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 Belgium

time.lex

milieu
Law & Policy Consulting

1 April 2014

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

This report was completed by Professor Jos Dumortier, time.lex. 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 Belgium

In Belgium competences in the area of health care are distributed between the federal State, the Regions (Flanders, Wallonia and Brussels) and the Communities (Flanders, French Language Community, German Language Community). On all these levels various government and bottom-up initiatives in the area of EHR have been taken in the last 10 years, such as the FLOW initiative which led to the creation of the 5 HUBS that are still in use today for the exchange of EHR data, the voluntary certification of EHR software applications or the development of a standardized patient summary (SUMEHR). An important boost has occurred by the establishment of the *eHealth-platform* created by law in 2008. As a government institution the eHealth-platform has received large competencies and is mandated to "define ICT related useful functional and technical norms, standards, specifications and basic infrastructure required to support [the eHealth] vision and strategy".

Generally speaking the Belgian landscape in the field of EHR starts to be progressively better embedded in the Belgian e-government model. This e-government model is characterized by five building blocks: the generalized use of the national unique identification number, the use of the electronic identity card as an authentication token, the use of validated authentic sources, the central role of service integrating bodies and the protection of privacy via specialized independent sector committees.

Since 2008 the eHealth-platform provides a series of so-called "basic services" which can be used by all actors in the healthcare sector and which can be integrated into the various – EHR and other - applications ("added-value services") offered by ICT-providers. Via the eHealth-platform these applications can also, under specific conditions and/or authorization, get access to so-called "validated authentic sources". These "authentic sources" are databases such as the National Register of physical persons residing in Belgium, the Register of accredited healthcare professionals, etc.

In the context of EHRs the most relevant example of a basic service provided by the eHealth-platform is the "Reference Directory". In the Reference Directory one can look up by which healthcare providers data are available for which patient. It consists essentially of two layers: 1) a first layer of information (called the "metahub") is available on the level of the eHealth-platform itself and refers to the regional or local network (the "hub") where further data for a given patient can be found; 2) a second layer is the so-called "hub" where one is referred to the actual location of the data, for example the local hospital.[1] There are currently 5 regional hubs functioning within the metahub system.

In recent years the eHealth-platform has succeeded in integrating additional databases and networks into its Reference Directory. One example is the *Vitalink* health vault of the Flanders Region where health-related data are shared between healthcare providers in areas which are regulated by this Region (for instance in the area of welfare and health prevention). Via the eHealth-platform a provider who has access to Vitalink can search if Vitalink contains information for a given patient. Another example of a system connected to the Reference Directory is the "pharmaceutical care data hub" which is used by the pharmacists to share their patient information.

The idea behind the Reference Directory is that it should be avoided to store health-related data on the central level of the eHealth-platform. Moreover it has been a solution to integrate to a maximum already existing initiatives in the area of shared EHRs (for example local hospital networks sharing

[1] See further https://www.ehealth.fgov.be/sites/default/files/assets/fr/pdf/Repertoire_reference/11-089-f139_reglement_hubs_metahub.pdf

patient data with the physicians in the region). As a consequence of the Reference Directory and of the fact that the data remain where they are generated, the healthcare providers remain responsible for the quality of the data being exchanged among healthcare professionals. Last but not least, the exchange of health-related data remains inside the hubs and data are not transferred via the the eHealth-platform.

Besides the Reference Directory the eHealth-platform provides an series of other basic services, such as user and access management, time stamping, end-to-end encryption, logging, anonymization and a secured mailbox. All actors in the healthcare sector are free to use the services of the eHealth-platform when they develop or introduce a solution in the field of eHealth. This is a of course a step-by-step process.
In Flanders more and more healthcare institutions are setting up local or regional hubs. A recent Flemish Decree creates a general legal obligation for healthcare providers to join a "network for sharing data between actors in healthcare". This network uses the basic services of the eHealth-platform. The decree also creates a Flemish "Agency for Cooperation in Data Sharing between Healthcare Actors".

In Wallonia the main initiative in this area is the "*Réseau Santé Wallon*" (RSW) which is a network created and managed by a non-profit association (FRATEM) in which major stakeholders in the healthcare sector are represented and that can be used by healthcare providers to securely share data. The RSW is structurally supported by the Wallonia region which is part of the FRATEM board. The RSW functions as a "hub" in the framework of the Reference Directory held by the eHealth-platform.

Finally one also has to mention "Abrumet", a network for healthcare providers (physicians) in the Brussels Capital Region.

2. Summary of legal requirements applying to EHRs

The Belgian legal framework applying to EHRs is complex. In this overview we make a distinction between three layers: 1) legal framework for the identification and authentication of actors in the healthcare domain, 2) legal framework relating to health records, applicable to paper as well as to electronic health records, and 3) legal framework for sharing health-related data among healthcare professionals.

A first layer of legal requirements relate to the identification and authentication of the actors in the healthcare domain. To allow the use of the "national identification number" for this purpose, healthcare institutions need an authorization to access the National Register.[2] The authorization is granted by one of the so-called "sector committees" which have been created by the Belgian general data protection legislation. The procedure to acquire this authorization has been considerably simplified by a "one-time" general authorization issued by the sector committee for the National Register (RN n° 21/2009 of 25 March 2009). To control the identity of a patient, every person registered under the Belgian social security system has received a social security chipcard (SIS-card) on which basic identity data are stored. This card is currently being replaced by the (general) Belgian electronic identity card (e-ID).

On a second layer EHRs are governed by a series of legal provisions applicable to all health records.

In Belgium a patient has the right to a *medical* record, carefully updated and safely stored by the health professional. Every health professional should keep a medical record about every patient to whom he provides healthcare services. Two Royal decrees of 3 May 1999 contain more detailed rules concerning the so-called General Medical Record (GMR) and concerning the medical records in hospitals. The first decree of 3 May 1999 contains precise rules about the content of the GMR. There

[2] Belgium has a central population register and every citizen residing in Belgium is identified by a national identification number. The access to the National Register and the use of the identification number are strictly regulated by law.

should be one GMR per patient, kept by the usual general practitioner. A patient can freely choose by which general practitioner his medical record should be kept and can modify this choice at any moment. He communicates his choice to his sickness fund, which forwards the number of patients per general practitioner to the Public Health administration. A medical record (not only the GMR) can be kept in paper or in electronic format.

The second decree of 3 May 1999 regulates the medical records to be kept by hospitals. Together with the nursing record, the medical record constitutes the "patient's record". The decree explicitly states that the medical record can be kept in electronic format. It needs to be kept for at least 30 years in the hospital. The decree also contains precise rules with regard to the content of the medical record. Some of the documents in the medical record need to be signed by the physician(s) who provided care to the patient.

On a third level there are a series of federal and regional regulatory texts specifically relating to electronic health-related data sharing. The most essential federal law of of course the law of 21 August 2008 on the establishment and the organization of the eHealth-platform. Following an amendment of this law in 2013, every healthcare provider who uses the services of the eHealth-platform is automatically authorized to use the identification number of the National Register. Another amendment has, under certain conditions, established an equivalent evidential value to electronic data (art. 36/1 of the eHealth-platform law).

Specifically with regard to the sharing of data via the Reference Directory, the eHealth-platform has issued a Regulation "with regard to the exchange of health data between health systems linked via the reference repertory of the eHealth-platform" (approved by the sector committee for social security and health on 18 February 2014 – n° 14/016). A Royal Decree of 20 September 2012 organises the information security when using the services of the eHealth-platform. In particular this Royal Decree contains provisions about the rights and duties of the healthcare professional in charge and of the information security officer.

On 21 April 2013 a first protocol agreement has been signed between the federal State and the Regions "with regard to the optimal electronic exchange and sharing of information and data between actors in the healthcare and welfare sectors". This protocol agreement is the first step towards a fundamental change in the legal status of the eHealth-platform which will gradually be transformed from a federal agency into an institution that is commonly regulated and managed by the federal State and the regions/communities together.

Last but not least one has to take into account the relevant opinions of the Sector Committee for Social Security and Health. Most relevant are the opinions of this Committee with regard to the concepts of "therapeutic relationship" (Opinion nr. 11/088 of 18 October 2011) and "informed patient consent" (Opinion nr. 11/046 of 17 May 2011 and Opinion nr. 12/047 of 19 June 2012). The opinions of the Sector Committee are in particular important because the legislation very often delegates to the Sector Committee the competence to authorize the exchange of health-related data. The opinions of the Sector Committee contain to some extent the criteria applied by the Committee when granting or refusing such authorizations.

3. Good practices

The Belgian situation has for a long time been characterized by fragmented but sometimes very progressive bottom-up initiatives. Since 2013, for example, an agreement has been reached between all major stakeholders about the external homologation of software applications for EHR used by physicians (GPs). The applications have to fulfil a series of criteria not only in the field of information security but also from the perspective of interoperability. In particular the applications should allow the extraction of a Summarized Electronic Health Record (SUMEHR). This feature can currently also be automatically checked by a validation tool available on the website of the eHealth-platform.

