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 Spain

March 2014

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

This report was completed by Marta Ballesteros. 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 […]

The healthcare system in Spain is a Social Security Health system, decentralised to the 17 Autonomous Communities which have the competence to establish their own healthcare systems while the State has competence for the establishment of the bases and overall coordination of health issues. The public health system covers about 85% of the health services in Spain.

The efficiency of healthcare in such decentralised structure required the establishment of interoperable systems enabling to share data and to include all players into integrated national healthcare services.

For the development of a common EHR system, the Spanish system required an agreement between the State and the regions within the framework of the Inter-Territorial Council of the National Health System to define the scope of EHR (e.g. content, access by professionals and control of access by patients). Prior to 2007, each Autonomous Community had developed its own system which did not enable the exchange of information. EHR is currently used in 15 regions and covers the health data of almost 20 million patients, about 3 million professional consultations at an average of 30,000 patient consultations per month. This system allows Spain to actively participate in European projects, such as epSOS.

The legal framework for the development of EHRs is composed by several legal instruments prior to the Directive 2011/24/EU regulating the the autonomy of patients and their rights and obligations in relation to clinical information and documentation and the cohesion and quality of the NHS and the establishment of the health card. In 2010, the effort to promote harmonisation and interoperability led to the adoption of the legislation introducing minimum set of data for clinical reports and for the establishment of the National Interoperability Framework. Only in 2014, the Royal Decree establishing detailed rules to ensure cross-border healthcare complemented this legal framework.

2. Summary of legal requirements applying to EHRs

A short summary of the main the legal requirements applying to EHRs in Spain:

The Spanish decentralised structure led the Spanish authorities to identify already in 2002 the need to impose a minimum content for the clinical history to be used in all regional health systems. However, the Law 41/2002 on patient autonomy and rights does not require the clinical history to be necessarily in electronic format. The Royal Decree 1093/2010 introduces the requirement of a minimum set of data for several health reports composing the patient's clinical history and in particular the summary of clinical history which is the only health document obligatory in electronic format created automatically and updated from data introduced by health professionals. This instrument allows for the continuity of care in the different Autonomous Communities which, when using the same platform, would be able to share the electronic data included in the summary of clinical history of a patient affiliated to the National healthcare system between health professionals in one Autonomous Community with those in another region.

The Health Spanish system is based on a personal identification number for health purposes including eHealth purposes. The content of clinical reports and specifically the summary of clinical history refer to this number. All health cards have to incorporate a common set of basic data and will be linked to the **unique personal identification code** for every citizen in the National Health System. The basic data on the health card should therefore include the personal identification code assigned by the regional health administration issuing the card (CIP-AUT), the name of the card holder and the unique personal identification code of the National Health System (CIP-SNS). This card provides basic

information on the status of the patient within the NHS and therefore needs to be used with the identification document in order to allow opening access to the EHRs.

Law 41/2002 on autonomy of the patient imposes each centre to file/archive all patients' clinical histories, whatever format they are kept on, so that they guarantee the safety, correct storage and retrieval of information. The Health authorities are required to establish the mechanisms to ensure the authenticity of the content of the clinical history and the changes in it, as well as the possibility of future reproduction.

Royal Decree 4/2010 regulating the National Interoperability Framework requires the application of the National Security Framework rules to ensure the preservation of electronic documents. The information systems should be subject to regular audit at least every two years to verify compliance with the requirements of the National Security Scheme. The most important audit is carried out by the patient. The Spanish system provides the patient with information about the clinical history and about who has access to that data. The patient has therefore the possibility to react in case the information has been accessed by someone who should not have.

The Spanish legislation does not require explicit consent for the creation and setting up of the EHRs or for enabling access to it by health professionals or sharing it with health professionals in different regions or countries. The Spanish legislation regarding health data is based on the consideration that implicit consent is granted by the patient when requesting consultation by the doctor in care processes. The Spanish law includes an exemption to the requirement of consent for processing of data when done for prevention, medical diagnosis, health care, health treatment or the management of health services and carried out by a professional subject to professional secrecy or someone under an equivalent obligation. The requirement to provide information on the purpose or use of EHR is not explicitly considered under Spanish Law 41/2002.

The responsibility for the completion of the clinical history in relation to the direct patient care lies on the professionals involved in it. Health professionals have the duty to cooperate in **creating** and **maintaining** an orderly and sequential clinical documentation of patient care process. Furthermore, health professional have the duty to complete the protocols, reports, statistics and other documents for administrative assistance in relation to the clinical processes they are involved in.

The Spanish legislation recognises the patient's right to the health records, in writing or in the most appropriate support, while the creation and updating of the information is the health professionals' responsibility.

The patient has the right to access the documents in the clinical history and to obtain a copy of the data contained therein. The right of access to documents of the patient's medical history cannot be exercised to the prejudice of the right of the professionals participating in the creation and processing of the data who can oppose the reserve of their subjective annotations. The patient has the right to access but has to request it explicitly to receive the necessary electronic personal identification.

Health care professionals performing the diagnosis or treatment of the patient have direct and immediate access to the patient's clinical history which is the fundamental instrument for ensuring the proper health care. Access is limited to the purpose of health care. However those health professionals from other institutions or regional health services that those responsible for keeping the health records are requested to submit the request including an explicit justification based on health care purposes. The information systems should enable the identification of the health professional trying to have access to EHRs and should verify the authorisation.

The National Security Scheme rules require that each user (patient or health professional) with access right to the information system must be **uniquely identified** so that it is known at all times, who gets access rights and of what kind or who has performed a certain activity.

There is currently not such broad access to EHRs from health professionals from different regions or countries due to the different stages of development and the lack of interoperability of platforms to enable it. Spanish regions have followed uneven rhythms but at present, most Autonomous Communities have introduced the electronic or digital clinical history.

No medical liability is regulated in the Spanish system regarding specifically the use of EHRs. There is general liability within the framework of healthcare obligations.

There is no legislation about the periods for the archiving or maintenance of information in electronic or paper format. The general approach is that health information is kept to ensure the quality and continuity of treatment of the patient. The personal data should be deleted when it is no longer necessary or relevant for the purpose for which it was collected or recorded. However, according to the Law 41/2002 every health centre is required to keep clinical documentation under conditions which ensure its correct and safe maintenance ensuring the proper patient care during the appropriate time according to each case and at least **during five years** from the date of discharge of each care process. More detail information is provided at regional level. For example, Art 19 of RD 38/2012 of the Basque Country refers to the need for archiving the clinical information for a **minimum of 5 years** from the end of the care process.

There is no obligation in Spanish legislation to destroy health data. At a regional level more detail rules may be adopted. For example, Art 21 of RD 38/2012 of the Basque Country refers to the situations where it may be decided to destroy a document. Specifically 10 years after the death of a patient, the documents may be destroyed or any clinical history that has remained without any movement for more than 15 years. The same provision establishes the need for keeping back-up copies to ensure the conservation of the necessary information.

The key rules and standards on interoperability are mainly established under the Law 16/2003 on the cohesion and quality of the NHS and the Royal Decree 4/2010 regulating the National Interoperability Framework in the field of eGovernment. They are applicable to health data. The National Interoperability Framework includes the criteria and recommendations for the security, standardization and storage of information, formats and applications that should be taken into account by public authorities to ensure an adequate level of organizational, semantic and technical interoperability of the data, information and services managed in the exercise of its competences.

The Royal Decree 4/2010 establishes the criteria and specific principles necessary to enable and promote the development of the interoperability in public administrations which apply to health data. The National Interoperability Framework will be developed through technical rules that would be complied with by public authorities and will cover issues such as the catalogue of Standards, electronic document with the minimum required metadata, digitization of documents, electronic signature policy or certificate and requirements for connection to the communications network of the Spanish public administrations. Furthermore specific instruments for interoperability will be developed such as an inventory of administrative procedures and services, semantic interoperability Centre of public administrations and a directory for free reuse of applications.

The National Interoperability Framework should be kept updated permanently. The interoperability of the system is based on an Agreement between the State and 15 Autonomous Communities that are interested in sharing data on the electronic clinical history.

Art 10 of Royal Decree 38/2012 of the Basque Country requires the competent department in the field of health to define technical requirements to facilitate the interoperability of information systems in relation to clinical reports in order to ensure compatibility of the clinical history of the whole NHS and in accordance with the relevant agreements of the Inter-Territorial Council of the NHS.

According to the information received, the different Autonomous Communities are in different stages to issue data on EHRs to other health professionals in other regions or receive it from them. The most

advanced with the highest level of reports or information available to be shared with other Autonomous Communities and being able to receive or have access from other regions are La Rioja, Baleares Islands, Valencia and Extremadura. They are also part of epSOS. The Basque Country is the only region that cannot share any data in their EHRs system but may receive access from others.

3. Good practices

The Spanish health system and in particular the EHRs system is based on a harmonisation process that started due to the decentralised structure for Health measures.

The system is based on an interoperability system developed with the aim to integrate the electronic health systems of all Autonomous Communities. The system is still in development and currently 15 regions have accepted to be part of it but none have completed the process.

Spain includes the exception for processing of data when it is used for health purposes. It is understood that the patient in consultation gives the consent for the EHRs to be created and accessed by health professionals. The consent is considered implicitly given by the patient's request for doctor's consultation and for the whole care process, giving the right to the health professional to have access to the information even if the patient is not in consultation. Other health professionals may also have access without the need for explicit consent if they are authorised by the health centre or service. The consent is not required to be explicit or in writing. However the patient has access to information on the persons who have access to the EHRs enabling to act against that implicit consent.

Problems related to the interoperability, accessing and sharing health data with other regions or Member States even with similar security systems are a key challenge. However, the development of an interoperable system with the aim to integrate the electronic health systems of all Autonomous Communities could be considered an example of good practice in Spain. The system is still in development and currently 15 regions have accepted to be part of it.

4. Legal barriers

The insufficient institutional and regulatory frameworks as well as the reluctance of changing well-established practices and patient behaviours are the key challenges in Spain for the implementation of eHealth.

Regarding the creation, access to and update of EHRs, Spain has a barrier to overcome in relation to the behaviour and practice of health professionals regarding the use of personal electronic ID (already issued to most of the population) as secure identification for having access to EHRs.

The new Regulation on Data Protection may turn the Spanish system impossible unless an opt-out for health issues with strong security control systems is integrated. A future new law on electronic identification and digital signature is currently being developed to enable consent easier more easily technologically.

The technology behind the security measures and, in particular, the electronic certificates both for patients and health professionals is expensive. The economic investment required for ehealth is a barrier. An existing barrier in Spain is the lack of specific legislative and regulatory framework defining both: the liability and the archiving duration of EHRs.

The lack of common European Platform providing an agreed upon minimum content for the EHRs appears to be a barrier for progress on the exchange of information and data related to EHRs for cross border situations.

Contents

List of abbreviations

EHRs	Electronic Health Records
NHS	National Health System
CISNS	Inter-territorial Council of the National Health Service *Consejo Inter-territorial del Servicio Nacional de Salud*
INGESA	National Institute for Health Management *Instituto Nacional de Gestión Sanitaria*

1. General context

1.1. EHR systems in place

According to the Bloomberg's ranking on efficiency of health systems, the Spanish Health system is the first one in Europe and the fifth in the world after Hong Kong, Singapur, Japan and Israel.

The healthcare system in Spain is a Social Security Health system, decentralised to the 17 Autonomous Communities which have the competence to establish their own healthcare systems. The public health system covers about 85% of the health services in Spain. The Spanish Health system is organised on the basis of the recognition of the right to health to all citizens and residents in Spain, regardless of their economic and employment situation as established by Article 43 of the Spanish Constitution adopted in 1978 (CE 1978) and Article 1 and 10 of the General Health Law. It is therefore based on three key principles: universality, gratuity in access and public financing. It is a non-contributory tax-funded health system where the State is responsible for guaranteeing this right by providing health planning and resources from the central budget. The State and the Autonomous Communities sign agreements (*consorcios)* for the transfer of responsibilities and the financing of the Spanish health system. The role of the State is mainly to ensure coordination between the regions. The management of the health services has been transferred to the distinct autonomous communities of Spain, while some coordination tasks are operated by the Ministry of Health and Social Services and Equality (Ministry of Health)[1]. Within this framework, decisions related to the National Health Service need to be taken collectively by the State and the representatives of the Autonomous Communities through the Inter-territorial Council of the National Health Service (Consejo Inter-territorial del Servicio Nacional de Salud de España, CISNS) which ensures cohesion in the system and the respect of the right to health throughout Spain.

The efficiency of healthcare in such decentralised structure requires the establishment of interoperable systems enabling to share data and to include all players into integrated national healthcare services. While the Ministry of Health is the primary health policy decision making body establishing national standards, decisions within the CISNS aiming to ensure a consistent policy across regions must be adopted consensually. Therefore an organisational agreement was adopted between the State and the regions in 2005 that led to the set-up of three consecutive plans on the Quality of the National Health System from 2006 to 2016 and representing an investment of EUR 500 million in eHealth. While establishing an eHealth system for crossborder healthcare, Spain built on existing systems and information exchange channels between the regions.

The main eHealth projects in Spain relate to the unique identification system through the ecard, the unique eHealth records, the e-prescription.

The unique identification system is based on the principle that each citizen has one identification number and each individual health card is considered the ID document for the identification of every citizen in access and use of services in the NHS. In order to identify every citizen in a secure way, the law regulates that the Ministry of Health has to generate a unique personal identification code by developing a database to collect basic information about users of the NHS. The unique identification number is linked to a single data base linking the 17 existing identification systems. There is a specific ID assigned by each Autonomous Community and a personal identification code for the NHS which ensures the interoperability between the Autonomous Communities. All clinical information of patients is linked to this unique identification number. The identification code helps locating health information of a patient which may be dispersed into the national health system, so that it can be

[1] The Ministry of Health, Social Services and Equality replaced the Ministry of Health, Social Policies and Equality previously called Ministry of Health and Consumer Affairs, through Royal Decree 1823/2011 of 21 December restructuring the ministerial departments.

located and assessed by health professionals. The implementation of this identification system took almost 10 years and ended in 2011 and contains the protected records of 44 million people registered.

The e-card incorporates the personal identification codes and links it with the individual clinical history (EHRs) which should include the minimum data agreed by law and any other additional reports that each Autonomous Communities has decided or been able to upload. Each Autonomous Community has its own platform and not all are interoperable so that the clinical history can be seen in other Autonomous Communities. The objective of current project is to promote that the full EHRs can be seen in all Spanish regions.

For the development of a common EHR system, the Spanish system required an agreement between the State and the regions to define the scope of EHR (e.g. content, access by professionals and control of access by patients). Prior to 2007, each Autonomous Community had developed its own system which did not enable the exchange of information. The CISNS approved the Minimum Data Set for clinical reports to be collected in clinical documents needed to develop the digital records of the NHS. EHR is currently used in 15 regions and covers the health data of almost 20 million patients, about 3 million professional consultations at an average of 30,000 patient consultations per month. This system allows Spain to actively participate in European projects, such as epSOS.

Spain followed the same approach for e-prescriptions and an agreement between the State and the regions enabled the establishment of a system that ensured that almost all prescriptions were exchanged electronically and the tracing of the expenditure on medical products.

It is considered[2] that the use of electronic technology for the National Health System in Spain contributed to the sustainability of healthcare services with specific support in less developed regions. It has enabled the development of an integrated national healthcare system while respecting the autonomy of the regional systems. Future projects will focus on chronic and dependency patients' management and mobile applications.

In Spain, public health services are linked to primary healthcare. General Practitioners are the first point of contact and gatekeepers in the health system and solve more than 80% of the citizens' health problems. Most Spanish hospitals are publicly owned. They function with an extensive network of outpatient ambulatory centres. In those, members of specialist teams of clinical departments cover outpatient care in ambulatory centres on rotation[3].

The Spanish government has reduced the expenditure in the National Health system during the last two consecutive years, 2012 and 2013 by reducing the budget and the coverage for certain groups; Furthermore, some Autonomous Communities started the process to privatise the management of health centres and hospitals. For example, the Law on Fiscal and Administrative measures adopted by the Autonomous Community of Madrid aimed at enabling this process. However, the Superior Court of Justice of Madrid, adopted injunction measures of the decisions for the adjudication of the management of hospitals to certain private companies. Given the legal problems of these measures, the Government of Madrid announced end of January 2014 that the privatisation process was abandoned.

The primary health care network is public almost in its entirety and most of the GP are professionals belonging to the public sector. 40% of the hospitals (70% beds) in Spain belong to the National Health System; the remaining hospitals are private owned with a big percentage belonging to the network of hospitals of public use or providing services under public contract.

There are some examples of e-Hospitals that take the decision to develop EHRs as a management tool, such as the Spanish Marina Salud Hospital[4]. This hospital is funded through a public and private

[2] Mr Muñoz Montalvo, General Adjoin vice-director, Information Technology, Ministry of Health in Spain.
[3] Country fiche Spain, eHealth Strategies, 2010
[4] Dr Vincent MONCHO MAS

investment partnership (PPIP) where the private entity is in charge to provide public services (e.g. healthcare services) with the condition that the costs of such services are co-financed by the private entity and the state. The Hospital uses new information communication technologies, increasing the efficiency of the hospital (i.e. clinical processes easier and faster, improved quality of care and patient safety). To this end, all paper-based clinical data have been transferred into Electronic Health Records (EHR) at the Marina Salud Hospital. The concept of EHR refers to the digitalised health information of patients, including e.g. the medical history, laboratory test results, clinical images of patients. However, this hospital is in one of the two Autonomous Communities that are not linked to the Spanish system for integration of all EHRs.

1.2. Institutional setting

The Spanish Constitution adopted in 1978 recognises the right to health and charges public authorities to safeguard public health by taking the necessary preventive measures and providing the necessary services (art 43 CE 1978). Rights and obligations related to health are established by law.

The State has exclusive competence (Article 149 CE 1978) over international health issues, the establishment of the bases and overall coordination of health and the adoption of pharmaceutical legislation. The Autonomous Communities in Spain have competence on policies determined by the Constitution and not specifically reserved to the State. The Constitution allows CCAA to take on competences in the field of Health issues (Article 148.21 CE 1978).

Under Article 40 of the General Health Law 14/1986 of 25 April, the State's competence on Health includes the establishment of health information systems (no. 13) and development of statistics and the setting up of systems for ensuring exchange of information and coordination between the State health administration and the Autonomous Communities (no 16). The general health coordination (*Coordinación General Sanitaria*) covers[5] the establishment of general minimum common criteria for evaluating resource needs including services and for assessing the efficiency and performance of health programmes and services as well as the definition of common objectives and priorities to achieve a coherent health system.

Within its competences, the State is responsible for approving annual or multi-annual health plans and may conclude joint health plans with Autonomous Communities within the framework of the **Inter-Territorial Council of the National Health System**[6] (Consejo Inter-territorial del Sistema Nacional de Salud, CISNS) composed of the Minister of Health and the competent councillors of the Autonomous Communities.

