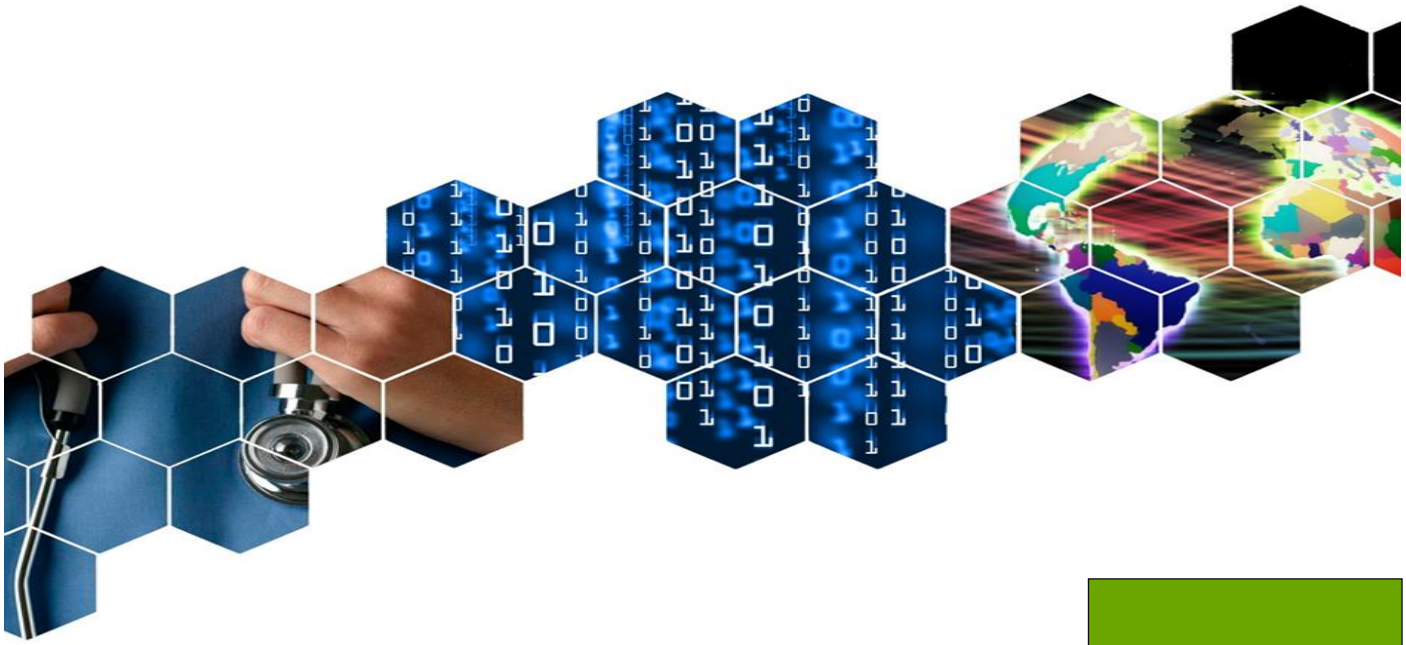
Overview of the national laws on electronic health records in the EU Member States and their interaction with the provision of cross-border eHealth services

Contract 2013 63 02

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

National Report for France



January 2014

milieu
Law & Policy Consulting

This Report has been prepared by Milieu Ltd for the Executive Agency for Health and Consumers under Contract 2013 63 02.

This report was completed by Adrien Lantieri and Florent Pelsy. 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. Please note that representatives of the following public organisations: ASIP (*Agence des systèmes d'information partagés de santé*) and CNIL *(Commission Nationale de l'Informatique et des Libertés*) were consulted for the completion of this report.

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 France

Personal Health Record (*dossier médical personnel*) (DMP) is the French national Electronic Health Record (EHR) scheme set in place by the Law n°2004-810.

It is the only EHR initiative in France that comprises the following four elements: the objective of creating a national framework, formalities on data-hosting institutions, modalities concerning the patient (consent and identification), and identification of health professionals.

After several rounds of negotiations and a first pilot phase in 2006, the DMP scheme was formally launched in 2011. It covers the entire French territory and is governed by national laws and regulations that apply uniformly throughout the French territory. As of December 2013, less than 1 per cent of the French population participated in the scheme, showing that the DMP is at an early development in France.

In September 2013, the Minister of Health (Marisol Touraine) has announced the launch of the 'DMP second generation' or 'DMP2' scheme. The modalities surrounding this modified scheme are still being discussed at the national level.

2. Summary of legal requirements applying to EHRs

France has not legislated on the type of data that can and may be included in DMP. The French legislation requires that information included in DMP must be 'necessary for the coordination of health-related care given to the care recipient' or be 'key elements of the stay' in a health institution.

However, the Public Health Code foresees the adoption of a Decree to determine the content and condition of access to the different information categories of the DMP. However, pending discussions on a DMP2 scheme any work on a Decree which will detail the DMP content is on hold.

The French legislation has adopted very detailed requirements applying to the institutions hosting EHRs data. Applicants must provide extensive information demonstrating that their hosting system is secure and sophisticated enough to ensure that the rules on EHRs (*e.g. consent, access, confidentiality*) are fulfilled and that health data is well protected especially considering the risk. Different commissions and committees are required to give their opinion on the application, and the authorisation is eventually granted by the Minister in charge of health issues. The authorisation procedure takes approximately eight months and authorisation is delivered for a period of three years.

A DMP is created by any health professional or administrative service of an hospital properly identified and authenticated, after informing the patient and obtaining his/her consent for the creation of the DMP. The consent does not need to be materialised on a piece of paper. Patients have a right to request modification, update or removal of information. A DMP can be created through calculation of the patient's National Health Service Login which is a number generated by a centralised system and that does not allow for identification of the person.

The access to the DMP is granted only to the patient and to health professionals provided they have received the patient's consent. Consent is presumed to have been delivered to the entire 'healthcare team' in the case of hospital. Upon creation of the DMP, the patient will receive a DMP login and password which s/he will use to create a One Time Password every time s/he seeks to access his/her DMP. Login onto a DMP and adding document in the DMP can be done by any health professional properly authenticated by the system. This authentication is done through specifically created and protected CPS cards or software certificates. Under emergency procedures, a DMP may be accessed

without a patient's prior consent. The patient can hide documents from his/her DMP, yet the physician regularly involved with the patient, the patient him/herself, and the author of a document can always access a document on the DMP, even though it has been hidden.