With the establishment of the eHealth-platform in 2008 the situation in the field of EHR becomes gradually more streamlined and there is a progressive evolution towards more and more health-related data sharing. In particular in Flanders such data sharing is conceived from a multidisciplinary perspective and no longer restricted to medical professionals.

Another positive evolution is the trend towards more bottom-up consensus-building on all levels. The eHealth-platform, although it has been created as a federal government body by the federal State, gradually moves to become a supra-federal body regulated and managed by the federal State and the regions together. Decision-making within the eHealth-platform is also more and more steered by consensus-building in an institutional framework with representatives of all relevant stakeholders.

On 20 December 2012, an « Action Plan 2013-2018 on eHealth » has been presented by a large and very representative group of stakeholders of the healthcare sector, with the overall objective of a widespread use of online health services around the patient for 2018. The plan is based on five pillars: (i) develop data exchange between caregivers on a common architecture; (ii) achieve a greater engagement and a better knowledge of e-Health by the patients; (iii) develop a terminology of reference; (iv) simplify and improve the efficiency of administrative tasks and; (v) establish a flexible and transparent governance structure in which all authorities and relevant stakeholders will be involved. The Action Plan 2013-2018 has been approved by the Interministerial Conference (ministers competent for health of the Federal State and the regions) on 28 January 2013 and published on a public website (http://www.rtreh.be/)

4. Legal barriers

There are very few remaining legal barriers for the deployment of EHRs in Belgium. Legislation and practice are quite pragmatic with regard to formal requirements (patient consent, approval of health institutions or individuals using EHRs etc), The last legal barriers – for example with regard to the equivalence of the evidential value of electronic data – have recently been removed.

Similar to what is done in most of the other Member States the organisation of the health-related data sharing architecture has been designed from a national perspective. Cross-border sharing of EHR is currently not considered as a priority.

Contents

List of abbreviations

ATC	Anatomical Therapeutic Chemical Classification System
DICOM	Digital Imaging and Communications in Medicine
EHRs	Electronic Health Records
EMR	Electronic Medical Record
GMR	Global Medical Record
GP	General Practitioner
HL7	Health Level 7
ICD	International Classification of Diseases
IHE	Integrating the Healthcare Entreprise
IHTSDO	International Health Terminology Standard Development Organization
ISO	International Organisation for Standardisation
KMEHR	Kind Messages for the Electronic Health Record
RSW	Réseau Santé Wallon
SUMEHR	Summarized Electronic Health Record
WHO	World Health Organization

1. General context

1.1. EHR systems in place

Similar to what happens in other EU Member States the development of EHRs started already at the end of the past century and it has been in a first stage mainly a bottom-up process. A large number of hospitals and physicians gradually introduced software applications with diverse functionalities such as, for example, the management of patient information. Sharing this information started first at the local level, for example, between a large hospital and the GPs and specialists in a given geographical area. Little by little more ambitious networks have been created at a regional level, such as, for example, the Réseau Santé Wallon, which is an initiative of a private non-profit association.

Meanwhile diverse eHealth-related initiatives were launched by other private associations. Relevant examples are those related to the voluntary certification of software packages for GPs and specialists and the development of a Belgian standard for the exchange of patient summaries (SUMEHR).

The eHealth-platform, created by (federal) law of 21 August 2008, started to provide a series of so-called "basic services" which can be used by all actors in the healthcare sector and which can be integrated into the various applications ("added-value services") offered by ICT-providers. Via the eHealth-platform these applications can also, under specific conditions, get access to the so-called "authentic sources". These "authentic sources" are databases such as the central population register ("National Register") or the register of accredited healthcare professionals.

One – for the context of EHRs very relevant - example of a basic service provided by the eHealth-platform is the so-called "Reference Directory". In the Reference Directory one can look up by which healthcare providers data are available for which patient. It consists essentially of two layers: 1) a first layer of information (called the "metahub") is available on the level of the eHealth-platform itself and refers to the regional or local network (the "hub") where further data for a given patient can be found; 2) a second layer is the so-called "hub" where one is referred to the actual location of the data, for example the local hospital.

In the past years the eHealth-platform has succeeded in integrating additional databases and networks into its Reference Directory. A recent example is the *Vitalink* health vault of the Flanders Region where health-related data are shared between healthcare providers in areas which are regulated by this Region (mainly in the area of welfare and prevention). Via the eHealth-platform a provider who has access to Vitalink can look up the information for a given patient. Another example is the "pharmaceutical care data hub" which is used by the pharmacists to share their patient information.

The idea behind the Reference Directory is that it should be avoided to store health-related data on the central level of the eHealth-platform. Moreover it has been a solution to integrate to a maximum already existing initiatives in the area of shared EHRs). As a consequence of the Reference Directory and of the fact that the data remain where they are generated, the healthcare providers remain responsible for the quality of the data being exchanged among healthcare professionals. Last but not least, the exchange of health-related data remains inside the hubs and not via the metahub on the level of the eHealth-platform.

Besides the Reference Directory the eHealth-platform provides an series of other basic services, such as the user and access management, time stamping, end-to-end encryption, logging, anonymization and a secured mailbox. All actors in the healthcare sector are free to use the services of the eHealth-platform when they develop or introduce a solution in the field of eHealth. This is a of course a step-by-step process. Currently, for example, a physician who has stand-by service during the weekend can use an online application via the eHealth-platform to communicate a report on a given patient to the usual physician who keeps the so-called global medical file of that patient. In Flanders more and more

healthcare institutions are setting up local or regional hubs. A Flemish Decree is currently under discussion in the Flemish Parliament which will create a general legal obligation for healthcare providers to join a "network for sharing data between actors in healthcare". This network uses the basic services of the eHealth-platform. The draft decree also creates a Flemish "Agency for Cooperation in Data Sharing between Healthcare Actors".

In Wallonia the main initiative in this area is the "Réseau Santé Wallon" (RSW) which is a network that can be used by healthcare providers (physicians) to securely share data. Contrary to the Flemish approach, participation in this network is entirely on a voluntary basis. The RSW functions as a "hub" in the framework of the Reference Directory held by the eHealth-platform. Part of the RSW is "Abrumet", a network for healthcare providers (physicians) in the Brussels Capital Region.

On 20 December 2012, an action plan on eHealth was presented by a large and very representative group of stakeholders of the healthcare sector, with the overall objective of a widespread use of online health services around the patient for 2018. The plan is based on five pillars: (i) develop data exchange between caregivers on a common architecture; (ii) achieve a greater engagement and a better knowledge of e-Health by the patients; (iii) develop a terminology of reference; (iv) simplify and improve the efficiency of administrative tasks and; (v) establish a flexible and transparent governance structure in which all authorities and relevant stakeholders will be involved. The action plan 2013-2018 has been approved by the Interministerial Conference (ministers competent for health of the Federal State and the regions on 28 January 2018 and published on the website http:// http://www.rtreh.be/)

1.2. Institutional setting

The Belgian Federal Government regulates and supervises all sectors of the social security system, including health insurance. However, responsibility for almost all preventive care and health promotion has been transferred to the communities and regions.[3]

The federal authorities determine the general legislative framework for the health system by issuing laws and by determining the annual budget. They regulate and finance the compulsory health insurance; determine accreditation criteria; finance hospitals and so-called heavy medical care units, and register and control pharmaceuticals. The regional governments (Flemish community, French community and Brussels) are responsible for health promotion and preventive healthcare; maternity and child health services; different aspects of elderly care; the implementation of hospital accreditation standards; and the financing of hospital investment.

The role of government as a policymaker is situated at the federal level. It is the Minister of Social Affairs, Public Health and the Environment together with the department of Public Health who elaborate the policy towards hospitals. It is also at this level that broad policy goals are translated into concrete objectives, such as the program for hospitals and the accreditation standards. The responsibility for health promotion and most preventive services is situated at the regional level. Regional authorities grant, for example, the licences and accreditations and supervise the quality standards and accreditation criteria.

With regard to eHealth in particular, the main institution is the eHealth-platform. It has been established at the federal level but currently transformed into a "super-federal" body shared by the federal State and the regions/communities. As already mentioned the eHealth-platform plays an important role in the eHealth development in Belgium via the provision of a range of basic services

[3] Belgium has three Regions (Flanders, Wallonia and Brussels Capital Region) and three Communities (Flanders, French Language Community, German Language Community). The Flemish Region and the Flemish Community have merged into "Flanders". It has consequently 7 ministers who are competent for health-related matters (there are two ministers competent for this field in the Brussels Capital Region: one for the Dutch speaking community and one for the French speaking community living in Brussels.

that can be used by all kinds of eHealth initiatives. In the context of EHRs the most important function of the eHealth-platform is the management of the Reference Directory.

On the regional level the competences in the area of eHealth in general and of EHRs in particular are mainly exercised by the regional government administrations. These administrations are more and more willing to co-operate with the eHealth-platform. On 21 April 2013 a first protocol agreement has been signed between the federal State and the regions "with regard to the optimal electronic exchange and sharing of information and data between actors in the healthcare and welfare sectors". This protocol agreement is the first step towards a fundamental change in the legal status of the eHealth-platform which will gradually be transformed from a federal agency into a "supra-federal" body that is commonly regulated and managed by the federal State and the regions/communities together.