Specifically the **Ministry of Health** (*Ministerio de Sanidad, Servicios Sociales e Igualdad- Secretaria General de Sanidad y Consumo)* is competent for establishing a **health information system** which allows the availability and exchange of information among healthcare authorities. Within the Ministy of Health, the **Health Information Institute** (*Instituto de Información Sanitaria*) is responsible for the functioning of the health information system[7], and ensuring its integrity, security and the confidentiality of personal data[8]. It is responsible for ensuring exchange of information regarding unique personal identification codes, health records and e-prescriptions[9] and the interoperability and data flow between regions and through the Health intranet and the day-to-day running of the infrastructure. It also hosts the national information nod. However, the objectives and content of the relevant information is to be agreed within the CISNS. **The National Institute for Health Management** (*Instituto Nacional de Gestion Sanitaria*) coordinates all autonomous regions.

[5] Art. 70(2), General Health Law.
[6] Art. 53(1), Ley 16/2003. Minimum content requirements are set out in the remainder of that article.
[7] Art. 58, Ley 16/2003.
[8] Art. 58(4), Ley 16/2003.
[9] Art. 54, Ley 16/2003.

The requirements and standards for the implementation of the **personal health card** (*tarjeta sanitaria individual*)[10] and for putting in place the **database** for the creation of personal unique identification codes[11] are established by the Ministry in cooperation with Autonomous Communities and other competent authorities. The State exercises a High Inspection (*Alta Inspección*) role to verify and guarantee the exercise of State and Autonomous Communities' competences in relation to healthcare. In particular, the High Inspection oversees the correspondence of Autonomous Communities' health plans with the general objectives established by the State[12], in cooperation with the inspection services of the Autonomous Communities[13].

Finally the monitoring and control of the National Health System is carried out by the **Observatory on the National Health System** (*Observatorio del Sistema Nacional de Salud*) dependent of the Ministry of Health.

1.3. Legal setting and future legal development

The legal framework for the implementation of eHealth policies is the following:

- **Law 14/1986** of 25/04/86 adopting the **Health Act** (***Ley General de Sanidad***)[14] recognises the patient's rights to information and to confidentiality and the State's responsibility to set up a health information system ensuring exchange of information between the State and the Autonomous Communities.
- Directive 95/46/EC on data protection was transposed by **Royal Decree No 156/1996 of 02/02/1996**[15], which however only designated the national data protection authority to represent Spain in the Working Group on the Protection of Individuals created by Art. 29 of the Directive.
  Organic Law 15/1999 of 13 December 1999[16] on personal data protection
  Ley Orgánica 15/1999 de 13 diciembre de 1999, de Protección de Datos de Carácter Personal
  It establishes the legal framework for data protection in Spain. This Act is further developed by:
  Royal Decree 1720/2007 of 21 December 2007 approving the Regulation implementing the Organic Law 15/1999 on personal data protection[17]
  Real Decreto 1720/2007*, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999 de 13 de diciembre, de protección de datos de carácter personal*.
- **Law 41/2002** of 14 November regulating the autonomy of patients and their rights and obligations in relation to clinical information and documentation.
  Ley 41/2002, de 14 Noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.
- Law 16/2003 of 28/05/03 on the cohesion and quality of the National Health Service
  Ley 16/2003 of 28/05/03 de cohesión y calidad del Sistema Nacional de Salud.
  It provides for establishment of a National Health communication network by the Health Ministry. The network is intended to enable the members of the National Health Service to safely exchange information, including clinical information, sanitary registers and e-prescriptions. However, the implementation is not yet complete and Real Decreto-ley 9/2011 requires the full roll out of the network by 1 January 2013. Article 57(4) of Law 16/2003 establishes the **personal health card** that enables the electronic processing of clinical information and access to it by duly authorised professionals.
- Law 44/2003 of 21 November on the organisation of sanitary professions.
  Ley 44/2003 de 21 de Noviembre de ordenación de las profesiones sanitarias.
- Royal Decree 183/2004 regulating the **health card** as amended by Royal Decree 702/2013 of 20 September.

[10] Art. 57(2), Ley 16/2003.
[11] Art. 57(3), Ley 16/2003.
[12] Art. 76(1)-(2), Ley 16/2003.
[13] Art. 79, Ley 16/2003.
[14] http://www.boe.es/buscar/doc.php?id=BOE-A-1986-10499
[15] http://www.boe.es/buscar/doc.php?id=BOE-A-1996-2991
[16] http://www.boe.es/diario_boe/txt.php?id=BOE-A-1999-23750
[17] http://www.boe.es/buscar/doc.php?id=BOE-A-2008-979

*Real Decreto 183/2004 por el que se regula la **tarjeta sanitaria** modificado por el Real Decreto 702/2013 de 20 de Septiembre*.

- Law 11/2007 of 22 June, on citizens' electronic access to public services.
  Ley 11/2007 de 22 junio, de acceso electrónico de los ciudadanos a los servicios públicos.
- Royal Decree 1093/2010 of 3 September 2010 approving the minimum set of data for clinical reports in the National Health Service
  Real Decreto 1093/2010 de 3 de septiembre, por el que se aprueba el conjunto mínimo de datos de los informes clínicos en el Sistema Nacional de Salud.
  It introduces the concept of a **summary clinical history** which must be maintained in electronic form as key part of the HER in Spain. It aims at harmonising the minimum content of different clinical documents that had been developed by the Autonomous Communities under Law 41/2002, in order to allow their use across all the members of the National Health Service.
- Royal Decree 1718/2010 of 17 December 2010 on prescriptions and dispensing orders.
  Real Decreto 1718/2010 sobre receta médica y órdenes de dispensación.
  While it states that private and public prescriptions may be on paper or in electronic form, it dedicates a chapter to e-prescriptions. Real Decreto-ley 9/2011 gives a mandate for the implementation of e-prescription by 1 January 2013, suggesting that – even though foreseen by the law – e-prescription may not have been fully implemented yet.
- Royal Decree 4/2010, of 8 of January, regulating the National Interoperability Framework in the field of eGovernment.
  Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- Real Decreto-ley 9/2011 of 19 August 2011 on measures to improve the quality and cohesion of the national health system, contributing to fiscal consolidation, and raising the maximum amount of State guarantees for 2011.
  Real Decreto-ley 9/2011 de 19 de Agosto, de medidas para la mejora de la calidad y cohesión del Sistema nacional de salud, de contribución a la consolidación fiscal, y de elevación del importe máximo de los avales del Estado para 2011.
- Real Decreto 81/2014 of 7 February 2014 establishing detailed rules to ensure cross-border healthcare and amending Royal Decree 1718 of 17 December on prescription and dispensing orders. It transposes Directive 2011/24/EU on the application of patients' rights in cross-border healthcare.
  Real Decreto 81/2014, de 7 de febrero, por el que se establecen normas para garantizar la asistencia sanitaria transfronteriza, y por el que se modifica el Real Decreto 1718/2010, de 17 de diciembre, sobre receta médica y órdenes de dispensación
- The Royal Decree-Law 16/2012 on urgent measures to ensure the sustainability of the health system and to improve the quality and safety of its performance introduced on 20 April 2012 the State Registry for Health Professionals as well as severe cuts in the Spanish National Health System[18].
  Real Decreto-ley 16/2012 de medidas urgentes para garantizar la sostenibilidad del Sistema de Salud y mejorar la calidad y seguridad de sus prestaciones.

[18] http://boe.es/buscar/doc.php?id=BOE-A-2012-5403

2. Legal requirements applying to EHRs in Spain

2.1. Health data to be included in EHRs

2.1.1. Main findings

As stated in the introduction to the Spanish health system, the decentralised structure and system of competences in Spain required the development of mechanisms to ensure coordination amongst regions. Within this framework, the Spanish authorities identified already in 2002 the need to impose a minimum content for the clinical history to be used in all regional health systems. However, the Law 41/2002 on patient autonomy and rights does not require the clinical history to be necessarily in electronic format.

Later on, the Royal Decree 1093/2010 introduces the requirement of a minimum set of data for several health reports composing the patients clinical history and in particular the **summary of clinical history** which is the only health report that is required to be in electronic format and is created automatically and updated from data introduced by health professionals. This instrument allows for the continuity of care in the different Autonomous Communities which, when using the same platform, will be able to share the minimum content of health reports including the summary of clinical history of a patient affiliated to the National healthcare system between health professionals in one Autonomous Community with those in another Autonomous Community. The minimum content of the summary clinical history includes an administrative part that covers the data on the institution emitting the document, data on the patient, including the Code NHS and European[19] or the clinical history number and address and, on the other side, the health data including the data in the protocol of clinical investigation, resolved, closed or inactive problems, problems and active episodes, treatment, nurses diagnostics, nursing results and interventions or subjective observations of professional staff.

The Royal Decree also harmonises the minima data categories that must be included in EHRs and the type of reports that may be developed and included in the EHRs. It sets specific data categories for the clinical report of discharge, outpatient clinical report, emergency clinical report, primary care clinical report, report of results of laboratory tests, report of results of image tests, report of nursing care. The minimum data required under the Royal Decree 1093/2010 does not prevent Autonomous Communities to develop other types of categories of data to be included in EHRs or provide access to the reports other than the minimum data under the summary clinical history.

In practice, the Autonomous Communities decide what should be the content of the Electronic Health Records (or electronic clinical history) that would be made accessible to health professionals and patients according to their resources. Some may decide to limit the information to the minimum content and the summary the clinical history and others to include additional reports as described above. Each regional health service developed a different system/platform for collecting and managing individual health data. However, citizens' mobility requires all Autonomous Communities to share at least the administrative data comprising the identification data provided by the General Administration and the regional authorities included in the individual ehealth card as well as the minimum content for clinical history of individual health records to be accessed by the health professionals in the regions.

The Health Spanish system is based on a personal identification number for health purposes including eHealth purposes. The content of clinical reports and specifically the summary of clinical history (basic eHealth document) refer to this number. All health cards have to incorporate a common set of basic data and will be linked to the **unique personal identification code** for every citizen in the National Health System. This harmonisation aims to provide standard data for each person regardless of the health administration that issues the card. The basic data on the health card should therefore

[19] This category was created in case of adoption of a European Code for the identification of patients.

include the personal identification code assigned by the regional health administration issuing the card (CIP-AUT), the name of the card holder and the unique personal identification code of the National Health System (CIP-SNS). This card provides basic information on the status of the patient within the NHS and therefore needs to be used with the identification document in order to allow opening access to the EHRs.

The ehealth card incorporates the personal identification codes and links it with the individual clinical history (EHRs) which should include the minimum data agreed and required under the Royal Decree 1093/2010 and any other additional reports that each Autonomous Communities might have decided or been able to upload. Each Autonomous Community had its own platform and not all of them are interoperable so that patients' clinical history can be seen in other Autonomous Communities. There is currently an initiative to harmonise all platforms and promote that the full EHRs can be shared and accessed by professionals in all Spanish regions.

Art 57(3) of Law 16/2003 requires the Ministry of Health, in order to generate the unique personal identification code, to develop a database collecting basic information about the users of the National Health System. This service enabled the emission of individual health cards for all users of the NHS. The citizens' access to health care services offered by the NHS is provided through this individual health card as an administrative document that certifies certain information from the holder (Article 57(1)). The Ministry of Health, in collaboration with the Autonomous Communities and other competent public authorities, established the requirements, content and the necessary standards that the health card should incorporate to store basic information. The applications that deal with that information should allow reading and verification of data in the whole territory of the State and it is now up and running. It should comply with the requirements in Annex to the Royal Decree 1093/2010.

In support of that system, Art 54 of Law 16/2003 requires the Ministry of Health to establish a **secure communications network** guaranteeing protection in the exchange of information on health issues. Through that network, information on the national identification number, clinical information and sanitary registers will be exchanged. Article 53(6) purports that the transfer of the data, including information necessary for the health information system, is subject to the legislation on protection of personal data and to the conditions agreed by the Inter-Territorial Committee of the National Health System. Art 56 specifies that any transfer or exchange of information should comply with the LO 15/1999 on data protection and Law 14/2002 on patients' and obligations regarding clinical information and documentation. Additional security requirements are presented in other sections of this report and include those developed within the framework of the **National Security Scheme**.

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?)		The EHRs in Spain refer to the whole clinical history related to a patient. While the definition does not require the clinical history to be of electronic character, it covers those in digital format. The minimum content for the clinical history was established by law 41/2002.
	Art 15 L 41/2002	The minimum content of the clinical history is: a) The documentation of the clínicoestadística sheet. b) The entry clearance. c) The urgency report. d) The history and physical examination. e) Evolution. f) The medical orders. g) The interconsultation sheet. h) Reports of additional examinations. i) Informed consent. j) The report of anaesthesia. k) The report record of operating room or delivery. l) The pathology report. m) The development and planning of nursing care. n) The therapeutic application of nursing. o) The graph of constants. o) The clinical report of discharge The only definition of health records in electronic format in Spanish legislation is related to the summary clinical history.
	Article 3 read in conjunction with Annex VIII to RD 1093/2010	The Royal Decree 1093/2010 requires a minimum set of data for the **summary of clinical history** that is **an electronic document** created automatically and updated from data introduced by health professionals. A minimum set of data is required for other clinical documents that could be in electronic form. **The summary of clinical history** should contain: The type of document and date of creation or update; Data on the Institution emitting the document: name and logo; Data on the patient including name, date of birth, sex, DNI, Code NHS and European, Clinical history number and address; Health Data including: Information reserved due to patient decision, existence of document with preliminary instructions, Data included in the protocol of clinical investigation Allergies, vaccinations, Resolved, closed or inactive problems, problems and active episodes;

Questions	Legal reference	Detailed description
		Treatment, Active Nurses diagnostics, nursing results, nursing interventions, alerts, subjective observations of professional staff. The Royal Decree also harmonises the minima data categories that must be included in health records on all support (i.e. paper and electronic). It sets specific data categories for: - Clinical report of discharge, detailed in Annex I of RD 1093/2010 - Outpatient clinical report, detailed in Annex II to RD 1093/2010 - Emergency clinical report, detailed in Annex III to RD 1093/2010 - Primary care clinical report, detailed in Annex IV to RD 1093/2010. - Report of results of laboratory tests, detailed in Annex V to RD 1093/2010. - Report of results of image tests, detailed in Annex VI to RD 1093/2010. - Report of nursing care, detailed in Annex VII to RD 1093/2010.
	In practice	The Autonomous Communities decide what should be the content of the Electronic Health Records (or electronic clinical history) that are accessible to health professionals and patients according to their resources. Some may decide to limit the information to the minimum content and the summary the clinical history and others to include additional reports. Each regional health service developed a system for collecting and managing individual health data. However, citizens' mobility requires all Autonomous Communities to share at least the administrative data and identification data provided by the General Administration, the individual ehealth card and the minimum content of individual electronic health records to be accessed by the health professionals in the regions.
Are these data restricted to purely medical information (e.g. physical or mental health, well-being)?	Art 3 and Annex IV of RD 1093/2010	Social and professional information in addition to the occupational or unemployment situation are required in the primary care clinical report which may be in electronic form. However it is not required in the summary clinical history (EHR). Primary care clinical report, detailed in Annex IV to RD 1093/2010 should include:. • The type of document; • Data on the Institution emitting the document including the address; • Data on the patient including name, date of birth, sex, DNI, Code NHS and European, Clinical history number and address; • Health Data including: Records, family hereditary diseases, Neonatal, Obstetric and Surgical records, allergies, toxic substances abuse, preventive actions, premedication, occupational situation, social and professional records, summary of results of tests, evolution and comments, diagnostics, procedures and treatment.
Is there a definition of EHR or patient's summary provided in the national legislation?	Art 3 RD 1093/2010	The **summary clinical history** is an electronic document, automatically generated and fed in and updated on the basis of data that healthcare professionals include in the full clinical history of the patient. This RD does not affect clinical documents created before the entry into force on 04/09/2010. Apart from the definition of the summary clinical history, the Spanish legislation provides

Questions	Legal reference	Detailed description
		general definition of EHRs:
	Art 3 L41/2002	**Clinical documentation**: the support of any type that contains a set of data and information related to health care. **Clinical history**: the set of documents containing data, assessments and information of any kind about the situation and the clinical evolution of a patient throughout the care process.
	Art 3(14) RD 81/2014	Under the RD 81/2014 **Clinical history or medical medical records** is defined as all documents, regardless of format, that contains the data, assessments and information of any kind about the situation and the clinical course of a patient throughout the care process. It is governed by the provisions of Law 41/2002.
	Art 3 and 4 RD 38/2012 Basque Country.	Other examples of the understanding of the (electronic) clinical history regionally are: The clinical history or medical record has to be unique for each patient, at least in each health centre or institution and should include all the documentation relevant to the patient identified through a unique number, exclusive to the person which would allow access to the records. The clinical history may be in any support but preferably in **electronic support** provided that the integrity, security and conservation are guaranteed.
	Art 14(1) L41/2002	This provision further defines each **patient's clinical history** as the set of documents related to the patient's care processes which include identification of the doctors and other professionals involved, in order to obtain the maximum integration of clinical documentation of each patient, at least within each centre.
	Art 3 L41/2002	**Clinical information**: any data, whatever its form, class or type, which allows to acquire or extend knowledge about a person's fitness and health, or how to preserve, care for, improve or recover it.
Are there any requirements on the content of EHRs (e.g. detailed requirements on specific health data or general reference to health data)?	Art 3 and Annexes to RD 1093/2010 In practice[20]	Spain sets very detailed requirement on the categories of health data that must be included in EHRs (see above) The e-card incorporates the personal identification codes and links it with the individual clinical history (EHRs) which should include the minimum data agreed and required under the Royal Decree 1093/2010 (and Royal Decree 81/2014 for prescriptions). These are the requirements on the content of EHRs. However, each Autonomous Communities may decide to include any other additional reports as part of the EHRs and to be shared with professionals in other regions. Each Autonomous Community had its own platform and not all of them were interoperable so that patients' clinical history could be seen in other Autonomous Communities. The

[20] Maravillas Izquierdo, Vice-Secretary General, Basic NHS Service Portfolio, Ministry of Health, Social Services and Equality. Interview 1st April 2014.

Questions	Legal reference	Detailed description
		objective of the current project/initiative is to promote that the full EHRs can be shared and accessed by professionals in all Spanish regions
Are there any specific rules on the use of a common terminology or coding system to identify diseases, disorders, symptoms and others?	RD 1093/2010	Coding system included in the **Summary of clinical history** • The data from the emitting institution are based on specific coding/terminology related to the regional Health services, including a reference to the National Hospitals Catalogue and to the Register of Health Establishments, Centres and Services of the Ministry of Health. • Data on the patient regarding personal information or the patient's Clinical History Number refer to the data in the e-card data base. • Information on active problems or episodes include a reference to the International Classification for primary care and the International Classification of diseases and to the Systematized Nomenclature of Medicine-Clinical Terms. • Data on the Treatment with pharmaceutical products refers to the official nomenclature accepted by the Ministry of Health and related to the Systematized Nomenclature of Medicine-Clinical Terms. • The data on Active Nurses diagnostics refers to the coding system NANDA (North American Nursing Diagnosis Association) • The data on nursing results refers to the coding system NOC (Nursing Outcomes Classification) • The data on nursing interventions refers to the coding system NIC (Nursing Interventions Classification). Other coding systems referred to in the data related to other clinical documents that may be in electronic format are: • Data on the document includes information on the service and refers to the Register of discharges of general hospitals of the NHS. • Data on the patient refer to data in the e-card data base. • Some data on the care process is based on a coding system such as: Data on the reason for admission at the hospital, data on principal diagnosis or other diagnostic refer to International Classification of Diseases, Systematized Nomenclature of Medicine-Clinical Terms and the pharmaceutical products used for treatment relates to the Nomenclature from the Ministry of Health and the Systematized Nomenclature of Medicine-Clinical Terms. • Health data related to episodes treated, active problems or episodes including a reference to the International Classification for primary care, • Diagnosis or procedures, pharmaceutical products, results from nursing tests or interventions are based on coding system.
Are EHRs divided into separate categories of health data with different levels of confidentiality (e.g. data related to blood type		The EHRs are divided into categories of data, separating administrative data from health data. Personal data appears separated from the institution data and the health data.