The national legislation does not set specific medical liability requirement related to the use of the DMP. As a result, the general rules on medical liability apply.

A DMP must be kept for a period of ten years after its closure. There are no specific rules on the secondary use of DMP health data (e.g. scientific research). The strict general rules on the secondary use of health data therefore apply. Discussions are on-going at the national level for reforming this system

The DMP provides a national infrastructure relying both on technical and semantic interoperability.

The DMP was designed to work together with the French pharmaceutical record. Although at the current stage of implementation they are not inter-connected.

3. Good practices

The French EHRs initiative has been launched since 2011 after nearly a decade of negotiations and different pilot phases. Since 2013, every pharmacists are required to feed into the French pharmaceutical record scheme.

The implementation of the DMP architecture is very thorough and more stringent than existing EU law on data privacy. In this sense, the DMP is in many ways considered and designed as being under the patient's control rather than the health professionals' file: the patient can in particular update, download, delete or hide documents from the DMP. However, safeguards have been set up for instance on the deletion of files, ensuring continuity of care. Moreover, the content of the DMP is open-ended and at the moment has not been regulated upon, as a result any document considered necessary for the coordination of health-related care can be updated to the DMP.

Consent with regard to the creation or access to a DMP is dematerialised, and arises after information has been delivered by a health professional. However, in emergency situations, the DMP may still be accessed using the 'ice-breaker' procedure. Consent is further considered delivered to an entire team in the context of hospitals.

Each health data hosting institution must be approved in a procedure that involves different stakeholders, ensuring all aspects are taken into account. Each secondary use of health data must be approved following a strict procedure whereby confidentiality of data is ascertained.

4. Legal barriers

Extensive control on EHRs by the patient can potentially void the aim of EHRs as a professional information tools, in particular the EHR does not indicate if a file is incomplete.

The current situation whereby the content of the DMP is potentially open-ended yet a Decree detailing what health data should be included is foreseen in the law, leads to uncertainty. An obstacle can arise in case of lack of harmonised content and categorisation requirements at the cross-border level.

The modalities surrounding consent concern the health professional in private practice or the 'medical team' within an hospital. It therefore ignores the cross-sectorial element often present in relation to medical care (e.g. e.g. ambulatory, medico-social, health and safety), and poses issues with regard to shared medical secrecy.This will evolve with the new law under preparation. France has moreover not regulated whether creating or updating a DMP can be considered part of the notions of 'medical act' or 'medical consultation' and issues of remuneration or financial incentives thereof.

Both the procedure for approval of health data institution or secondary use of data are seen as repetitive and complex, potentially altering the progress of public health.

The national legislation does not set specific medical liability requirement related to the use of the DMP. As a result, the general rules on medical liability apply which has been described by stakeholders as fostering reluctance of health professionals to use and develop the system.

Work on a register of health professionals and health-related semantics are ongoing. They are therefore not yet implemented. Whilst the DMP system is completely interoperable throughout France, it is not yet interoperable with the French pharmaceutical record, despite the law providing for their coordinated use.

CONTENTS

LIST OF ABBREVIATIONS

ASIP Santé	National Agency of health shared information systems
CPS	Card for Health Professionals
CNIL	National Commission on information technology and liberties
CNOM	Physicians' Order National Council
DP	Pharmaceutical Record
DMP	Personal Health Record
EHRs	Electronic Health Records
Electronic and liberty law	Law n°78-17 of 6 January 1978 on computers, files and freedoms
INS	National Health Login
OTP	One Time Password

1 GENERAL CONTEXT

1.1 EHR SYSTEMS IN PLACE

Personal Health Record (*dossier médical personnel*) (DMP) is the French national Electronic Health Record (EHR) scheme set in place by the Law n°2004-810 of 13 August 2004 on the national healthcare (*loi n°2004-810 du 13 Aout 2004 relative à l'assurance maladie*). It is the only EHR initiative in France that comprises the following four elements: the objective of creating a national framework, formalities on data-hosting institutions, modalities concerning the patient (consent and identification), and identification of health professionals. A wide range of other EHRs are being held in France by every health professionals and institutions. Whilst these EHRs include some of the aforementioned elements, they are however not designed for a shared access and are therefore not detailed in this study.

With regard to the national framework of the scheme, after a first and short pilot phase in 2006 and further negotiations between the State and different stakeholders, the DMP scheme was formally launched in 2011 in four regions (Alsace, Aquitaine, Franche-Comté and Picardie). The DMP scheme has since been generalised, now covering the entire French territory[1]. It is governed by national laws and regulations that apply uniformly throughout the French territory. As of 11 December 2013, nearly five hundred thousand DMPs have been created in France, for a population of over 65 million (less than 1 per cent) and 385 health institutions participate in the scheme[2]. This clearly shows that the DMP is at an early development in France and that it has not become a substitute to other health records (whether electronic or not). According to a stakeholder[3], 15-20% of the population that have been informed about DMPs and proposed to create one have refused, indicating that potentially 80% of the persons covered under the National Healthcare (*assurance maladie*) could possess a DMP once the scheme would have reached its full development. Moreover, an estimated 85% of the French population is in favour of the DMP[4].

Concerning issues relating to the patient, provided the individual has consented to the creation of a DMP[5], each patient covered under the National Healthcare (*assurance maladie*) can have a free DMP[6]. Any information whether diagnostic or therapeutic can be included in the DMP provided it is 'necessary for the coordination of health-related care given to the care recipient' or represents 'key elements of the stay' in a health institution[7] (see Section 2.1). The DMP scheme also foresees the inclusion of information that are not purely medical.

In its current architecture, the DMP has been designed as the patient's possession. Therefore, the patient has extended rights in relation to the management of his/her DMP, which has been qualified by a stakeholder as 'exorbitant prerogatives' (*prérogatives exorbitantes*)[8]. These include the possibility to

[1] For a map of the deployment by region of the DMP in France: http://www.dmp.gouv.fr/nb-es-par-region (last access January 2014). Also, see the Press release of the National Commission on information technology and liberties (*Commission Nationale de l'Informatique et des Libertés*) on the deployment of the DMP scheme on the entire French territory: http://www.cnil.fr/linstitution/actualite/article/article/la-cnil-autorise-le-deploiement-du-dossier-medical-personnel-sur-lensemble-du-territoire/ (last access January 2014)

[2] Information gathered from the DMP official website: http://www.dmp.gouv.fr/nb-es-par-region

[3] Interview with the Physicians' Order National Council (*Conseil de l'ordre national des médecins*) (CNOM) on 22nd January 2014.