1.3. Summary of legal requirements applying to EHRs

The Belgian legal framework applying to EHRs is complex. In this overview we make a distinction between three layers: 1) legal framework for the identification and authentication of actors in the healthcare domain, 2) legal framework relating to health records, applicable to paper as well as to electronic health records, and 3) legal framework for sharing health-related data among healthcare professionals.

A first layer of legal requirements relate to the identification and authentication of the actors in the healthcare domain. To allow the use of the "national identification number" for this purpose, healthcare institutions need an authorization to access the National Register.[4] The authorization is granted by one of the so-called "sector committees" which have been created by the Belgian general data protection legislation. The procedure to acquire this authorization has been considerably simplified by a "one-time" general authorization issued by the sector committee for the National Register (RN n° 21/2009 of 25 March 2009). To control the identity of a patient, every person registered under the Belgian social security system has received a social security chipcard (SIS-card) on which basic identity data are stored. This card is currently being replaced by the (general) Belgian electronic identity card (e-ID).

On a second layer EHRs are governed by a series of legal provisions applicable to all health records.
In Belgium a patient has the right to a *medical* record, carefully updated and safely stored by the health professional. Every health professional should keep a medical record about every patient to whom he provides healthcare services. Two Royal decrees of 3 May 1999 contain more detailed rules concerning the so-called General Medical Record (GMR) and concerning the medical records in hospitals. The first decree of 3 May 1999 contains precise rules about the content of the GMR. There should be one GMR per patient, kept by the usual general practitioner. A patient can freely choose by which general practitioner his medical record should be kept and can modify this choice at any moment. He communicates his choice to his sickness fund, which forwards the number of patients per general practitioner to the Public Health administration.

A medical record (not only the GMR) can be kept in paper or in electronic format. According to the code of professional ethics of the Order of Physicians it should be archived during 30 years. The second decree of 3 May 1999 regulates the medical records to be kept by hospitals. Together with the nursing record, the medical record constitutes the "patient's record". The decree explicitly states that the medical record can be kept in electronic format. It needs to be kept for at least 30 years in the hospital. The decree also contains precise rules with regard to the content of the medical record. Some of the documents in the medical record need to be signed by the physician(s) who provided care to the patient but this obstacle has been removed by introducing an equivalence between electronic records and paper documents for evidential purposes, if a series of security conditions are fulfilled. A separate

[4] Belgium has a central population register and every citizen residing in Belgium is identified by a national identification number. The access to the National Register and the use of the identification number are strictly regulated by law.

Royal decree of 21 September 2004 regulates the patient's record to be held by homes for elderly care, rest homes or centers for daycare.

Finally, on a third level there are a series of federal and regional regulatory texts specifically relating to electronic health-related data sharing. The most essential federal law of of course the law of 21 August 2008 on the establishment and the organization of the eHealth-platform. Following an amendment of this law in 2013, every healthcare provider who uses the services of the eHealth-platform is automatically authorized to use the identification number of the National Register. Another amendment has, under certain conditions, established an equivalent evidential value to electronic data (art. 36/1 of the eHealth-platform law).

Specifically with regard to the sharing of data via the Reference Directory, the eHealth-platform has issued a Regulation "with regard to the exchange of health data between health systems linked via the reference repertory of the eHealth-platform" (approved by the sector committee for social security and health on 18 February 2014 – n° 14/016). A Royal Decree of 20 September 2012 organises the information security when using the services of the eHealth-platform. In particular this Royal Decree contains provisions about the rights and duties of the healthcare professional in charge and of the information security officer.

Last but not least at the federal level one has to take into account the relevant opinions of the Sector Committee for Social Security and Health.[5] Most relevant are the opinions of this Committee with regard to the concepts of "therapeutic relationship" (Opinion nr. 11/088 of 18 October 2011) and "informed patient consent" (Opinion nr. 11/046 of 17 May 2011 and Opinion nr. 12/047 of 19 June 2012).

[5] The Sector Committees were established within the Privacy Commission by law, either by the Privacy Act or by a specific act for the sector in question. Apart from a few exceptions, half of each sector committee consists of Privacy Commission members, and the other half of experts familiar with the sector concerned. The Sector Committee for Social Security and Health protects the privacy of beneficiaries of the Belgian social security network, and ensures particular supervision of the communication of health-related data. It consists of two sections: the Social Security Section and the Health Section. The Health Section of the Sector Committee of Social Security and Health consists of six members: two Privacy Commission members and four external members (physicians).

2. Legal requirements applying to EHRs in Belgium

2.1. Health data to be included in EHRs

2.1.1. Main findings

Two Royal decrees of 3 May 1999 contain more detailed rules concerning the so-called General Medical Record (GMR) and concerning the medical records in hospitals. The first decree of 3 May 1999 contains precise rules about the content of the GMR. There should be one GMR per patient, kept by the usual general practitioner. A patient can freely choose by which general practitioner his medical record should be kept and can modify this choice at any moment. He communicates his choice to his sickness fund, which forwards the number of patients per general practitioner to the Ministry of Health.

The second decree of 3 May 1999 regulates the medical records to be kept by hospitals. Together with the nursing record, the medical record constitutes the "patient's record". The decree explicitly states that the medical record can be kept in electronic format.

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?)	Royal decrees of 3 May 1999	There are no special rules for EHRs, but the general rules regarding patient records applies to both manual and electronic health records. Two Royal decrees of 3 May 1999 contain more detailed rules concerning the so-called General Medical Record (GMR) and concerning the medical records in hospitals. The first decree of 3 May 1999 contains precise rules about the content of the GMR. There should be one GMR per patient, kept by the usual general practitioner. A patient can freely choose by which general practitioner his medical record should be kept and can modify this choice at any moment. According to the code of professional ethics of the Order of Physicians it should be archived during 30 years. The second decree of 3 May 1999 regulates the medical records to be kept by hospitals. Together with the nursing record, the medical record constitutes the "patient's record". The decree explicitly states that the medical record can be kept in electronic format. It needs to be kept for at least 30 years in the hospital. The decree also contains precise rules with regard to the content of the medical record. Some of the documents in the medical record need to be signed by the physician(s) who provided care to the patient.
Are these data restricted to purely medical information (e.g. physical or mental health, well-being)?	Royal Decrees of 3 May 1999	The legal provisions mentioned before mainly relate to health-related data but there are also rules on identity information and attributes of the patient
Is there a definition of EHR or patient's summary provided in the national legislation?		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..
Are there any requirements on the content of EHRs (e.g. detailed requirements on specific health data or general reference to health data)?	Royal Decrees of 3 May 1999	The Royal Decrees of 3 May 1999 contain a detailed list of data to be included in the GMR and in the EMR.
Are there any specific rules on the use of a common terminology or coding system to identify diseases, disorders,		In practice most Belgian EHR systems are designed to enable the extraction of a SUMEHR but this not a legal obligation. In practice EHR software applicatons in Belgium try to comply with the criteria put forward by the

Questions	Legal reference	Detailed description
symptoms and others?		eHealth-platform. Compliance with those criteria is necessary in order to get registered on the eHealth-platform. The registration is not obligatory but serves as a guarantee that the data processed by the software application comply to the standards used by the hub- en metahub system of the eHealth-platform.
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)?	Royal Decrees of 3 May 1999	EHRs in Belgium are not standardized and the general rules with regard to the GMR or to the EMR don't contain such distinction.
Are there any specific rules on identification of patients in EHRs?		In the context of EHRs patients can be identified by various criteria and there is no legal obligation to use one or more of these criteria. In practice however more and more EHR systems and networks are making use of the the national identification number as a unique identifier. The user and access management of the eHealth-platform is based on the national identification number and on the Belgian e-ID. Therefore, as soon as a patient needs to be identified via the hub- and metahub system of the eHealth-platform, the use of the national identification number is a conditio sine qua non.
Is there is a specific identification number for eHealth purposes?		The use of the national identification number and of the e-ID in the health sector has been approved by the Belgian Privacy Commission

2.2. Requirements on the institution hosting EHRs data

2.2.1. Main findings

As in many other countries healthcare providers or healthcare institutions don't necessarily perform the processing of health-related data entirely on their own. Many providers and institutions will make use of external service providers, for example for the storage of the EHRs. Outsourcing these tasks to external providers, using cloud services or not, is not regulated on a central level. Healthcare institutions and healthcare providers are in principle free to outsource storage and management of EHR.

The external providers will be considered as "processors" in the context of the general data protection legislation (for Belgium: the Privacy Act of 8 December 1992). All requirements that have to be fulfilled by the controller of the data, will automatically generate repercussions for the processor.

On the most general level an institution hosting EHR data will need to fulfill the requirements that are imposed on all controllers and processors of personal data, for example with regard to data security. In Belgium these general security requirements have been literally copied from the European data protection directive 95/46/EC.

