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 Sweden

time.lex

milieu
Law & Policy Consulting

4 March 2014

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

This report was completed by Christine Kirchberger. The views expressed herein are those of the consultants alone and do not necessarily represent the official views of the Consumers, Health and Food Executive Agency (Chafea)

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 Sweden

Health care in Sweden has been using EHRs for many years e.g. the Prescription Act which created an EHR for prescription has been in force since 1997. Based on the constitutional set-up between the state, county councils (*landsting*) and municipalities (*kommuner*), health care is mainly provided by regional and local public agencies. There are also a number of private organisations providing health care. In order to enable the cooperation and interoperability between the different health care providers, the national IT-strategy for health care started in 2005/06 and was complemented by the national eHealth project (*nationell eHälsa*)[1] established in 2010. Its aim is a strategy for accessible and secure information in health and social care.

Another national project is the National Patient Journal (*Nationell patientöversikt – NPÖ*). The idea of NPÖ is that a health care professional should be able to directly access a patient's medical records that are kept by other health care providers, if certain legal requirements are fulfilled. All of the 21 county councils' health care providers in Sweden have implemented NPÖ at this point; private organisations should follow the next few years.

In the beginning of 2014 a new authority was established – the Swedish eHealth Agency (*Ehälsomyndigheten*)[2]. Its aim is to increase the development of the national e-health infrastructure, both regarding e-prescriptions and individuals' access to their health data by building a personal health account (*HälsaFörMig service*). The e-prescription part of the agency's task was taken over from another body (previously the state monopoly for prescriptions). The personal health account is a new task that only recently started developing. The Swedish eHealth Agency is actively involved in the epSOS project as a national contact point.

Besides the eHealth Agency, several other public authorities are involved in eHealth in Sweden, The National Board of Health and Welfare (*Socialstyrelsen*) has issued several regulations and guidelines on interoperability. The Swedish Association of Local Authorities and Regions (SALAR, *Sveriges Kommuner och Landsting – SKL*) represents the interests of the county councils and municipalities in the various projects. The Centre for eHealth in Sweden (CeHis)[3] part of Inera[4] (private company owned by county councils) works on many eHealth projects and publish reports within the field. The Swedish Data Inspection Board (*Datainspektionen*)[5] is the responsible supervisory authority with regards to data protection in general and patient data in specific. The Board aim is to protect individuals privacy without unnecessarily preventing or complicating the use of new technology

2. Summary of legal requirements applying to EHRs

Swedish legislation is rather general with regard to the health data to be included in EHRs. EHRs are regulated by the Personal Data Act. All data processing of patient's health care records (including ePrescriptions) has to be in accordance with the personal data Act. For specific subject there are corresponding legislation but it has to be based on the personal data Act.

Chapter 3 Section 5 of the Swedish Patient Data Act [*Patientdatalag (2008:355)*] stipulates that a patient journal may only contain personal data that is needed for the purposes mentioned in the Act. These purposes include, *inter alia,* guaranteeing good and safe health care. Chapter 3 section 6 of the

[1] www.nationellehalsa.se
[2] www.ehalsomyndigheten.se
[3] www.cehis.se
[4] www.inera.se
[5] www.datainspektionen.se

Act states what information has to be included. Sections 7 -19 contains further provisions on the contents in patients journals.

Health care providers in general have to register with the supervisory authority - Health and Social Care Inspectorate (*Inspektionen för vård och omsorg – IVO*) - according to Chapter 2 Section 1 of the Swedish Patient Security Act [*Patientsäkerhetslag (2010:659)*]. There is no specific license necessary for EHRs, instead electronic patient journals are encouraged by legislation and public agencies. Information security is an important requirement for processing of EHRs and the National Board of Health and Welfare's Regulation SOSFS 2008:14 stipulate that information security policies have to be implemented and strong authentification has to be applied when using open networks. The Regulation also encourages standards with regards to information security and requires logs to be kept regarding access to EHRs by health care staff.

Swedish legislation on patient journals deals on one hand with the EHRs administered by the health care provider and with access to EHRs by other health care providers (coordinated patient overview – *sammanhållen journalföring*) on the other hand. The Patient Data Act stipulates specific requirements for both situations.

Chapter 4 Section 1 Patient Data Act stipulates that health care staff employed by healthcare providers are allowed to access documented records about a patient if she or he participates in the care of the patient or for other reasons where they need information for their work within health care (inner secrecy – *inre sekretess*). Patients themselves have the right to receive information about their EHRs according to Chapter 8 Patient Data Act.

Though Chapter 3 of the Swedish Patient Data Act stipulates an obligation to keep patient summaries, it does not explicitly regulate any liability with regard to it. The Act only refers in Chapter 10 to the general liability provisions in the Personal Data Act.

The Patient Data Act stipulates an archiving period of at least ten years after the patient summary was amended the last time (Chapter 3 Section 17). The legislative approach is more focused on *must* be archived than *should* be deleted after the archiving period. With regards to secondary uses, the purpose principles apply, i.e. if the secondary use falls within the stated purposes or is in line with them, secondary uses should be allowed. In other words, the original purpose for collecting the data decides if any subsequent uses of the data are allowed. If the subsequent use is in line with the original purpose, the processing is allowed.

There is no central EHRs system in Sweden, but the databases are kept by the different health care providers, e.g. the country councils. In addition, Chapter 3 Section 2 of Regulation SOSFS 2008:14 stipulates that patients' records should be documented by using nationally decided terms, classifications and other codes. In this regard, The National Board of Health and Welfare [*Socialstyrelsen*] has developed two standards; the National Information Structure (NI) and the National Interdisciplinary Terminology for Health and Social Care. The latter is partly based on the clinical terminology SNOMED CT.

