professionals are under an obligation to keep and update health records. This is mandatory, and non-compliance can lead to disciplinary sanctions. Patient consent is not required, and patients' refusal of having information registered must not be respected, as this will be a violation of the professional duty to keep and update patient record.
Is a materialised consent needed?		See answer above
Are there requirements to inform the patient about the purpose of EHRs and the consequences of the consent or withholding consent to create EHRs?	HA, Art. 16-17.	Patient must in general terms be informed about the collection of data taking place in the health care services. This is part of the obligation to provide patients with information relevant for their decisions in regards to treatment (HA, Art. 15-16). It is not required to provide specific/individualised information. It is sufficient that general information – e.g. in a patient leaflet – is available.
Are there specific national rules on consent from the patient to share data?	HA, Art. 41.1, 42, 42a.6, 42a.10, 42b, 43.1, 44, 157.9, and 157a.5	The Health Act includes a number of provisions requiring patient consent to share information in various situations. The rules are in many ways constructed as a "Chinese box". In general, Art. 41.1, stipulates that patient consent is required when disclosing information to other health care professionals (explicit oral consent) and the same applies according to Art. 42.1 when disclosing information for other purposes than patient treatment (explicit written consent). However, there are a number of derogations from the main rule that allows for disclosure of information based on "implied acceptance" from the patient (Art. 41.2.1-3). This is the situation when communication among health care professionals or institutions involved in the treatment of a particular patient is necessary to provide care and treatment, or when sending a discharge letter from the hospital to the patient's General Practitioner. In these situations patients are entitled to refuse disclosure of information on their own initiative (Art. 41.4). Information may also be disclosed without patient consent in situations of necessity or efficiency (Art. 41.2.4-5 and Art. 43.1-3).

Questions	Legal reference	Detailed description
		Art. 42a-42c are specifically targeting access to EHRs. Art. 42a.1 and Art. 42a.2.1-4 lists a number of situations where patient information can be accessed without an explicit consent based on the assumption of "implied acceptance" and necessity of having access to information to provide treatment to the patient ("treatment relation").[25] In these situations patients are entitled to refuse disclosure of information (Art. 42a.7. In addition access to EHRs is allowed in cases of necessity or efficiency (Art. 42a.5 and Art. 42a.8). Apart from these situations, explicit, oral consent from the patient is necessary (Art. 42a.6 and Art. 42a.10) In regards to patient information in the SMR (medicine and vaccination) HA articles 157.1 and 157a.1 list a number of situations where health care professionals can retrieve information from the EMR without patient consent. In situations where information is shared for purposes outside the scope of the list, consent is needed (Art. 157.9 and Art. 157a).
Are there any opt-in/opt-out rules for patient consent with regard to processing of EHRs?	HA Art. 29.1	The HA Art. 29.1 allows patients to opt-out in regards to further use of biological material for others purposes than those related to treatment and other closely related purposes (e.g. quality control). In practice, this means that the patient is entitled to refuse to have his or her biological samples used for research purposes. No similar rule exists in regards to other health data.
Are there any opt-in/opt-out rules for patient consent with regard to sharing of EHRs?	HA Art. 41.4 and Art. 42a.7	In some situations, where the HA allows for sharing of patient data without prior consent, patients are entitled to refuse disclosure or access to their data (Art. 41.4 and Art. 42a.7). See also above. The same option is not available in regards to SMRs.
Are there requirements to inform the patient about the purpose of EHRs and the consequences of consent or withholding consent on the sharing of EHRs?	APPD Art. 28-30 and HA Art. 16	According to APPD Art. 28-29 citizens must be informed about the purpose of the processing for which their data are intended. This general rule also applies in the health care services. There are no specific obligations to inform the patient about the consequences of consenting or withholding consent to sharing of EHRs.

[25] In practice, the "treatment relation"-requirement may be difficult to establish when health care professionals access EHRs. This explains why GPs and specialists are required to obtain patient consent when accessing the E-journal.