On a second level additional general requirements can be found in, for example, the federal rules applicable to hospitals and in the Royal decrees concerning the GMR and the EMR. These rules are applicable to health records, irrespective of the fact whether they are in electronic form or not.

Finally there are specific rules applicable to particular networks. One example is the Regulation issued by the eHealth-platform concerning the exchange of health data between health systems connected to the Reference Directory. Another example are the Internal Rules adopted in the framework of the Réseau Santé Wallon. Other specific rules are included in the draft Flemish decree on the exchange of health data between healthcare providers in Flanders. Contrary to the RSW, the Flemish Platform is considered as a controller of the personal data whereas the RSW considers itself as a processor.

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?	Art. 16 of the Belgian Privacy Act of 8 December 1992.	There are no specific national rules about hosting and management of data from EHRs. The general rules on processing of personal data apply and the management of health records apply. These rules are mostly formulated in abstract terms (for example, the duty of due care imposed on physicians in the framework of the management of their patient records). As in the general European data protection directive, the Belgian Privacy Act contains similar provisions with regard to processors of personal data. Generally speaking a controller should, via a written contract, impose on his processors the same obligations with regard to the processing of personal data than the one he is submitted to as a controller.
Is there a need for a specific authorisation or licence to host and process data from EHRs?	Law of 21 August 2008 on the creation and the organisation of the eHealth-platform	No specific authorization is needed unless the EHR data are being exchanged via the eHealth-platform. In that case a healthcare institution will need an authorization from the Sector Committee for Social Security and Health.
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)?		The negative answer to this question doesn't mean that organisations hosting and managing data from EHR are not submitted to various sorts of internal rules or contracts. Typical are, for example, the Service Level Agreements annexed to cloud service contracts in the healthcare sector.
In particular, is there any obligation to have the information included in EHRs encrypted?		Again there is no such general obligation but the duty to encrypt the data will be included if data are exchanged via the eHealth-platform. Similar obligations can be found in the internal rules of the RSW. The Flemish Agency created by the draft Flemish decree on the exchange of health-related data delegates the competence to issue specific security rules, such as end-to-end encryption, to the Flemish health agency (that will be created by this decree.
Are there any specific auditing requirements for institutions hosting and processing EHRs?		The healthcare institutions and healthcare providers connected to the Reference Directory of the eHealth-Platform are requested to designate an internal security officer.

2.3. Patient consent

2.3.1. Main findings

Article 7, § 2, j) of the Belgian Law of 8 December 1992 on the protection of private life with regard to the processing of personal data is a literal transposition of article 8 (3) of the European Data Protection Directive 95/46/EC. It thus states that the prohibition to process personal data concerning health shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy. As a consequence healthcare professionals are allowed to process health-related data concerning their patients in the form of an EHR. They don't need an informed consent of the patient to do this. On the contrary, Belgian law contains an obligation for healthcare professionals to hold a patient record, under the condition that they have a therapeutic relationship with that patient. One implication of this last condition is that the healthcare professional who wishes to access patient data in a EHR will need to provide evidence of such a therapeutic relationship. This proof can be provided via diverse means which have been listed, in an opinion nr. 11/088 of 18 October 2011, by the Sector Committee for Health. The most commonly used proof for the existence of a therapeutic relationship is the reading of the e-ID for which the patient needs to provide his/her PIN code. Patients have always a possibility to exclude individual healthcare professionals from accessing their EHR via a portal application of the eHealth-platform website or via the regional hubs.

Nevertheless, according to article 5, 4°, b) of the eHealth-platform law of 21 August 2008, the inclusion of an EHR in the Reference Directory of the eHealth-platform is only possible on the basis of the informed consent of the patient. In practice this means that health-related data can't be shared via the hub- and metahub of the eHealth-platform without such a consent. The consent needs to be explicit but not necessarily in the form of a signed document. It suffices that the consent is effectively registered and that this registration is securely logged. In practice the consent is registered via the web portal of the eHealth-platform or via the hubs, and functions as a one-time "all or nothing" consent. This means that the consent is the basis for all health-related data sharing that makes use of the Reference Directory, including for example the EHR held by GPs or hospitals, the Vitalink health vault in Flanders, the shared pharmaceutical record of the pharmacists, etc. A patient doesn't, in other words, have a possibility to select among these applications. In the future, the possibility for the patient to select applications after having provided his overall content will be considered.

It is evident that the consent can only be registered after having sufficiently informed the patient concerned. In theory every patient has the possibility to provide his consent by filling in the relevant form on the web portal of the eHealth-platform or via the hubs, after having been authenticated by means of the e-ID.

In such case the patient can read detailed information about the hub- and metahub system and the rules governing the access to the EHR. In practice most patients will give their consent in the context of a visit to the hospital or to the GP's cabinet. In this situation it is important that the healthcare professional or the administrative staff member provides sufficient and clear information on the way the health-related data will be processed and shared. In is important to mention at this stage that, although the Flemish regional legislation contains an obligation for all healthcare professionals to use the Vitalink health vault, the inclusion of a patient's health-related data will only be possible after the explicit consent of that patient. As mentioned earlier, it suffices for a patient to provide this consent once, for all data sharing applications. An additional consent for Vitalink is not needed. The condition for a data sharing application to make use of the one-time informed consent given by the patient is an authorization for this application by the Sector Committee for Health.

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?	Article 7, § 2, j) of the Belgian Law of 8 December 1992 on the protection of private life with regard to the processing of personal data	Article 7, § 2, j) of the Belgian Law of 8 December 1992 on the protection of private life with regard to the processing of personal data is a literal transposition of article 8 (3) of the European Data Protection Directive 95/46/EC. It thus states that the prohibition to process personal data concerning health shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy. As a consequence healthcare professionals are allowed to process health-related data concerning their patients in the form of an EHR. They don't need an informed consent of the patient to do this. On the contrary, Belgian law contains an obligation for healthcare professionals to hold a patient record, under the condition that they have a therapeutic relationship with that patient. One implication of this last condition is that the healthcare professional who wishes to access patient data in a EHR will need to provide evidence of such a therapeutic relationship. This proof can be provided via diverse means which have been listed, in an opinion nr. 11/088 of 18 October 2011, by the Sector Committee for Health. The most commonly used proof for the existence of a therapeutic relationship is the reading of the e-ID for which the patient needs to provide his/her PIN code. Patients have always a possibility to exclude individual healthcare professionals from accessing their EHR via a portal application of the eHealth-platform website. Nevertheless, according to article 5, 4°, b) of the eHealth-platform law of 21 August 2008, the inclusion of an EHR in the Reference Directory of the eHealth-platform is only possible on the basis of the informed consent of the patient. In practice this means that health-related data can't be shared via the hub- and metahub of the eHealth-platform without such a consent.
Is a materialised consent needed?	Article 5, 4°, b) of the eHealth-platform law of 21 August 2008,	The consent needs to be explicit but not necessarily in the form of a signed document. It suffices that the consent is effectively registered and that this registration is securely logged. In practice the consent is registered via the

Questions	Legal reference	Detailed description
		web portal of the eHealth-platform and functions as a one-time "all or nothing" consent. This means that the consent is the basis for all health-related data sharing that makes use of the Reference Directory, including for example the EHR held by GPs or hospitals, the Vitalink health vault in Flanders, the shared pharmaceutical record of the pharmacists, etc. A patient doesn't, in other words, have a possibility to select among these applications. This will be made possible in the future but only after the patient has provided his overall consent.
Are there requirements to inform the patient about the purpose of EHRs and the consequences of the consent or withholding consent to create EHRs?	Article 9 of the Belgian Law of 8 December 1992 on the protection of private life with regard to the processing of personal data	It is evident that the consent can only be registered after having sufficiently informed the patient concerned. In theory every patient has the possibility to provide his consent by filling in the relevant form on the web portal of the eHealth-platform, after having been authenticated by means of the e-ID. In such case the patient can read detailed information about the hub- and metahub system and the rules governing the access to the EHR. In practice most patients will give their consent in the context of a visit to the hospital or to the GP's cabinet. In this situation it is important that the healthcare professional or the administrative staff member provides sufficient and clear information on the way the health-related data will be processed and shared. In is important to mention at this stage that, although the Flemish regional legislation contains an obligation for all healthcare professionals to use the Vitalink health vault, the inclusion of a patient's health-related data will only be possible after the explicit consent of that patient.
Are there specific national rules on consent from the patient to share data?	Article 5, 4°, b) of the eHealth-platform law of 21 August 2008	According to article 5, 4°, b) of the eHealth-platform law of 21 August 2008, the inclusion of an EHR in the Reference Directory of the eHealth-platform is only possible on the basis of the informed consent of the patient. In practice this means that health-related data can't be shared via the hub- and metahub of the eHealth-platform without such a consent.
Are there any opt-in/opt-out rules for patient consent with regard to processing of EHRs?	Article 7, § 2, j) of the Belgian Law of 8 December 1992 on the protection of private life with regard to the processing of personal data	Consent – in the form of opt-in or opt-out – is not needed for processing health-related data where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