Questions	Legal reference	Detailed description
is less confidential than data related to sexual diseases)?		
Are there any specific rules on identification of patients in EHRs?		See above on minimum content of clinical documents.
Is there is a specific identification number for eHealth purposes?		The Health Spanish system is based on a personal identification number for health purposes including eHealth purposes. The content of clinical reports and specifically the summary of clinical history (basic eHealth document) refer to this number.
	57(3) of Law 16/2003	Art 57(3) of Law 16/2003 requires the Ministry of Health, in order to generate the unique personal identification code, to develop a database collecting basic information about the users of the National Health System. This service should enable the emission of individual health cards. The citizens' access to health care services offered by the NHS is provided through this individual health card as an administrative document that certifies certain information from the holder (Article 57(1)). The Ministry of Health, in collaboration with the Autonomous Communities and other competent public authorities, should establish the requirements and the necessary standards for the health card.
	54 of Law 16/2003	Art 54 of Law 16/2003 requires the Ministry of Health to establish a **secure communications network** guaranteeing protection in the exchange of information on health issues. Through that network, information on the national identification number, clinical information and sanitary registers will be exchanged.
	54 of Law 16/2003	Article 53(6) purports that the transfer of the data, including those necessary for the health information system, is subject to the legislation on protection of personal data and to the conditions agreed by the Inter-Territorial Committee of the National Health System.
	56 of Law 16/2003	Art 56 specifies that any transfer or exchange of information should comply with the LO 15/1999 on data protection and Law 14/2002 on patients' and obligations regarding clinical information and documentation.
	Art 3(1) and (2) Royal Decree 183/2004 as modified by Royal Decree 702/2013	All health cards have to incorporate a common set of basic data and will be linked to the **unique personal identification code** for every citizen in the National Health System. This harmonisation aims to provide standard data for each person regardless of the health administration issuing the card. The basic data on the health card should therefore include the personal identification code assigned by the regional health administration issuing the card (CIP-AUT), the name of the card holder and the unique personal identification code of the National Health System (CIP-SNS).
	Art 3(5) Royal Decree 183/2004	The Ministry of Health, in agreement with the regions and other relevant public authorities is to establish the requirements and the standards that cards should incorporate to store basic information, and the applications that deal with that information should allow reading and verification of data in the whole territory of the State. It should comply with the requirements in Annex to the Royal Decree.

Questions	Legal reference	Detailed description
	In practice[21]	This card provides basic information on the administrative status of the patient within the NHS and therefore needs to be used with the identification document in order to allow opening access to the EHRs.

[21] Interview 16.04.2014, Arturo Romero Gutiérrez, Director Project HCDSNS, Vice-direction general for Health Information and Innovation, Ministry of Health

2.2. Requirements on the institution hosting EHRs data

2.2.1. Main findings

Health centres are required to take appropriate measures to ensure the patients' rights to confidentiality of data related to health (including the need for prior authorisation/consent to access it), and to develop, where appropriate, the rules and protocoled procedures to ensure legal access to patient data.

Law 41/2002 on autonomy of the patient imposes each centre to file/archive all patients' clinical histories, whatever format they are kept on, so that they guarantee the safety, correct storage and retrieval of information. The Health authorities are required to establish the mechanisms to ensure the authenticity of the content of the clinical history and the changes in it, as well as the possibility of future reproduction. However, it is up to the Autonomous Communities to adopt the necessary measures to ensure that health centres can take the appropriate technical and organisational measures to archive and protect medical records and prevent their destruction or accidental loss.

The Law 41/2002 states that the legislation governing the hosting and management of files containing personal data, such as the Law 15/1999 on Protection of Personal Data, is applicable to patient's clinical history. Institutions hosting and managing patient's clinical history are bound by the legislation governing the hosting and management of files containing personal data, such as the Law 15/1999 on Protection of Personal Data.

Healthcare facilities are required to keep clinical documentation under conditions which ensure its correct and safe maintenance, even if not in the original support. The management of clinical documentation should ensure the proper patient's care during the appropriate time according to each case and at least during five years from the date of discharge of each care process.

Within the institutions, the health professionals have the duty to cooperate in creating and maintaining an orderly and sequential clinical documentation of the patient care process. Health professionals who develop their activity individually are responsible for the management and custody of healthcare documentation generated.

The management of clinical history is prescribed to be carried out by the admissions and documentation unit in those Healthcare centres that have in-patients or those which attend a sufficient number of patients in any other healthcare modality. The unit will be held responsible for integrating into a single archive all clinical histories. Responsibility for keeping these clinical histories lies on the Management of the Health centre.

Royal Decree 4/2010 regulating the National Interoperability Framework requires the application of the National Security Scheme rules to ensure the preservation of electronic documents and imposes minimum security requirements and security measures appropriate to the means the documents are stored in. All governing bodies of public administration (who are directly responsible for implementing the action of the government at central, regional or local level in a specific sector of activity) must formally have its security policy following the minimum security requirements as listed under Art 11 Royal Decree 3/2010. The minimum security requirements under National Security Scheme rules entail different headings including the management of staff which require that in order to ensure accountability and control of the access to EHRs, each user with access right to the information system must be uniquely identified so that it is known at all times, who gets access rights and of what kind or who has performed a certain activity. Art 11 (4) of the Royal Decree 38/2012 of the Basque Country requires each health institution or health service to establish the necessary mechanisms for access to medical records, and in particular, methods that allow access at all times to the clinical history of each patient by the professionals.

Art 22 (4) of Royal Decree 3/2010 requires public administrations to have a policy of electronic signature and certificates in order to guarantee the electronic signature on the preservation of electronic document. The policy of electronic signature and certificates develops the processes for the generation, validation and maintenance of electronic signatures, and the characteristics and requirements applicable to electronic signature systems.

Under Law 41/2002, healthcare centres are required to establish a mechanism for active and diligent custody of clinic history. The custody should allow the collection, integration, retrieval and communication of information subject to the principle of confidentiality. This obligation is recognised as a right of the patient to it.

The RD 1277/2003 establishes the basis for the authorisation procedure of Health Centres and Services by the Autonomous Communities and the Catalogue and Registry of Health Centres and Services. The Autonomous Communities have the competence to issue an administrative decision authorising the establishment, functioning and modification of the Health Centres enabling them to exercise their activity. Those decisions are collected in the State Registry of Health Centres and Services.

To comply with the minimum requirements established in this Royal Decree, public administrations are required to apply the security measures listed in Annex II which includes, inter alia, the hosting or processing of encrypted information. However, the relevant Spanish legislation, e.g. Royal Decree 3/2010 or the Royal Decree 81/2014, does not require explicitly in the body of the text the information to be encrypted as there are different security options and the legislation refers to security systems rather than a specific one such as encrypting the information.

The Spanish system has several mechanisms to ensure control and accountability. The Autonomous Communities have the responsibility to ensure the quality of services, according to the provisions in Chapter VI of the Cohesion and quality of the NHS Act. To do this, they can conduct independent audits. Information systems and facilities for the treatment and storage of data are to be submitted at least every two years to an internal or external audit to verify compliance with the data protection rules under the Regulation implementing the OL15/1999.

Under Royal decree 3/2010 the security of the systems should be subject to maintenance, review and audit by qualified, dedicated and trained professional in all phases of its life cycle: installation, maintenance, incident management and decommissioning. The information systems should be subject to regular audit at least every two years to verify compliance with the requirements of the National Security Scheme. The audit report shall assess the degree of compliance with the Royal Decree, identify gaps and suggest possible corrective or complementary measures and recommendations deemed appropriate. It shall likewise include the methodological audit criteria used, the scope and purpose of the audit, and data, facts and observations on which the conclusions are based

In practice, the Ministry of Health is subject to an audit twice a year, one external and another one internal, within the frame of the ISO 27001 certification it was awarded. The audit focuses on the management of the systems in place to ensure the integrated service and the coordination. However the Ministry does not have access to any health information, but it has developed a reference index to keep track of where the information is.

The most important audit is carried out by the patient. The Spanish system provides the patient with information about the clinical history and about who has access to that data. The patient has therefore the possibility to react in case the information has been accessed by someone who should not have.

Further to the independent audits, the Observatory of the National Health System is an agency of the Ministry of Health that provides an ongoing analysis of the National Health System as a whole, by comparing the health services of the Autonomous Communities regarding their organisation, provision of services, health management and results. In addition, the State shall exercise the High Inspectorate

as a guarantee and verification of compliance of state and the autonomous communities' competences in health and health care in the National Health System, in accordance with the provisions of the Constitution, the statutes of autonomy and laws. It will be in charge of evaluating compliance with common goals and objectives and identify difficulties, generic or structural deficiencies that impair or distort the functioning of a coherent, harmonious and united healthcare system. The Officials of the Central Government exercising this role shall have the authority for those purposes and may request the necessary collaboration by other public authorities for the performance of the functions they are legally mandated. The Inspectorate will create and maintain a shared database with the inspection services of the NHS.

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 7(2) L41/2002	Health centres are required to take appropriate measures to ensure the patients' rights to confidentiality of data related to health (including the need for prior authorisation/consent to access it), and to develop, where appropriate, the rules and protocoled procedures to ensure legal access to patient data.
	Art 14(2) L41/2002	Imposes each centre to file/archive all patients' clinical histories, whatever format they are kept on, so that they guarantee the safety, correct storage and retrieval of information. The Health authorities are required to establish the mechanisms to ensure the authenticity of the content of the clinical history and the changes in it, as well as the possibility of future reproduction. However, it is up to the Autonomous Communities to adopt the necessary measures to ensure that health centres can take the appropriate technical and organisational measures to archive and protect medical records and prevent their destruction or accidental loss.
	Art 17 Law 41/2002	The Law 41/2002 states that the legislation governing the hosting and management of files containing personal data, such as the Law 15/1999 on Protection of Personal Data, is applicable to patient's clinical history.
Is there a need for a specific authorisation or licence to host and process data from EHRs?	Art 19 Law 41/2002	Healthcare centres are required to establish a mechanism for active and diligent custody of clinic history. The custody should allow the collection, integration, retrieval and communication of information subject to the principle of confidentiality. This obligation is recognised as a right of the patient to it.
	Royal Decree 1277/2003	The RD 1277/2003 establishes the basis for the authorisation procedure of Health Centres and Services by the Autonomous Communities and the Catalogue and Registry of Health Centres and Services. The Autonomous Communities issue an administrative decision authorising the establishment, functioning and modification of the Health Centres enabling them to exercise their activity. Those decisions are collected in the State Registry of Health Centres and Services.
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)?	Art 17 Law 41/2002	Healthcare facilities are required to keep clinical documentation under conditions which ensure its correct and safe maintenance, even if not in the original support. It should ensure the proper patient care during the appropriate time according to each case and at least during five years from the date of discharge of each care process. Health professionals have a duty to cooperate in creating and maintaining an orderly and sequential clinical documentation of the patient care process. The management of clinical history is prescribed to be carried out by admissions and documentation unit in those Healthcare centres that have inpatients or those which attend a sufficient number of patients in any other healthcare modality. The unit will be held responsible for integrating into a single archive all clinical histories. Responsibility for keeping these clinical histories lies on the Management of the Health centre.

Questions	Legal reference	Detailed description
		Health professionals who develop their activity individually are responsible for the management and custody of healthcare documentation generated. Institutions hosting and managing patient's clinical history are bound by the legislation governing the hosting and management of files containing personal data, such as the Law 15/1999 on Protection of Personal Data.
	Art 22 RD 4/2010	RD 4/2010 requires the application of the National Security Scheme rules to ensure the preservation of electronic documents and specifically those provisions related to the fulfilment of the basic principles and minimum security requirements through the application of the security measures appropriate to the means the documents are stored in.
	Art 27 RD 3/2010	All governing bodies of public administration (who are directly responsible for implementing the action of the government at central, regional or local level in a specific sector of activity) must formally have its security policy following the minimum security requirements as listed under Art 11 RD 3/2010.
	Art 14 RD 3/2010	The minimum security requirements under National Security Scheme rules entail different headings including the management of staff which requires that in order to correct or ensure accountability and control of access each user with access right to the information system must be uniquely identified so that it is known at all times, who gets access rights and of what kind or who has performed a certain activity.
	Art 22(4) RD4/2010	Art 22 (4) refers to the requirement for public administrations to have a Policy of electronic signature and certificates in order to guarantee the electronic signature on the preservation of electronic document.
	Art 11(4) RD 38/2012 Basque Country	Art 11 (4) of the Royal Decree 38/2012 of the Basque Country rquires each health institution or health service to establish the necessary mechanisms for access to medical records, and in particular, methods that allow access at all times to the clinical history of each patient by the professionals.
	Art 33 of RD 3/2010	The Royal Decree 3/2010 on the National Security Scheme regulates electronic signatures and requires the application of the mechanisms listed in its Annex II in accordance with the rules in the Policy of electronic signatures and certificates and those established in the National Interoperability Framework. The policy of electronic signature and certificates develops the processes for the generation, validation and maintenance of electronic signatures, and the characteristics and requirements applicable to electronic signature systems.

Questions	Legal reference	Detailed description
In particular, is there any obligation to have the information included in EHRs encrypted?	In practice[22]	Yes
	Art 22 RD 4/2010	The application of the National Security Scheme rules to the EHRs is required by RD 4/2010 and RD 3/2010 establishing the National Security Scheme which imposes minimum security requirements and security measures appropriate to the means the documents are stored in.
	Art 11 RD 3/2010	The National Security Scheme entails minimum security requirements listed under Art 11 of the RD 3/2010.
	Art 27 RD 3/2010	To comply with the minimum requirements established in this Royal Decree, public administrations are required to apply the security measures listed in Annex II which includes the hosting or processing of encrypted information.
	In practice[23]	The relevant Spanish legislation, e.g. Royal Decree 3/2010 or the Royal Decree 81/2014, does not require explicitly in the body of the text the information to be encrypted as there are different security options and the legislation refers to security systems rather than a specific one such as encrypting the information.
Are there any specific auditing requirements for institutions hosting and processing EHRs?	Art 28 L 16/2003	The Autonomous Communities have the responsibility to ensure the quality of services, according to the provisions in Chapter VI of the Cohesion and quality of the NHS Act. To do this, they can conduct independent audits.
	Art 63 L 16/2003	The Observatory of the National Health System is an agency of the Ministry of Health to provide an ongoing analysis of the National Health System as a whole, by comparing the health services of the autonomous communities in the field of organisation, provision of services, health management and results.
	Art 76 L16/2003	The State shall exercise the High Inspectorate as a guarantee and verification of compliance of state and the autonomous communities' competences in health and health care in the National Health System, in accordance with the provisions of the Constitution, the statutes of autonomy and laws. It will be in charge of evaluating compliance with common goals and objectives and identify difficulties, generic or structural deficiencies that impair or distort the functioning of a coherent, harmonious and united healthcare system. The Officials of the Central Government exercising this role shall have the authority for those purposes and may request the necessary collaboration by other public authorities for the performance of the functions they are legally mandated.

[22] Interview Doctor and Director of Ambulatory of Pais Vasco, 15.03.2014.
[23] Maravillas Izquierdo, Vice-Secretary General, Basic NHS Service Portfolio, Ministry of Health, Social Services and Equality. Interview 1st April 2014.

Questions	Legal reference	Detailed description
		The Inspectorate will create and maintain a shared database with the inspection services of the NHS.
	Art 96 RD 1720/2007	Information systems and facilities for the treatment and storage of data are to be submitted at least every two years to an internal or external audit to verify compliance with the data protection rules under the Regulation implementing the OL15/1999.
	Art. 15 RD 3/2010	The security of the systems should be subject to maintenance, review and audit by qualified, dedicated and trained professional in all phases of its life cycle: installation, maintenance, incident management and decommissioning. The information systems should be subject to regular audit at least every two years to verify compliance with the requirements of this National Security Scheme.
	Art 34 (1) RD 3/2010	The audit report shall rule on the degree of compliance with the Royal Decree, identify gaps and suggest possible corrective or complementary measures and recommendations deemed appropriate. Shall likewise include the methodological audit criteria used, the scope and purpose of the audit, and data, facts and observations on which the conclusions are based
	Art 34(5) RD 3/2010	The Ministry of Health is subject to an audit twice a year, one external and another one internal, within the frame of the ISO 27001 certification it was awarded. The audit focuses on the management of the systems in place to ensure the integrated service and the coordination. However the Ministry does not have access to any health information, but it has developed a reference index to keep track of where the information is.
	In practice[24]	The most important audit is carried out by the patient. The Spanish system provides the patient with information about the clinical history and about who has access to that data. The patient has therefore the possibility to react in case the information has been accessed by someone who should not have.

[24] Interview Ministry of Health, 18.03.2014 – Juan Fernando Munoz

2.3. Patient consent

2.3.1. Main findings

The Spanish legislation does not require explicit consent for the creation and setting up of the EHRs or for enabling access to it by health professionals or sharing it with health professionals in different regions or countries. The Spanish legislation regarding health data is based on the consideration that implicit consent is granted by the patient when requesting consultation by the doctor in care processes.

According to the Law 41/2002 all activities aimed at obtaining, using, storing, conserving and transferring information and clinical documentation will be subject to the principles of dignity of human beings respect to their autonomy and privacy. Every action in the field of health requires, in general, the prior consent of patients or users. The consent must be obtained after the patient receives adequate information and shall be in writing in the cases provided for in the law. This provision refers to the patient's consent required for acceptance of health interventions or actions.

The data protection legislation in Spain (OL 15/1999) stipulates that the processing of personal data requires the unambiguous consent of the person affected, unless the law provides otherwise. The Organic Law establishes that the health public or private institutions or centres and individual professionals may be able to process Personal Data relating to the health of patients or to be treated thereof if done in compliance with the provisions of the legislation on health.

Under the OL on the protection of Personal Data, consent is not needed when data of personal character are gathered in the exercise of Public Administration functions or when the processing of data is required for the protection of a vital interest of the person concerned such as those listed in this law (art 7). Those interests include the processing of personal data related to health which then can be carried out if, for reasons of general interest, it is prescribed by law or under explicit consent by the person concerned. However, Article 7(6) states that no consent is needed for prevention, medical diagnosis, health care, health treatment or the management of health services when carried out by a professional subject to professional secrecy or someone under an equivalent obligation. No explicit reference to consent for the setting up of EHR is found in this law but it is understood within the context referred to management of health services.