Questions	Legal reference	Detailed description
		However, in situations where sharing of EHRs serves the purpose of treating the patient, general requirement of patient information laid down in HA Art. 16 applies. This means that patients must be informed about the possible consequences for the planned treatment if information cannot be communicated to other health care professionals.
Can the patient consent to his/her EHRs being accessed by a health practitioner or health institution outside of the Member State (cross-border situations)?	HA Art. 49 and Art. 15 of Executive Order No. 665 of 14 September 1998 on information, consent and disclosure of health information	There are no specific rules on EHRs. However, according to Art. 15.2.1 of Executive Order No. 665 of 14 September 1998 on information, consent and disclosure of health information patient can give consent to disclosure of health data to third countries.
Are there specific rules on patient consent to share data on a cross-border situation?	HA Art. 49 and article 15 of Executive Order No. 665 of 14 September 1998 on information, consent and disclosure of	See above.

2.4. Creation, access to and update of EHRs

2.4.1. Main findings

In general, the Danish health care legislation perceives creation of health records and making use of health data primarily as a matter of quality assurance and patient safety. Licensed health care professionals are under an obligation to keep records, and non-compliance can lead to disciplinary sanction (and in severe cases even to withdrawal of license). Likewise, health care professionals who do not consult the patients record may also be subject to criticism for not providing due care. The patient's right to self-determination and confidentiality is of course also recognised in Danish health care legislation. However, the regulation relies to a large degree on the assumption, that patients, who have consented to treatment, have accepted that health care professionals store and access data whenever this is necessary to ensure provision of qualified care. Patients are still in some situations entitled to refuse access to their medical records. In such situations, the health care professional must consider whether it is possible to provide due care without knowing the patient's medical history.

The patient has full right to access his/her own health records. Actually, the development of an eHealth architecture has enforced patients' rights in this respect. It has been legally acknowledged that if patients should profit from the opportunities provided by the technological development, previous rules, which allowed health care professionals to refuse access to patients in special situations, had to be abandoned. In the current legislation there are no restrictions on patients' right to access health data registered after 1 January 2010 when the current rules came into force. This may be one of the major practical achievements of the establishment of sundhed.dk and the digital platforms hosted by sundhed.dk (Sundhedsjournalen, E-journal, P-journal and SMR). One group of patients is, however, exempted from direct on-line access to EHRs. For patients under the age of 15 years the legislation allow health care professionals to limit parents' access to health information concerning their child. As this can not be monitored technically in the EHRs, it has been necessary to exclude on-line access to this group of patients' EHRs.

2.4.2. Table on creation, access to and update of EHRs

Questions	Legal reference	Detailed description
Are there any specific national rules regarding who can create and where can EHRs be created?	AOA Art. 22-25. Executive Order no. 3 of 2 January 2013 on licensed health care professionals' patient records. HA Art. 157-157a and Art. 193 b Executive Order no. 160 of 12 February 2013 on Standards for use of ICT in the Health Care Services	In general, there are no specific rules regarding who can create and where EHRs can be created. The general rules in APPD on processing of personal data apply in combination with the regulation in AOA health care professionals duties to keep health records. This implies that all licensed health care professionals must ensure that health records are created and kept updated in accordance with rules on health records. Dependent on the health care institution it is a managerial or/and individual responsibility to ensure that records are created and patient information properly registered to ensure updated patient records. In addition to the general rules on patient records Art. 157 and Art. 157a of HA contains a few provisions specifically allocating the task of creating and hosting particular EHRs to specific health care actors. According to Art. 157 of HA the Danish Health and Medicine Authority is responsible for setting up and hosting a personal medical profile (part of the SMR) and Statens Serum Institut is – according to Art.157a.1 – responsible for setting up and hosting the national vaccination register (the other part of SMR). Finally, Art. 193b of HA delegate power to the Minister of Health of appointing an authority to be responsible for setting up a National Patient Index. Statens Serum Institut has been appointed by Executive Order 160 0f 12 February 2013 on Standards for use of ICT in the Health Care Services. However, the project of setting up of a National Patient Index has been currently been put on hold (see general introduction).
Are there specific national rules on access and update to EHRs?	AOA Art. 22-25 Executive order no. 3 of 2 January 2013 on Licensed Health Care Professionals' Patient records.	The general rules in AOA and APPD on access and update to health records apply. In regards to access to EHRs here are a few rules stipulating different access rights for different health professionals (see below). In addition, patients have access to their own health records.