[4] *Sondage BVA, Octobre 2013* (last access January 2014).

[5] Public Health Code (*Code de la santé publique*), Article L.1111-8.

[6] Public Health Code, Article L.1111-14.

[7] Public Health Code, Article L.1111-15.

[8] Interview with the National Commission on information technology and liberties (*Commission Nationale de l'Informatique et des Libertés*) (CNIL) on 24th January 2014. The notion of 'exorbitant prerogatives of common law' is used in French Public Law in relation to the administration and other public bodies which, by definition, use powers that are out of the ordinary scope of common law. The stakeholder was therefore indicating that the patient retains an incomparably high amount of rights with regard to his/her DMP.

update, hide (*droit au masquage*) and delete health data from the DMP as well as completely close the DMP (see Section 2.4). The DMP is therefore set up under the control of the patient, who grants access to it to the professionals and institutions s/he chooses (see Section 2.3).

The DMP scheme has been designed to be accessible through specific softwares (this access is only granted to health professionals), but also through a one-stop governmental website[9] whether the person seeking access is a patient or a health professional. In order to ensure security and continuity of the information stored and exchanged, the DMP scheme relies on three further important features:

- Approval of hosting institutions

Each health data hosting institution must be approved (*agrément*) ensuring security and confidentiality of DMP storage (see Section 2.2).

- Certification of health professionals

The certification of health professionals is twofold (NB. health professionals is a notion that comprises over 20 different categories in France, including physicians, nurses, chemists, etc.).

On one hand, physicians are delivered a Card for Health Professional (*Carte de Professionel de Santé*) (CPS). These cards are certificates issued by a government agency (*ASIP Santé*) (see below) which function as professional ID cards. They are required to establish secure connections with the DMP, allowing professionals to create a DMP, log on to the system and update data to a particular DMP. The use of the CPS as an identification tool is not restricted to the DMP and serves in a range of other medical activities (including for instance access to a physician's private practice's EHRs).

On the other hand, health professionals working in health institutions log into the DMP system under the responsibility of the head of this institution through a 'software certificate' delivered to each individual institution and provided by the ASIP Santé. Therefore, in the context of health institutions, access to the DMP is presumed to have been granted to the entire 'healthcare team' (see Section 2.4).

Finally, the law creating the DMP foresees the use of the CPS system or of an 'equivalent system' (*un dispositif équivalent*)[10]. To-date, no other such system has been set up in France for DMP purposes.

- Certification of patients: the DMP login system

Upon creation of a DMP, patients are provided with a National Health Service Login (*Identifiant National de Santé*) (INS) calculated through a specific algorithm. The INS is an identifier assigned to each patient covered under the national healthcare. It is used by health professionals to assign health information to the individual (see Section 2.3). The patient is further provided with personal DMP login and password details. Upon seeking access to their DMP, patients will obtain a One Time Password (OTP) through their personal DMP login and password (see Section 2.4)[11].

Therefore, the DMP offers a national infrastructure system using national standards that avoids any interoperability problems within France.

[9] Public Health Code, Article L.1111-19 provides for the creation of a 'DMP Portal' (*Portail du dossier medical personnel*). See the website at: http://www.dmp.gouv.fr/ (last access December 2013).
[10] Public Health Code, Article L.1110-4.
[11] Interview with the ASIP Santé on 20th January 2014.

1.2 INSTITUTIONAL SETTING

The main institutions involved in the development and deployment of the DMP scheme in France are:

- The Ministry of social affairs and health (*Ministère des Affaires sociales et de la Santé*)

The Ministry of social affairs and health is responsible for public health and the organisation of the healthcare system. As such, it is responsible for overseeing the implementation of the DMP scheme in France. It is in charge of monitoring the incremental development of the scheme throughout the territory by the National Agency of shared health information systems (see below). It is in particular in charge of delivering approval to data hosting institutions.

- The National Agency of shared health information systems (*Agence nationale des systèmes d'information partagés de santé*) (ASIP Santé)

The National Agency of shared health information systems is a public interest group, i.e. it is a non-profit legal entity regulated by public law filling out a mission of general interest (*intérêt public*). The Agency's purpose is to promote the development of shared information systems in the health and medico-social sectors, as well as to promote the quality of care services. Reformed in 2009[12], the ASIP Santé is in charge of the implementation of safety devices (identification, authentication, signature and encryption) required to protect the confidentiality of data and thus ensure the confidence of users of health information systems (CPS cards, global directories of health professional, etc.). The Agency continues to structure the national framework of shared health information systems, in consultation with all relevant stakeholders.

- The National Commission on information technology and liberties (*Commission Nationale de l'Informatique et des Libertés*) (CNIL)

The CNIL is a French independent administrative authority in charge of ensuring that information technology and electronic systems are at the service of citizens, and do not affect human identity, nor human rights, the right to privacy, as well as individual and public liberties. As the DMP scheme contains an element of personal data processing which may undermine the freedoms and privacy of the patient, it has been subject to authorisation by the CNIL as required by law[13]. The CNIL also issues opinions on hosting institutions' applications[14] and recommendations on other issues linked to the implementation of the DMP[15].

1.3 LEGAL SETTING AND FUTURE LEGAL DEVELOPMENT

The DMP was set up in 2004 through a specific law that modified existing provisions or incorporated new ones in the Public Health Code (*Code de la santé publique*)[16]. A number of provisions were also

[12] Order of 8 September 2009 approving the convention establishing a public interest group (*Arrêté du 8 septembre 2009 portant approbation de la convention constitutive d'un groupement d'intérêt public*).

[13] Article 25 of the Electronic and liberty law.
See for instance the latest authorisation related to the national implementation of the DMP scheme: Deliberation n°2010-449 of 2 December 2010 authorising the treatment of personal data by health professionals and health institutions necessary to the first phase of general implementation of the DMP scheme (*Délibération n°2010-449 du 2 décembre 2010 portant autorisation des traitements de données personnelles mis en œuvre par les professionnels et établissements de santé nécessaires à la première phase de déploiement généralisé du dossier médical personnel*) http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000023308516&fastReqId=1988022943&fastPos=10 (last access January 2014).

[14] A list of all approved hosting data institutions is available at : http://esante.gouv.fr/services/referentiels/securite/hebergeurs-agrees (last access January 2014).