The Regulation[25] developing the OL 15/1999 clearly states that the individual's consent to the disclosure of personal health data will not be necessary, including if it is carried out through electronic means, between agencies, institutions and services of the National Health System when performed for health care of people, as to the provisions of the Law 16/2003 on cohesion and quality of the NHS.

The fourth additional provision of OL 15/1999 amends the Tax Code stating that the transfer and process of personal data that needs to be made by the tax authorities will not require the consent of the person. Information from the tax authorities is needed to define the status of the patient with regards to contributions to the health system (pharmaceutical services). In this sense, the Law 29/2006 on guarantees and rational use of medicines and health products refers to the capacity of certain bodies of the Public Administration to process information without the consent of the patient when the data is processed with the sole purpose of integrating the information in the individual health card. Specifically it states that the National Institute of Social Security, the Social Marine Institute, the authorities responsible for tax matters and other relevant government bodies, may treat or communicate the data contained that are essential for determining the amount of the contribution of beneficiaries in pharmaceutical services or their exemptions. This treatment does not require the consent of the person concerned and should be fully subject to the provisions of Law 15/1999.

[25] Royal Decree 1720/2007

In brief, the creation and access to the EHRs is subject to the rule recognised in Article 7(6) and (8) of OL 15/1999 and Article 10 of RD 1720/2007establishing that there is no need for consent. The consent is considered implicitly given by the patient's request of a doctor's care process.

The same concept of implicit consent is also currently applied to the cases where sharing of data is related to prescriptions in cross border situations. Art 19 of Royal Decree 1718/2010 as modified by Royal Decree 81/2014 includes specific rules aiming to ensure the continuity of the pharmaceutical care to the patient. It states that the consent by the patient to the treatment or the sharing of data based on information systems for prescriptions on paper or electronic form is not needed. This is consistent with Article 7, 8 and 11 of the OL 15/1999 on data protection

There is no legal obligation in Spanish law that requires providing information about EHRs and their consequences. Patients may ask as they see the doctor writing in the computer otherwise it is assumed a tacit consent. In general doctors do not inform patients that the information on the interventions will be included in the EHRs. Patients do not seem to be worried about where the information goes.

The legislation requires information about the purpose and nature of any intervention, the risks and consequences should be provided orally (noting it in the clinical history) to the patient. Information on the use of EHR is not explicitly considered under Law 41/2002 and therefore the patient's consent legally required in those cases is not applicable. The rules governing patient's consent under the EHRs system are those in Article 7 and 8 of OL 15/1999 and Art 10 of Regulation 1270/2007. As no explicit consent is required, no information obligation is required. However, the patient may be informed if he/she asks about the EHRs.

Under Article 12 patients have the right to receive all information on the Health Centre's services and units available, their quality and requirements for access. This is because in Spain, patients have the right to choose doctor or health centers both for primary and specialized care. Under that situation, the use of EHR might be part of the information that is delivered to the patient, although no explicit reference can be found in the law.

The Spanish law requires the implicit patient consent for processing of EHRs. No rules for opt-in/opt out are foreseen or needed in Spanish law. However, while the patient's consent is considered implicit, the Spanish Data Protection Regulation implementing the Data Protection Act (OL 15/1999) recognises the **right to object** to the processing of the personal data. This is a possibility granted in all cases when the consent is not required for the processing of data. Furthermore, with regard to the sharing of data the patient may decide to hide parts of the clinical history from access by other health professionals (in other services, regions or countries). The GP would however always have access to the fact that the patient wanted to hide that information.

The patient has access to information regarding the persons that had access to the EHRs. This may trigger the reaction through complaints when access has been provided to a person not contacted by the patient. This is conceived as a safeguard to ensure patient's protection in a system where the consent for data processing is implicit. Additional security safeguards are established under the Spanish law to ensure patient's protection when the system is based on implicit consent. The National Security Scheme entails minimum security requirements listed under Art 11 of the RD 3/2010 under different headings including the management of staff which requires that in order to correct or ensure accountability and control of access each user with access right to the information system must be **uniquely identified** so that it is known at all times, who gets access rights and of what kind or who has performed a certain activity. This capacity to identify who has access rights is complemented with the possibility under this Royal Decree 3/2010 for the user activities to be recorded keeping the information necessary to monitor, analyze, investigate and document improper or unauthorized activities, allowing time to identify each person acting on it. The law requires it to be carried out in full guarantees of the right to honor, personal and family privacy and image of the affected itself, and according to the rules on protection of personal data, public or occupational function, and other applicable provisions. On that basis the patient may act against any mistreatment of data

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?	Art 2(1) Law 41/2002	All activities aimed at obtaining, using, storing, conserving and transferring information and clinical documentation will be subject to the principles of dignity of human beings respect to their autonomy and privacy.
	Art 2(2) Law 41/2002	Every action in the field of health requires, in general, the prior consent of patients or users. The consent must be obtained after the patient receives adequate information and shall be in writing in the cases provided for in the law. This provision is interpreted as related to the patient's consent required for acceptance of health interventions or actions.
	Art 6 OL 15/1999	The processing of personal data requires the unambiguous consent of the person affected, unless the law provides otherwise.
	Art. 8 OL 15/1999 on data protection	The health public or private institutions or centres and individual professionals may be able to process Personal Data relating to the health of patients or to be treated thereof according to the provisions of the legislation on health.
	Art 6 and 7(3) and (6) of the OL 15/1999 on data protection	Under the OL on the protection of Personal Data, consent is not needed when data of personal character are gathered in the exercise of Public Administration functions or when the processing of data is required for the protection of a vital interest of the person concerned such as those listed in this law (art 7). Those interests include the processing of personal data related to health which then can be carried out if, for reasons of general interest, it is prescribed by law or under explicit consent by the person concerned. However, it states that no consent is needed for prevention, medical diagnosis, health care, health treatment or the management of health services when carried out by a professional subject to professional secrecy or someone under an equivalent obligation. No explicit reference to consent for the setting up of EHR is found in this law but it is understood within the context referred to management of health services.
	Art 10(5) RD 1720/2007	The Regulation developing the OL 15/1999 refers to Article 7 and 8 of the OL 15/1999 and clearly states that the individual's consent to the disclosure of personal health data will not be necessary, including if it is carried out through electronic means, between agencies, institutions and services of the National Health System when performed for health care of people, in compliance with the provisions of the Law 16/2003 on cohesion and quality of the NHS.
	Fourth additional provision of LO 15/1999	Amends the Tax Code to read that the transfer and process of personal data that needs to be made by the tax authorities will not require the consent of the person. Information from the tax authorities is needed to define the status of the patient with regards to contributions to the health system (pharmaceutical services)

Questions	Legal reference	Detailed description
	Art 94 (b) of Law 29/2006	In this sense, the Law 29/2006 on guarantees and rational use of medicines and health products refers to the capacity of certain bodies of the Public Administration to process information without the consent of the patient when the data is processed with the sole purpose of integrating the information in the individual health card. Specifically it states that the National Institute of Social Security, the Social Marine Institute, the authorities responsible for tax matters and other relevant government bodies, may treat or communicate the data contained that are essential for determining the amount of the contribution of beneficiaries in pharmaceutical services or their exemptions. This treatment does not require the consent of the person concerned and should be fully subject to the provisions of Law 15/1999.
Is a materialised consent needed?	Art 2(2) Law 41/2002	Law 41/2002 states that every action in the field of health requires, in general, the prior consent of patients or users. The consent is to be delivered in writing in the cases provided for in the law. This provision relates to the patient's consent required for acceptance of health interventions or actions and should be delivered orally as a general rule and it is required in writing when it relates to surgery, invasive diagnostic and therapeutic procedures and, in general, procedures involving risks and disadvantages of notorious and predictable negative impact on the patient's health.
	7(6) of the OL 15/1999 on data protection.	This consent is different to the consent for processing data or setting up the EHR. As stated above, no consent is needed for prevention, medical diagnosis, health care and treatment or the management of health services when carried out by a professional subject to professional secrecy or someone under an equivalent obligation.
	Art 27 of Law 11/2007	In any case, under Art 27 of Law 11/2007 on citizens' electronic access to Public Services, the consent can be issued and collected by electronic means with relation to communications between Public Administration and citizens who have expressly consented.
Are there requirements to inform the patient about the purpose of EHRs and the consequences of the consent or withholding consent to create EHRs?	Art 4 and 8 Law 41/2002	Information on the purpose or use of EHR is not explicitly considered under Law 41/2002. This law only refers to the information to the patient about the purpose and nature of any intervention, the risks and consequences should be provided orally (noting it in the clinical history). Therefore the patient's consent legally required in those cases is not applicable.
	Art 12 Law 41/2002	Under Article 12 patients have the right to receive all information on the Health Centre's services and units available, their quality and requirements for access. This is because in Spain, patients have the right to choose doctor or health centers both for primary and specialized care. Under that situation, the use of EHR might be part of the information that is delivered to the patient, although no explicit reference can be found in the law.

Questions	Legal reference	Detailed description
	In practice[26]	For the creation and access to the EHRs, the rule currently applied is Art 7(6) and (8) of OL 15/1999 and Art 10 of RD 1720/2007establishing that there is no need for explicit consent. The consent is considered implicitly given by the patient's petition of a doctor's consultation for every care process. Therefore, information about the EHRs is generally not provided to the patients in consultation. Patients may ask as they see the doctor writing in the computer and it is assumed a tacit consent.
Are there specific national rules on consent from the patient to share data?	Art 10(5) RD 1720/2007	The Regulation developing the OL 15/1999 refers to Article 7 and 8 of the OL 15/1999 and cclearly states that the individual's consent to the disclosure of personal health data will not be necessary, including if it is carried out through electronic means, between agencies, institutions and services of the National Health System when performed for health care of people, in compliance with the provisions of the Law 16/2003 on cohesion and quality of the NHS.
	Art 6(2)b) and 9 of L 11/2007	Citizens have the right not to provide the information and documents held by the public authorities (Art 6 (2) b)). For the effective exercise of this right, every administration should facilitate access to the other public authorities to data in their possession, specifying the conditions and technical or functional criteria for accessing them with the maximum guarantees of security and in compliance with legislative provisions on data protection, including those related to patient consent as described above. Data to be shared is limited to data required by the competent authorities for the exercise of their competences and within the conditions established by the legislation on data protection.
	Art 11 Law 41/2002	The communication of the information to a third party is subject to more stringent restrictions. The personal data subject to processing may only be disclosed to a third party for purposes directly related to the legitimate functions of the body processing it and subject to the person concerned prior consent, which is of revocable character. However, the consent would not be needed when the transfer of personal data concerning health is necessary to resolve an emergency that requires access to a file or to conduct epidemiological studies in the terms established in the legislation. Again in practice, the rule of implicit consent is applied on cases of sharing data. Transfer of health data between States will not require explicit consent by the patient.
	In practice[27]	The patient may decide to hide certain parts of the clinical history blocking access to it for specific consultations by different doctors or between different regions. The GP would

[26] Interview Ministry of Health, 18.03.2014 – Juan Fernando Munoz
[27] Interview Ministry of Health, 18.03.2014 – Juan Fernando Munoz

Questions	Legal reference	Detailed description
		always have access to the fact that the patient wanted to hide that information
Are there any opt-in/opt-out rules for patient consent with regard to processing of EHRs?		The patient consent required for the processing of EHRs is implicit. No rules for opt-in/opt out are foreseen or needed in Spanish law. (see above)
	Art 63 RD 1720/2007	However, while the patient's consent is considered implicit, the Spanish Data Protection Regulation implementing the Data Protection Act (OL 15/1999) recognises the **right to object** to the processing of the personal data. This is a possibility granted in all cases when the consent is not required for the processing of data.
	In practice[28]	Furthermore, the patient may decide to hide parts of the clinical history from access by other health professionals (in other services, regions or countries).
Are there any opt-in/opt-out rules for patient consent with regard to sharing of EHRs?	In practice[29]	The patient may decide to hide certain parts of the clinical history blocking access to it for specific consultations by different doctors or between different regions. The GP would always have access to the fact that the patient wanted to hide that information. The patient has access to information regarding the persons that had access to the EHRs. This may trigger the reaction through complaint when access has been provided to a person not contacted by the patient.
	Art 14 RD 3/2010	The National Security Scheme entails minimum security requirements listed under Art 11 of the RD 3/2010 under different headings including the management of staff which requires that in order to correct or ensure accountability and control of access each user with access right to the information system must be **uniquely identified** so that it is known at all times, who gets access rights and of what kind or who has performed a certain activity.
	Art 23 RD 3/2010	This capacity to identify who has access rights is complemented with the possibility to for the user activities to be recorded retaining the information necessary to monitor, analyze, investigate and document improper or unauthorized activities, allowing time to identify each person acting on it. The law requires it to be carried out in full guarantees of the right to honor, personal and family privacy and image of the affected itself, and according to the rules on protection of personal data, public or occupational function, and other applicable provisions.
	Art 63 RD 1720/2007	On that basis the patient may act against any mistreatment of data. Furthermore the patient is granted the **right to object** to the processing of the personal data. This is a possibility provided by the Regulation implementing the data protection Act in all cases when the consent is not required for the processing of data.
Are there requirements to inform the patient	Art 2(5) L41/2002	Information on the use of EHR is not explicitly considered under Law 41/2002. This law

[28] Interview Doctor and Director of Ambulatory of Pais Vasco, 15.03.2014
[29] Interview Ministry of Health, 18.03.2014 – Juan Fernando Munoz

Questions	Legal reference	Detailed description
about the purpose of EHRs and the consequences of consent or withholding consent on the sharing of EHRs?		only refers to the information to the patient about the purpose and nature of any intervention, the risks and consequences should be provided orally (noting it in the clinical history). Information on the use of EHR is not explicitly considered under Law 41/2002. However, certain provisions could be interpreted as requiring professionals to actually provide that information. For example, Art 2(5) requires professionals to implement the duties to inform the patients and to provide them with clinic documents.
	Art 4(1) L41/2002	Patients have the right to know all available information on any action in the field of health, saving the cases excepted by law. The information which, as a general rule, is provided verbally is written it in the medical record and comprises at least the purpose and nature of the intervention, its risks and consequences.
	In practice[30]	In practice no information is provided on the creation of EHRs or its purpose and the use and scope of the implicit consent except if requested during consultation by the patient. Furthermore, the EHRs system is not well developed and used in all Autonomous Communities and therefore, data is not always possible to be transferred or shared. Thus no need for informing the patient.
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)?	*Art 10(5)* RD 1720/2007	The Regulation developing the OL 15/1999 refers to Article 7 and 8 of the OL 15/1999 and clearly states that the individual's consent to the disclosure of personal health data will not be necessary, including if it is carried out through electronic means, between agencies, institutions and services of the National Health System when performed for health care of people, in compliance with the provisions of the Law 16/2003 on cohesion and quality of the NHS.
	Art 33 OL 15/1999	Temporary or permanent transfers of Personal Data to countries that do not provide an equivalent level of protection to that provided by this Act are banned unless prior authorization from the Director of the Agency of Protection is obtained. The equivalent level of protection of a country is evaluated by the Data Protection Agency according to the specific circumstances in the transfer of data. Therefore, the personal data may be transferred to EU Member States where similar standards based on EU Data protection legislation are applied.
	Art 34 OL 15/1999	The consent of the person is not needed when the transfer of data is necessary for prevention, medical diagnosis, the provision of medical care or treatment or the management of health services. No specific reference to Electronic Health Records is made in this law.
Are there specific rules on patient consent to		The provisions on implicit consent are currently applied.

[30] Interview Doctor and Director of Ambulatory of Pais Vasco, 15.03.2014
Interview Ministry of Health, 18.03.2014 – Juan Fernando Munoz
Maravillas Izquierdo, Vice-Secretary General, Basic NHS Service Portfolio, Ministry of Health, Social Services and Equality. Interview 1st April 2014.

Questions	Legal reference	Detailed description
share data on a cross-border situation?		Article 10(5) of RD 1720/2007 stating that individual's consent to the disclosure of personal health data will not be necessary is also applicable to cross-border situation.
	Art 66 RD 1720/2007	Furthermore, Art 33 and 34 are further implemented by RD 1720/2007 whose Art 66 stipulates that there is no need for patient's consent for the transfer of data between Member States when it is necessary for prevention, medical diagnosis, the provision of medical care or treatment or the management of health services.
	Art 19 of RD 1718/2010 as modified by RD 81/2014.	Art 19 of Royal Decree 1718/2010 as modified by Royal Decree 81/2014 includes specific rules aiming to ensure the continuity of the pharmaceutical care to the patient. It states that the consent by the patient to the treatment or the sharing of data based on information systems for prescriptions on paper or electronic form is not needed. This is consistent with Article 7, 8 and 11 of the OL 15/1999 on data protection.

2.4. Creation, access to and update of EHRs

2.4.1. Main findings

Creation/Update

The Law 41/2002 states that the completion of the clinical history in relation to the direct patient care is the responsibility of the professionals involved in it. Health professionals have the duty to cooperate in **creating** and **maintaining** an orderly and sequential clinical documentation of patient care process. Furthermore, health professional have the duty to complete the protocols, reports, statistics and other documents for administrative assistance in relation to the clinical processes they are involved in. The Spanish legislation recognises the patient's right to the health records, in writing or in the most appropriate support, with the information obtained during its care process carried out by health professionals.

This is confirmed by the Royal Decree 1093/2010 on the minimum data from clinical reports in the NHS where it is established that the summary clinical history is an electronic document, automatically generated and fed in and updated on the basis of data that **healthcare professionals** include in the full clinical history of the patient.

The Law 41/2002 states that the clinical history's main purpose is to facilitate healthcare, ensuring that data is recorded which would enable accurate and **updated** knowledge of patients' health status. The updating of the information is the health professionals' responsibility.

There is an obligation to keep health records of patients and update them accordingly in whatever format they are, paper or electronic. This is an obligation on doctors as the health information needs to be updated to ensure proper health care and treatments are proposed. The updating of the information is needed for traceability and procedural requirements. For the same reason, the whole sequence of health data should be available. For example, information on a patient's cholesterol level needs to cover longer periods rather than punctual situations in order to estimate the health problem and the adequate treatment. A common platform ensuring the minimum content and requirements in the EHRs regarding this type of information is needed.

The EHRs are created by the GP for every patient in consultation within the regional system or in the hospital (in the public system). The EHRs may be composed only by the summary clinical history but also any other of the reports described in the sections above. The Autonomous Communities may decide what reports would be issued and what information would be digitalised for this purpose. Not all Autonomous Communities enable access to the same reports.

Access

The patient's access to the Spanish Health System is based on the individual ehealth card, as an administrative document which certifies the holder's data. The card must incorporate the technical devices to store basic information and allow that reading and checking the data is technically possible in the whole State and all public administrations. For this, the Ministry of Health in collaboration with the Autonomous Communities and other competent public authorities, established the necessary requirements and standards. The Ministry of Health is responsible for the development of the database to collect basic information about residents who benefit from the NHS enabling the creation of the unique personal identification code.