Questions	Legal reference	Detailed description
	APPD	Licensed health care professionals are under an obligation to keep health records updated (AOA, Art. 22-25 and Executive order no. 3 of 2 January 2013 on Licensed Health Care Professionals' Patient Records, Art. 9.3)
Are there different categories of access for different health professionals?	HA, Art. 41.1, 42, 42a.6, 42a.10, 42b, 43.1, 44, 157, and 157a.	HA contains rules stipulating different access rights for different health care professionals. In regards to EHRs in general, HA, Art. 42a.1 list a number of health care professionals who have immediate access to EHRs. This list includes doctors, dentists, midwifes, nurses, social- and health assistants, radiographer and ambulance technician with special competences. Other licensed health care professionals have more limited access to the content of EHRs (restricted to patients at their own ward – Art. 41a.2), but they may be authorised by the local data controller to have more comprehensive access, if this is justified (Art. 41a.4). Medical students may also be granted access by their medical supervisor (Art. 41a.8). In regards to access to data in SMR's, there are also different access rights for different health professionals. Doctors and – especially General Practitioners and specialists – have more extensive access than other groups of health care professionals (HA, Art. 157.2). Other groups with access to SMR's includes dentists, midwifes, nurses, social assistants, pharmacists, and even non-health care professionals.
Are patients entitled to access their EHRs?	HA, Art. 36-39	As from 1 January 2010, patients have been entitled to complete access to data registered in his/her health record (HA, art. 36) after this date. In regards to data registered before 1 January 2010, the health care professional may deny access, if this is justified either in substantial interest of the patient, or for the protection of other private interests (HA, Art. 37.3). In regards to electronic records, the patient can have direct on-line access using his/her NemID (Easy-ID), which is is a common secure login solution that can be used on all public websites in Denmark and for Internet banking. Data in E-journalen (the E-Record) is first open to the patient 14 days after being registered. This practice serves the purpose of protecting patients from accessing unexpected

Questions	Legal reference	Detailed description
		information before it has been communicated to the patient from a health care professional.[26] In case of children under the age of 15 years, direct online access to EHRs is, however, not possible. To ensure the interests of minor patients' right to privacy and to protect the best interest of the child, the HA Art. 37.2 allows health care professionals to limit parents' access to health information concerning their child. As this can not be monitored technically in the EHRs, it has been necessary to exclude on-line access to this groups of patients' EHRs.
Can patient have access to all of EHR content?	HA, Art. 36-39	Patients have – with the limits mentioned above – access to all information in health records. This also includes access to the log file, which allows the patient to see who else have had access to the health records. For data registered in health records before 1 January 2010 it is, however, possible to deny access if this is justified either in substantial interest of the patient, or for the protection of other private interests (HA, Art. 37.3).
Can patient download all or some of EHR content?		Data, which the patient can access directly, can normally be downloaded.
Can patient update their record, modify and erase EHR content?	Executive Order no. 436 of 11 May 2011 regarding the Danish Health and Medicine Authority's Electronic Registration of Information regarding Individual Citizens' Medicine	Patients are not allowed to update, modify or erase EHR content. However, in regards to the medicine part of the SMR, patients are allowed to register information about use of non-prescribed medicine, and are also entitled to erase such information (Art. 25 in Executive Order no. 436 of 11 May 2011 regarding the Danish Health and Medicine Authority's Electronic Registration of Information regarding Individual Citizens' Medicine)
Do different types of health professionals have the same rights to update EHRs?	Executive Order no. 436 of 11 May 2011 regarding the Danish Health and Medicine Authority's Electronic Registration of Information regarding Individual Citizens' Medicine	Licensed health care professionals responsibility for keeping health records updated is based on his/her involvement in treatment and care of the patient. In regards to update of information in the medicine part of the SMR there are detailed rules about the responsibilities of various type of health care professionals and others for ensuring update of records (Art. 17-24 in Executive Order no. 436 of 11 May 2011 regarding the Danish Health and Medicine Authority's Electronic

[26] This was mentioned as an example of a possible legal barrier in the interview with Chief Consultant Pia Jespersen, The National eHealth Authority