The Swedish ePrescription systems are being administered by the Swedish eHealth Agency (*eHälsomyndigheten*). There are a few specific databases that are being used in connection with ePrescriptions. They are not directly linked to the EHR managed by the different health care providers, so there is no direct access between the different systems. There are mainly three databases in place that concern ePrescriptions: Pharmaceutical Register (*Läkemedelsförteckningen*), Prescription depot (*Receptdepån*) and High Cost Database (*Högkostnadsdatabasen*).

3. Good practices

According to the stakeholders interviewed, the current legal framework is considered adequate The Patient Data Act is, however, under review. The government report in the context of this review has

recently been published.

Good practices include the fact that county councils were encouraged to implement the National Patient Overview – NPÖ by being offered an economic stimulus if they had joined NPÖ by September 2012.

The amount of ePrescriptions in Sweden today reaches more than 90 % at the moment, based on a clear legal framework.

There is an option in Chapter 4 Section 11 Regulation by the National Board of Health and Welfare's Regulation SOSFS 2008:14 to have patient's journals in other languages than Swedish.

4. Legal barriers

With regards to legal barriers due to consent, the Swedish framework for the coordinated patient journal builds upon an opt-out and an opt-in solution. There is one national legislation for opt-in/opt-out/consent. Counties cannot change this. In theory a county could refuse to participate in an exchange with another county for security reasons. In such cases the national superviser has to react.

Related to this issue, the question of liability in cross-border transfer of EHRs was mentioned in two interviews. Who is liable if a patient receives health care in Member State B and the health care staff in B relies on EHRs from the Member State A?

One of the main challenges that were identified in the interviews is the implementation of the legal rules, and not so much the law itself. Health care providers in Sweden have had digital systems and EHRs for quite a while which requires adaptations of the existing systems to a large extent, if they do not fully fulfil the legal requirements.

Another potential legal barrier within Sweden is how to treat consent from people with dementia.

Contents

List of abbreviations

EHRs	Electronic Health Records
NPÖ	National Patient Overview
SALAR	Swedish Association of Local Authorities and Regions
SOSFS 2008:14	National Board of Health and Welfare's Regulation on information processing and journals within the health and welfare sector [*Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården*]

1. General context

1.1. EHR systems in place

Traditionally the health and medical records have been kept regionally by the different health care providers, which are generally the county councils in Sweden.[6] The eHealth projects or initiatives are built upon this existing framework and infrastructure and aim at improving it through increased access and interoperability while guaranteeing patients' safety.

Already in 2005 and 2009 groups with different stakeholders were established in Sweden in order to improve the development of eHealth in the country.[7] The work was intensified in 2010 when the national eHealth project (*nationell eHälsa*)[8] was established. Its aim is to set a strategy for accessible and secure information in health and social care.[9] The project is a cooperation between the Ministry of Health and Social Affairs, the Swedish Association of Local Authorities and Regions (SALAR) (*Sveriges Kommuner och Landsting – SKL*), the National Board of Health and Welfare (*Socialstyrelsen*), the Association of Private Care Providers (employers' organisation for private care providers) and Famna (The Swedish Association for Non-Profit Health and Social Service Providers). The project aims at increasing the cooperation and interoperability among stakeholders with regard to eHealth. This is partly done by organising conferences and annual national eHealth days.

With regards to the eHealth infrastructure, there are several different systems/platforms that are needed in order to guarantee a functioning national eHealth approach in Sweden. Some of them include:

- Sjunet - communication network used by health and medical care providers, implemented by almost all county councils' health care providers and many other ones
- HSA (*Nationell katalogtjänst*) – information about health care staff tasks and roles, implemented in all county councils and municipalities since spring 2012.
- SITHS (*Nationell identifieringstjänst*) – national security solution for electronic identification and secure communication of information. By using a SITHS-card health care staff can identify themselves. SITHS is connected with HSA and has been implemented in all county councils and municipalities since spring 2012.
- NEF – national e-prescription format
- SIL – Swedish information database for medicine
- Pascal – dosage management
- Security services (*säkerhetstjänster*) – services that regulate access, authorisation, patients' consent, locking of records, logging of access in general, etc

All health care providers (e.g. county council and others) are responsible for their own patient journal system(s). By 2012 all county councils had fully implemented EHR in hospitals, psychiatry and primary care. There is, though, no common national database for patient journals. . In order to increase cooperation and allow care providers to access patients' records stored at another provider, the National Patient Summary (*Nationell patientöversikt – NPÖ*) was initiated several years ago. The idea of NPÖ set by INERA is that health care staff is able to directly access a patient's medical records that are kept by other health care providers, if certain legal requirements are fulfilled. All of the 21 county

[6] About 95 % of hospitals are owned by county councils (*landsting*), about 40 % of primary care, however, is provided by private caregivers (due to patient's choice).
[7] National High-Level Group for eHealth in 2005 and The Advisory Group for eHealth in 2009.
[8] www.nationellehalsa.se
[9] Read more about the strategy at www.nationellehalsa.com/national-ehealth

councils' health care providers in Sweden have implemented NPÖ at this point[10], but the plan is that all health care providers, including private ones will be linked to NPÖ in the next few years.
In practice, there are not too many different EHR-systems in place. There are five suppliers (Siemens, Evry, Cambio, CompuGroup and Norrbotten County Council) that dominate the market and account for 96 % of all users.[11]

In addition, a system of national quality registries (*nationella kvalitetsregister*)[12] has been established in the Swedish health and medical services in the last decades. A national quality registry contains individualised data concerning patient problems, medical interventions, and outcomes after treatment. The idea is to build a knowledge system for continuous learning, quality improvement and management of healthcare services.[13] This system is only for research in order to create a structured system for an on-going overview of the health system for developing and securing the quality of health care. Individual data is used for creating statistic but is not allowed to be used for any other purpose. The DPA has closed down several because of breach of security. Patients whose data can be used in the system have the right to opt-out and must be informed of the possibility of being part of the system and the right to opt-out.

With regards to systems for research purposes, the portal Register-Based Research (*Registerforskning*)[14] provides an overview over some of the databases that exist.