Questions	Legal reference	Detailed description
Are there any opt-in/opt-out rules for patient consent with regard to sharing of EHRs?	Article 5, 4°, b) of the eHealth-platform law of 21 August 2008	According to article 5, 4°, b) of the eHealth-platform law of 21 August 2008, the inclusion of an EHR in the Reference Directory of the eHealth-platform is only possible on the basis of the informed consent of the patient. In practice this means that health-related data can't be shared via the hub- and metahub of the eHealth-platform without the opt-in of the patient.
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?	Opinion nr. 12/047 of 18 June 2012 issued by the Sector Committee for Social Security and Health	The Opinion of the Sector Committee contains the text of the form which has to be submitted to the patient before including the EHR of this patient in the Reference Directory of the eHealth-Platform or for any other sharing of data via the eHealth-platform. It mentions, for example, that every additional sharing of the EHR data needs a prior authorization issued by the Sector Committee for Social Security and Health.
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)?		In principle the answer is positive but the cross-border sharing of health data is not envisaged by the Belgian federal or regional legislators. On the other hand nothing prevents an healthcare institution outside the Belgian borders to become part of the hub- and metahub system of the eHealth-platform for the data concerning patients who are Belgian residents. For non-Belgian residents this would, at least at this stage, difficult because the user and access management in the framework of the eHealth-platform is entirely based on the Belgian national identification number and on the use of the e-ID as an identity token.
Are there specific rules on patient consent to share data on a cross-border situation?		Belgian neither national nor regional legislation mentions cross-border sharing of health-related data. This situation is not envisaged by the legislators at this stage. As a consequence the general rules of the Privacy Act will apply. This means that, for example, a transfer of health-related personal data to a third country outside the EU can be carried out on the basis of the informed consent of the patient concerned.

2.4. Creation, access to and update of EHRs

2.4.1. Main findings

The patient has the right to a medical record, carefully updated and safely stored by the health professional. Every health professional should keep a medical record about every patient to whom he provides healthcare services.

Two Royal decrees of 3 May 1999 contain more detailed rules concerning the so-called General Medical Record (GMR) and concerning the medical records (EMR)in hospitals.

The first decree of 3 May 1999 contains precise rules about the content of the GMR. There should be one GMR per patient, kept by the usual general practitioner. A patient can freely choose by which general practitioner his medical record should be kept and can modify this choice at any moment. He communicates his choice to his sickness fund, which forwards the number of patients per general practitioner to the Ministry of Health.

A medical record (not only the GMR) can be kept in paper or in electronic format. According to the code of professional ethics of the Order of Physicians it should be archived during 30 years.

The second decree of 3 May 1999 regulates the medical records to be kept by hospitals. Together with the nursing record, the medical record constitutes the "patient's record". The decree explicitly states that the medical record can be kept in electronic format. It needs to be kept for at least 30 years in the hospital. The decree also contains precise rules with regard to the content of the medical record. Some of the documents in the medical record need to be signed by the physician(s) who provided care to the patient.

Hospitals should archive the records of all patients who left the service, preferably in a central database or at least per service and in electronic format with a unique number per patient. The archive should be accessible to physicians who are involved in the provision of care to the patient.

Patients have the right to access their own medical records. A patient's request to access his medical record shall be granted as soon as possible and not later than 15 days following the request. The health professional's personal notes and information relating to third parties are excluded from the right of access to medical records. Personal notes are limited to notes which are never accessible to others, not even to the other members of a medical care team.

Patients have a right to obtain a copy of their medical records, in whole or in part, at cost price, as soon as possible and not later than 15 days following the request. Again personal notes and information relating to third parties are excluded. Each copy shall clearly indicate that it is strictly personal and confidential. A health professional can refuse to supply a copy if there are clear signs that the patient has been pressured to ask a copy of his medical record at the instigation of a third party.

The law determines, finally, also the conditions under which the next of kin may consult the deceased patient's medical record.

A Royal decree of 21 September 2004 regulates the patient's record to be held by homes for elderly care, rest homes or centers for daycare.

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?	Royal Decrees of 3 May 1999 regarding the GMR and regarding the EMR in hospitals + Royal Decree of 28 December 2006 regulating the minimum conditions for the nursing record in hospitals + the Law of 19 April 1999 regarding non-conventional medical practices. See also the Code of Medical Deontology issued by the Order of Physicians + Law of 22 August 2002 concerning the patient rights	Two Royal decrees of 3 May 1999 contain more detailed rules concerning the so-called General Medical Record (GMR) and concerning the medical records (EMR)in hospitals. The first decree of 3 May 1999 contains precise rules about the content of the GMR. There should be one GMR per patient, kept by the usual general practitioner. A patient can freely choose by which general practitioner his medical record should be kept and can modify this choice at any moment. The second decree of 3 May 1999 regulates the medical records to be kept by hospitals. Together with the nursing record, the medical record constitutes the "patient's record". The decree also explicitly states that the medical record can be kept in electronic format. It needs to be kept for at least 30 years in the hospital. The decree contains precise rules with regard to the content of the medical record. A separate decree contains quite precise rules on the creation and management of nursing records in hospitals. All physicians have an obligation to keep a record on the medical care provided to patients, resulting from the Professional Code of Medical Deontology issued by the Order of Physicians. In Belgium there is a legal recognition of "non-conventional medical practices". These practitioners have also on obligation to to keep a record on the medical care provided to patients Last but not least the right of patients to have a health record results from the Law of 22 August 2002 concerning the patient rights .
Are there specific national rules on access and update to EHRs?	Royal Decrees of 3 May 1999 regarding the GMR and regarding the EMR in hospitals + Royal Decree of 28 December 2006 regulating the minimum conditions for the nursing record in hospitals the Law of 19 April 1999 regarding non-conventional	General rules on access (the "need to know principle", etc.) and update (the obligation to keep data accurate, etc.) are included in the laws and decrees mentioned before (often formulated in general terms). On the other hand there are more and more specific rules introduced when EHR data start to be shared. For example in order to get connected to the hub- and metahubsystem of the eHealth-platform EHRs have to fulfill the rules contained in the Regulation concerning the exchange of health-related data between healthcare systems linked to the Reference

Questions	Legal reference	Detailed description
	medical practices. See also the Code of Medical Deontology issued by the Order of Physicians + Law of 8 December 1992 protecting private life in the context of processing personal data ("Privacy Act") + Internal rules of the eHealth-platform, Vitalink, RSW, Abrumet, etc.	Directory of the eHealth-platform. These rules are not issued by a legislator but they have been validated by the Sector Committee for Social Security and Health (in this case by Opinion nr 14/06 of 18 February 2014). There are also specific and precise rules for data sharing within Vitalink, RSW and Abrumet. For Flanders future precise rules are integrated in the draft decree on healthcare data sharing between healthcare providers (currently under discussion in the Flemish Parliament).
Are there different categories of access for different health professionals?	Law of 8 December 1992 protecting private life in the context of processing personal data ("Privacy Act") + Royal Decree nr. 78 of 10 November 1967 regarding the exercise of healthcare professions + Royal Decrees of 3 May 1999 regarding the GMR and regarding the EMR in hospitals + Royal Decree of 28 December 2006 regulating the minimum conditions for the nursing record in hospitals + the Law of 19 April 1999 regarding non-conventional medical practices. See also the Code of Medical Deontology issued by the Order of Physicians + Law of 22 August 2002 concerning the patient rights	These rules result primarily from the general principle that personal data should only be accessed on a "need to know" basis (Art. 16 of the Belgian Privacy Act but also included in many other legal and regulatory texts). Generally speaking there is a trend in Belgium to include more and more all categories of healthcare professionals in a wide sense into the EHR data sharing networks and systems. Nevertheless many authorizations remain the reserved domain of a narrow circle of health professionals as defined in a Royal decree nr. 78 of 10 November 1967 (physician, dentist, pharmacist, physical therapist, nurse, etc.) or even for physicians in the strictest sense.
Are patients entitled to access their EHRs?	Law of 22 August 2002 concerning the patient right + + Law of 8 December 1992 protecting private life in the context of processing personal	Patients have the right to access their own medical records and this principle is also applied in the current "hub-metahub" system described before. A patient's request to access his medical record shall be granted as soon as possible and not later than 15 days following the request. The health professional's personal notes and information relating to third

Questions	Legal reference	Detailed description
	data ("Privacy Act")	parties are excluded from the right of access to medical records. Personal notes are limited to notes which are never accessible to others, not even to the other members of a medical care team. Patients have a right to obtain a copy of their medical records, in whole or in part, at cost price, as soon as possible and not later than 15 days following the request. Again personal notes and information relating to third parties are excluded. Each copy shall clearly indicate that it is strictly personal and confidential. A health professional can refuse to supply a copy if there are clear signs that the patient has been pressured to ask a copy of his medical record at the instigation of a third party.
Can patient have access to all of EHR content?	Law of 22 August 2002 concerning the patient rights + Law of 8 December 1992 protecting private life in the context of processing personal data ("Privacy Act") + Opinion of the National Council of the Order of Physicians of 20 January 2007.	There are two exceptions to the right of the patient to access his EHR: 1) personal notes of the healthcare provider and 2) rights of third persons. Besides these two exceptions a healthcare professional, on the basis of the therapeutic relationship, can judge that communication to the patient of certain details of his health status could harm this patient. To make use of this possibility a healthcare professional needs to consult a colleague and insert a motivated note about the refusal in the EHR.
Can patient download all or some of EHR content?	Law of 22 August 2002 concerning the patient right + + Law of 8 December 1992 protecting private life in the context of processing personal data ("Privacy Act")	Patients have a right to obtain a copy of their medical records, in whole or in part, at cost price, as soon as possible and not later than 15 days following the request.
Can patient update their record, modify and erase EHR content?	Law of 22 August 2002 concerning the patient right + + Law of 8 December 1992 protecting private life in the context of processing personal data ("Privacy Act")	Updating of the EHR by the patient is in principle excluded but is not excluded and perhaps even recommended for EHR software applications to provide separate fields where patients can add their own information in the EHR.
Do different types of health professionals have the same rights to update EHRs?	Royal Decrees of 3 May 1999 regarding the GMR and regarding the EMR in hospitals +	The rights and duties to update EHRs are spread over various general and specific legal and regulatory texts and are also part of the internal rules of specific EHR networks such as the hub-metahubsystem.