Questions	Legal reference	Detailed description
		Registration of Information regarding Individual Citizens' Medicine)
Are there explicit occupational prohibitions? (e.g. insurance companies/occupational physicians…)		There are no specific prohibitions laid down in the regulatory framework. However, as access to EHRs are restricted to health care professionals providing treatment and care to patients, it limits access for health care professionals working for insurance companies, social services etc. In regards to access to SMR's there is an exhaustive list of health care professionals and others, with access rights, and this list only includes persons involved in treatment and care of the patient.
Are there exceptions to the access requirements (e.g. in case of emergency)?		There are no explicit exceptions laid down in the regulatory framework in cases of emergency. However, according to HA, Art. 42a.5 health care professionals, who would normally not be authorised to access EHRs, may, in case of vital interests of society, the patient or other private interests, access EHRs. In addition, general legal principles of emergency powers also apply in this area.
Are there any specific rules on identification and authentication for health professionals? *Or are they aggregated?*		There are different rules for identification and authentication dependent on the EHR. Information available at sundhed.dk is available for health care professionals with a digital signature.
Does the patient have the right to know who has accessed to his/her EHRs?	Executive Order no. 528 of 15 June 2000 on Security Measures for the Protection of Personal Data Processed for Public Authorities Executive order no. 3 of 2 January 2013 on Licensed Health Care Professionals' Patient records. Executive Order no. 436 of 11 May 2011 regarding the Danish	Executive Order no. 528 of 15 June 2000 on Security Measures for the Protection of Personal Data Processed for Public Authorities includes an obligation to keep a log file on all processing of personal data. This also applies to health records in the public health care sector. Even though the Executive Order is only directly applicable in the public sector, data controllers in the private sector are advised to follow the same standard to comply with the general data security rules laid down in APPD. However, APPD does not entitle the patient to get access to the logfile as the file is not considered to be a "processing of personal data"[27]. In contrast to APPD, the general health legislation protects patients' interest in knowing about who has accessed his/her EHRs. According to

[27] The Data Protection Agency have taken a stance on this issue in a complain filed by a patient. The decision is available (in Danish) at this link http://www.datatilsynet.dk/afgoerelser/seneste-afgoerelser/artikel/klage-over-sikkerheden-i-praktiserende-laeges-journalsystem/ (last accessed February 2014)

Questions	Legal reference	Detailed description
	Health and Medicine Authority's Electronic Registration of Information regarding Individual Citizens' Medicine	Art. 28 of Executive order no. 3 of 2 January 2013 on Licensed Health Care Professionals' Patient records, patient records must contain information about who have had access to the date or to whom data has been disclosed. This information is available for the patient as part of a right to assess his/her patient record. In addition, there are special rules regarding logging of access to SMR's and patients have right to access to log files (Art. 4 and 13 in Executive Order no. 436 of 11 May 2011 regarding the Danish Health and Medicine Authority's Electronic Registration of Information regarding Individual Citizens' Medicine). The Data Protection Agency has stipulated special conditions in regards to GP's and specialists accessing the Sundhedsjournalen/E-journalen. If a GP access data on patients not registered as his normal patient (e.g. in situations where the patient's GP is not available), the patient will receive a written notification.[28]
Is there an obligation on health professionals to update EHRs?		See answer above regarding right to update
Are there any provisions for accessing data on 'behalf of' and for request for second opinion?	HA Art. 42a.8-9	There are special provisions regarding medical students access to EHR's (HA, Art. 42a.8) and access for secretaries to provide technical assistance to licensed health car professionals (HA, Art. 42a.9)
Is there in place an identification code system for cross-border healthcare purpose?		Not to my knowledge
Are there any measures that consider access to EHRs from health professionals in another Member State?		Not to my knowledge

[28] See decision from the Data Protection Agency of 10. May 2012, journalnummer 2011-082-0234 on Sundhedsjournalen og det Nationale Patient Indeks (NPI). The decision is available at http://www.datatilsynet.dk/afgoerelser/arkiv-over-afgoerelser/artikel/vedroerende-sundhedsjournalen-og-det-nationale-patient-indeks-npi/ (last accessed February 2014).