1.2. Institutional setting

The responsibility for health and medical care in Sweden is shared by the central government, county councils (*landsting*) and municipalities (*kommuner*). The role of the central government is to establish principles and guidelines, and to set the political agenda for health and medical care. It does this through laws and ordinances or by reaching agreements with the Swedish Association of Local Authorities and Regions (SALAR) (*Sveriges Kommuner och Landsting – SKL*)[15], which represents the county councils and municipalities. In other words, the main providers of medical care in Sweden are county councils and municipalities, together with private organisations.

The supervisory authority within the health sector is the Swedish government agency Health and Social Care Inspectorate (*Inspektionen för vård och omsorg – IVO*)[16] which was created in June 2013 and took over the supervisory activities of the National Board of Health and Welfare (*Socialstyrelsen*). It is thus the Health and Social Care Inspectorate (IVO) that now supervises health and medical care as well as social services. The Inspectorate is also responsible for the consideration of permits in these areas and its main task is to supervise that the public receives safe, good quality health and social care in accordance with laws and other regulations.

In the beginning of 2014 another new government agency was established – the Swedish eHealth Agency (*eHälsomyndigheten*)[17]. Its aim is to develop the national e-health infrastructure, both regarding e-prescriptions and individuals' access to their health data by building a personal health account (*HälsaFörMig service*). The e-prescription part of the agency's task was taken over from another body (previously the state monopoly for prescriptions). The personal health account is a new

[10] CeHis, *eHealth in Swedish County Councils*, Inventory by the SLIT group, compiled by Lars Jerlvall and Thomas Pehrsson, 2012,
http://cehis.se/images/uploads/dokumentarkiv/Rapport_eHalsa_i_landstingen_SLIT2012_eng_rapport_121019.pdf,, at 3.
[11] CeHis, *eHealth in Swedish County Councils*, 2012, at 8.
[12] There are about 73 registries and eight competence centres in Sweden at the moment.
[13] www.kvalitetsregister.se/om_kvalitetsregister/quality_registries
[14] registerforskning.se
[15] www.skl.se
[16] www.ivo.se
[17] www.ehalsomyndigheten.se

task that only recently started developing. The Swedish eHealth Agency is actively involved in the epSOS project.[18]

The National Board of Health and Welfare (*Socialstyrelsen*)[19] is another main government agency involved in health and social care, especially regarding eHealth. The agency is specifically mentioned in the Patient Data Regulation [*Patientdataförordning (2008:360)*] as one of the responsible authorities for patient data issues. The National Board is authorized by the government, together with the DPA, to issue regulations supplementing the Patient Data Act. One of its main tasks is to build a basis for documentation and interoperability. It has done so by developing the National Information Structure and the National Interdisciplinary Terminology[20], in cooperation with the Centre for eHealth in Sweden (CeHis) and the Swedish Association of Local Authorities and Regions (SALAR, *Sveriges Kommuner och Landsting – SKL*).

The company Inera AB[21] is heavily involved in the development of eHealth in Sweden, especially with regards to coordination of the county councils. Inera provides information on several of the Swedish databases, platforms and registers on its website and even offers a demo of NPÖ – the National Patient Summary.[22]

The supervisory authority responsible for processing of personal data in general is the Swedish Data Inspection Board (*Datainspektionen*). The Board is also supervising the application and implementation of the Swedish Patient Data Act, which is the main legislation with regards to personal processing of EHR.

1.3. Legal setting and future legal development

The legal framework in Sweden with regards to EHRs consists of a system of Parliamentary Acts, governmental ordinances and regulations by authorized public authorities. The authorities sometimes publish guidelines and recommendations as supplements to regulations etc. The main legislative acts were replaced in 2008 and 2010, so the legal provisions in force are rather new.

The Health and Medical Service Act *(Hälso- och sjukvårdslag (1982:763)*) regulates the responsibilities of county councils and municipalities, and gives local governments a certain freedom within health and medical care. The Act (Section 3) establishes that every county council must offer good health and medical care. County councils are allowed to outsource certain parts of the health care.

The Patient Safety Act [*Patientsäkerhetslag (2010:659)*] regulates the requirements for health care providers, their registration, and supervision. The Patient Safety Act, chapter 6 stipulates obligations for health care professionals. Chapter 6, section 12 regulates secrecy for health care professionals.

The Patient Data Act [*Patientdatalag (2008:355)*] regulates processing of personal health data within health and medical services. It is applicable in addition to the general Swedish Personal Data Act [*Personuppgiftslag (1998:204)*] and deals not only with EHR but with health care records in general, also manually processed ones.[23] The Act does not force health care providers to process health data electronically, but intends to create the legal framework to have electronic journal records.[24]

[18] http://www.ehalsomyndigheten.se/Om-oss-/Uppdrag-och-verksamhet/Other-languages1/Swedish-eHealth-Agency/
[19] www.socialstyrelsen.se/english
[20] See above.
[21] The company is owned by the country councils, inera.se.
[22] in Swedish at www.inera.se/TJANSTER--PROJEKT/NPO/Demomiljo/
[23] Government Bill (*Regeringens proposition*) 2007/08:126, Patientdatalag m.m., [cit Prop 2007/08:126], at 48.
[24] Prop 2007/08:126, at 35.

As most health care providers are county councils and municipalities, and therefore public authorities, the Public Access to Information and Secrecy Act (2009:400) [*Offentlighets- och sekretesslag (2009:400)*][25] applies too, especially its Chapter 25 that regulates secrecy of health data. The Act does, however, not apply to private entities providing health care. The Act is therefore supplemented by the Patient Safety Act as it regulates obligations for all health care professionals.

In addition, there are several other, very specific laws that apply to very specific circumstances or databases, e.g. the Act on biobanks within health and medical care (*lagen (2002:297) om biobanker i hälso- och sjukvården m.m.*), Act on genetic integrity (*lagen (2006:351) om genetisk integritet m.m.*), Act on blood safety (*lagen (2006:496) om blodsäkerhet*)[26], etc.