Questions	Legal reference	Detailed description
	Royal Decree of 28 December 2006 regulating the minimum conditions for the nursing record in hospitals the Law of 19 April 1999 regarding non-conventional medical practices. See also the Code of Medical Deontology issued by the Order of Physicians + Law of 8 December 1992 protecting private life in the context of processing personal data ("Privacy Act") + Internal rules of the eHealth-platform, Vitalink, RSW, Abrumet, etc.	
Are there explicit occupational prohibitions? (e.g. insurance companies/occupational physicians…)	Art. 95 of the Insurance Contract Act of 15 June 1992 + Opinionsof the National Council of the Order of Physicians of 16 November 1996, 19 June 2004 and 25 November 2006	In normal circumstances an insurance company is not allowed to have access to or to receive a copy of the EHR. Healthcare professionals can however provide attestations directly to their patients if they need those for insurance purposes. An evident exception is the delivery of the attestation of the cause of death, which will be provided directy to the insurance company.
Are there exceptions to the access requirements (e.g. in case of emergency)?	Law of 8 December 1992 protecting private life in the context of processing personal data ("Privacy Act")	The most obvious exception is the "vital interest" exception mentioned as one of the legitimate grounds for processing personal data in Art. 5 of the Belgian Privacy Act (see also Art. 7 of the European Data Protection Directive 95/46/EC). These exclusions are also clearly described in the Hubs-meta hub internal rules.
Are there any specific rules on identification and authentication for health professionals? *Or are they aggregated?*	Law of 21 August 2008 regulating the creation and the organisation of the eHealth-Platform and Opinion nr. 11/088 of 18 October 2011 of the Sector Committee for Social Security and Health concerning the Note on the electronic means of evidence of a therapeutic	The eHealth-plaform has a strict user and access management system and checks in authentic sources wheter or not a health professional is registered. Additionally the healthcare professional has to provide evidence of a therapeutic relationship with the patient from whom he request to access health-related data. The evidence of the therapeutic relationship can be provided by various means. They are summarized Opinion nr. 11/088 of 18 October 2011 of the Sector Committee for Social Security and Health concerning the Note on the electronic means of evidence of a therapeutic relationship and a care relationship. In the

Questions	Legal reference	Detailed description
	relationship and a care relationship.	near future specfic databases will be created to register the therapeutic relationship between healthcare providers and patients. A patient can register himself his therapeutic relationship with a healthcare provider or can delegate this to his physician (GP or specialist). A GP can be mandated by a patient to register and manage all the therapeutic relationships for this patient. Sometimes a therapeutic relationship can be deducted from other elements, for example from the fact that a patient has chosen a physician to hold his GMD.
Does the patient have the right to know who has accessed to his/her EHRs?	Law of 22 August 2002 concerning the patient right + + Law of 8 December 1992 protecting private life in the context of processing personal data ("Privacy Act")	In principle patients have such a right but they will have to send a request to obtain this information in almost all cases. The hub-metahub system provides the possibilty to access this information directly online. This practice is more and more recommended.
Is there an obligation on health professionals to update EHRs?	Royal Decrees of 3 May 1999 regarding the GMR and regarding the EMR in hospitals + Royal Decree of 28 December 2006 regulating the minimum conditions for the nursing record in hospitals + the Law of 19 April 1999 regarding non-conventional medical practices. See also the Code of Medical Deontology issued by the Order of Physicians + Law of 8 December 1992 protecting private life in the context of processing personal data ("Privacy Act")	The rights and duties to update EHRs are spread over various general and specific legal and regulatory texts and are also part of the internal rules of the hub-metahub system.
Are there any provisions for accessing data on 'behalf of' and for request for second opinion?		No
Is there in place an identification		Cross-border access is not envisaged in the Belgian legislation. This

Questions	Legal reference	Detailed description
code system for cross-border healthcare purpose?		might change after the adoption of the European EIDAS Regulation.
Are there any measures that consider access to EHRs from health professionals in another Member State?		Cross-border access is not envisaged in the Belgian legislation. This might change after the adoption of the European EIDAS Regulation.

2.5. Liability

2.5.1. Main findings

Civil liability of a physician arises when an obligation is not fulfilled. Obligations originate either from a contract or from tort. The Belgian courts have acknowledged the possibility of a contract for medical services existing between a physician and his patient or between the employer of a physician (a hospital) and a patient. Non-contractual or tortuous liability is only relevant in the case of damage to a third party or when services are rendered to a patient when the latter is not in a position to give consent to treatment.

It is not surprising that hospital physicians are more involved in malpractice actions than general practitioners, and, in general, physicians who practice outside the premises of a hospital. Many malpractice cases before courts relate to medical apparatus: actions based on the use of defective equipment, inexpert use of available apparatus and/or lack of supervision on the technicians using the apparatus. Especially anesthesiologists have been confronted with this sort of claims. A third category of malpractice suits relating to medical apparatus is based on the fact that no use was made of a piece of equipment, although it was available and in good shape at the time. In the future malpractice could however also relate to, for example, negligence in the update of an EHR.

Characteristic of hospital medicine is that a patient is not confronted with one physician but with a medical team. This often complicates the determination of responsibilities when an accident happens. Matters are still complicated because a surgeon may employ their own nursing personnel while anesthesiologists can make use of personnel employed by the hospital. Also the physician may act under different statutes: as an employee, a civil servant or as a private service provider on his own account. The difference between these situations is directly relevant for the nature of the contractual relationship with the patient and consequently also for the discussion about liability for damages.

One of the most important legal obligations owed by a physician to a patient is the protection of confidences revealed by the patient to the physician. Article 458 of the Criminal Code lays upon a physician a legal obligation not to disclose confidential information concerning a patient which he learns in the course of his professional practice.
The obligation of non-disclosure applies not only to information acquired directly from the patient, but also to information concerning the patient which the doctor learns from other sources.
The duty of medical secrecy is not limited to physicians who are providing healthcare to the patient. A physician who medically investigates a person at the request of an employer or an insurance company, is also bound by the duty, although he may inform in such a case the employer or the insurer within the limits of his mission.

Article 458 of the Criminal Code has a large field of application and not only applies to physicians alone but to everyone who, in the course of his professional practice, is being informed of confidential information. Therefore it is generally accepted that not only physicians but also nursing and paramedical personnel are bound to a duty of secrecy. Because all the members of a medical team are obliged to respect the confidentiality of the patient's information, one accepts that this information may circulate within the team (so-called "shared medical secret").

A law of 31 March 2010 on the compensation of damage as a consequence of healthcare introduced the concept of faultless liability in the health sector. The basic principle of this law is that victims of damage as a consequence of healthcare do no longer have to proof the existence of a fault committed by the health professional. Under certain conditions victims of damage as a consequence of healthcare can be compensated by a dedicated "Fund for medical accidents". The system introduced by the law of 31 March is however only applicable to damage as a consequence of healthcare in the strictest sense. Damage as a consequence of incorrect fulfilment of other duties of the healthcare provider – for example non-respect of medical secrecy or inaccuracy in the update of an EHR – remains under the

normal liability rules. In the last hypothesis one should evidently not forget that, according to Belgian and European data protection law – cfr art. 23 of the 95/46/EC Directive - , a data subject who has suffered damage as a result of an unlawful processing operation or of any act incompatible with European or national data protection provisions, is entitled to receive compensation from the controller for the damage suffered. The controller may only be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.