2.5. Liability

2.5.1. Main findings

In regards to *liability* issues there are no specific rules in Danish law addressing liability in connection with the creation, updating, storage and use of information in EHRs. However, general liability measures apply which involves both disciplinary and penal liability. Keeping health records is part of licensed health care professionals obligation, and non-compliance can lead to disciplinary sanctions issued by the Disciplinary Board. Likewise, confidentiality is also a professional obligation for which violations can be met with both disciplinary sanctions (from the Disciplinary Board) and penal sanctions (Criminal Court). Finally, violation of the data protection legislation may also result in economic liability or penal sanctions.

.

2.5.2. Table on liability

Questions	Legal reference	Detailed description
Does the national legislation set specific medical liability requirements related to the use of EHRs?	AOA, Art. 6-9, Art. 17 and Art. 75 Executive order no. 3 of 2 January 2013 on Licensed Health Care Professionals' Patient Records, Art. 29 Consolidating Act no. 1113 of 7 November 2011 on Complaints and Compensation within the Health Care Services, Art. 3 Executive Order no. 436 of 11 May 2011 regarding the Danish Health and Medicine Authority's Electronic Registration of Information regarding Individual Citizens' Medicine, Art. 28. Consolidating Act no 1028 of 22 August 2013 – Penal Code, Art. 152b-c	The national legislation does not specify special medical liability requirement related to the use of EHRs. Hence, the general rules on medical liability apply. These include both disciplinary and penal liability. In special cases economic liability may also be applicable. In general, licensed health care professionals are under an obligation to provide "due care" (AOA, Art. 17), and as keeping health records is part of health care professionals obligations (AOA, Art. 20-25), failure to comply with this obligation may lead to disciplinary sanctions. The Disciplinary Board can issue a reprimand (Consolidating Act no. 1113 of 7 November 2011 on Complaints and Compensation within the Health Care Services, Art. 3), and in cases of a series of reprimands or in serious cases, the National Board of Health and Medicine has the authority to issue more severe sanctions (AOA, Art. 6-9). This could also include withdrawal of licence. In severe cases, penal sanctions may also be justified (AOA, Art. 75 and Executive order no. 3 of 2 January 2013 on licensed health care professionals' patient records, Art. 29). In regards to SMR's there are special regulation of penal sanctions for violating rules concerning registration and correction of data in as well as unauthorised access to SMR's (Executive Order no. 436 of 11 May 2011 regarding the Danish Health and Medicine Authority's Electronic Registration of Information regarding Individual Citizens' Medicine, Art. 28) Breach of professional secrecy will both be a violation of professional duty to provide "due care" provoking disciplinary sanctions (see above) as well as a breach of the Penal Code (Consolidating Act no 1028 of 22 August 2013 – Penal Code, Art. 152b-c), which can be met with penal sanctions (fine or imprisonment up to 6 month) The Danish health care system has a no-fault compensation system. If a patient has been harmed in the health care services due to e.g. failure to register or registration of wrong information in the health record, it may –

Questions	Legal reference	Detailed description
		dependent of the specific circumstances – be possible for patient to receive compensation under this scheme. The individual health care professional is not him-/herself economically responsible (Consolidating Act no. 1113 of 7 November 2011 on Complaints and Compensation within the Health Care Services)
Can patients be held liable for erasing key medical information in EHRs?		It is not possible for patients to erase medical information in EHRs
Can physicians be held liable because of input errors?		See answers above
Can physicians be held liable because they have erased data from the EHRs?		See answers above
Are hosting institutions liable in case of defect of their security/software systems?	APPD, Art. 70	APPD allow both for economic damages and penal sanctions in cases of defects. According to APPD, Art. 69, the data controller shall compensate any damage caused by the processing of data in violation of the provisions of this Act unless it is established that such damage could not have been averted through the diligence and care required in connection with the processing of data In addition, APPD, Art. 70, stipulates that, in the absence of more severe punishment being prescribed under other legislation, violations of the a number of rules in the APPD – including the regulation of security measures – can be met with penalties (fine or prison up to 4 months)
Are there measures in place to limit the liability risks for health professionals (e.g guidelines, awareness-raising)?		There are general guidelines regarding professional secrecy and processing of medical data but no measures which specifically aims at limiting liability risks in this area
Are there liability rules related to breach of access to EHRs (e.g. privacy breach)?	APPD, Art. 70	According to APPD, Art. 70, the data controller may be liable to a fine or imprisonment (up till 4 month)
Is there an obligation on health professionals to access EHRs prior to take a decision involving the patient?		There are no clear rules, but accessing EHRs prior to decisions involving the patient may be part of individual health care professionals duty to provide "due care" (AOA, Art. 17)
Are there liability rules related to the	Consolidating Act no 1028	Fine or imprisonment (up till 6 month) may be imposed if information