According to the data protection Organic Law 15/1999, the person concerned has the right to request and obtain information regarding the processing of his personal data, the origin of such data as well as their communication already made or predicted to be made. The right to have access may be exercised

only at intervals not inferiors to twelve months unless the applicant can demonstrate a legitimate interest in which case it could be exercised before.

The interested party also has the right to cancellation or correction of the personal data whose treatment is not in accordance with the Data Protection law, and in particular, when such data are inaccurate or incomplete. The controller has the obligation to fulfill the right of rectification or cancellation within 10 days. Cancellation will result in the blocking of data that is retained only at the disposal of the public administration, judges and courts for the attention of potential liabilities arising from the processing of the data up to the prescription deadline.

The patient has the right to access the documents in the clinical history and to obtain a copy of the data contained therein. Healthcare centres are required to adopt the measures establishing the procedure to ensure the observance of these rights. The right of access to documents of the patient's medical history cannot be exercised to the prejudice of the right of the professionals participating in the creation and processing of the data who can oppose the reserve of their subjective annotations. The data protection legislation recognises that the rights of access, rectification, cancellation and opposition are personal and shall be exercised by the person concerned.

The patient has the right to access but has to request it explicitly to receive the necessary electronic personal identification. For reasons of security of data, the patient will receive either a special card or use the electronic ID with additional requirements to have access to the clinical history electronically and, for example, request an appointment (only with health professional for primary health care), information on discharges, interventions or treatment. The patient does not have information to the subjective comments by the health professionals. Indeed Article 11(6) of the RD 38/2012 Basque Country requires the requests for access to patients' data to follow the procedures established in that Royal Decree and Article 12 requires the patient to submit the request to the person responsible at the relevant centre or the relevant health service; the request should include the reason and purpose of the request and the specific care process. Once access is provided, a system is being developed to allow the patient to introduce some data related to the result of treatments or on-line appointments

Health care professionals performing the diagnosis or treatment of the patient have direct and immediate access to the patient's clinical history which is the fundamental instrument for ensuring the proper health care. The Law 41/2002 requires each health center to establish methods that allow access to each patient's clinical history at all times by those professionals that provide the care for him.

Art 13 of the Royal Decree 38/2012 Basque Country requires the authorisation by the health institution according to established access criteria and it should be recorded who had access, the date and the part of the health records accessed to. The health professionals in charge of diagnosis and treatment have direct and immediate access to the health records and other clinical information. Access is limited to the purpose of health care. However those health professionals from other institutions or regional health services that those responsible for keeping the health records are requested to submit the request including an explicit justification based on health care purposes. The information systems should enable the identification of the health professional trying to have access to EHRs and should verify the authorisation..

The individual health card should enable access to data by duly authorized professionals, with the aim of helping to improve the quality and continuity of care.

In practice, access to the whole clinical history is limited to the health professionals such as doctors or nurses and only they can introduce data on the EHRs. Administrative or auxiliary staff only has access to the administrative part of the clinical history. The Health Centre's administration and management staff can only access the data in the clinical history when is related to their own functions. The duly accredited medical personnel who perform inspection, evaluation, accreditation and planning functions, have access to clinical records when necessary to fulfil their duties of checking the quality

of care and always respecting patients' rights. Personnel accessing data from the clinical history in the exercise of their duties is subject to the duty of secrecy.

Article 15 of the Royal Decree 38/2012 refers to Article 16 of the Law 41/2002 regarding the access for accredited health professionals with inspection, evaluation or planning responsibilities to the clinical history. A similar provision covers professionals with management of health service functions. This type of access would require technical justifications related to the effectiveness or efficiency of the health services. Article 16 continues by requiring in those cases to preserve the data for the identification of the patient and be separated from the health care data ensuring anonymity.

The health professionals have to be registered according to the law. The L 16/2003 requires that information on human resources is included in the Health Information System of the NHS.

The Law 44/2003 on Health professions refers to public registers of professionals as a guarantee for health professionals and patients. The Regional Health Services are required to set those registers of health professionals which include all those providing services in the Health Centres. Almost all Autonomous Communities have regulated their health care records based on the decision adopted by the Inter-Territorial Council of the National Health System on the records of health professionals, from March 2007. The coordination of the information contained in these Registers is necessary. Therefore the Royal Decree-Law 16/2012 established the State Register of Health Professionals. The integration of the Register in the Information System of the National Health System enables the connection with other Registers according to the demanding needs of both citizens and institutions of the health system. His public character, as to certain data, and digital media make the records readily accessible. However, there is still the need to determine the functioning and organization of the State Registration of Healthcare Professionals. For that reason a new Royal Decree is foreseen to be adopted by May 2014.

Safety requirements include the management of electronic signature providing access to EHRs. The National Security Scheme entails minimum security requirements listed under Art 11 of the RD 3/2010 under different headings including the management of staff which requires that in order to correct or ensure accountability and control of access each user with access right to the information system must be **uniquely identified** so that it is known at all times, who gets access rights and of what kind or who has performed a certain activity.

Further to the register, a specific authorisation based on electronic professional certificate or electronic ID is required as safety requirement for the professionals to access EHRs. Some Autonomous Communities have provided some or all of their health professionals with such identification. While the State has provided every patient with the electronic card and the electronic ID is well established in Spain, doctors are reticent to use private tools such as the ecard or the ID for professional use.

The Royal Decree 3/2010 on National Security Scheme regulates electronic signatures and requires the application of the mechanisms listed in its Annex II and in accordance with the rules in the Policy of electronic signatures and certificates, as well as in those established in the National Interoperability Framework. The Policy of electronic signature and certificates develops the processes for the generation, validation and maintenance of electronic signatures, and the characteristics and requirements applicable to electronic signature systems. A new Regulation for identification and electronic signature is foreseen to be adopted in the next months to enable the use of ID in the cloud.

In relation to the access to data by professionals from other Member States, the legislation requires the health care provider to ensure that the patient have access to a copy of the medical records enabling a continued health care to the patients seen or treated in Spain but coming from other Member States within the scope of cross-border healthcare.

In order to promote continuity of care, the Spanish patient receiving healthcare in other Member States shall be granted health care by ensuring cooperation with those Member States in the exchange of

information and providing electronic access to clinical documentation through information systems. Access to a copy of the clinical reports, results of diagnostic tests and therapeutic procedures is guaranteed. Similarly health care is guaranteed to patients from other Member States seen or treated in Spain. Access to a copy of the clinical reports, results of diagnostic tests and therapeutic procedures is guaranteed and electronic access to clinical documentation through information systems.

The cooperation with other Member States in the exchange of information is carried out within the framework of the European network of electronic health and is based on national, European and international standards for communications of the electronic Health Records or the electronic clinical history. Both cases are subject to the provisions on data protection under Organic Law 15/1999 and law 41/2002.

However, in practice different Public Administrations in the same Autonomous Community do not always share access to the clinical history. Similarly not all Autonomous Communities have the capacity to share access to the EHRs. Only few Member States may share access to the data / information in the clinical history. A French national in a hospital in Madrid will be treated but doctors will not have access to his/her clinical history and the patient will receive the information of the clinical history on paper in order to ensure continuity of the treatment in France. Access is provided only within the epSOS project. Information and data on the EHRs are generally not shared between Member States yet.

There is currently not such broad access to EHRs from health professionals from different regions or countries due to the different stages of development and the lack of interoperability of platforms to enable it. Spanish regions have followed uneven rhythms but at present, most Autonomous Communities have introduced the electronic or digital clinical history. Specifically Navarra, Extremadura, Galicia and Murcia, while acknowledging that the use of certificate is still a problem - and Cantabria have extended the use of electronic clinical history to the 100% of their services. In Valencia the use covers 95% and in Asturias – is complete with the exception of two hospitals. Catalonia has introduced it at 97% of specialty care, 88% of primary care, 76 in geriatric and 51% for mental health. Meanwhile, in the Baleares Islands, all public community hospitals have electronic medical records of patients and professionals can access the electronic clinical history, however it still needs to extend it to primary as in the Basque Country. On the opposite side are Andalucía, Castilla y León, Madrid, Aragon and the Canary Islands with 100% in primary care but much lower levels for specialised care ranging from 55% to few hospitals in the region depending on the Autonomous Community. Meanwhile, Castilla-La Mancha, does not have specific date for the completion of this project, although progress is being made on compatibility of data from primary and specialized in all health centres and are preparing protocols to unify all patient health information to be accessible from any centre[31].

[31] Gaceta Médica.com, 'La implantación de la historia clínica digital sigue diferentes ritmos in las CC.AA. 16 April 2014.

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?	Art 15 L 41/2002	The L 41/2002 states that the completion of the clinical history in relation to the direct patient care is the responsibility of the professionals involved in it. This is confirmed in other regional measures, for example in Art 7 of Royal Decree 38/2012 Basque Country.
	Art 7 RD 38/2012 Basque Country	Health professionals have the duty to cooperate in creating and maintaining an orderly and sequential clinical documentation of patient care process.
	Art 17(3) L41/2002	Furthermore, health professional have the duty to complete the protocols, reports, statistics and other documents for administrative assistance in relation to the clinical processes they are involved in.
	Art 23 L41/2002	The summary clinical history is an electronic document, automatically generated and fed in and updated on the basis of data that **healthcare professionals** include in the full clinical history of the patient.
	Art 3 RD 1093/2010	The EHRs are created by the GP for every patient in consultation within the regional system or in the hospital (in the public system).
	In practice	As shown in the previous section, the EHRs may be considered the summary clinical history but also any other of the above described normalised reports. The Autonomous Communities may decide what reports would be issued and what information would be digitalised for this purpose. Not all Autonomous Communities provide the same reports.
Are there specific national rules on access and update to EHRs?	Art 16 Law 41/2002	Health care professionals from the Institution or centre performing the diagnosis or treatment of the patient have access to the patient's clinical history as the fundamental instrument for ensuring the proper health care. Each center shall establish methods that allow access to each patient's clinical history at all times by those professionals providing the care.
	Art 13 RD 38/2012 Basque Country	Art 13 of the RD 38/2012 Basque Country requires the authorisation by the health institution according to established access criteria and it should be recorded who had access, the date and the part of the health records accessed to. The health professionals in charge of diagnosis and treatment have direct and immediate access to the health records and other clinical information. However those health professionals from other institutions or regional health services that those responsible for keeping the health records are requested to submit the request including the justification based on health care purposes.
	Art 17 Law 41/2002	The Law 41/2002 further requires the legislation governing the hosting and management

Questions	Legal reference	Detailed description
		of files containing personal data, such as the Law 15/1999 on Protection of Personal Data, to be applicable to the patient's clinical history.
	Art. 53 L 16/2003	Furthermore, under the legislation on the cohesion and quality of the Health National System the transfer of the data, including those necessary for personal health information system is subject to the legislation on protection of personal data and the conditions agreed in the Inter-Territorial Council of the National Health SystemThe information on the unique personal identification code, gives the right to access the clinical information and health records, electronic prescriptions and other information which circulates through Health Communication Network.
	Art 54 L16/2003	The mechanism established for the electronic exchange of health clinical and individual data aims at allowing both patients and professionals involved in health care accessing the medical records but only those that are strictly necessary to ensure the quality of the care and respecting the confidentiality and integrity of the information. The exchange of information needs to comply with data protection provisions under Law 15/1999 and Law 41/2002.
	Art 56 L16/2003	According to the data protection legislation, the person concerned has the right to request and obtain information regarding the processing of his personal data, the origin of such data as well as their communication already made or predicted to be made. According to this law, the right to have access may be exercised only at intervals not inferiors to twelve months unless the applicant can demonstrate a legitimate interest in which case it could be exercised before.
	Art 13 RD 38/2012 Basque Country	In practice, for the patient to have access to the EHRs, he/she may request it in order to receive the necessary devices with enough guarantee of security when having access to the EHRs.
	Art 15 OL 15/199	The interested party also has the right to cancellation or correction of the Personal Data whose treatment is not in accordance with the Data Protection law, and in particular, when such data are inaccurate or incomplete. The controller has the obligation to fulfill the right of rectification or cancellation within 10 days. Cancellation will result in the blocking of data that is retained only at the disposal of the public administration, judges and courts for the attention of potential liabilities arising from the processing of the data up to the prescription deadline.
	In practice[32]	Access to the whole clinical history is limited to the health professionals such as doctors or nurses and only they can introduce data on the EHRs. Administrative or auxiliary staff only has access to the administrative part of the clinical history.

[32] Interview Doctor and Director of Ambulatory of Pais Vasco, 15.03.2014.

Questions	Legal reference	Detailed description
	In practice[33]	There is currently not such broad access to EHRs from health professionals from different regions or countries due to the different stages of development and he lack of interoperability of platforms to enable it. Spanish regions have followed uneven rhythms but at present, most Autonomous Communities have introduced the electronic or digital clinical history. Specifically Navarra, Extremadura, Galicia and Murcia, while acknowledging that the use of certificate is still a problem - and Cantabria have extended the use of electronic clinical history to the 100% of their services. In Valencia the use covers 95% and in Asturias – is complete with the exception of two hospitals. Catalonia has introduced it at 97% of specialty care, 88% of primary care, 76 in geriatric and 51% for mental health. Meanwhile, in the Baleares Islands, all public community hospitals have electronic medical records of patients and professionals can access the electronic clinical history, however it still needs to extend it to primary as in the Basque Country. On the opposite side are Andalucía, Castilla y León, Madrid, Aragon and the Canary Islands with 100% in primary care but much lower levels for specialised care ranging from 55% to few hospitals in the region depending on the Autonomous Community. Meanwhile, Castilla-La Mancha, does not have specific date for the completion of this project, although progress is being made on compatibility of data from primary and specialized in all health centers and are preparing protocols to unify all patient health information to be accessible from any centre[34].
Are there different categories of access for different health professionals?	*Art 16 Law 41/2002*	The Health Centre's administration and management staff can only access the data in the clinical history when is related to their own functions. The duly accredited medical personnel who perform inspection, evaluation, accreditation and planning functions, have access to clinical records when necessary to fulfil their duties of checking the quality of care and always respecting patients' rights. Personnel accessing data from the clinical history in the exercise of their duties is subject to the duty of secrecy. The Autonomous Communities should regulate the procedure for recording the access to patient's clinical history and its use.
	Art 13 of RD 38/2012	For example Article 13 of the RD 38/2012 of the Basque country, the professionals are granted authorisation for access in a selective way according to their role in the health care process and the category. The information systems should enable the identification of the health professional trying to have access to EHRs and should verify the authorisation. However those professionals who are in charge of the diagnosis or treatment of the patient have direct and immediate access to the EHRs of their patients. Access is limited to the purpose of health care.
	Art 15 of RD 38/2012	When the health professionals are in other health services, an explicit justification based

[33] Maravillas Izquierdo, Vice-Secretary General, Basic NHS Service Portfolio, Ministry of Health, Social Services and Equality. Interview 1st April 2014.
[34] Gaceta Médica.com, 'La implantación de la historia clínica digital sigue diferentes ritmos in las CC.AA. 16 April 2014.

Questions	Legal reference	Detailed description
		on care purposes have to be argued.
	Art 57 (4) L 16/2003	Article 15 of the Royal Decree 38/2012 refers to Article 16 of the Law 41/2002 regarding the access for accredited health professionals with inspection, evaluation or planning responsibilities to the clinical history. A similar provision covers professionals with management of health service functions. This type of access would require technical justifications related to the effectiveness or efficiency of the health services. Article 16 continues by requiring in those cases to preserve the data for the identification of the patient and be separated from the health care data ensuring anonymity. The individual health card should enable access to data by duly authorized professionals, with the aim of helping to improve the quality and continuity of care.
	In practice[35]	In practice doctors and nurses have access to the whole clinical history including treatment, hospital admissions and discharges. Admin staff only has access to the administrative side of the clinical history. The patient may request the confidential treatment of part of the information in his/her clinical history.
Are patients entitled to access their EHRs?	Art. 18 Law 41/2002	The patient has the right to access the documents in the clinical history and to obtain a copy of the data contained therein. Healthcare centres or regional health services are required to adopt the measures establishing the procedure to ensure the observance of these rights. The right of access to documents of the patient's medical history cannot be exercised to the prejudice of the right of the professionals participating in the creation and processing of the data and who can oppose to the right of access, the reserve of their subjective annotations.
	Art 23 RD 1720/2007	The data protection legislation recognises that the rights of access, rectification, cancellation and opposition are personal and shall be exercised by the person concerned.
	Art 11 RD 38/2012 of the Basque Country	Indeed Article 11(6) of the RD 38/2012 Basque Country requires the requests for access to patients' data to follow the procedures established in that Royal Decree and Article 12 requires the patient to submit the request to the person responsible at the relevant centre or the relevant health service; the request should include the reason and purpose of the request and the specific care process. Once access is provided, a system is being developed to allow the patient to introduce some data related to the result of treatments or on-line appointments
	In practice[36]	The patient has the right to access but has to request it explicitly to receive the necessary electronic personal identification. For reasons of security of data, the patient needs to use not only the health card but also should receive either a special card or use the electronic

[35] Interview Doctor and Director of Ambulatory of Pais Vasco, 15.03.2014.
[36] Interview Doctor and Director of Ambulatory of Pais Vasco, 15.03.2014.

Questions	Legal reference	Detailed description
		ID in order to allow the individual verification of the person's identity and right to access. The Central governments and regional authorities are exploring the possibility not only to have access to the clinical history electronically but also to request an appointment (only with health professional for primary health care), information on discharges, interventions or treatment. The patient does not have information to the subjective comments by the health professionals. The patient may decide to hide part of the information in the EHRs for access to third persons (not the GP) and every patient has access to information regarding who (i.e. health services) had access to the EHRs. This enables patients to complaint if data is leaked to inappropriate persons.
Can patient have access to all of EHR content?	Art. 18 Law 41/2002 In practice[37]	The patient has the right to access the documents in the clinical history and to obtain a copy of the data contained therein. Healthcare centres or regional health services are required to adopt the measures establishing the procedure to ensure the observance of these rights. The right of access to documents of the patient's medical history cannot be exercised to the prejudice of the right of the professionals participating in the creation and processing of the data and who can oppose to the right of access, the reserve of their subjective annotations. The patients may request explicitly to have access to the EHRs and, generally they are provided with a special card to allow access with the guarantee of security. No comments by the patient can be included for the moment. Article 12 of RD 38/2012 Basque Country refers to Article 18 of the Law 41/2002 and recognises the patient's right to access the documentation in the clinical history and a copy of the data in it with the limitations related to therapeutical needs decided by the health professional or the health professionals right to oppose reservation of their subjective annotations. In its paragraph 6, it establishes the need for the request for access to be addressed directly to the responsible person at the health centre or health service or to the body responsible for the customer's care service.
Can patient download all or some of EHR content?	In practice[38]	The patient can download part of the EHRs content. No reference to downloading has been found in Spanish legislation (State or regional level).
Can patient update their record, modify and erase EHR content?	In practice[39]	No rules have been found in the Spanish legislation. In principle the health professional is the only one entitled to create and modify the

[37] Interview Doctor and Director of Ambulatory of Pais Vasco, 15.03.2014.
[38] Interview Doctor and Director of Ambulatory of Pais Vasco, 15.03.2014.
[39] Maravillas Izquierdo, Vice-Secretary General, Basic NHS Service Portfolio, Ministry of Health, Social Services and Equality. Interview 1st April 2014.