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?		Civil liability of a physician arises when an obligation is not fulfilled. Obligations originate either from a contract or from tort. The Belgian courts have acknowledged the possibility of a contract for medical services existing between a physician and his patient or between the employer of a physician (a hospital) and a patient. Non-contractual or tortuous liability is only relevant in the case of damage to a third party or when services are rendered to a patient when the latter is not in a position to give consent to treatment.
Can patients be held liable for erasing key medical information in EHRs?		No
Can physicians be held liable because of input errors?	Art. 15 bis of the Law of 8 December 1992 protecting private life in the context of processing personal data ("Privacy Act")	According to Belgian and European data protection law – cfr art. 23 of the 95/46/EC Directive - , a data subject who has suffered damage as a result of an unlawful processing operation or of any act incompatible with European or national data protection provisions, is entitled to receive compensation from the controller for the damage suffered. The controller may only be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.
Can physicians be held liable because they have erased data from the EHRs?	Art. 15 bis of the Law of 8 December 1992 protecting private life in the context of processing personal data ("Privacy Act")	Idem as supra
Are hosting institutions liable in case of defect of their security/software systems?	Art. 16 of Law of 8 December 1992 protecting private life in the context of processing personal data ("Privacy Act")	It is a duty of the controller to specify the liability of the processor in the form of a written agreement. In practice the processor will be liable for every incorrect execution of this contract.
Are there measures in place to limit the liability risks for health professionals (e.g guidelines, awareness-raising)?		No

Questions	Legal reference	Detailed description
Are there liability rules related to breach of access to EHRs (e.g. privacy breach)?	Art. 15 bis of the Law of 8 December 1992 protecting private life in the context of processing personal data ("Privacy Act") + Article 458 of the Criminal Code	One of the most important legal obligations owed by a physician to a patient is the protection of confidences revealed by the patient to the physician. Article 458 of the Criminal Code lays upon a physician a legal obligation not to disclose confidential information concerning a patient which he learns in the course of his professional practice. The obligation of non-disclosure applies not only to information acquired directly from the patient, but also to information concerning the patient which the doctor learns from other sources. The duty of medical secrecy is not limited to physicians who are providing healthcare to the patient. A physician who medically investigates a person at the request of an employer or an insurance company, is also bound by the duty, although he may inform in such a case the employer or the insurer within the limits of his mission. Article 458 of the Criminal Code has a large field of application and not only applies to physicians alone but to everyone who, in the course of his professional practice, is being informed of confidential information. Therefore it is generally accepted that not only physicians but also nursing and paramedical personnel are bound to a duty of secrecy. Because all the members of a medical team are obliged to respect the confidentiality of the patient's information, one accepts that this information may circulate within the team (so-called "shared medical secret").
Is there an obligation on health professionals to access EHRs prior to take a decision involving the patient?		No
Are there liability rules related to the misuse of secondary use of health data?	Art. 15 bis of the Law of 8 December 1992 protecting private life in the context of processing personal data	Art. 15 bis of the Law of 8 December 1992 protecting private life in the context of processing personal data applies ("Privacy Act")

2.6. Secondary uses and archiving durations

2.6.1. Main findings

In practice the duration of storage for medical records varies among healthcare institutions. Many hospitals don't apply any limit on the archiving period and never destroy or delete the patient record, while other institutions only keep the record up to five years after the last contact with the patient.

Article 46 of the code of professional ethics, established by the Order of Physicians, states that the physician should keep the medical file for a period of 30 years after the last contact with the patient. A similar provision is included in the Royal Decree of 3 May 1999 on the general minimum conditions for medical records in the hospital. Art. 1, § 3 of the Royal Decree of 28 December 2006 establishing the minimum conditions for the nursing record prescribes however an archiving duration of 20 years. Fortunately the prescribed archiving duration is, in all cases, only a minimum. In healthcare institutions where the medical record and the nursing record are merged into one EHR the data will normally be kept for 30 years, or, as far as it is justified under the general data protection legislation, for a longer period.

Data in EHRs can be used for *secondary purposes* (e.g. research and quality control) in accordance with the general data protection rules. In general, data can be used for quality control, research and statistics without the patient's consent, provided there is compliance with the Belgian data protection law of 8 December 1992. In some situations, in particular in cases where the health-related data are not further processed in an anonymized form, an authorization from the Privacy Commission will be necessary. The authorizations for further processing of health-related data for research purposes are published on the website of the Privacy Commission (www.privacycommission.be)

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?	Royal Decree of 3 May 1999 on the general minimum conditions for medical records in the hospital + Art. 1, § 3 of the Royal Decree of 28 December 2006 establishing the minimum conditions for the nursing record + Article 46 of the Code of Professional Ethics, established by the Order of Physicians,	In practice the duration of storage for medical records varies among healthcare institutions. Many hospitals don't apply any limit on the archiving period and never destroy or delete the patient record, while other institutions only keep the record up to five years after the last contact with the patient. Article 46 of the Code of Professional Ethics, established by the Order of Physicians, states that the physician should keep the medical file for a period of 30 years after the last contact with the patient. A similar provision is included in the Royal Decree of 3 May 1999 on the general minimum conditions for medical records in the hospital. Art. 1, § 3 of the Royal Decree of 28 December 2006 establishing the minimum conditions for the nursing record prescribes however an archiving duration of 20 years. Fortunately the prescribed archiving duration is, in all cases, only a minimum. In healthcare institutions where the medical record and the nursing record are merged into one EHR the data will normally be kept for 30 years, or, as far as it is justified under the general data protection legislation, for a longer period
Are there different archiving rules for different providers and institutions?	Royal Decree of 3 May 1999 on the general minimum conditions for medical records in the hospital + Art. 1, § 3 of the Royal Decree of 28 December 2006 establishing the minimum conditions for the nursing record + Article 46 of the Code of Professional Ethics, established by the Order of Physicians,	See the description supra
Is there an obligation to destroy (…) data at the end of the archiving	Art. 4 of the Belgian Privacy Act (Law of 8	There is no specific legal obligation to destroy EHRs or any other record when the mandatory storage period has expired. In addition the general

Questions	Legal reference	Detailed description
duration or in case of closure of the EHR?	December 1992 on the protection of private life with regard to the processing of personal data)	rules of the Belgian data protection legislation require 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?	n/a	No
Can health data be used for secondary purpose (e.g. epidemiological studies, national statistics...)?		Data in EHRs can be used for *secondary purposes* (e.g. research and quality control) in accordance with the general data protection rules. In general, data can be used for quality control, research and statistics without the patient's consent, provided there is compliance with the Belgian data protection law of 8 December 1992. In some situations, in particular in cases where the health-related data are not further processed in an anonymized form, an authorization from the Privacy Commission will be necessary. The authorizations for further processing of health-related data for research purposes are published on the website of the Privacy Commission (www.privacycommission.be)
Are there health data that cannot be used for secondary use?		No
Are there specific rules for the secondary use of health data (e.g. no name mentioned, certain health data that cannot be used)?	Royal Decree of 21 February 2001 implementing the Law of 8 December 1992 on the protection of private life with regard to the processing of personal data	In the framework of the secondary legislation implementing the Privacy Act Belgium has introduced a detailed regulatory framework with regard to the secondary use of personal data for scientific, statistical and historical purposes. The framework makes a distinction between three situations: a) secondary use of personal data in anonymised form, b) secondary use of personal data in pseudonymous form, and 3) use of personal data in idenfiable form. The Royal decree regulates the procedure for transforming personal data into pseudonymous form. In some cases this can only be done via an independent intermediary organisation. In the health sector the role of intermediary organisation in such case is taken up by the eHealth-platform as a service within its basic services package. If the secondary use of health data is not possible without the keeping the patients idenfiable, an

Questions	Legal reference	Detailed description
		authorization is needed from the Sector Committee for Social Security and Health. In any case such secondary use will only be possible after prior informed consent of the patient.
Does the law say who will be entitled to use and access this data?		See description supra
Is there an opt-in/opt-out system for the secondary uses of eHealth data included in EHRs?		See description supra

2.7. Requirements on interoperability of EHRs

2.7.1. Main findings

In Belgium there is no legally prescribed format or model for EHRs. The law only prescribes the minimal content. In practice the structure and the format varies considerably between healthcare institutions. One reason is that there are several providers of EHR systems. Many of these start from an "empty box" which is subsequently filled in according to the preferences of each healthcare institution. There are also considerable differences with regard to the volume. Some institutions use a hospital-wide EHR which includes also the obligatory nursing file and the pharmaceutical record. In other institutions however this is not the case and the nursing file or the pharmaceutical record are sometimes even still kept in paper format. Some specific services within hospitals – for example intensive care – have sometimes their own EHR.

The variety of EHRs is without any doubt still an obstacle for the interoperability between the different systems and it is a real challenge for the current hub- and metahubsystem rolled out at the federal level. These projects also encounter difficulties because EHRs often contain "free text" fields where information can be added without using standard coding such as ICD or ATC.