Questions	Legal reference	Detailed description
misuse of secondary use of health data?	of 22 August 2013 – Penal Code, Art. 152d	covered by professional secrecy is misused for secondary purposes (Consolidating Act no 1028 of 22 August 2013 – Penal Code, Art. 152d)

2.6. Secondary uses and archiving durations

2.6.1. Main findings

According to the general rules on health records, EHRs must as a main rule be stored for a period of ten years after the last recording of data. However, for some health care professionals the archiving period is only five years. There is no legal obligation to delete the data after the mandatory archiving period has expired, but the data protection legislation generally requires that data are not kept longer than necessary for the purpose for which they were collected.

Data in EHRs can be used for *secondary purposes* (e.g. research and quality control) in accordance with the general health regulation and the APPD. In general, data can be used for quality control, research and statistics without the patient's consent, provided there is compliance with the APPD. In some situations a notification and/or approval from the Data Protection Agency is necessary (e.g. research or quality control carried out in the public sector), whereas this is not the case in other situations (e.g. research carried out in the private sector). Normally, patient consent is not necessary, and research on health data does not need approval from a research ethics committee.

2.6.2. Table on secondary uses and archiving durations

Questions	Legal reference	Detailed description
Are there specific national rules on the archiving durations of EHRs?	AOA, Art. 25 Executive order no. 3 of 2 January 2013 on Licensed Health Care Professionals' Patient Records, Art. 14-16	There are no special rules for archiving of EHRs, which follow the general rules for archiving of health records. According to AOA, Art. 25 health records must normally be stored for a period of minimum 10 years after the last recording in the record. More detailed rules are laid down in Art. 14-16 of Executive order no. 3 of 2 January 2013 on Licensed Health Care Professionals' Patient Records
Are there different archiving rules for different providers and institutions?	Executive order no. 3 of 2 January 2013 on Licensed Health Care Professionals' Patient Records, Art. 14	According to Art. 14.1 of Executive order no. 3 of 2 January 2013 on Licensed Health Care Professionals' Patient Records, doctors, dentists, chiropractors, midwifes, clinical nutritionists, clinical dental technicians and dental assistants must keep health records stored for a period of minimum 10 years after that last recording in the record. The storage period is normally 5 years for health records kept by other health care professionals, cf. Art. 14.2 of Executive order no. 3 of 2 January 2013 on Licensed Health Care Professionals' Patient Records. If such health care professionals share records with health care professionals listen in Art. 14.1 the record must be stored for 10 years.
Is there an obligation to destroy (…) data at the end of the archiving duration or in case of closure of the EHR?		There is no specific legal obligation to destroy EHRs or any other record when the mandatory storage period has expired. However, special criteria stipulated by the Data Protection Agency may call for destruction of the records or transfer to a special archive facility. In addition the general rules in APPD requires that data are not kept longer than necessary for the purpose for which they were collected.
Are there any other rules about the use of data at the end of the archiving duration or in case of closure of the EHR?	Art. 14.1 of Executive order no. 3 of 2 January 2013 on Licensed Health Care Professionals' Patient Records	Art. 18 of Executive order no. 3 of 2 January 2013 on Licensed Health Care Professionals' Patient Records stipulates that when electronic equipment are changed it must be secured that EHRs are not accessible to unauthorised persons
Can health data be used for secondary purpose (e.g. epidemiological studies, national	HA, Art. 32, 43-44 and 46-48	Health data can be used for at number of secondary purposes, and are widely used for scientific and statistical purposes. As a general requirement, processing of data for scientific purposes must comply with