The Patient Data Act is currently under review. A governmental report has been issued, see SOU 2014:23.

[25] A summary is available here www.government.se/sb/d/11929/a/131397.
[26] The Act is based on Directive 2002/98/EC of the European Parliament and of the Council of 27 January 2003 setting standards of quality and safety for the collection, testing, processing, storage and distribution of human blood and blood components and amending Directive 2001/83/EC.

2. Legal requirements applying to EHRs in Sweden

2.1. Health data to be included in EHRs

2.1.1. Main findings

The Swedish Patient Data Act [*Patientdatalag (2008:355)*], chapter 3, section 5 regulates the mandatory contents of patient journals. The Act is supplemented by a governmental ordinance and applicable Regulation by the National Board of Health and Welfare's Regulation - SOSFS 2008.

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?)	Patient Data Act [*Patientdatalag* (*2008:355)*] National Board of Health and Welfare's Regulation on information processing and journals within the health and welfare sector [*Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården*] - SOSFS 2008:14	Chapter 3 Section 5 regulates the mandatory contents of a patient's journal such the identity of the patient, necessary information on the reasons for health care, diagnosis, given health care, planned health care, information given to the patient about reasons for chosen healthcare treatment and options for the patient. The amount and type of personal data is determined by the purpose of the health care.[27] Chapter 3 Section 4 – 7 SOSFS 2008:14 supplements the Act by regulating the methodology to be used for writing/creating a patients journal/record.
Are these data restricted to purely medical information (e.g. physical or mental health, well-being)?	Patient Data Act (2008:355)	The Act is for a health care providers processing of personal data in health care. Processing such data is allowed if it is needed for needed health care which can also include data that is not strictly medical.
Is there a definition of EHR or patient's summary provided in the national legislation?	Patient Data Act (Chapter 1 Section 3)	The Patient Data Act defines journal record (*journalhandling*), patient journal (*patientjournal*) and access to another health providers patient's journal (*sammanhållen journalföring*). Journal record is any record that contains data on a patient's health or medical condition, other personal information or intended health care measures. Patient

[27] Prop 2007/08:126, at 63.

Questions	Legal reference	Detailed description
	Personal Data Act (1998:204)	journal is one or several journal records that refer to the same patient. Coordinated patient journal is an electronic system that allows a health care provider to have direct access to another health providers patient's journal ("*Ett elektroniskt system, som gör det möjligt för en vårdgivare att ge eller få direktåtkomst till personuppgifter hos en annan vårdgivare.*") While the terms journal record and patient journal are technology neutral and also include written paper records, the term coordinated patient journal is focused on electronic systems and refers to enabling other health care providers direct access to their EHRs. Personuppgiftslagen (1998:204) is the implementation of the directive 95/46/EG. This Act is always the basis for any other Acts on personal data. If special Acts. e.g. The Patient Data Act do not have regulations on for a specific situation the Personal Data Act is to be used.
Are there any requirements on the content of EHRs (e.g. detailed requirements on specific health data or general reference to health data)?		Several. The main are: Patient Data Act, Personal Data Act, the Prescription Record Act (1996:1156), governmental ordinances supplementing this Acts
Are there any specific rules on the use of a common terminology or coding system to identify diseases, disorders, symptoms and others?		National Board of Health and Welfare have an ongoing project for this. The Boards Regulation on information processing and journals within the health and welfare sector - SOSFS 2008:14 has references to Swedish standard for information security
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)?		no
Are there any specific rules on identification of patients in EHRs?		Chapter 3, section 6. 1. Patient Data Act states that the patients' identification has to set down in the patients' journal. Every domicile of Sweden has a personal id-number which is always used in any case for identification.

Questions	Legal reference	Detailed description
Is there is a specific identification number for eHealth purposes?		no

2.2. Requirements on the institution hosting EHRs data

2.2.1. Main findings

All EHR have to be handled in accordance with the Personal Data Act (1998:204). Health care providers in general have to register with the supervisory authority - agency Health and Social Care Inspectorate (*Inspektionen för vård och omsorg – IVO*) - according to Chapter 2 Section 1 of the Swedish Patient Security Act [*Patientsäkerhetslag (2010:659)*]. There is no specific license necessary for EHRs but the National Board exercises a quality control. Information security is an important requirement for processing of EHRs and the National Board of Health and Welfare's Regulation stipulates that information security policies have to be implemented and strong authentication has to be applied when using open networks. The Regulation also encourages standards with regards to information security and requires logs to be kept regarding access to EHRs by health care staff.

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?	National Board of Health and Welfare's Regulation on information processing and journals within the health and welfare sector (Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården) - SOSFS 2008:14	The Regulation requires institutions to have an information security policy (Chapter 2 Sections 1-2), to appoint employees or staff members as responsible for information security (Chapter 2 Section 3), and to use standards (Chapter 2 Section 4, at the moment SS-ISO/IEC 27001:2006 and SS-ISO/IEC 27002:2005). The handbook of the National Board of Health and Welfare also refers to a standard within electronic health care – ISO/IEC 27002 (ISO 27799:2008).[28]
Is there a need for a specific authorisation or licence to host and process data from EHRs?		In general, any provider of health or medical care needs to be approved by IVO, according to Chapter 2 of the Swedish Patient Safety Act [*Patientsäkerhetslag (2010:659)*]. There is, however, no particular license for EHRs in specific. Only health and medical care providers can, however, process personal health data.
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)?	National Board of Health and Welfare's Regulation on information processing and journals within the health and welfare sector (*Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården*) - SOSFS 2008:14	The Regulation requires institutions to have an information security policy (Chapter 2 Sections 1-2), to appoint employees or staff members as responsible for information security (Chapter 2 Section 3), and to use standards (Chapter 2 Section 4, at the moment SS-ISO/IEC 27001:2006 and SS-ISO/IEC 27002:2005). The handbook of the National Board of Health and Welfare also refers to a standard within electronic health care – ISO/IEC 27002 (ISO 27799:2008).[29]
In particular, is there any obligation to have the information included in EHRs encrypted?	National Board of Health and Welfare's Regulation on information processing and journals within the health and welfare sector - SOSFS 2008:14	The regulation SOSFS 2008:14 does not explicitly mention encryption but states that measures should be taken to prevent unauthorised access to data when using open networks. Chapter 2 Section 2 talks about accessibility, accuracy, secrecy and traceability. Chapter 2 Section 5 SOSFS 2008:14 stipulates strong authentication should

[28] *Handbok till SOSFS 2008:14 - informationshantering och journalföring*, Socialstyrelsen, april 2009, [cit Handbok till SOSFS 2008:14], http://www.socialstyrelsen.se/regelverk/handbocker/handbokominformationshanteringochjournalforing.