[15] CNIL *conclusions du 20 Février 2007 sur l'utilisation du NIR comme identifiant de santé :* http://www.cnil.fr/fileadmin/documents/approfondir/dossier/NIR/Rapport%20NIR.pdf (last access January 2014).

[16] Law n°2004-810 of 13 August 2004 on the national healthcare (Loi n° 2004-810 du 13 août 2004 relative à l'assurance maladie).

included to this Code through regulatory instruments, starting from 2003[17]. At the time of writing the latest amendments to the Chapter on DMP under the Public Health Code were adopted in 2011[18].
These provisions of the Public Health Code often refer to compliance with the general principles on personal data protection set up in the 'Electronic and liberty law' of 1978 as last amended in 2002[19]. Moreover, they must be read in conjunction with the generic right given to patients to be informed of their health status pursuant to a law adopted in 2002[20].

It should be noted that, pursuant to Article 45 of the Medical Deontology Code, every physician must, at the patient's request or with his/her consent, transmit useful information and documents ensuring continuity of care to the physicians who participate in the patient's care management or those s/he intends to consult the documents. This principle applies to any health professional, whether working in private practice or in health institution.

In September 2013, following the publication of a report (*Rapport Cordier*)[21] and criticisms raised by the Court of Auditors of the Republic (*Cour des Comptes*), the Minister of Health (Marisol Touraine) has announced the launch of the 'DMP second generation' or 'DMP2' scheme. On that occasion, the Minister declared that 'the credibility of the tool and its full ownership by users and professionals depend on the speed of its implementation'. 'It must be reoriented […] as a tool for coordination. It will include new services such as sharing medical synthesis'. Moreover, a 'secure health messaging' service will be implemented in parallel[22]. Interview with a national stakeholder, who has detailed the medical professions' revendications, has shed light into the on-going discussions at the national level and what this DMP2 may entail[23]. The stakeholder believed that the DMP had not managed to deploy properly due to a lack of concrete and reasoned objectives with regard to its usage. In this light, the stakeholder recommended using a general opt-out procedure, whereby all the persons covered under the National Healthcare would have a DMP created and provided with login details (at the moment DMPs are created on an individual basis during consultations). This DMP will then be an empty-shell, and will be filled in around the patient's actual needs for coordination of health-related care received, rather than through a series of files that may or may not be used by different professionals in their specific sectors (problem of the segmentation of information rather than treatment). The objective should be one of coordination of health-related care as set out in the law, not of creating an all-in registry of medical history. The patient, duly informed, would always remain in control with regard to the creation and updating of folders within the DMP. Different folders would therefore be created as required by the patient's pathologies and needs, and, depending on the circumstances, access from one folder to the next would not be automatic but may be provided with the patient's consent (e.g. an oncologist requiring access to a patient's pulmonary records, and vice-versa). This system of interrelated folders (*système des vases communicants*) under the patient's control would be a further achievement towards patient's privacy that the current DMP scheme falls short of[24]. It would further ensure proper usage of the scheme as only folders that have a purpose would be open, and the situation with regard to health professional's liability issues would be clarified (non-disclosure by the patient would mean the patient bears responsibility, and, in other circumstances, a proper traceability of what information has or has not been shared). In this perspective, the stakeholder recommended developing the DMP scheme in priority for pregnant women, and for the child at birth, as well as for individuals

[17] Decree n°2003-462 of 21 May 2003 on the regulatory provisions of part I, II, and III of the Public Health Code (*Décret n° 2003-462 du 21 mai 2003 relatif aux dispositions réglementaires des parties I, II et III du code de la santé publique*).
[18] See for further information the list of legislation below in this sub-section.
[19] Electronic and liberty law.
[20] Law n° 2002-303 of 4 March 2002 on the rights of patients and the quality of the health system (*Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé, dite 'Loi Kouchner'*).
[21] The report is available at: http://www.social-sante.gouv.fr/IMG/pdf/RAPPORT-CORDIER.pdf (last access Janaury 2014).
[22] See for instance : http://esante.gouv.fr/actus/politique-publique/marisol-touraine-presente-sa-strategie-pour-la-e-sante, as well as http://www.fhf.fr/Actualites/Medecins/E-sante/Les-orientations-du-DMP-2e-generation-se-dessinent or http://www.pcinpact.com/news/82514-le-gouvernement-devoile-sa-feuille-route-en-matiere-d-e-sante.htm (websites last access January 2014).
[23] Interview with the CNOM on 22nd January 2014.
[24] At the moment, a health professional logging into a DMP has access to all information that has not been previously hidden (*masquage*) (more information in Section 2.1 and Section 2.4).

concerned with long-term pathologies (e.g. diabetes, cancer, etc.). This deployment method would reduce segmentation of data in relation purely to specialisation of the health profession. Furthermore, it would ensure quasi-immediate coordination of health-related care for the millions of patients in France where such coordination is required (including for instance with the ambulatory sector currently left out of the DMP scheme), and would result in a relatively rapid general use, and therefore actual development, of the scheme throughout the French territory.

List of relevant national legislation:

- Public Health Code (*Code de la santé publique*) as amended by :
  - Law n° 2011-940 of 10 August 2011 modifying provisions of the Law n°2009-879 of 21 July 2009 reforming the hospital organisation, *and on patients, health and territories (Loi n° 2011-940 du 10 août 2011 modifiant certaines dispositions de la loi n° 2009-879 du 21 juillet 2009 portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires)*
  - Law n°2009-879 of 21 July 2009 reforming the hospital organisation, and on patients, health and territories (*la loi n° 2009-879 du 21 juillet 2009 portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires)*
  - Law n°2004-810 of 13 August 2004 on the national healthcare (Loi n° 2004-810 du 13 août 2004 relative à l'assurance maladie)
  - Law n° 2002-303 of 4 March 2002 on the rights of patients and the quality of the health system (*Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé, dite 'Loi Kouchner')*
  - Decree 2007-960 on confidentiality of health data kept or transferred on electronic support *(Décret n°2007-960 du 15 mai 2007 relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique et modifiant le code de la santé publique)*
  - Decree n°2003-462 of 21 May 2003 on the regulatory provisions of part I, II, and III of the Public Health Code *(Décret n° 2003-462 du 21 mai 2003 relatif aux dispositions réglementaires des parties I, II et III du code de la santé publique)*

The Public Health Code contains most provisions related to the DMP scheme in France both in its legislative part and regulatory part. It provides for instance for the creation of the DMP scheme as well for the process under which data hosting institutions are to be approved.