Questions	Legal reference	Detailed description
		patient's EHRs in order to preserve the accuracy and medical nature of the system. However, a system called "la carpeta de salud del paciente" is currently being developed in the Basque Country to enable the patient to add information in the EHRs, in relation to the treatment followed enabling the patient to add specific comments. It is worth stressing that there is no possibility currently or foreseen for the future to erase or modify the information created by the health professionals.
Do different types of health professionals have the same rights to update EHRs?	In practice	Only doctors and nurses can update the health data of the EHRs.
Are there explicit occupational prohibitions? (e.g. insurance companies/occupational physicians…)	Art 16(5) RD 38/2012 of the Basque Country	The general legislation does not refer to this aspect. However, some regional legislation limits the access to administrative and health data to certain occupational situations. For example, Article 16(5) of Royal Decree 38/2012 of the Basque Country limits the right of access to health information by private insurance companies to data in the clinical history that are essential for billing purposes. Any other clinical information requested by the insurance company requires the express consent of the individual patient.
Are there exceptions to the access requirements (e.g. in case of emergency)?	*In practice*	The patient has access to information on the persons who have had access to his/her EHRs. The patient may decide to hide part of the information but the GP has access to the fact that the patient decided to hide data and only for emergency vital reasons the GP may overrule this decision.
Are there any specific rules on identification and authentication for health professionals? Or are they aggregated?	*Art 9 RD-L 16/2012 introducing a new 10th additional provision in Law 16/2003complementingArt 53 on the Health information System.* *Art 5(2) Law 44/2003* *Art 16 Law 55/2003* Royal Decree-Law 16/2012	Health professionals are registered according to the law. The L 16/2003 requires that information on human resources is included in the Health Information System of the NHS . The Law 44/2003 on Health professions refers to public registers of professionals as a guarantee for health professionals and patients. It refers to private health centres, insurance companies operating in the health field, professional associations and Autonomous Communities. Regional Health Services are required to set those registers of health professionals which include all those providing services in the Health Centres. Almost all Autonomous Communities have regulated their health care records based on the decision adopted by the Inter-Territorial Council of the National Health System on the records of health professionals, from March 14, 2007. The coordination of the information contained in these Registers is necessary. Therefore the Royal Decree-Law 16/2012 established the State Register of Health Professionals. The integration of the Register in the Information System of the National

Interview Doctor and Director of Ambulatory of Pais Vasco, 15.03.2014.

Questions	Legal reference	Detailed description
		Health System enables the connection with other Registers according to the demanding needs of both citizens and institutions of the health system. His public character, as to certain data, and digital media make the records readily accessible. However, there is still the need to determine the functioning and organization of the State Registration of Healthcare Professionals. For that reason a new Royal Decree is foreseen to be adopted by May 2014. Further to the register, a specific authorisation based on electronic professional certificate or electronic ID is required as safety requirement for the professionals to access EHRs. Some Autonomous Communities have provided some or all of their health professionals with such identification. While the State has provided every patient with the electronic card and the electronic ID is well established in Spain, doctors are reticent to use private tools such as the ecard or the ID for professional use. Safety requirements include the management of electronic signature providing access to EHRs. The National Security Scheme entails minimum security requirements listed under Art 11 of the RD 3/2010 under different headings including the management of staff which requires that in order to correct or ensure accountability and control of access each user with access right to the information system must be **uniquely identified** so that it is known at all times, who gets access rights and of what kind or who has performed a certain activity.
	Art 11 of the RD 3/2010	
	Art 33 of RD 3/2010	The Royal Decree 3/2010 on National Security Scheme regulates electronic signatures and requires the application of the mechanisms listed in its Annex II and in accordance with the rules in the Policy of electronic signatures and certificates, as well as in those established in the National Interoperability Framework. The Policy of electronic signature and certificates develops the processes for the generation, validation and maintenance of electronic signatures, and the characteristics and requirements applicable to electronic signature systems. A new Regulation for identification and electronic signature is foreseen to be adopted in the next months to enable the use of ID in the cloud.
Does the patient have the right to know who has accessed to his/her EHRs?	*Art 14* RD 3/2010	Yes The National Security Scheme entails minimum security requirements listed under Art 11 of the RD 3/2010 under different headings including the management of staff which requires that in order to correct or ensure accountability and control of access each user with access right to the information system must be **uniquely identified** so that it is known at all times, who gets access rights and of what kind or who has performed a certain activity.

Questions	Legal reference	Detailed description
Is there an obligation on health professionals to update EHRs?	Art 15(1) RD 2002	The clinical history incorporates information deemed crucial for the accurate and **updated** knowledge of the patient health status. The Spanish legislation considers that it is the right of the patient to have a record, in writing or in the most appropriate support, of the information obtained during its care process carried out by health professionals.
	Art 15(2) RD 2002	The clinical history's main purpose is to facilitate healthcare, ensuring that data is recorded which would enable accurate and **updated** knowledge of patients' health status.
	Article 15(3) RD 2002	The updating of the information is the health professionals' responsibility. The RD 2002 states that the completion of the clinical history in relation to the direct patient care is the responsibility of the professionals involved in it.
	Art 17 (3) RD 2002	Health professionals have the duty to cooperate in creating and maintaining an orderly and sequential clinical documentation of patient care process.
	Art 23 RD 2002	Furthermore, health professional have the duty to complete the protocols, reports, statistics and other documents for administrative assistance in relation to the clinical processes they are involved in.
	Art 30 RD 38/2012 Basque Country	The Royal Decree 38/2012 of the Basque Country mirrors these provisions and states the obligation of health professionals to create and maintain clinical documentation well organised, truthful, updated, sequential and understandable, regardless the support it is in.
	In practice[40]	There is an obligation to keep health records of patients and update them accordingly in whatever format they are, paper or electronic. This is an obligation on doctors as the health information needs to be updated to ensure proper health care and treatments are proposed. The updating of the information is needed for traceability and procedural requirements. For the same reason, the whole sequence of health data should be available. For example, information on a patient's cholesterol level needs to cover longer periods rather than punctual situations in order to estimate the health problem and the adequate treatment. A common platform ensuring the minimum content and requirements in the EHRs regarding this type of information is needed.
Are there any provisions for accessing data on 'behalf of' and for request for second opinion?	Art 17 Law 41/2002	The right to access the patient's medical history may be exercised not only by the patient but also by a duly accredited representative.
Is there in place an identification code system for cross-border healthcare purpose?	*Art 23 RD 81/2014*	Identification of patients is based on the individual identification number. It is included in the ecard and has been provided to all citizens and residents in Spain. The health professionals do not have a specific identification unless the Autonomous Community has decided to provide them with one.

[40] Maravillas Izquierdo, Vice-Secretary General, Basic NHS Service Portfolio, Ministry of Health, Social Services and Equality. Interview 1st April 2014

Questions	Legal reference	Detailed description
		As described in previous sections, the EHRs includes references to coding systems of international character and that are used at European level such as the CIE (*Código Internacional de Enfermedades*) International Codes of Diseases.
	In practice[41]	A code for identifying the patient and ensuring access to EHRs enabling cross border health care is foreseen but not developed yet.
Are there any measures that consider access to EHRs from health professionals in another Member State?	Art 8(7) RD 81/2014	The health care provider shall ensure that the patient have access to a copy of the medical records enabling a continued health care to the patients seen or treated in Spain but coming from other Member States within the scope of cross-border healthcare.
	Art 5(3)a) and c) RD 81/2014	In order to promote continuity of care, the Spanish patient receiving healthcare in other Member States shall be granted health care by ensuring cooperation with those Member States in the exchange of information and providing electronic access to clinical documentation through information systems. Access to a copy of the clinical reports, results of diagnostic tests and therapeutic procedures is guaranteed. The cooperation with other Member States in the exchange of information will be carried out within the framework of the European network of electronic health and will be based on national, European and international standards for communications of the electronic Health Records or the electronic clinical history.
	Art 6(3) RD 81/2014	Similarly health care is guaranteed to patients from other Member States seen or treated in Spain. Access to a copy of the clinical reports, results of diagnostic tests and therapeutic procedures is guaranteed and electronic access to clinical documentation through information systems. The cooperation with other Member States in the exchange of information is carried out within the framework of the European network of electronic health and is based on national, European and international standards for communications of the electronic Health Records or the electronic clinical history. Both cases are subject to the provisions on data protection under Organic Law 15/1999 and law 41/2002.
	In practice[42]	Different Public Administrations in the same Autonomous Community do not always share access to the clinical history. Similarly not all Autonomous Communities have the capacity to share access to the EHRs. So doctors in Bilbao treating a patient from Madrid might not have access to his/her clinical history. Only few Member States may share access to the data / information in the clinical

[41] Maravillas Izquierdo, Vice-Secretary General, Basic NHS Service Portfolio, Ministry of Health, Social Services and Equality. Interview 1st April 2014

[42] Interview Doctor and Director of Ambulatory of Pais Vasco, 15.03.2014.
Interview Ministry of Health, 18.03.2014 – Juan Fernando Munoz

Questions	Legal reference	Detailed description
		history. A French national in a hospital in Madrid will be treated but doctors will not have access to his/her clinical history and the patient will receive the information of the clinical history on paper in order to ensure continuity of the treatment in France. Access is provided only within the epSOS project. Information and data on the EHRs are generally not shared between Member States yet.

2.5. Liability

2.5.1. Main findings

No medical liability is regulated in the Spanish system regarding specifically the use of EHRs. There is general liability within the framework of healthcare obligations. The General Health Law establishes that breaches of healthcare obligations are to be subject to appropriate administrative sanctions, prior investigation proceedings, without prejudice to any civil, criminal or other responsibilities. In cases where violations could constitute a crime, the administration will pass it on to the competent jurisdiction and shall not follow the disciplinary procedure until the judicial authority has issued final judgment. When the judicial authorities did not estimate that a crime existed, the Administration will continue the disciplinary proceedings based on the facts that the courts have considered proven.

Some of these obligations are related to the use of individual clinical history or EHRs. For example, and as we have already seen, under the Law 41/2002 the completion of the clinical history regarding the direct patient care will be the responsibility of the professionals involved in it. Health professional have the duty to cooperate in creating and maintaining an orderly and sequential clinical documentation of patient care process. Health professionals developing their activity individually are responsible for the management and custody of the documentation created.

Violations on the provisions of the RD 2002 are subject to sanctions established under Chapter VI Title I of Law 15/1986 on General Health, subject to civil, criminal liability or any applicable statutory responsibility.

According to the General Health Law, violations are classified as minor, serious and very serious, according to the criteria of health risk, profit made, intentionality, severity of health and social disruption caused, generalization of the offense and recidivism.

Breaches in health will be fined according to the following scale:

- Minor offenses, to 3,005.06 euros.
- Serious offenses, from 3005.07 to 15025.30 euros and can exceed that amount up to five times the value of the goods or services related to the infringement.
- Very serious offenses, from 15,025.31 to 601,012.10 euros, and may exceed that amount up to five times the value of the goods or services related to the infringement

Furthermore under the Spanish legislation on data protection, patients suffering injury or damage to their property or rights as a result to a breach of the provisions regarding data protection are entitled to compensation. In case of publicly owned files, liability is required under the law governing the liability regime of public administration. The data protection legislation recognises the right of rectification, cancellation and opposition to the person concerned. These rights are the basis for any action for liability.

Liability of professionals is regulated in general terms under RD 81/2014 which requires health professionals practicing in the field of private healthcare to sign an appropriate liability insurance, guarantee or other financial security to cover compensation for damage to persons caused during the assistance or services being provided. In the field of public health care, the health administration of each region may enter and maintain appropriate insurance contracts, guarantees or financial securities including both the civil liability of public health service and its employees. When requested by the patient, the health care professional is required to provide the relevant information regarding the insurance coverage for professional liability.

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?	*6th Additional provision of Law 41/2002*	No medical liability is regulated in the Spanish system regarding specifically the use of EHRs. There is general liability within the framework of healthcare obligations.
	Art 15(3) L 41/2002	Violations on the provisions of the Law 41/2002 are subject to sanctions established under Chapter VI Title I of Law 15/1986 on General Health, subject to civil, criminal liability or any applicable statutory responsibility.
	Art 17(3) L41/2002	Amongst other obligations required regarding the use of clinical records, Law 41/2002 establishes that the completion of the clinical history regarding the direct patient care will be the responsibility of the professionals involved in it.
	Art 17(5) L41/2002	Health professional have the duty to cooperate in creating and maintaining an orderly and sequential clinical documentation of patient care process. Health professionals developing their activity individually are responsible for the management and custody of the documentation created.
	Art 32 L 14/1986 General Health Act	Breaches of healthcare obligations will be subject to appropriate administrative sanctions, prior investigation proceedings, without prejudice to any civil, criminal or other responsibilities. In cases where violations could constitute a crime, the administration will pass it on to the competent jurisdiction and shall not follow the disciplinary procedure until the judicial authority has issued final judgment. When the judicial authorities did not estimate that a crime existed, the Administration will continue the disciplinary proceedings based on the facts that the courts have considered proven.
	Art 34 L 14/1986 General Health Act	Violations are classified as minor, serious and very serious, according to the criteria of health risk, profit made, intentionality, severity of health and social disruption caused, generalization of the offense and recidivism.

Questions	Legal reference	Detailed description
	Art 36 L 14/1986 General Health Act	Breaches in health will be fined according to the following scale: a) Minor offenses, to 3,005.06 euros. b) Serious offenses, from 3005.07 to 15025.30 euros and can exceed that amount up to five times the value of the goods or services related to the infringement. c) Very serious offenses, from 15,025.31 to 601,012.10 euros, and may exceed that amount up to five times the value of the goods or services related to the infringement
	Art 19 OL 15/1999	Patients suffering injury or damage to their property or rights as a result to a breach of the provisions regarding data protection are entitled to compensation. In case of publicly owned files, liability is required under the law governing the liability regime of public administration.
	Art 23 RD 1720/2007	The data protection legislation recognises the right of rectification, cancellation and opposition to the person concerned. These rights are the basis for any action for liability.
Can patients be held liable for erasing key medical information in EHRs?		At the moment patients do not have the possibility to modify the information in the EHR.
Can physicians be held liable because of input errors?		Not specific rules are established to cover this type of cases. However, they could be covered through the existing legislation if damages occur.
Can physicians be held liable because they have erased data from the EHRs?		No rules are adopted to cover this type of situation. . However, they could be covered through the existing legislation if damages occur.
Are hosting institutions liable in case of defect of their security/software systems?		No rules establish the liability of defect in security/software systems
Are there measures in place to limit the liability risks for health professionals (e.g guidelines, awareness-raising)?	Art 9 RD 81/2014 and Art 46 L 44/2003	Liability of professionals is regulated in general terms under RD 81/2014 which requires health professionals practicing in the field of private healthcare to sign an appropriate liability insurance, guarantee or other financial security to cover compensation for damage to persons caused during the assistance or services being provided. In the field of public health care, the health administration of each region may enter and

Questions	Legal reference	Detailed description
		maintain appropriate insurance contracts, guarantees or financial securities including both the civil liability of public health service and its employees. When requested by the patient, the health care professional is required to provide the relevant information regarding the insurance coverage for professional liability.
Are there liability rules related to breach of access to EHRs (e.g. privacy breach)?		No liability rules related explicitly to EHR.
Is there an obligation on health professionals to access EHRs prior to take a decision involving the patient?		No. Sometimes doctors might need to take a decision only based on the information provided by the patient.
Are there liability rules related to the misuse of secondary use of health data?		General rules for breaches of provisions imposing healthcare obligations would apply. For example, the obligation to limit the use of health data to the purposes foreseen would be applicable.

2.6. Secondary uses and archiving durations

2.6.1. Main findings

Archiving duration

The Spanish legislation does not provide for specific rules on archiving durations of health records in general or of EHRs in particular. The clinical histories are archived in the servers of the regional Public Health Service following the general security requirements such as keeping the information encrypted. Some Autonomous Communities might decide to archive at the level of the hospital and health centre or may decide to centralise the archiving system at the level of the regional Public Health Service. The Ministry does not have any information or access to the EHRs. The Ministry keeps the reference index to ensure knowledge management about where the information is.

There is no legislation about the periods for the archiving or maintenance of information in electronic or paper format. The general approach is that health information is kept even longer than 15 years from the entry of the data, to ensure the quality and continuity of treatment of the patient. According to the Law 41/2002 on the autonomy of the patient, the clinical history is a tool primarily to ensure adequate health care for the patient. Health professionals performing the diagnosis or treatment of the patient have access to the medical history to ensure the proper healthcare. The archiving of the data needs to be done in respect of this role of the clinical history and in support of the health professionals' function to provide health care. The Regulation implementing the OL 15/1999 on Data Protection requires the personal data to be deleted when it is no longer necessary or relevant for the purpose for which it was collected or recorded. No other legislation specifies what is considered necessary.

However, it may be decided to apply similar periods to those required for auditing (around 5 years). According to the Law 41/2002 on the patient's autonomy and right to documentation, every health centre is required to archive the patients' clinical history in whatever format they are kept (paper, audio-visual, digital…) so that the safety, correct conservation and recuperation of the information are guaranteed. They are required to keep clinical documentation under conditions which ensure its correct and safe maintenance, even if not in the original support. It should ensure the proper patient care during the appropriate time according to each case and at least **during five years** from the date of discharge of each care process. More detail information is provided at regional level. For example, Art 19 of RD 38/2012 of the Basque Country refers to the need for archiving the clinical information for a **minimum of 5 years** from the end of the care process.

There are certain rules with regards to the documents that provide jointly information on the individual health clinical history and the personal administrative data. For example, certain procedures have changed and, for example no requests for specific tests with information on the personal data and the reasons for the request can be sent by fax.

The Organic Law 15/1999 on Data Protection foresees as well the need to keep the data for the time required by a case of liability or legal obligation or the performance of a contract. According to this Law, once this period is completed, the data can only be preserved if dissociated. Further implementing regulations are needed to establish the procedure to determine, exceptionally, the maintenance of certain data due to historical, statistical or scientific value in accordance with specific legislation. The General Data Protection Register established by the Law on Data Protection must contain the electronic files owned by the Public Administrations and those electronic files owned by private body.

The Law on citizen's rights to electronic access to public services requires Public administrations to create electronic registers for the receipt and referral of applications, documents and communications. The electronic registers may accept standardized electronic documents related to services, procedures

and formalities as specified in the rule for the creation of the registry. In each Public Administration there has to be a register system enabling reception of all kinds of applications, documents and communications to that Public Administration. The Central Public Administration is responsible for guaranteeing the interconnection between all register offices and the sharing of information electronically. For example, information in the registry of the Social Security System regarding the personal administrative data or information on the status of functionality of the individual is shared with the Health services but no health data is shared with the Central Public Administrations.