Questions	Legal reference	Detailed description
		be used if open networks are being used to transfer EHRs. As even the network between health care providers – Sjunet – is open, the National Board of Health and Welfare recommends in its handbook[30] that encryption is used in addition to strong authentication (i.e. two-way authentication, e.g. password, smartcard and/or fingerprint).
Are there any specific auditing requirements for institutions hosting and processing EHRs?	Chapter 4 Section 3 Patient Data Act	The provisions regarding auditing do not stipulate any external auditing, but measures that have to be implemented within the health care provider. According to Chapter 4 Section 3 Patient Data Act health care providers have to make sure that access to patient data is documented and can be verified. Health care providers have to check systematically and recurring if any unauthorised person accessed any patients' data.
	Chapter 2 Section 11 National Board of Health and Welfare's Regulation on information processing and journals within the health and welfare sector - SOSFS 2008:14	According to Chapter 2 Section 11 SOSFS 2008:14 health care providers are responsible to implement measures to keep logs on the access to patients' records. The logs should contain information on the processing of patients' data, which department and date and time of the access, the identity of the patient and the user accessing the data. The verification of logs should be done regularly and systematically and be documented. The logs should be stored for at least 10 years.

[30] Handbok till SOSFS 2008:14, at 26 and 27.

2.3. Patient consent

2.3.1. Main findings

All health records have to be in accordance with the requirements of the Personal Data Act (1998:204). Health records for patients have also to be in accordance with the Patients Data Act (2008:355). Depending on the specific situation there may be also other requirements in parliamentary Acts or governmental ordinances.

All health providers have to have a system for keeping a patients journal and with specified contents, all in accordance with the Patients Data Act (2008:355). The creation of the health record is mandatory and not dependent on the patients consent. A patient has the right to opt-out in cases of direct access to patients journals between different health providers. A patient has also the right to block certain information so that any health provider or health professional not involved in this particular treatment has no possibility to get at that information.

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?	Patient Data Act (2008:355) chapter 2, chapter 3	Health care providers are obliged to keep patient's records (in paper or electronic form). The patient cannot oppose the keeping of a mandatory health record/patients journal. A patient can opt-out when a health provider gives another health provider direct access to patients journal. Health records that are not allowed by the Patient Data Act can be permitted if the patient gives his/hers consent.
Is a materialised consent needed?	Patient Data Act, Chapter 2	Se text 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?	Patent Data Act Chapter 8	Every authority/health care provider keeping an EHR has to give information in accordance with the requirements in chapter 8, specially chapter 8 section 6
Are there specific national rules on consent from the patient to share data?	Patient Data Act, Chapter 2 section 3, chapter 6 Section 2; chapter 4 section1, 4	As a general rule an EHR may always be created with a patient's expressed consent With regards to the coordinated patient journals (*sammanhållen journalföring*) through direct access to health care records the patient has the right to opt-out of the system. Only health professionals participating in a specific health care situation have the right to direct access to patients journals. Other health professionals at the same health provider do not have right to access. Patients have the right to block certain information so only certain health professionals have right to access.
Are there any opt-in/opt-out rules for patient consent with regard to processing of EHRs?		Se above

Questions	Legal reference	Detailed description
Are there any opt-in/opt-out rules for patient consent with regard to sharing of EHRs?	Patient Data Act, Chapter 6 Section 2	Se text above
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?	Patient Data Act, Chapter 6 Section 2 Chapter 2 Section 12 SOSFS 2008:14	Chapter 6 Section 2 Paragraph 3 specifically states that the patient should be informed on health providers sharing of EHR through direct access.
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)?		The Patient Data Act does not consider any cross-border access to EHRs. In the Government Bill[31], the only situation considered was that Swedish quality registers are accessed from outside the country. In this case, the Personal Data Act [*Personuppgiftslag (1998:204)]* and the Public Access to Information and Secrecy Act [*Offentlighets- och sekretesslag (2009:400)]* were deemed applicable, which would mean that expressed consent by the patient would enable

[31] Prop 2007/08:126, at 200.

Questions	Legal reference	Detailed description
		the transfer of the patient's data. However there are no legal barriers for cross-border exchange as long as the patient gives his/hers consent and the information is taken from the existing EHR but not through direct access but by other technical solution e.g. a "picture" of an ePrescription.
Are there specific rules on patient consent to share data on a cross-border situation?	The Patient Data Act (2008:355), Chapter 2 section 3	No, but there are neither no legal barriers to hinder a cross-border exchange as long as the purpose of the exchange is within the requirements of the personal data act (implementation of the directive 95/46/EG) and the patient data act and other acts which may be applicable to the specified situation. A cross-border exchange need also to be based on patients expressed consent. The Patient Data Act (2008:355), Chapter 2 section 3 also states that EHR which is not allowed by the Act may be allowed if the patient has given his/hers expressed consent.