- Code of Social Security (*Code de la sécurité sociale*) as amended by :
  - Law n°2004-810 of 13 August 2004 on the national healthcare (Loi n° 2004-810 du 13 août 2004 relative à l'assurance maladie)
  - Law n° 2002-303 of 4 March 2002 on the rights of patients and the quality of the health system (Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé, dite 'Loi Kouchner'

The Code of Social Security has been amended to reflect the principles and objectives of the DMP scheme, it moreover contains provisions relating to the right to privacy and secrecy applicable to health practices.

- Order of 8 September 2009 approving the convention establishing a public interest group (Arrêté du 8 septembre 2009 portant approbation de la convention constitutive d'un groupement d'intérêt public)

This Order provides for the creation of the ASIP Santé and as such contains the elements relating to its missions, including the implementation of the DMP scheme.

- Law n°78-17 of 6 January 1978 on computers, files and freedoms (loi n°78-17 of 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite 'Loi informatique et liberté') (Electronic and liberty law) as amended by :

- Law n° 2002-303 of 4 March 2002 on the rights of patients and the quality of the health system (Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé, dite 'Loi Kouchner')

This law provides for the creation of the CNIL and details its missions. This law also legislates on safeguards relating to keeping electronic files.

- Medical Deontology Code (*Code de déontologie médicale*)

The Medical Deontology Code sets the moral duties of the medical professions. This Code is now an integral part of the Public Health Code.

- Criminal Code (*Code Pénal*)

The Criminal Code includes provisions relating to the liability of individuals and companies.

2 LEGAL REQUIREMENTS APPLYING TO EHRS IN FRANCE

2.1 HEALTH DATA TO BE INCLUDED IN EHRS

2.1.1 Main findings

France has not legislated on the type of data that can and may be included in DMP.

The French legislation requires that information included in DMP must be 'necessary for the coordination of health-related care given to the care recipient' (*nécessaire à la coordination des soins de la personne prise en charge*) or be 'key elements of the stay' in an hospital (*les principaux éléments résumés relatifs à ce séjour*)[25]. However, the Public Health Code in its Article L.1111-21 foresees the adoption of a Decree to determine, inter alia, the content and condition of access to the different information categories of the DMP. Before being approved, this Decree will be subject to an opinion of the CNIL.

Indeed, the needs and demand of the DMP as a healthcare coordination tool was expected to be clarified during the early stages of the deployment of the DMP. The elaboration of a Decree detailing the DMP content was therefore understood as a second step in the deployment of the DMP. The 2010 CNIL authorisation to deploy the DMP[26] indeed required a revaluation of the legal framework after three years, in particular in relation to the content of the DMP. However, pending discussions on a DMP2 scheme, in particular concerning a possible reorientation towards long-term pathologies or senior citizens, the demand for the continuing deployment of the scheme is on hold at the CNIL, as is any work on a Decree which will detail the DMP content.

The DMP scheme is therefore at present regulated principally with regard to its architecture rather than its content.

Indications of the elements that are contained in the DMP can at the moment be extrapolated, inter alia, from the leaflet informing patients of the DMP: patient's past history (including elements such as diseases and surgery), allergy, medicine taken, records from physician consultation, hospitalisation, results from examination (x-ray photography, biological analysis)[27].

[25] Public Health Code, Article L.1111-15.
[26] CNIL Deliberation n°2010-449 of 2 December 2010 http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000023308516&fastReqId=1988022943&fastPos=10 (last access January 2014).
[27] See page 05 of the 'Patient leaflet' on the ASIP Santé website : http://esante.gouv.fr/sites/default/files/BrochurePatient_023%20(2).pdf (last access January 2014).

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?)	Public Health Code, Art. L.1111-15 (last amended in 2009)	Pursuant to Article L.1111-15 of the Public Health Code, the DMP must contain personal data gathered or produced whether diagnostic or therapeutic provided such information is 'necessary for the coordination of health-related care given to the care recipient'. Moreover, following a stay in a health institution, health professionals bring summaries of the key elements of the stay to the DMP. The Public Health Code in its Article L.1111-21 foresees the adoption of a Decree to determine the content and condition of access to the different information categories of the DMP. Such a Decree has yet to be adopted[28], therefore at present there are no clear rules on the content of the DMP. At present, the leaflet informing patients of the DMP provides for an indication of the elements that are contained in the DMP: patient's past history (including elements such as diseases and surgery), allergy, medicine taken, records from physician consultation, hospitalisation, results from examination (x-ray photography, biological analysis)[29]. Finally, the law foresees that each institution may provide, on the basis of a decision of the Medical Board Commission or Institution Medical Conference (*Commission Médicale d'Établissement ou Conférence Médicale d'Établissement*)[30], an automated update of certain contents to their patients' DMP. In practice, this means that health institutions may agree a fortiori that certain categories of data should be considered necessary for the coordination of health-related care or key elements of

[28] See for instance CNIL Deliberation n°2010-449 off 2 December 2010 which refer to this Article: http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000023308516&fastReqId=1988022943&fastPos=10 (last access January 2014).
[29] See page 05 of the 'Patient leaflet' on the ASIP Santé website: http://esante.gouv.fr/sites/default/files/BrochurePatient_023%20(2).pdf (last access January 2014).
[30] Each health institutions possesses, depending on its type, a Medical Board Commission or Institution Medical Conference which constitutes the representative body of the medical community (physicians and midwives), pharmaceutical and dental. This body may adopt decisions relating to the organisation of the institution at large. These bodies are governed by Articles L.6144-1, L.6144-2 et R.6144-1 à R.6144-6 du code de la santé publique.