According to this general Law 11/2007, all electronic documents used in administrative activities may be stored electronically. Electronic documents containing administrative acts affecting rights or interests of individuals must be kept in electronic supports, whether in the same format in which the document was created or in any other to ensure the identity and integrity of the information. The support systems, in which the documents are stored, must ensure the integrity, authenticity, confidentiality, quality, protection and preservation of the stored documents. In particular, they will ensure the identification of users and control in the access as well as compliance with the data protection legislation.

There is no obligation in Spanish legislation to destroy health data. However, the Royal Decree 4/2010 requires public authorities to take the necessary technical and organizational measures to ensure interoperability in the recovery and preservation of electronic documents throughout their life cycle. Such measures include

- The definition of period of preservation of records according to the legislation, administrative rules and legal obligations that may apply in each case.
- If the result of the assessment procedure so establish it, the information would be deleted or where appropriate, physically destroyed according to the law that is applicable, leaving record or such deletion.

At a regional level more detail rules may be adopted. For example, Art 21 of RD 38/2012 of the Basque Country refers to the situations where it may be decided to destroy a document. Specifically 10 years after the death of a patient, the documents may be destroyed or any clinical history that has remained without any movement for more than 15 years. The same provision establishes the need for keeping back-up copies to ensure the conservation of the necessary information.

Secondary use

In addition to this health care function, access to the clinical history is possible also for other purposes such as for judicial, epidemiological, public health, investigation/research or education/teaching but within the framework of the rules and provisions of the OL 15/1999 on data protection and the General Health Act 14/1986. The legislation on Data protection requires that the personal data processed is not used for purposes incompatible with those for which the data were collected. However, it does not consider incompatible with those purposes the processing of data for historical, statistical or scientific purposes. This is confirmed by the Law 44/2003 on the organisation of the sanitary professions which states that the whole structure of the healthcare system is required to be available to be used for health research and for teaching.

The Regulation developing the OL 15/1999 further establishes that the personal data may only be collected for compliance with the specific, explicit and legitimate purposes of the controller. The personal data processed shall not be used for purposes incompatible with those for which the data were collected.

The Law 42/2002 requires that the access to medical records for judicial, epidemiological, public health, investigation/research or education/teaching purposes is carried out preserving the personal identification data of the patient, keeping it separate from those of clinical health character so that as a rule the anonymity is secured, unless the patient has consented to not separate them.

Exempted from this rule are those cases where the investigations by judicial authority would considered it essential the unification of the identifying data with the health and medical records. In those cases the information will be available to the extent the judges and courts request it in each relevant process. Access to data and medical record documents is limited strictly to the specific purposes of each case.

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?	Art 8(6) RD1720/2007	There are not rules on archiving durations of EHR. The clinical histories are archived in the servers of the regional public health service following the general security requirements including the need for keeping the information encrypted. Some Autonomous Communities might decide to archive at the level of the hospital or the health centre instead or in complement to the archiving system by the regional public health service.
	Art 14(2) Law 41/2002	The Ministry does not have any information or access to the EHRs. The Ministry keeps the reference index to ensure knowledge management about where the information is.
	Art 17 Law 41/2002	There is no legislation about the periods for the archiving or maintenance of information in electronic or paper format. The general approach is that health information is kept even longer than 15 years. Similar periods to those required for auditing are sometimes applied.
	Art 4(5)(6) LO 15/1999	However, there are certain rules with regards to the documents that provide jointly information on the individual health clinical history and the personal administrative data. For example, certain procedures have changed and, for example no requests for specific tests with information on the personal data and the reasons for the request can be sent by fax[43].
	Art 39 OL 15/1999	The Regulation implementing the OL 15/1999 on Data Protection requires the personal data to be deleted when it is no longer necessary or relevant for the purpose for which it was collected or recorded. Therefore they may be processed to enable the right to access them whilst cancellation is not applicable.
	Art 24 L 11/2007	They may be kept for the time required by a case of liability or legal obligation or the performance of a contract. Having completed the period, the data can only be preserved after their dissociation, Every health centre is required to archive the patients' clinical history in whatever format they are kept (paper, audio-visual, digital…) so that the safety, correct conservation and recuperation of the information are guaranteed. Healthcare facilities are required to keep clinical documentation under conditions which ensure its correct and safe maintenance, even if not in the original support. It should ensure the proper patient care during the appropriate time according to each case and at least during **five years** from the date of discharge of each care process. The Data Protection Organic Law requires the personal data to be deleted when it is no

[43] Interview Doctor and Director of Ambulatory of Pais Vasco, 15.03.2014

Questions	Legal reference	Detailed description
		longer necessary or relevant for the purpose for which it was collected. Regulations shall establish the procedure to determine, exceptionally, the maintenance of certain data due to historical, statistical or scientific value in accordance with specific legislation. The General Data Protection Register established by the Law on Data Protection must contain the electronic files owned by the Public Administrations and those electronic files owned by private body. The Public administrations will create electronic registers for the receipt and referral of applications, documents and communications. The electronic registers may accept standardized electronic documents related to services, procedures and formalities as specified in the rule for the creation of the registry. In each Public Administration there will be a register system enabling reception of all kinds of applications, documents and communications to that Public Administration. The General Public Administration is responsible for guaranteeing the interconnection between all register offices and the sharing of information electronically. In practice, the information in the registry of the Social Security System regarding the personal data or information on the functionality of the individual is shared with the Health services or Centres but no health data is shared with Public administrations. All electronic documents used in administrative activities may be stored electronically. Electronic documents containing administrative acts affecting rights or interests of individuals must be kept in electronic supports, whether in the same format in which the document was created or in any other to ensure the identity and integrity of the information. The support systems, in which the documents are stored, must ensure the integrity, authenticity, confidentiality, quality, protection and preservation of the stored documents. In particular, they will ensure the identification of users and control in the access as well as compliance with the data protection legislation.
	Art 31 L 11/2007	
	Art 19 of RD 38/2012 of the Basque Country	More detail information is provided at regional level. For example, Art 19 of RD 38/2012 of the Basque Country refers to the need for archiving the clinical information for a minimum of 5 years from the end of the care process.
Are there different archiving rules for different providers and institutions?		No
Is there an obligation to destroy (…) data at the end of the archiving duration or in case of closure of the EHR?	Art 21 RD 4/2010	However the Royal Decree 4/2010 requires public authorities to take the necessary technical and organizational measures to ensure interoperability in the recovery and preservation of electronic documents throughout their life cycle. Such measures include • The definition of period of preservation of records, by the relevant commission, according to the legislation, administrative rules and legal obligations that may apply in each case. • If the result of the assessment procedure so establish it, the information would be deleted or where appropriate, physically destroyed according to the law that is

Questions	Legal reference	Detailed description
		applicable, leaving record or such deletion. At a regional level more detail rules may be adopted. For example, Art 21 of RD 38/2012 of the Basque Country refers to the situations where it may be decided to destroy a document. Specifically 10 years after the death of a patient, the documents may be destroyed or any clinical history that has remained without any movement for more than 15 years. The same provision establishes the need for keeping back-up copies to ensure the conservation of the necessary information.
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?		No
Can health data be used for secondary purpose (e.g. epidemiological studies, national statistics...)?	Art 16 L41/2002 Art 11 L 44/2003 Art 4(2) LO 15/1999 Art 8 RD 1720/2007	According to the law on the autonomy of the patient, the clinical history is a tool primarily to ensure adequate health care for the patient. Health professionals from the center performing the diagnosis or treatment of the patient have access to the medical history of this fundamental instrument to ensure the proper healthcare. However, access to the clinical history is possible for judicial, epidemiological, public health, investigation/research or education/teaching but within the framework of OL 15/1999 on data protection and the General Health Act 14/1986. The whole structure of the healthcare system is required to be available to be used for health research and for teaching. The legislation on Data protection requires that the personal data processed is not used for purposes incompatible with those for which the data were collected. However, it does not consider incompatible with those purposes the processing of data for historical, statistical or scientific purposes. For data protection purposes, the personal data may only be collected for compliance with the specific, explicit and legitimate purposes of the controller. The personal data processed may not be used for purposes incompatible with those for which the data were collected.
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)?	Art 16 L41/2002	Access to medical records for judicial, epidemiological, public health, investigation/research or education/teaching purposes requires preserving the personal identification data of the patient, keeping it separate from those of clinical health character so that as a rule the anonymity is secured, unless the patient has consented to not separate them. It is exempted from this rule those cases where the investigations by judicial authority would considered essential the unification of the identifying data with the medical records. In those cases the information will be available to what judges and courts request in each relevant process. Access to data and medical record documents is limited strictly to the specific purposes of each case.
Does the law say who will be entitled to use		

Questions	Legal reference	Detailed description
and access this data?		
Is there an opt-in/opt-out system for the secondary uses of eHealth data included in EHRs?	Art 16 L41/2002	Access to medical records for judicial, epidemiological, public health, investigation/research or education/teaching purposes requires preserving the personal identification data of the patient, keeping it separate from those of clinical health character so that as a rule the anonymity is secured, unless the patient has consented to not separate them.

2.7. Requirements on interoperability of EHRs

2.7.1. Main findings

The Royal Decree 4/2010 defines interoperability as the ability of information systems and procedures to which they provide support, to share data and to enable the exchange of information and knowledge between them.

Law 11/ 2007 of 22 June, on electronic access of citizens to public services, recognizes the need for interoperability and for common regulatory provisions adopted by the State. Interoperability is recognised within the partnership principle under Article 4 and in the fourth title on the cooperation between administrations to boost eGovernment. Article 40 requires the Sectoral Committee of eGovernment to ensure interoperability of systems and applications used by public administrations, as well as cooperation between public administrations to provide citizens with clear and up to date information. Article 41 requires public authorities to apply the necessary computer, technological and organizational measures, as well as security measures to ensure an adequate level of technical, semantic and organizational interoperability.

Article 42.1 establishes the National Interoperability Framework which includes a set of criteria and recommendations on safety, maintenance and standardization of the information, formats and applications to be taken into account by public authorities when making technology decisions to ensure interoperability. Art 43 establishes the development of a Network of public administrations that adopt the necessary measures to enable the interconnectivity between Public Administration's information systems and the exchange of information and services between them and with the network of the EU and Member States.

The key rules and standards on interoperability are mainly established under the Law 16/2003 on the cohesion and quality of the NHS and the Royal Decree 4/2010 regulating the National Interoperability Framework in the field of eGovernment. They are applicable to health data.

The Ministry of Health is in charge of creating the Health Information System to guarantee the availability of information and the exchange of data between different health administrations. The Inter-Territorial Committee of the National Health System is responsible for approving its objectives, content and technical requirements for the integration of the information. Individual health cards should be adapted, where necessary, to any standardization that may be established for all public administrations and within the European Union. The Institute for Health Information is responsible for collecting, processing and distributing information that meets the needs of the National Health System, based on the principles of transparency and objectivity of the information generated in accordance with guidelines established by the Interregional Council National Health System. The interoperability is also based on a system of reference services and centres which public authorities are required to guarantee all patients access to. The law 16/2003 establishes certain guarantees of quality of health systems and the establishment of national reference centers. The Inter-Territorial Council of the NHS, designates the reference services, their number and strategic location within the NHS, with a focus on a global planning in particular for those pathologies which require the concentration of resources for the diagnosis and therapeutic care with the aim to ensure quality, safety and efficiency. The Ministry of Health will accredit those reference services according to quality criteria and should reassess them periodically. The health care in reference centres should be funded through the National Health Cohesion Fund.

The National Interoperability Framework includes the criteria and recommendations for the security, standardization and storage of information, formats and applications that should be taken into account by public authorities to ensure an adequate level of organizational, semantic and technical interoperability of the data, information and services managed in the exercise of its competences.

The Royal Decree 4/2010 establishes the criteria and specific principles necessary to enable and promote the development of the interoperability in public administrations which apply to health data.

An important element is the development and maintenance of inventories of information, services, administrative bodies and register offices responding to specific coding systems. Each public administration will be responsible for creating and maintaining these inventories which should be linked to the Inventory of the General Public Administration.

The National Interoperability Framework will be developed through technical rules that would be complied with by public authorities and will cover issues such as the catalogue of Standards, electronic document with the minimum required metadata, digitization of documents, electronic signature policy or certificate and requirements for connection to the communications network of the Spanish public administrations. Furthermore specific instruments for interoperability will be developed such as an inventory of administrative procedures and services, semantic interoperability Centre of public administrations and a directory for free reuse of applications.

Public administrations will link their infrastructures and services with the infrastructure and services provided by the General Administration of the State in order to facilitate interoperability and sharing information and services among all public administrations. Public authorities shall take the necessary technical and organizational measures to ensure interoperability in the recovery and preservation of electronic documents throughout their life cycle. Such measures include:

- the definition of a document management policy for their treatment according to the specific rules and procedures used in their creation
- The use of an electronic index signed by the acting entity or body that ensures the integrity of electronic records and allow their recovery.
- The definition of period of preservation of records, by the relevant commission, according to the legislation, administrative rules and legal obligations that may apply in each case.
- The full and immediate access to documents through online consultation methods, document retrieval, copying or downloading online at original formats and printing paper documents that are needed
- Transfer of the records between different electronic sources for conservation purposes, in accordance with the provisions of the legislation so that they can ensure their conservation and recovery in the medium and long term.
- If the result of the assessment procedure so establish it, the information would be deleted or where appropriate, physically destroyed according to the law that is applicable, leaving record or such deletion.
- Implementation and control of document management, and its processing and storage in electronic archives or repositories staff.
- The documentation of procedures to ensure interoperability, treatment and control of electronic documents.

The National Interoperability Framework should be kept updated permanently. The interoperability of the system is based on an Agreement between the State and 15 Autonomous Communities that are interested in sharing data on the electronic clinical history.

Art 10 of Royal Decree 38/2012 of the Basque Country requires the competent department in the field of health to define technical requirements to facilitate the interoperability of information systems in relation to clinical reports in order to ensure compatibility of the clinical history of the whole NHS and in accordance with the relevant agreements of the Inter-Territorial Council of the NHS.

According to the information received, the different Autonomous Communities are in different stages to issue data on EHRs to other health professionals in other regions or receive it from them. The most advanced with the highest level of reports or information available to be shared with other Autonomous Communities and being able to receive or have access from other regions are La Rioja,

Baleares Islands, Valencia and Extremadura. They are also part of epSOS. The Basque Country is the only region that cannot share any data in their EHRs system but may receive access from others.

The key element for the interoperability of the EHRs is the ecard. However a difference needs to be draw between the interoperability within the system for health care between Member States and within the system under the Social Security Coordination Regulations where the European Health Card was developed. The Royal Decree 81/2014 provides for different coverage to patients that have access to health systems in other countries than to patients under treatment in different regions in the same country.

In relation to the operability with other Member States, the Spanish legislation requires individual health cards of the NHS to adapt to any new EU criteria of standardisation that would facilitate circulation of patients and improve health care at EU level.

Public administrations will preferably use the communications network of the Spanish public administrations to communicate among themselves. They will therefore connect to it through their interoperability nodes, so that the exchange of information and services is promoted between them, and the interconnection with the networks of the institutions of the European Union and other Member States is facilitated. The Red SARA provides such communication network of the Spanish public administrations.

The exchange of information is to be carried out according to Regulation EU 1024/2012 on administrative cooperation through the System of the Internal Market Information.

Article 4 of Royal Decree 81/2014 requires the cross border health care to be ensured on the basis of the principles of universality, high quality, equity and solidarity. Article 23 of the Royal Decree refers both to the European Network for eHealth aiming to Article 23 of Royal Decree 81/2014 refers both to the European Network for eHealth aiming to promote cooperation and exchange of information with other Member States. The Ministry of Health will participate in the network through a nominated national authority responsible for eHealth. The agencies of the Spanish network of evaluation agencies for the evaluation of health technologies will participate in the network.

The law does not consider interoperability with Member States in detail yet. However Spain is an active member of the epSOS project providing data on about 7 million of patients from certain pilot regions (i.e. Baleares, Extremadura, La Rioja, Valencia) but only 40 to 50 health centres in touristic areas. This project is based on agreements for access and sharing of information.

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?	*Law 11/ 2007*	Law 11/ 2007 of 22 June, on electronic access of citizens to public services, recognizes the need for interoperability and establishes the obligation for the public authorities to develop interoperability based on common regulatory provisions adopted by the State. Interoperability is recognised within the partnership principle under Article 4 and in the fourth title on the cooperation between administrations to boost eGovernment. It is applicable to eHealth. Article 40 requires the Sectoral Committee of eGovernment to **ensure interoperability** of systems and applications used by public administrations, ensure cooperation between public administrations to provide citizens with clear and up to date information. Article 41 requires public authorities to apply the necessary **technological, organizational and security measures** to ensure an adequate level of **technical, semantic and organizational interoperability**. Article 42.1 establishes the **National Interoperability Framework** which includes a set of criteria and recommendations on safety, maintenance and standardization of the information, formats and applications to be taken into account by public authorities when making technology decisions to ensure interoperability Art 43 establishes the development of a Network of public administrations that adopt the necessary measures to enable the interconnectivity between Public Administration's information systems and the exchange of information and services between them and with the network of the EU and Member States.
	RD 4/2010	Definition of interoperability: Interoperability is the ability of information systems and procedures to which they provide support, to share data and to enable the exchange of information and knowledge between them. The system in place to ensure interoperability is:
	Art 56 L16/2003	The Ministry of Health is in charge of creating the **Health Information System** to guarantee the availability of information and the exchange of data between different health administrations. The Inter-Territorial Committee of the National Health System is responsible of approving its objectives, content and technical requirements for the integration of the information. It is designed to answer the needs of health authorities, health professionals, citizens and health associations. The Ministry of Health is in charge of providing the information system with a **secure network of communications** that guarantees the protection in the exchange of health data.