2.4. Creation, access to and update of EHRs

2.4.1. Main findings

Patient Data Act Chapter 4 Section 1 stipulates that only health professionals participating in a direct health care situation and in need to information for their work are allowed to access patients' journal(inner secrecy – *inre sekretess*). No other health professionals even if there are employed by the same health provider, are allowed access to a patients journal.
In addition, the activities have to be logged as well by the health care provider (see above on information security). The access to EHRs stored by other health care providers only includes accessing, but not adding or changing information. Patients have the right to receive information about their own EHRs, but at the moment only two county councils offer direct electronic access.

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?	Personal Data Act, Patient Data Act and Patient Safety Act	To provide health care is regulated (Patient Safety Act). The creation of EHR is regulated by the Personal Data Act and Patient Data Act. Other acts can also be applicable depending on the specific reason for the creation and usage of the specific EHR. All EHR are supervised by the Swedish DPA.
Are there specific national rules on access and update to EHRs?	Patient Data Act Chapter 4 Section National Board of Health and Welfare's Regulation on information processing and journals within the health and welfare sector - SOSFS 2008:14	Patient Data Act Chapter 4 Section 1 stipulates that only healthcare professionals in direct health care situation and in need of the information for the work are allowed to access a patien'ts journal (inner secrecy – *inre sekretess*). A health care provider have to be have a methodology to ensure that only health care professional are authorised to access EHRs to the extent necessary for good and safe care, SOSFS 2008:14 Chapter 2 Section 6
Are there different categories of access for different health professionals?	Patient Data Act Chapter 3 Section 3	Is is mandatory for a health care provider to keep patients' journals. But it is the health care providers (who are usually also the data controllers) who decide on different access levels (e.g. access, add, change, and erase) for its employees.
Are patients entitled to access their EHRs?	Patient Data Act Chapter 5 Section 5 Chapter 2 Section 13 National Board of Health and Welfare's Regulation on information processing and journals within the health and welfare sector - SOSFS 2008:14	Chapter 5 Section 5 Patient Data Act allows health care providers to offer patients **direct access** to their own patient journals. There is no obligation for health care providers to offer such access, but a mere possibility. If the access is offered via the Internet, high security is one of the main requirements. Two-way authentication is a requirement for the access (Chapter 2 Section 13 SOSFS 2008:14), i.e. the identity has to be verified by something the patient knows (e.g. password), something the patient has (smart card, mobile phone, one-time codes) and/or via the patient herself (e.g. finger print or iris scan). Two-way authentication in Sweden can be done by the electronic IDs which fulfil two of the stated ways to authenticate oneself.
Can patient have access to all of EHR content?		Yes if it is in accordance with the regulations for a patients access which means that in certain cases there is a possibility for denial.
Can patient download all or some of EHR content?		There is no legal obligation for health care providers to give patients direct access, there is however no true legal barrier as long as security can be kept.

Questions	Legal reference	Detailed description
Can patient update their record, modify and erase EHR content?		Not at the moment, but there are a few pilot projects under development that would allow patients to access their patient journals e.g. in Uppsala and Stockholm.
Do different types of health professionals have the same rights to update EHRs?		There is no national regulation that stipulates different access rights. As mentioned above, each health care provider has to organise access to EHRs.
Are there explicit occupational prohibitions? (e.g. insurance companies/occupational physicians…)	All applicable acts and ordinances	EHR/patient journals can only be accessed by health care professionals when in a care situation and in need for information to solve the care situation. for research the access can be allowed under certain conditions.
Are there exceptions to the access requirements (e.g. in case of emergency)?	Personal Data Act section 16 Patient Data Act Chapter 6 Section 4	In case of emergency the health provider has the right to access information. Patient Data Act Chapter 6 Section 4 allows health care providers to access EHRs in situations where the life or health of a patient is in serious danger and the patient is not able to give consent. In case the EHRs are locked, the health care provider is allowed to find out which health care provider has locked the data in the first place. If the health care provider assesses then that the EHRs stored at the other health care provider are of importance for the present treatment of the patient, it can contact the other health care provider in order to release the lock. If the EHRs are open, the health care provider may access first the information about which health care provider has the original records. If it then assesses that the data is important for the present treatment of the patient, it may access the EHRs stored at the other health care provider, without the patient's consent.
Are there any specific rules on identification and authentication for health professionals? *Or are they aggregated?*	National Board of Health and Welfare's Regulation on information processing and journals within the health and welfare sector - SOSFS 2008:14	Chapter 2 Section 2 of the Regulation by the National Board of Health and Welfare stipulates the requirements of accessibility, accuracy, secrecy and traceability. The latter refers to the obligation for health care providers to have routines and systems that allow to identify unauthorised and wrong activities and link them to a specific health professional or employee.[32] In

[32] Handbok till SOSFS 2008:14

Questions	Legal reference	Detailed description
		other words, due to the requirement of traceability in the Regulation, the activities of health professionals and employees have to be tracked within the system. SITHS (*Nationell identifieringstjänst*) is a national security solution for electronic identification and secure communication of information. By using a SITHS-card health care staff can identify themselves. SITHS is connected with HSA and has been implemented in all county councils and municipalities since spring 2012.
Does the patient have the right to know who has accessed to his/her EHRs?	Patient Data Act Chapter 8 Section 5 Chapter 2 Section 12 National Board of Health and Welfare's Regulation on information processing and journals within the health and welfare sector - SOSFS 2008:14	Yes, upon request. Health care providers have to **inform the patient** – upon request – if and how the patient's personal data has been accessed. Concerning the "how", information about the date, time and which department of a health care provider has accessed the data. The information about the logs does not have to contain names of the health care staff.[33] Logs can also be accessed if the health care provider is a public agency. In this case the logs are considered public records according to Chapter 2 Freedom of the Press Act [*Tryckfrihetsförordning (1949:105)]* and can therefore be requested by anybody.[34] Secrecy only applies to a certain extent in this situation.
Is there an obligation on health professionals to update EHRs?	Patient Data Act Chapter 3 Section 9	The patients journal have to be updated with new information each time there is a health care situation. Though the Act does not specify who exactly could update EHRs or patients' records in general (see above),
Are there any provisions for accessing data on 'behalf of' and for request for second opinion?		There are no explicit provisions. With the consent of the patient there is no legal barriers for sharing information. If the data is accessed within the purpose of giving health care and the second opinion can be deemed as a patient relation, the processing should be deemed as within the Patient Data Act.