Questions	Legal reference	Detailed description
		the stay, and therefore should always be updated in the DMPs. Physicians retain the right to withhold a specific information.
Are these data restricted to purely medical information (e.g. physical or mental health, well-being)?	Public Health Code, Art. L.1111.14 (last amended in 2011)	The DMP's vocation is open-ended in terms of content, and therefore any information relevant to health-related care coordination should be included, including information that is not purely medical information[31]. At present, under the Public Health Code, the DMP must include a part on prevention. It is expected that this part will include medico-social information, as well as information on prevention examination, etc.[32] Moreover, under the Public Health Code, when opening a DMP, the care-recipient must be informed of organ donation. With regard to future developments, as mentioned above, a Decree has yet to be adopted identifying the different elements that would or should always be included in the DMP[33]. This includes, through the DMP interface, a common window available to all health professionals s (*socle commun*) that would include information that is not purely medical information[34].
Is there a definition of EHR or patient's summary provided in the national legislation?		The sole requirements are that the information be 'necessary for the coordination of health-related care given to the care recipient' or be 'key elements of the stay' in a health institution. The Public Health Code in its Article L.1111-21 foresees the adoption of a Decree to determine the content and condition of access to the different information categories of the DMP. Such a Decree has yet to be adopted[35].
Are there any requirements on the content of EHRs (e.g. detailed	Public Health Code, Art. R.1112-2 (last amended in	As explained above, at the moment France limits itself to requiring that personal health data updated on DMP is 'necessary for the coordination

[31] Interview with the ASIP Santé on 20th January 2014.
[32] Interview with the ASIP Santé on 20th January 2014.
[33] It is interesting to note that the CNOM is not in favour of regulating upon the content of a DMP (interview with the CNOM on 22nd January 2014).
[34] Interviews with the CNOM on 22nd January 2014, and with the CNIL on 24th January 2014.
[35] See for instance CNIL Deliberation n°2010-449 off 2 December 2010 which refer to this Article: http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000023308516&fastReqId=1988022943&fastPos=10 (last access January 2014).

Questions	Legal reference	Detailed description
requirements on specific health data or general reference to health data)?	2006)	of health-related care given to the care recipient' or be 'key elements of the stay' in a health institution.
Are there any specific rules on the use of a common terminology or coding system to identify diseases, disorders, symptoms and others?		The ASIP Santé is involved in international negotiations for the establishment of health-related semantics. In that perspective, the DMP is foreseen to make use of the development of international norms developed for instance under the Clinical Document Architecture initiative such as IHE or HL7 standards recognised by the ISO that use the Logical Observation Identifiers Names and Codes (LOINC) database and universal standard[36]. However, this has not been legislated upon and is therefore not a legal requirement of the DMP.
Are EHRs divided into separate categories of health data with different levels of confidentiality (e.g. data related to blood type is less confidential than data related to sexual diseases)?		According to the DMP practical guide[37], a healthcare professional can access documents from a DMP according to his profession. However, this option was removed after 2009 considering the implementation of the rules surrounding consent and the right to opposition of the Electronic and liberty law which resulted in the possibility for a patient to hide data (*droit au masquage*) (see Section 2.3)[38]. In spite of this, the physician regularly involved with the patient (*médecin traitant*) has access to all of the DMP's data, regardless of their confidentiality level or that they have been hidden to other health professionals (to note that a patient can designate several physicians as his/her *médecin traitant* provided these physicians share the same medical speciality and work for the same health institution[39]). Moreover, the person who authored the document and the patient are always entitled to access a document on the DMP (see Section 2.4).

[36] Interview with the ASIP Santé on 20th January 2014.
[37] Practical guide of the DMP project in health institutions (*Guide pratique du projet DMP en établissement de santé*), available at: http://www.dmp.gouv.fr/documentation/guide-dmp-en-es (last access December 2013).
[38] Interview with the CNIL on 24th January 2014.
[39] Code of Social Security, Article L.162-5-3
'*Les médecins exerçant dans le cadre de la même spécialité au sein d'un cabinet médical situé dans les mêmes locaux ou dans un centre de santé mentionné à l'article L.6323-1 du code de la santé publique peuvent être conjointement désignés médecins traitants.*'

Questions	Legal reference	Detailed description
		Announcements on the DMP2 (see Section 1.3), foresees that the system would evolve towards more and more categories 'of added value', including for instance a detailed part on prevention, clinical imagery, ePrescriptions, parts on specific pathologies (e.g. diabetes)[40], etc.
Are there any specific rules on identification of patients in EHRs?	Public Health Code, Art. R.1112-3 (last amended in 2003)	According to the CNIL decision of February 2007, the creation of a DMP must be done through a system that does not allow deducing information on individuals. Use of the Number of Inscription to the Registry has therefore been refused and as a result the DMP is created through the INS[41]. The INS is an identifier assigned to each beneficiary of the national healthcare through the patient's Healthcare Card (*carte vitale*)[42] that is used for the creation and access by professionals to the DMP. However, this card is not a substitute to an ID and a verification procedure of identity is required during creation or access by professionals to a DMP[43]. Finally, the EHRs kept in institutions (i.e. EHRs other than DMPs) contain the identification of the patient, as well as that of their proxy (*personne de confiance*), if any[44]. Depending on the institution, this information is likely to be considered necessary for the coordination of health-related care or key elements of the stay, and therefore incorporated in the DMP.
Is there is a specific identification number for eHealth purposes?		The INS is sufficient in that respect. It is unique to each individual throughout France, and serves many purposes.

[40] CNIL Deliberation n°2010-449 of 2 December 2010 : http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000023308516&fastReqId=1988022943&fastPos=10 (last access January 2014).
[41] The use of this number is also due to evolve together with the deployment of the DMP. See for instance: http://esante.gouv.fr/services/referentiels/identification/les-raisons-d-etre-et-le-cadre-reglementaire-de-l-ins or http://www.dmp.gouv.fr/documentation/ins (last access January 2014).
[42] Each patient covered under the National Healthcare (*assurance maladie*) is provided with this card. It is used for identifying patients at the physician, health institution, pharmacists, etc.
[43] Interview with the ASIP Santé on 20th January 2014.
[44] Public Health Code, Article R.1112-3

2.2 REQUIREMENTS PLACED ON THE INSTITUTION HOSTING EHRS DATA

2.2.1 Main findings

The French legislation has adopted very detailed requirements applying to the institutions hosting EHRs data (See Article L1111-8 and Articles R1111-9 to 15 of the Public Health Code). These rules apply not only to the DMP scheme, but also to any EHR initiative in France such as compulsory EHR of health institutions or physicians working in private practice.

According to the Public Health Code, any individual or legal person can apply for an authorisation to host personal health data through electronic means (*support informatique*).

Applicants must provide extensive information demonstrating that their hosting system is secure and sophisticated enough to ensure that the rules on EHRs (*e.g. consent, access, confidentiality*) are fulfilled and that health data is well protected especially considering the risk[45]. The CNIL, and the 'authorisation committee' (*comité d'agrément*)[46] composed of different stakeholders, are each required to give their opinion on the applicant's submission. This assessment also involves an evaluation of the financial capacities of the applicant. The authorisation is granted by the Minister in charge of health issues.