Since more than a decade Belgium progresses steadily toward a specific Belgian model for data sharing in the healthcare sector. In 2013 an agreement has been reached about the homologation of software applications for EHR used by physicians. The applications have to fulfil a series of criteria not only in the field of information security but also from the perspective of interoperability. In particular the applications should allow the extraction of a Summarized Electronic Health Record (SUMEHR). SUMEHR is a KMEHR message, used for the exchange of medical information. KMEHR (Kind Messages for Electronic Healthcare Record) is a proposed Belgian medical data standard introduced in 2002, designed to enable the exchange of structured clinical information. It is funded by the Belgian federal Ministry of public health and assessed in collaboration with Belgian industry.The initiative lead to the specification of about 20 specific XML messages (the Kind Messages for Electronic Healthcare Records - Belgian implementation standard or KMEHR-bis). The KMEHR standard consists of an XML(eXtensible Markup Language) message format defined by the KMEHR XML Schema and a set of reference tables. The folder itself gathers the information about a patient, where each folder identifies the patient and contains at least one medical transaction. The medical transaction item gathers the information reported by one healthcare professional at a given instance. Its attributes are type, author, date and time.

SUMEHR summarizes the minimal set of data that a physician needs in order to understand the medical status of the patient in a few minutes and to ensure the continuity of care. The SumEHR standard was introduced in 2005 and an EHR software package used by a physician (GP) should be capable of exporting a SumEHR message (KMEHR message level 4) for any given patient. This feature can be controlled by a validation tool available from the eHealth-platform. Currently more than 80% of all GPs across Belgium use certified EHR systems with this capability. For technical information about the SUMEHR the reader can best be referred to the KMEHR website held by the Federal Government Service of Public Health
(https://www.ehealth.fgov.be/standards/kmehr/content/page/home)

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 the eHealth-platform received a general competence to promote interoperability of EHRs in Belgium. Interoperability is also one of the main topics of the Belgian eHealth Roadmap 2013-2018.
Are there any specific rules/standards on the interoperability of EHR?		Belgium developed and uses a standard for the exchange of minimal medical transaction information, called SUMEHR.
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

Usually a distinction is made between prescriptions in an hospital context and prescriptions outside an hospital context (so-called "ambulant care"). For the hospital context the ePrescription system has been made possible by a Royal Decree of 7 June 2009. One of the main legal obstacles eliminated by this Royal Decree was the obligation – stated in the Royal Decree of 3 May 1999 on the general minimum requirements for medical records in hospitals – that a prescription should be *signed.* This signature has been replaced by a time stamping service provided by the eHealth-platform.

For the ambulant care context an ePrescription system is currently being rolled out (see http://www.recip-e.be). The exchange of e-prescriptions from the healthcare provider (GP, specialist, dentist, etc.) to the pharmacists or other provider of prescribed goods or services (physical therapist, etc.) is organised via the eHealth-platform. All electronic prescriptions are stored on the central Recip-e server (the physician creates the electronic prescription within the software application used for the administration of the medical practice and sends it in encrypted form via the eHealth-platform to the Recip-e server; the pharmacist or other provider of prescribed goods or services chosen by the patient gets access to the electronic prescription stored on the server).

Both ePrescription systems are designed for use within Belgium only, at least for the moment. The ePrescription system for the hospital context is however open enough to allow authentication by healthcare professionals without a Belgian e-ID (the hospitals are free to choose the authentication method: username and password, e-ID or other authentication means). The electronic prescriptions are stored by the hospital in a structured KMEHR format.

In the ambulant care context the Recip-e project presupposes that the healthcare provider is referenced in an authentic source in order to get access to the Recip-e server.

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 outside the hospital context ("Recip-E") is integrated in the software applications used by physicians to manage their electronic medical records. As already explained the nursing file and the medical file form, in many hospitals, together the patient record (but certain hospitals still keep an independent pharmaceutical file as part of their hospital pharmacy application). In most hospitals this patient record is kept in electronic form.
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 but in most hospitals it is integrated in the EHR. In the context of ambulant care the ePrescription functionality is integrated in the software application used by physicians to manage their electronic patient files.

- ***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?		As explained above, the ePrescription system can operate on its own but in most hospitals it is integrated in the EHR. In the context of ambulant care the ePrescription functionality is integrated in the software application used by physicians to manage their electronic patient files. As a consequence the healthcare provider who writes the prescription will normally also have access to the local EHR kept by her/him. On the other and a pharmacist who has access to the ePrescription on the Recip-e server will not have access to the EHR kept by the healthcare provider.
Can those health professionals write ePrescriptions without having access to EHRs?		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

Questions	Legal reference	Detailed description
		duty to write a prescription without prior consultation of the patient's health records. In practise, it is common that doctors and dentists write prescriptions 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 Belgium and for their cross-border transfer in the EU.

Various government and bottom-up initiatives in the area of EHR have been taken in the last 10 years, such as the FLOW initiative, the voluntary certification of EHR software applications or the development of a standardized patient summary (SUMEHR).

An important boost has occurred by the establishment of the *eHealth-platform* created by law in 2008. As a government institution the eHealth-platform has received large competencies and is mandated to "define ICT related useful functional and technical norms, standards, specifications and basic infrastructure required to support [the eHealth] vision and strategy". population register ("National Register") or the register of accredited healthcare professionals.

Generally speaking the Belgian landscape in the field of EHR starts to progressively be better embedded in the Belgian e-government model. This e-government model is characterized by five building blocks: the generalized use of the national unique identification number, the use of the electronic identity card as an authentication token, the use of validated authentic sources, the central role of service integrating bodies and the protection of privacy via specialized independent sector committees.

Since 2008 the eHealth-platform provides a series of so-called "basic services" which can be used by all actors in the healthcare sector and which can be integrated into the various – EHR and other - applications ("added-value services") offered by ICT-providers. Via the eHealth-platform these applications can also, under specific conditions and/or authorization, get access to so-called "validated authentic sources". These "authentic sources" are databases such as the National Register of physical persons residing in Belgium, the Register of accredited healthcare professionals, etc. In the context of EHRs the most relevant example of a basic service provided by the eHealth-platform is the "Reference Directory".

In recent years the eHealth-platform has succeeded in integrating additional databases and networks into its Reference Directory. One example is the *Vitalink* health vault of the Flanders Region where health-related data are shared between healthcare providers in areas which are regulated by this Region (for instance in the area of welfare and health prevention). Via the eHealth-platform a provider who has access to Vitalink can search if Vitalink contains information for a given patient. Another example of a system connected to the Reference Directory is the "pharmaceutical care data hub" which is used by the pharmacists to share their patient information.

The idea behind the Reference Directory is that it should be avoided to store health-related data on the central level of the eHealth-platform. Moreover it has been a solution to integrate to a maximum already existing initiatives in the area of shared EHRs (for example local hospital networks sharing patient data with the physicians in the region). As a consequence of the Reference Directory and of the fact that the data remain where they are generated, the healthcare providers remain responsible for the quality of the data being exchanged among healthcare professionals. Last but not least, the exchange of health-related data remains inside the hubs and data are not transferred via the the eHealth-platform.

Besides the Reference Directory the eHealth-platform provides series of other basic services, such as user and access management, time stamping, end-to-end encryption, logging, anonymization and a secured mailbox. All actors in the healthcare sector are free to use the services of the eHealth-platform when they develop or introduce a solution in the field of eHealth. This is a of course a step-by-step process.

In Flanders more and more healthcare institutions are setting up local or regional hubs. A Flemish Decree is currently under discussion in the Flemish Parliament which will create a general legal

obligation for healthcare providers to join a "network for sharing data between actors in healthcare". This network uses the basic services of the eHealth-platform. The draft decree also creates a Flemish "Agency for Cooperation in Data Sharing between Healthcare Actors".

In Wallonia the main initiative in this area is the "*Réseau Santé Wallon*" (RSW) which is a network created and managed by a non-profit association (FRATEM) in which major stakeholders in the healthcare sector are represented and that can be used by healthcare providers to securely share data. Contrary to the Flemish approach, participation in this network is entirely on a voluntary basis. The RSW functions as a "hub" in the framework of the Reference Directory held by the eHealth-platform. Part of the RSW is "Abrumet", a network for healthcare providers (physicians) in the Brussels Capital Region.

With the establishment of the eHealth-platform in 2008 the situation in the field of EHR becomes gradually more streamlined and there is a progressive evolution towards more and more health-related data sharing. In particular in Flanders such data sharing is conceived from a multidisciplinary perspective and no longer restricted to medical professionals.

Another positive evolution is the trend towards more bottom-up consensus-building on all levels. The eHealth-platform, although it has been created as a federal government body by the federal State, gradually moves to become a supra-federal body regulated and managed by the federal State and the regions together. Decision-making within the eHealth-platform is also more and more steered by consensus-building in an institutional framework with representatives of all relevant stakeholders.

On 20 December 2012, an « Action Plan 2013-2018 on eHealth » has been presented by a large and very representative group of stakeholders of the healthcare sector, with the overall objective of a widespread use of online health services around the patient for 2018. The plan is based on five pillars: (i) develop data exchange between caregivers on a common architecture; (ii) achieve a greater engagement and a better knowledge of e-Health by the patients; (iii) develop a terminology of reference; (iv) simplify and improve the efficiency of administrative tasks and; (v) establish a flexible and transparent governance structure in which all authorities and relevant stakeholders will be involved. The Action Plan 2013-2018 has been approved by the Interministerial Conference (ministers competent for health of the Federal State and the regions) on 28 January 2013 and published on a public website (http://www.rtreh.be/)