Questions	Legal reference	Detailed description
statistics...)?	APPD, Art. 10 Act 593 of 14 June 2011 on Research Ethics Review of Health Research Projects	APPD. Apart from that, no particular authorisation or consent from the patient is required (HA, Art. 46-48). Health data can also be used for quality assurance purposes without consent (HA, Art. 43). Any other secondary use (e.g. for employment and insurance purposes or in connection with applications for social benefits etc) will normally require an explicit consent from the patient (HA. Art. 44).
Are there health data that cannot be used for secondary use?	HA, Art. 32	In regards to research on biological samples it is possible for the patient to opt-out (HA, Art. 32)
Are there specific rules for the secondary use of health data (e.g. no name mentioned, certain health data that cannot be used)?	APPD, Art. 10	APPD, Art. 10, allows for research on sensitive personal data without consent of the data subject. According to APPD, Art. 10.2, it is prohibited to use the data for other purposes than scientific or statistical purposes. It is furthermore a general precondition and requirement, that personal data processed for scientific or statistical purposes may not published in a way revealing the identity of the data subject /patient.
Does the law say who will be entitled to use and access this data?		No
Is there an opt-in/opt-out system for the secondary uses of eHealth data included in EHRs?		As mentioned above, it is only possible to opt-out in regards to research on biological samples (HA, Art. 32)

2.7. Requirements on interoperability of EHRs

2.7.1. Main findings

Some Danish EHRs are centralised in one database at a national level. This is the case for both the SMR, E-journalen, P-journalen and Sundhedsjournalen. In regards to the SMR the HA, Art.157 and Art.157a clearly presupposes that registration of prescribed medicine and vaccinations will take place in one centralised database. Furthermore, the HA, Art. 193a authorises the Minister of Health with power to issue executive orders to ensure applications of standards, and Art. 193b has the aim to ensure the establishment of a National Patient Index. Although the initial ideas and visions regarding the National Patient Index has turned out to be too ambitious, the development of the national Sundhedsjournal rely on this legal basis.

2.7.2. Table on interoperability of data requirements

Questions	Legal reference	Detailed description
Are there obligations in the law to develop interoperability of EHRs?		There are no specific requirements in law on interoperability, but there are a few provisions aiming at ensuring interoperability (see below)
Are there any specific rules/standards on the interoperability of EHR?	HA, Art.157-157a and Art. 193a-193b	HA, Art.157 and Art.157a presuppose that registration of prescribed medicine and vaccinations in the SMRs will take place in centralised databases. HA, Art. 193a-193b also serves the aim of ensuring better interoperability of EHRs. Art. 193a authorises the Minister of Health with power to issue executive orders to ensure applications of standards. Standards have been laid down in Executive Order no. 160 of 12 February 2013 on Standards for ICT use in the Health Care Services. In addition, HA Art. 193b has the aim to ensure the establishment of a National Patient Index.
Does the law consider or refer to interoperability issues with other Member States systems?		No

2.8. Links between EHRs and ePrescriptions

2.8.1. Main findings

The Danish ePrescription system and the SMR work closely together but are not dependent of each other. This means that patients with a manual prescription will have data about prescribed medicine registered in the SMR, and that patients without a SMR (e.g. a person visiting Denmark as a tourist) in principle can make use of ePrescriptions. However, when ePrescriptions are used, it facilitates the pharmacies procedure in keeping the SMR updated.

Pilot testing of cross border use of electronic prescriptions is currently taking place within the framework of the epSOS collaboration.

ePrescriptions are covered by the same regulation as other prescriptions[29], and health care professionals are under the same obligation as with other prescriptions to provide due care (AOA, Art. 17) which may include an obligation to consult the patient's EHRs (as well as available paper records).

[29] Executive Order no. 1671 of 12 December 2013 on Prescriptons

2.8.2. Table on the links between EHRs and ePrescriptions

- ***Infrastructure***

Questions	Legal reference	Detailed description
Is the existence of EHR a precondition for the ePrescription system?		The ePrescription system can – in principle – operate without an EHR. However, as the Danish ePrescription system is closely linked to the patient's Personal Medicine Profile and the SMR the ePrescription system is organisationally linked to this EHR
Can an ePrescription be prescribed to a patient who does not have an EHR?		As explained above, the ePrescription system can operate on its own. If a patient does not have a Personal Medicine Profile – e.g. when the patient is a tourist consulting a Danish GP – it is possible to make an ePrescription without creating a Personal Medicine Profile on the patient. In practise, it may, however, be difficult for the pharmacies to identify the prescription in the system, when the patient does not have a Danish personal identification number.