The authorisation is delivered not to a hosting institution, but with regard to the delivery of a specific hosting service. As such, the same company could be potentially hosting several different types of EHRs[47]. Pursuant to a call for tender and authorisation by the CNIL, the DMP data are being hosted since March 2010 by a consortium held by the groups Atos Origin and La Poste through their branches Santeos and Extelia.

The authorisation process takes approximately eight months and the authorisation lasts three years, after which it may be renewed. Since 2009, the CNIL delivered 142 opinions on applications with a rough approximate of half of the requests currently being denied[48].

The three stakeholders interviewed confirmed that the very thorough and rigid procedure had become redundant, heavy, and complex. They therefore agreed that, whilst a thorough procedure is highly necessary with regard to public order (i.e. to maintain security and foster confidence in the system), the current procedure has aged since its adoption in 2002 and could now be simplified.

Finally, as part of its controlling duties, the CNIL elaborates a yearly control programme (*programme des contrôles*) whereby a number of personal data processors are being checked *a posteriori*, that is to say after an authorisation has been delivered. EHRs hosting institutions are registered again in this programme every year, demonstrating the importance afforded by the CNIL to the issue, and the willingness of the institutions to foster confidence in the system by its users[49].

[45] Electronic and liberty law, Article 34.
[46] Please see the question on authorisation in the table below for further information on the role of the authorisation committee' (*comité d'agrément*)
[47] Interview with the CNIL on 24th January 2014.
[48] Interview with the CNIL on 24th January 2014.
[49] Interview with the CNIL on 24th January 2014.

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?	Public Health Code, Art. R.1111-9 to Art. R.1111-15 (last amended in 2006 and 2009)	Articles R.1111-9 to R.1111-15 of the Public Health Code set specific rules for the institutions hosting personal health data through electronic means. According to these Articles any individual or legal person can apply for an authorisation to host data on computer support if they comply with several conditions (e.g. on security of access, guarantee of confidentiality). These conditions are explained in depth in the remaining rows of this table.
Is there a need for a specific authorisation or licence to host and process data from EHRs?	As above	In order to host personal health data on electronic support any individual or legal person must be granted an authorisation (*agrément*) by the Minister in charge of health issues. This authorisation is delivered after the CNIL and an authorisation committee have issued their opinion on the application. According to Article R.1111-12 of the Public Health Code, the application for the authorisation must contain the following information: - The identity and address of the person in charge of the hosting service - Names, qualifications and experience of operators responsible for implementing the service and the categories of persons who, by reason of their duties or for the needs of the service, have access to the data ; - The indication of the place where data will be stored ; - A description of the proposed services ; - Models of contracts to be concluded between the operator hosting the data and the individuals or legal persons that produced personal health data (e.g. physicians, hospitals) ; - The measures to ensure security of data and guarantee the confidentiality of health data as protected by law (further detailed below) ; - If applicable, an indication of the use of external technical service providers and contracts concluded with them ; - A document outlining the provisional accounts of the hosting company, and possibly the last three balance sheets and the composition of the ownership of the applicant and, in the case of a

Questions	Legal reference	Detailed description

		renewal application, the income statements and reports related to the hosting company since the last approval.
		
		The CNIL opinion considers the measures proposed by the applicant to ensure the protection of the processed data. The CNIL must issue its opinion within two months of receiving the application. The CNIL opinion is sent to the authorisation committee that must in turn provide an opinion on all aspects of the application (i.e. ethical, deontological, technical, financial, and economic) within a month. Then, the Minister in charge of health issues has two months to decide whether or not to grant the authorisation. If the Minister has remained silent until the end of this period, the application is deemed rejected.
		
		The authorisation committee is composed of:
		
		- A member of the General Inspectorate on Social Affairs (*l'inspection générale des affaires sociales*)[50] ;
		- Two representatives of relevant health associations as authorised according to Article L.1114-1 of the Public Health Code[51] ;
		- Two representatives of health professionals, one nominated by the National Council of the College of Physicians (*Collège national des médecins*) and the other on a proposal from the National Union of Health Professions (*Union nationale des professions de santé*)[52] ;
		- Three qualified persons
		  o A person with expertise in ethics and law ;
		  o A person with expertise in security of information systems and technology ;
		  o A person with expertise in economics and finance.

[50] General Inspectorate on Social Affairs is the interministerial service on control audit and evaluation of social policies.
[51] According to this Article, associations active in the field of health and care of patients accredited by the competent regional or national administrative authority. The accreditation is subject to the particular effective and public activity of the association for the defense of the rights of patients and users of the health system as well as training and information, the transparency of its management, its representativeness and independence.
[52] These bodies are set up by law in France in order to allows the dialogue of different unions of health professionals, together with other partners of the national healthcare.

Questions	Legal reference	Detailed description
		With regard to the measures on security and confidentiality of data, Article R1111-14 of the Public Health Code requires that applicants specify: Concerning the rights of the persons concerned by the data hosted : - The procedure ensuring the possibility for the person concerned to consent to hosting of their health data ; - The methods selected for the access to health data and their possible transmission under the consent of the person concerned ; - The methods to take into account the requests for modification of personal data ; - The means to ensure compliance with the provisions of Article L.1111-7 on people's access to their health information, particularly in terms of timing and modalities of consultation ; - Procedures for reporting serious incidents, including data corruption or unauthorised disclosure of personal health data ; - Provision upon request of all historical data access and consultations, as well as content of the information consulted and possibly surgery treatments, to the person concerned by the data hosted. Concerning security of access to information : - Arrangements to ensure security of access and data transmissions of health institutions or professionals producing these data and the people concerned by these data ; - The measures taken in respect of control and traceability of access, and processing fees ; - The conditions for verifying the content of traces of access and processing to detect break-in attempts or unauthorised access ; - The procedure to verify the register of persons entitled to access hosted data ; - Technical processes used for identification and authentication of health professionals ;