[33] Handbok till SOSFS 2008:14 at 51 and Prop 2007/08:126, at 264 ff.
[34] Handbok till SOSFS 2008:14, at 51.

Questions	Legal reference	Detailed description
Is there in place an identification code system for cross-border healthcare purpose?		No
Are there any measures that consider access to EHRs from health professionals in another Member State?		A governmental review has looked into the question.Tthere is no decision on this.

2.5. Liability

2.5.1. Main findings

In general, patients in Sweden who suffer an injury while in the health care system may be entitled to compensation under the Patient Injury Act [*Patientskadelag (1996:799)*]. All Swedish county councils and regions have taken out patient insurance with Landstingens Ömsesidiga Försäkringsbolag (the Patient Insurance LÖF).[35] Some 10,000 patient injuries are reported to the Patient Insurance LÖF each year. About 45% of the reported injuries are compensated. The requirements for receiving compensation do not mention anything about medical negligence with regards to the use of EHRs explicitly.

Though the Swedish Patient Data Act, chapter 3 stipulates an obligation to keep patient journals it does not explicitly regulate any liability with regards to it. The Patient Data Act Chapter 10 refers to the general liability provisions in the Personal Data Act. To date there have been no known cases where the liability with regards to EHRs has been tested.

[35] Read more in English at www.patientforsakringen.se/resurser/dokument/andra_sprak/English_If-you-are-injured-in-the-health-care-system.pdf

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?		The provisions of the Personal Data Act are to be applied
Can patients be held liable for erasing key medical information in EHRs?		Patients can only access EHRs for reading
Can physicians be held liable because of input errors?		Physician can be held liable under the liability act and other applicable acts.
Can physicians be held liable because they have erased data from the EHRs?		Se AB 91.
Are hosting institutions liable in case of defect of their security/software systems?		Yes, as in any case for damages/liability, se AB 91
Are there measures in place to limit the liability risks for health professionals (e.g. guidelines, awareness-raising)?		No
Are there liability rules related to breach of access to EHRs (e.g. privacy breach)?	Personal Data Act, section 48 Chapter 4 Section 9 c of the Swedish Criminal Code	The data controller can be held liable and have to pay damages for unlawful access to EHR If a health care employee accesses patients' records of somebody she/he does *not* have a patient relation to, the health care employee can be held liable according to Chapter 4 Section 9 c of the Swedish Criminal Code [*Brottsbalk (1962:700)*] for hacking (*dataintrång*).
Is there an obligation on health professionals to access EHRs prior to take a decision involving the patient?		No, no specific obligation, only the obligation to provide safe health care.
Are there liability rules related to the misuse of secondary use of health data?		Ordinary rules for unlawful access applies.

2.6. Secondary uses and archiving durations

2.6.1. Main findings

The Patient Data Act stipulates an archiving period of at least ten years after the patient summary was amended the last time (Chapter 3 Section 17). With regards to secondary uses, the purpose principles apply, i.e. if the secondary use falls within the stated purposes or is in line with them, secondary uses should be allowed. In other words, the original purpose for collecting the data decides if any subsequent uses of the data are allowed. If the subsequent use is in line with the original purpose, the processing is allowed.

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?	Patient Data Act Chapter 3 Section 17	The Patient Data Act stipulates an archiving period of at least ten years after the patient journal was amended the last time. Under certain circumstances, the archiving period can be longer, which can be decided in by governmental ordinance or a regulation by a public agency.
Are there different archiving rules for different providers and institutions?		For research purposes, EHRs can be stored longer based on various legislative acts. If the health care provider is a public authority, the general archiving obligations for public authorities according to the Swedish Archiving Act [*Arkivlag (1990:782)*] apply.
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 explicit obligation to destroy patient data in the Patient Data Act. The approach is rather that personal data *may* be destroyed after the archiving duration has ended. To the contrary, Patient Data Act Chapter 8 Section 4 requires a specific decision by the Health and Social Care Inspectorate (*Inspektionen för vård och omsorg – IVO*) to destroy a specific patient summary upon request by the patient or someone who is mentioned in the patient summary. This provision applies, however, before the archiving period ends.
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?		Swedish legislation is focused on the archiving not on destroying. For public records there are severeal applicable Acts etc for the maintaining but also what happens when the general period has passed. Those Acts are in force also for EHRs.
Can health data be used for secondary purpose (e.g. epidemiological studies, national statistics...)?	Patient Data Act Chapter 2 Section 4	As long as the purpose for using is in accordance with the Acts requirements there is no difference made between the "first and secondary use". Chapter 2 Section 4 regulates the approved purposes for processing personal data within health care. Some of the mentioned purposes include: • To systematically and regularly develop and safeguard the quality of health care • Administration, planning, follow-up, evaluation and supervision of health care • To create statistics

Questions	Legal reference	Detailed description
		The Patient Data Act also allows for certain national and regional quality registers (Chapter 7). Though consent from the patient is required, the purpose is approved in Chapter 2 Section 4.
Are there health data that cannot be used for secondary use?		As long as the processing falls within the purposes stipulated in Chapter 2 Section 4 Patient Data Act, secondary use is allowed.
Are there specific rules for the secondary use of health data (e.g. no name mentioned, certain health data that cannot be used)?		In general no, but in certain cases, data has to be anonymised, which depends on the specific register.
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?		Not as long as it is within the usage for health care. If the secondary use is for research the opt-out situation is to be applied.