Questions	Legal reference	Detailed description
		This network will use the common communication infrastructure used by the Public Administrations linking all Autonomous Communities. The Ministry of Health coordinates the mechanism for **the electronic exchange of health clinical and individual data** to allow both patients and professionals involved in health care accessing the medical records that are strictly necessary to ensure the quality of the care and the confidentiality and integrity of the information. It shall establish a procedure that enables the electronic exchange of information as legally required for the exercise of the competences by public authorities. The exchange of information needs to comply with data protection provisions under Law 15/1999 and Law 41/2002.
	Art. 57 L16/2003	The access to the Spanish Health System is based on the **individual ehealth card**, as an administrative document which certifies the holder's data. The card must incorporate the technical devices to store basic information and allow that reading and checking the data is technically possible in the whole State and all public administrations. For this, the Ministry of Health in collaboration with the Autonomous Communities and other competent public authorities, is in charge of establishing the necessary requirements and standards. The Ministry of Health is responsible for the development of the **database** to collect basic information about residents who benefit from the NHS enabling the creation of the **unique personal identification code**.
	Art 58 L16/2003	The **Institute for Health Information** is responsible for collecting, processing and distributing information that meets the needs of the National Health System, based on the principles of transparency and objectivity of the information generated in accordance with guidelines established by the Interregional Council National Health System. It will also collect data from other sources, both national and international, in order to complement the inherent information to the National Health System, enabling the establishment of correlations and to facilitate comparability with other field areas. The Institute shall ensure the integrity and security of trusted data and guarantee personal privacy in accordance with Law 15 /1999.
	Art 60 L 16/2003	The **Agency for the Quality of the National Health System** is created under the Ministry of Health in order to ensure the development and maintenance of the elements of quality infrastructure for the NHS.
	Art 63 L 16/2003	The **Observatory of the National Health System** is an agency of the Ministry of Health to provide an ongoing analysis of the National Health System as a whole, by comparing the health services of the autonomous communities in the field of organisation, provision of services, health management and results. This observatory identified that the Autonomous

Questions	Legal reference	Detailed description
		Communities had developed different electronic health systems that were not interoperable.
Are there any specific rules/standards on the interoperability of EHR?	Art 57 L 16/2003	Individual health cards should be adapted, where necessary, the standardization can be established for all public administrations and within the European Union.
	Art. 1 RD 4/2010	The National Interoperability Scheme include the criteria and recommendations for the security, standardization and storage of information, formats and applications that should be taken into account by public authorities to ensure an adequate level of organizational, semantic and technical interoperability of the data, information and services managed in the exercise of its competences. The RD 4 /2010 establishes the criteria and recommendations, together with the specific principles necessary to enable and promote the development of the interoperability in public administrations.
	Art 9 RD 4/2010	An important element is the development and maintenance of inventories of information, services provided, administrative bodies and register offices responding to specific coding systems. Each public administration will responsible for creating and maintaining these inventories which should be linked to the Inventory of the General Public Administration.
	Art 11 RD 4/2010	The Public Administrations will use open standards and complementary standards that are widely used by citizens.
	Art 12 RD 4/2010	Public administrations will link their infrastructures and services with the infrastructure and services provided by the General Administration of the State in order to facilitate interoperability and sharing information and services among all public administrations.
	Art 21 RD 4/2010	Public authorities shall take the necessary technical and organizational measures to ensure interoperability in the recovery and preservation of electronic documents throughout their life cycle. Such measures include • the definition of a document management policy for their treatment according to the specific rules and procedures used in their creation • The use of an electronic index signed by the acting entity or body that ensures the integrity of electronic records and allow their recovery. • The definition of period of preservation of records, by the relevant commission, according to the legislation, administrative rules and legal obligations that may apply in each case. • The full and immediate access to documents through online consultation methods, document retrieval, copying or downloading online at original formats and printing paper documents that are needed • Transfer of the records between different electronic sources for conservation purposes, in accordance with the provisions of the legislation so that they can ensure their

Questions	Legal reference	Detailed description
		conservation and recovery in the medium and long term. • If the result of the assessment procedure so establish it, the information would be deleted or where appropriate, physically destroyed according to the law that is applicable, leaving record or such deletion. • Implementation and control of document management, and its processing and storage in electronic archives or repositories staff. • The documentation of procedures to ensure interoperability, treatment and control of electronic documents.
	Art 22 RD 4/2010	The National Interoperability Framework should be kept updated permanently.
	First Additional provision RD 4/2010	The National Interoperability Framework will be developed through technical rules that would be complied with by public authorities and will cover issues such as the catalogue of Standards, electronic document with the minimum required metadata, digitization of documents, electronic signature policy or certificate and requirements for connection to the communications network of the Spanish public administrations. Furthermore specific instruments for interoperability will be developed such as an inventory of administrative procedures and services, semantic interoperability Centre of public administrations and a directory for free reuse of applications. The interoperability applies as well for the use of Reference Centres between regions but also at EU level: Requires public authorities to guarantee all patients access to references services and centres.
	Art 24(2) L 16/2003 Art 28 L 16/2003	This provision establishes certain guarantees of quality of health systems and the establishment of national reference centers. The Inter-Territorial Council of the NHS, designates the reference services, their number and strategic location within the NHS, with a focus on a global planning in particular for those pathologies which require the concentration of resources for the diagnosis and therapeutic care with the aim to ensure quality, safety and efficiency. The Ministry of Health will accredit those reference services according to quality criteria and should reassess them periodically. The health care in reference centres should be funded through the National Health Cohesion Fund.
	Art 10 of RD 38/2012 of the Basque Country	The interoperability of the system is based on an Agreement between the State and 15 Autonomous Communities that are interested in sharing data on the electronic clinical history. For example, Art 10 of Royal Decree 38/2012 of the Basque Country requires the competent department in the field of health to define technical requirements to facilitate the interoperability of information systems in relation to clinical reports in order to ensure compatibility of the clinical history of the whole NHS and in accordance with the relevant agreements of the

Questions	Legal reference	Detailed description
		Inter-Territorial Council of the NHS.
	In practice[44]	According to the information received, the different Autonomous Communities are in different stages to issue data on EHRs to other health professionals in other regions or receive it from them. The most advanced with the highest level of reports or information available to be shared with other Autonomous Communities and being able to receive or have access from other regions are La Rioja, Baleares Islands, Valencia and Extremadura. They are also part of epSOS. The Basque Country is the only region that cannot share any data in their EHRs system but may receive access from others. The key element for the interoperability of the EHRs is the ecard. However a difference needs to be draw between the interoperability within the system for health care between Member States and within the system under the Social Security Coordination Regulations where the European Health Card was developed. The Royal Decree 81/2014 provides for different coverage to patients that have access to health systems in other countries than to patients under treatment in different regions in the same country.
Does the law consider or refer to interoperability issues with other Member States systems?	RD 81/2014	Article 4 of the Royal Decree 81/2014 refers to the cross border health care should be ensured on the basis of the principles of universality, high quality, equity and solidarity.
	Art 5(3) RD 81/2014	In order to promote continuity of care, the Spanish patient receiving healthcare in other Member States shall be granted health care by ensuring cooperation with those Member States in the exchange of information and providing electronic access to clinical documentation through information systems. Access to a copy of the clinical reports, results of diagnostic tests and therapeutic procedures is guaranteed. The cooperation with other Member States in the exchange of information will be carried out within the framework of the European network of electronic health and will be based on national, European and international standards for communications of the electronic Health Records or the electronic clinical history.
	Art 6(3) RD 81/2014	Similarly health care is guaranteed to patients from other Member States seen or treated in Spain. Access to a copy of the clinical reports, results of diagnostic tests and therapeutic procedures is guaranteed and electronic access to clinical documentation through information systems. The cooperation with other Member States in the exchange of information is carried out within the framework of the European network of electronic health and is based on national, European and international standards for communications of the electronic Health Records

[44] Juan Fernando Munoz, Vice Director General IT, Ministry of Health. Phone interview on 19/03/2014.
Maravillas Izquierdo, Vice-Secretary General, Basic NHS Service Portfolio, Ministry of Health, Social Services and Equality. Interview 1st April 2014.
Arturo Romero Gutiérrez, Director Project HCDSNS, Vice-direction general for Health Information and Innovation, Ministry of Health, Interview 16.04.2014

Questions	Legal reference	Detailed description
		or the electronic clinical history. Both cases are subject to the provisions on data protection under Organic Law 15/1999 and law 41/2002.
	Art 8 RD 81/2014	The health care professional shall ensure that the patient have access to a copy of the medical records enabling a continued health care to the patients seen or treated in Spain but coming from other Member States within the scope of cross-border healthcare. This provision read in relation to Articles 5 and 6 means that the patient would receive the information in electronic format when that is possible both in Spain but also for the other Member State.
	Art 23 RD 81/2014	Article 23 and refer both to the European Network for eHealth aiming to promote cooperation and exchange of information with other Member States. The Ministry of Health, will participate in the network and nominate the national authority responsible for eHealth. The agencies of the Spanish network of evaluation agencies for the evaluation of health technologies will participate in the network.
	Additional Provision of RD 183/2004	The individual health cards of the NHS must adapt to any new EU criteria of standardisation that would facilitate circulation of patients and improve health care at EU level.
	Art 13 RD 4/2010	Public administrations will preferably use the communications network of the Spanish public administrations to communicate among themselves. They will therefore connect to it through their interoperability nodes, so that the exchange of information and services is promoted between them, and the interconnection with the networks of the institutions of the European Union and other Member States is facilitated.
	Art 16(2) Proposal for Royal Decree on the State Registry of Health Professionals	The exchange of information is to be carried out according to Regulation EU 1024/2012 on administrative cooperation through the System of the Internal Market Information.
	In practice[45]	The law does not consider interoperability with Member States in detail yet. However Spain is an active member of the epSOS project providing data on about 7 million of patients from certain pilot regions (i.e. Baleares, Extremadura, La Rioja, Valencia) but only 40 to 50 health centres in touristic areas. This project is based on agreements for access and sharing of information.

[45] Juan Fernando Munoz, Vice Director General IT, Ministry of Health. Phone interview on 19/03/2014.

2.8. Links between EHRs and ePrescriptions

2.8.1. Main findings

Under the Spanish system the prescription (including the eprescription) must be complemented through a patient information sheet, in which the information is collected about the treatment necessary to facilitate proper use of prescribed drugs or pharmaceutical products. The prescriber must record on the prescription and the information sheet the personal identification number of the patient, reflected in their individual health card, assigned by the competent Health Administration.

The EHRs are integrated with the eprescription both for prescription and for its dispense. According to the legislation the ecard is linked to the EHR. The ecard, linked to the EHRs, provides the information on the eprescription requested by the health professional. The ecard provides access to the EHRs partially or totally according to the competences of the health professionals. The pharmacy will have access to the section of the EHRs related to the prescription and to the information regarding whether it has been already distributed to the patient or not. The prescription can be dispensed in any pharmacy within the same Autonomous Community but not always outside it yet.

In Spain every patient has EHRs of some sort. The ePrescription is normally linked to the EHRs. However some prescriptions are still handed over on paper. Furthermore, doctors might issue prescriptions to ensure continuity of treatment or answer a patient's request on the basis of the information provided by the patient without having access to EHRs. For example under Article 3 and 5 of Royal Decree 1718/2010 as modified by Royal Decree 81/2014 the eprescription should include the reference to the personal identification code in the health card which will enable access to the EHRs if the systems are in place.

However, the eprescription and the ecard are not 100% linked yet. A doctor may issue a prescription or eprescription without accessing the EHRs to ensure the continuity of health care or treatment on the basis of the information provided by the patient.

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?	*Art 3 RD 1718/2010 as modified by RD 81/2014*	The EHRs and the eprescription are linked but the HER is not a precondition for ePrespription which is less broadly established. Under the Spanish system the prescription (including the eprescription) must be complemented through a patient information sheet, in which the information is collected about the treatment necessary to facilitate proper use of prescribed drugs or pharmaceutical products. The prescriber must record on the prescription and the information sheet the personal identification number of the patient, reflected in their individual health card, assigned by the competent Health Administration. The EHRs are integrated with the eprescription both for prescription and for its dispense. According to the legislation the ecard is linked to the EHR. The ecard, linked to the EHRs, provides the information on the eprescription requested by the health professional. The ecard provides access to the EHRs partially or totally according to the competences of the health professionals. The pharmacy will have access to the section of the EHRs related to the prescription and to the information regarding whether it has been already distributed to the patient or not. The prescription can be dispensed in any pharmacy within the same Autonomous Community but not always outside it yet.
Can an ePrescription be prescribed to a patient who does not have an EHR?		In Spain every patient has EHRs of some sort. The ePrescription is normally linked to the EHRs. However some prescriptions are still handed over on paper. Furthermore, doctors might issue prescriptions to ensure continuity of treatment or answer a patient's request on the basis of the information provided by the patient without having access to EHRs.

Questions	Legal reference	Detailed description
	Art 3 and 5 RD 1718/2010 as modified by RD 81/1014	For example under Article *3 and 5 of Royal Decree 1718/2010 as modified by Royal Decree 81/2014 the eprespection* should include the reference to the personal identification code in the health card which will enable access to the EHRs if the systems are in place.

- ***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?	*In practice*	In principle, doctors in the patient's region have access to the EHRs in order to issue the prescription. Pharmacists only have access to the section related to the prescription and specifically to those that are still active.
Can those health professionals write ePrescriptions without having access to EHRs?	*In practice*	However, the eprescription and the ecard are not 100% linked yet. A doctor may issue a prescription or eprescription without accessing the EHRs to ensure the continuity of health care or treatment on the basis of the information provided by the patient.

2.9. Other requirements

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

The insufficient institutional and regulatory frameworks as well as the reluctance of changing well-established practices and patient behaviours are challenges for the implementation of eHealth. In Spain, no challenges have been identified in relation to the Health data included in EHRs. While Autonomous Communities developed their own health systems and access to electronic records in different ways, there has been a harmonisation of minimum content that seems enough for sharing information amongst them.

The requirements on the institution hosting EHRs data are a competence of the Autonomous Communities. There is basic legislation on the management of data, archiving and consent of the patient that is generally applicable.

However the main barriers for the development of an eHealth integrated system in Europe seem to be linked to the patient consent. The future EU legislation on data protection could be considered a barrier for e health development[46].

Spanish interpretation within a correct transposition of the Directive on Data protection can be seen as a **good practice** as, being strict with the protection objective and security of systems, it includes the exception of data used for health purposes. It therefore includes the possibility to apply implicit consent for the transfer of health and personal data with some security requirements and with some restrictions. It is understood that the patient in consultation gives the consent for the EHRs to be created and accessed by health professionals. The consent is considered implicitly given by the patient's petition of a doctor's consultation, giving the right to the health professional to have access to the information even if the patient is not in consultation. The consent is not required to be explicit or in writing. Other health professionals may also have access without the need for explicit consent if they are authorised by the health centre or service. However the patient has access to information on the persons who have access to the EHRs enabling to act against that implicit consent. However exchange of information with EU Member States is not easy if they did not include the exception of health data or require explicit consent or consent in writing even for each consultation and health professional.

The new Regulation on Data Protection may turn the Spanish system impossible unless an opt-out for health issues with strong security control systems is integrated. A future new law on electronic identification and digital signature is currently being developed to enable consent easier technologically[47].

Regarding the creation, access to and update of EHRs, Spain has a barrier to overcome in relation to the behaviour and practice of health professionals regarding the use of personal electronic ID (already issued to most of the population) as secure identification for having access to EHRs.

The technology behind the security measures and, in particular, the electronic certificates both for patients and health professionals is expensive. The economic investment required for ehealth is a barrier[48].

An existing barrier in Spain is the lack of specific legislative and regulatory framework defining both: the liability and the archiving duration of EHRs[49].

[46] Juan Fernando Munoz, Vice Director General IT, Ministry of Health. Phone interview on 19/03/2014.
[47] Juan Fernando Munoz, Vice Director General IT, Ministry of Health. Phone interview on 19/03/2014.
[48] Juan Fernando Munoz, Vice Director General IT, Ministry of Health. Phone interview on 19/03/2014.
[49] Juan Fernando Munoz, Vice Director General IT, Ministry of Health. Phone interview on 19/03/2014.

Problems related to the interoperability, accessing and sharing health data with other regions or Member States even with similar security systems are a key challenge. However, the development of an interoperable system with the aim to integrate the electronic health systems of all Autonomous Communities could be considered an example of **good practice** in Spain. The system is still in development and currently 15 regions have accepted to be part of it. Further requirements on interoperability of EHRs with other Member States are being applied within the epSOS project where Spain is very active. Furthermore and based on this system, the integration between EHRs and ePrescriptions can also be seen as **good practice** in Spain. They are fully integrated within Autonomous Communities but not between them and the sharing of data and dispense of prescription in different regions will be applied in a near future maybe by end of 2015[50].

The lack of common European Platform providing an agreed upon minimum content for the EHRs appears to be a barrier for progress on the exchange of information and data related to EHRs for cross border situations. Indeed, the agreement reached on the minimum requirements for the eprescription under Article 15 bis) of Royal Decree 1718/2010 as modified by Royal Decree 81/2014 evidences the benefits that such a EU approach brings. The lack of common platform for EHRs is generating unnecessary burden and cost in EU Member States which have to develop their own systems and then negotiate bilaterally with other Member States to ensure their recognition. A common approach would help save time and resources at national level; the EU act would be justified given there is a need in all EU Member States[51].

For example, Article 20 Royal Decree 81/2014 and additional transitory provision modifying Article 15bis of Royal Decree 1718/2010, ensures the interoperability of prescriptions issued in different regions and any other EU Member State on the basis of a minimum content agreed upon at EU level. This level of harmonization should be reached for the content of EHRs.

The minimum requirements established by the EU legislation and included in the Spanish legislation regarding prescriptions for medicines for human use whose marketing has been authorized by the Spanish Agency for Medicines and Health Products, or under Regulation (EC) n . 726/ 2004 that have been created in another Member State for a given patient and subject to compliance with the provisions of Law 29/ 2006 of 26 July, on guarantees and rational use of medicines and health products are as follows:

- Patient Identification: Name (s) , name (in full , not just initials) and date of birth
- Authentication Recipe : Date of issue
- Identification of the prescribing healthcare professional : Name (s) , name (in full , not just initials) , professional qualifications , contact details (email and phone or fax, these international prefix) , business address (and member State) , and signature (written or digital, depending on the means chosen to issue the recipe)
- Identification of the drug, medication or sanitary product : Common name , as defined in Article 1 of Directive 2001/83/EC establishing a Community code relating to medicinal for human use ; trademark if it is a biological medicine and as considered necessary from a medical point of view and , if so, the recipe should briefly justify the trade name, dosage form, quantity, dose as defined in Article 1 of Directive 2001/83/EC.

Furthermore, need for EU action is needed to develop specific tools to facilitate information sharing between regions and health professionals. Stimulating professionals to share protocols would require measures at EU level to ensure compliance with internal market competition rules[52].

[50] Juan Fernando Munoz, Vice Director General IT, Ministry of Health. Phone interview on 19/03/2014.
[51] Maravillas Izquierdo, Vice-Secretary General, Basic NHS Service Portfolio, Ministry of Health, Social Services and Equality. Interview 1st April 2014
[52] Maravillas Izquierdo, Vice-Secretary General, Basic NHS Service Portfolio, Ministry of Health, Social Services and Equality. Interview 1st April 2014

The system of Reference Centres established under 2003 Act and designated under Royal Decree 1302/2006 of 10 November setting the procedural rules for the designation and accreditation of centres and units of reference within the National Health System, is generating discrimination problems in the treatment of patients depending on what region they live in. The discretionary power granted to the Autonomous Communities to decide on the centres once designated by the Inter-territorial Committee does not always enable patients to be referred to the reference Centres. Through Article 21 of the Royal Decree 81/2014 the national reference centres may belong to the European reference network. However, additional rules need to be adopted to ensure that all patients have the same rights for the best treatment possible[53]. The EU legislation should define how the interoperability system related to the reference centres in Europe works and how patients are allocated to the reference centres ensuring non-discriminatory treatment, in particular for rare pathologies.

[53] Maravillas Izquierdo, Vice-Secretary General, Basic NHS Service Portfolio, Ministry of Health, Social Services and Equality. Interview 1st April 2014