- ***Access***

Questions	Legal reference	Detailed description
Do the doctors, hospital doctors, dentists and pharmacists writing the ePrescription have access to the EHR of the patient?	HA, Art. 157	Both doctors, hospital doctors, dentists and pharmacists have access to the patient's SMR. In addition, doctors, hospital doctors and dentists may also have access to the patient's E-journal.
Can those health professionals write ePrescriptions without having access to EHRs?	AOA, Art. 17	It is possible to write an ePrescription without having access to the patient's EHRs. However, as licensed health care professionals are under an obligation to provide due care, it may be a violation of their professional duty to write a prescription without prior consultation of the patient's health records. In practise, it is common that doctors and dentists write ePrescriptions without prior consultation of patient's EHR.

2.9. Other requirements

None identified

3. Legal barriers and good practices for the deployment of EHRs in Denmark and for their cross-border transfer in the EU.

Good practices for the development of EHRs in Denmark

Based on an analysis of the legislative framework and the interviews it seems that there are several features of the Danish legislation, which could be considered good practice.

The flexible and comprehensive approach to finding a balance between on the one hand the importance of respecting patients' right to self-determination and privacy, and on the other hand ensuring speedy and qualified care based on all available information, is mentioned as a good legal practise in the interviews. It is, however, also mentioned, that perhaps the legislation is too generous in giving widespread access to health care professionals and others in situations where this is not evident to the patient. This may endanger trust and confidentiality in patients' relation to the health care services.

Another example of good practice is the (few) examples of regulation, which promotes interoperability at national level. The SMR legislation, and HA Art. 193a also lay the legal ground for a Sundhedsjournal and a National Patient Index based on existing data resources.

Legislation promoting widespread and direct access for patients to their EHRs is also an example of good legislative practice. It is important that the technological development is not exclusively used to facilitate access for health care professionals and to make the patient more transparent to the "system". Taking advantage of the technological opportunities to promote patients' rights to access, and thereby also making the system more transparent to the patient is an important asset of the legal framework surrounding EHRs.

In addition to good legal practices, other practices have also been mentioned in the interviews. The existence of Sundhed.dk – a comprehensive e-health platform – is praised as a useful tool for both patients and health care professionals. It has also been mentioned, that even though the EHR-development in the hospital sector is not very coherent, it is a clear advantage, that information is digitalised and the health record available instead of being stored in a wrong place.

Legal barriers for developing EHRs in Denmark

The analysis shows that Danish legislation has developed gradually along with the use of IT and EHRs in the health care services. Several legal initiatives have been taken to amend and change the existing legislation to make it easier to profit from the advantages provided by having easy and quick assess to comprehensive patient data. It is, thus, difficult to identify a legal barrier, and in the interviews, only a few obstacles have been brought up. One of these was a possible legal barrier for ensuring emergency doctors sufficient access to the patients EHR at his/her GP.

In regards to patient's access to health data, it has also been mentioned that at the moment it is not possible to allow parents (and patients) direct online access to EHRs when the patient is under the age of 15 years. To ensure the interests of minor patients' right to privacy and to protect the best interest of the child, the health legislation allow health care professionals to limit parents access to health information concerning their child. As this restriction can not be monitored technically in EHRs, it has been necessary to exclude on-line access to the EHRs of patients under the age of 15 years.

Another possible legal barrier linked to the patients' access to EHRs has also been raised. It is presupposed in the legislation that data will only be available to patients 14 days after registration to ensure that patients are not being informed by coincidence before they have received information about their health status from the responsible health care professional. This means that patients are

denied access to information, which may wish to know about in order to e.g. plan future treatment initiatives.

In addition the issue of ensuring trust and confidentiality was also raised in an interview. It was mentioned that the Danish legislation may be too permissive in allowing many different groups of health professionals to have widespread access to patient records. This could undermine confidentiality and trust between the patient and the primary caregiver (e.g. the GP) and thus be an impediment for providing the best possible care. The widespread access to the SMR together with an obligation for GP's to provide patient data to the regions for planning purposes was mentioned as another example of rules, which could potentially undermine confidentiality in the doctor – patient relationship.