2.7. Requirements on interoperability of EHRs

2.7.1. Main findings

There is no central EHRs system in Sweden, but the databases are kept by the different health care providers, e.g. the country councils. The National Patient Overview NPÖ tries to increase the interoperability between the systems. In addition, Regulation SOSFS 2008:14 Chapter 3 Section 2, stipulates that patients' records should be documented by using nationally decided terms, classifications and other codes. In this regard, The National Board of Health and Welfare [*Socialstyrelsen*] has developed two standards that are partly based on European or international standards with regards to terminology; the National Information Structure (NI) and the National Interdisciplinary Terminology for Health and Social Care. The latter is partly based on the clinical terminology SNOMED CT.

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?	Patient Data Act, chapter 6 National Board of Health and Welfare's Regulation on information processing and journals within the health and welfare sector [*Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården*] - SOSFS 2008:14	No, the system of giving health providers direct access to other health providers patient journals is a possibility for health providers. Chapter 3 Section 2 of the Regulation stipulates that patients' records should be documented by using nationally decided terms, classifications and other codes.
Are there any specific rules/standards on the interoperability of EHR?	National Information Structure (NI) and National Interdisciplinary Terminology for Health and Social Care, both issued by the National Board of Health and Welfare [*Socialstyrelsen*]	The National Board of Health and Welfare [*Socialstyrelsen*] has developed two standards within Sweden that partly are based on European or international standards with regards to terminology. The National Information Structure (NI) is a comprehensive description of health and social care activities and stakeholders' information needs. It describes how the information should be structured. NI uses basic concepts that are based on the WHO definition of eHealth (health condition, health problem, health care request, health process, health process plan). The National Interdisciplinary Terminology for Health and Social Care in Sweden includes concepts and terms that have been agreed on a national basis and published in the Board's terminology database, statistical classifications and coding systems that have been agreed on national and international basis, as well as clinical terminology SNOMED CT. Both NI and the terminology are currently being tested by ten different health care providers. In its latest report from 2013, the National Board of Health and Welfare

Questions	Legal reference	Detailed description
		recommended that a national standard terminology for lab medical codes should be based on NPU (Nomenclature of Properties and Units) in the future.[36]
Does the law consider or refer to interoperability issues with other Member States systems?		Both the National Information Structure (NI) and the National Interdisciplinary Terminology for Health and Social Care are partly based on European and/or international standards. The law does not explicitly refer to interoperability with other Member States.

[36] Nationell informationsstruktur och nationellt fackspråk – Användning och tillgängliggörande, lägesrapport 2013, www.socialstyrelsen.se/publikationer2013/2013-12-9

2.8. Links between EHRs and ePrescriptions

2.8.1. Main findings

The Swedish ePrescription systems are being administered by the Swedish eHealth Agency (*Ehälsomyndigheten*). There are a few specific databases that are being used in connection with ePrescriptions. They are not directly linked to the EHR managed by the different health care providers, so there is no direct access between the different systems. There are mainly three databases in place that concern ePrescriptions: Pharmaceutical Register (*Läkemedelsförteckningen*), Prescription depot (*Receptdepån*) and High Cost Database (*Högkostnadsdatabasen*).

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?	Prescription Registration Act [*Lag (1996:1156) om receptregister*] Pharmaceutical Register Act [*Lag (2005:258) om läkemedelsförteckning*], Prescription Registration Act [*Lag (1996:1156) om receptregister*] Pharmaceutical Registers Act Lag (2005:258) om läkemedelsförteckning	The ePrescription systems are being administered by the Swedish eHealth Agency (*Ehälsomyndigheten*). There are a few specific databases that are being used in connection with ePrescriptions. They are not directly linked to the EHR managed by the different health care providers, so there is no direct access between the different systems. There are mainly three databases in place that concern ePrescriptions: Pharmaceutical Register (*Läkemedelsförteckningen*), Prescription depot (*Receptdepån*) and High Cost Database (*Högkostnadsdatabasen*). All three are regulated by specific laws (see legal reference to the left). Individuals can access the information in PDF of the information stored.
Can an ePrescription be prescribed to a patient who does not have an EHR?		It is possible for doctors to send ePrescriptions even if the patient's records are on paper.

- ***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?	Prescription Registration Act [*Lag (1996:1156) om receptregister*] Pharmaceutical Register Act	As the three main ePrescription systems are managed and administered by the Swedish eHealth Agency (*Ehälsomyndigheten*), health care professionals can only access the data stored in them under certain circumstances. In other words, pharmacists are not able to access the patient summary. Physicians and other health care professionals are in certain specified situation able to access the

Questions	Legal reference	Detailed description
	[*Lag (2005:258) om läkemedelsförteckning*]	ePrescriptions system.
Can those health professionals write ePrescriptions without having access to EHRs?	Prescription Registration Act [*Lag (1996:1156) om receptregister*] Pharmaceutical Register Act [*Lag (2005:258) om läkemedelsförteckning*]	Yes.

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

A cross-border exchange of EHR with EU countries or countries associated with EU has to be based on applicable EU legislation, mostly directive 95/46 EG and directive 2011/24/EU. However EU legislation does not cover legal questions and those questions have to be met either by new national legislation or bilateral/multilareal agreements between exchanging countries.

Direct access to EHR f0r o foreign health care provider is for the moment not possible but access to patient summaries could be possible in the future.

The cross-border exchange of ePrescriptions have been tested through the LSP epSOS. The technical system as such will to great extend in continued use between the Nordic countries who are at the moment creating a system for such an exchange, starting with a bilateral exchange between Finland and Sweden.

Main topics to be solved between the Nordic countries, and probable in an exchange situation with other EU member states are e.g. different approaches to patient consent (opt-out/opt-in), liability for damages, reimbursement, jurisdiction, forum shopping, different authorisation systems, technical security.

Telemedicine as such is not a term used in Sweden as it is normally used as part of the eHealth-solutions. But there are many good examples of telemedicine in Sweden, where health care staff can be with the patient, while the doctor on call is in the hospital. Another one includes medical equipment sending data directly to the EHRs in order for the health care staff to be able to monitor the patient's health on a distance.