Questions	Legal reference	Detailed description
		Concerning the durability of hosted data - procedures to ensure, at the time of data transfer to the host system, the secure reception and the integrity of data, their inclusion in the information of the host system and monitoring of this support ; - procedures to take into account all information on data from their creation to identify them, describe them and determine their technical properties and to ensure traceability ; - The procedures for data replication on various computer media in different locations ; - The conditions for the implementation of a warning system for data encoding formats, intended to inform the person recording data, in case of obsolescence of the format and the procedures to perform, with the permission of the person recording data, migration data formats, if they no longer ensure the readability of information and the traceability of such migrations. In terms of organisation and internal control procedures to ensure the security of processing and data: - The appointment of a safety and a quality manager ; - The definition of the tasks , powers and obligations of the host staff and any sub-contractors, authorised to process personal health data ; - The methods adopted for periodic risk assessment and audit of the protective measures in place to ensure data security and to make the necessary changes in case of fault detection ; - Regular malfunction simulation devices to verify the effectiveness of mechanisms to ensure the continuity of services ; - The means used to educate and train staff on protection measures implemented and their obligations of confidentiality and professional secrecy ; - The conditions for implementing the physical security of computer sites , measures to protect the technical infrastructure, especially in

Questions	Legal reference	Detailed description
		terms of network security, servers and workstations ; - The measures taken with regard to the operation of the technical infrastructure ; - The conditions of implementation of IT disaster recovery plan including in particular measures to inform on the state of this plan the natural or legal persons recording personal health data and the measures taken to resume activities.
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)?	Public Health Code Art. R.1111-9 (last amended in 2006)	According to Article R.1111-9 of the Public Health Code the hosting operators must: - Provide all guarantees for the exercise of this activity , including the use of personnel qualified in security and archiving of data and the implementation of technical solutions, organisation and control procedures to ensure the safety, protection, conservation and restoration of data entrusted , as well as use in accordance with law ; - Define and implement a policy of confidentiality and security, in particular for ensuring compliance with the legal requirements of confidentiality and secrecy ; - Individualise within its organisation, its hosting activities and the means dedicated to it, as well as the data management and data flow ; - Define and implement information tools for the people that input data in the database, particularly in cases of substantial change in conditions for carrying out such activity ; - Identify the people in charge of the hosting activity, including a physician, indicating their contractual relationship with the hosting operator.
In particular, is there any obligation to have the information included in EHRs encrypted?		It is not explicitly required by the law that the information included in EHRs must be encrypted. However, in practice as underlined by the CNIL in its deliberation n°2010-449[53] personal health data managed by hosting institutions are encrypted according to the advanced encryption standard (AES-256).

[53] CNIL Deliberation n°2010-449 of 2 December 2010: http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000023308516 (last access January 2014).

Questions	Legal reference	Detailed description
Are there any specific auditing requirements for institutions hosting and processing EHRs?	Public Health Code, Art. R.1111-15 (last amended in 2009)	Approval is delivered for a period of three years. At the end of those three years, a hosting institution can ask for renewal. The renewal application should include, inter alia, an external audit undertaken at the hosting institution's costs. The Public Health Code states that this audit should attest the implementation of privacy and security policy.

2.3 PATIENT CONSENT

2.3.1 Main findings

A DMP is created by any health professional or administrative service of an hospital properly identified and authenticated, after informing the patient and obtaining his/her consent for the creation of the DMP.

The consent does not need to be materialised on a piece of paper, but it is reported on the DMP together with other authorisations relating to the patient's consent such as access to the DMP for certain professionals. The patient therefore needs to consent to the sharing of data. Patients are moreover entitled to request that certain information do not figure on their DMP. They may also limit what information is being shared and with whom. Finally, patients have a right to request modification, update or removal of information that is no longer correct, complete, or that is obsolete.

A DMP can be created through calculation of the patient's National Health Service Login (*Identifiant National de Santé*) (INS). The use of the INS results of the conclusions of 20 February 2007[54] of the CNIL whereby the use of the Number of Inscription to the Registry (*Numéro d'Inscription au Répertoire* also called *Numéro de sécurité sociale*) was rejected. Indeed, the Number of Inscription to the Registry is a 22 characters sequence attributed to every individual born in France or covered under the national social security including the national healthcare and, as an already existing, general and widespread system providing a unique number per person, would have been an obvious identification choice for DMP purposes. However, the CNIL found that the sequence of numbers composing the Number of Inscription to the Registry allows for the identification of the gender, year of birth, etc. of an individual, and therefore would constitute an element of vulnerability to the DMP system.

It was therefore agreed that the INS system will be used. The INS is generated by a centralised system. The INS is private and therefore protected by personal data laws[55]. The INS is calculated through an algorithm that uses the person's first name, birthdate and Number of Inscription to the Registry (*Numéro d'Inscription au Répertoire* also called *Numéro de sécurité sociale*) retrievable in particular from the patient's Healthcare Card (*carte vitale*)[56]. The INS system is therefore highly secure and yet does not completely exclude the possibility for doublons, hence collisions of login details. Discussions are on-going at the national level on improving the INS system or eventually returning to the Number of Inscription to the Registry with additional protection.

After calculation of the INS and creation of a DMP, the patient will receive a DMP login and password, s/he will use for accessing his/her DMP (see Section 2.4).

[54] CNIL *conclusions du 20 Février 2007 sur l'utilisation du NIR comme identifiant de santé:* http://www.cnil.fr/fileadmin/documents/approfondir/dossier/NIR/Rapport%20NIR.pdf (last access January 2014).
[55] Cf. http://www.dmp.gouv.fr/documentation/ins (last access January 2014).
[56] Each patient covered under the National Healthcare (*assurance maladie*) is provided with this card. It is used for identification of a patient at the physician, health institution, pharmacists, etc.

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?	Public Health Code, Art. L.1111-8 (last amended in 2010)	In France, there are three requirements that need to be met prior to creating a DMP: delivery of prior information (see below), consent from the patient, identification of the patient (see below). These different requirements can be complied with at different moments in time. Pursuant to Article L.1111-8 of the Public Health Code the consent for the hosting of data for setting-up DMPs must be explicit (*exprès*). There is no written contract for the consent, nor is there a registration of refusal, to create a DMP, but the declaration of consent is indicated in the DMP as well as any linked authorisations, namely: – the patient's consent to the creation of the DMP; – his/her permission to access the DMP by the health institution; – it permission to access the DMP in emergencies Upon creating a DMP, these are set to YES by default in the system.
Is a materialised consent needed?		According to the DMP practical guide[57], the consent does not need to be materialised on a piece of paper.
Are there requirements to inform the patient about the purpose of EHRs and the consequences of the consent or withholding consent to create EHRs?	Public Health Code, Art. L.1111-14 (last amended in 2011)	The CNIL in its authorisation for the implementation of DMP details that in order to give his/her consent the patient must be provided with an information paper leaflet drafted in a clear language and accessible to all. This document constitutes the mandatory prior information required by law and has since been published by the ASP Santé: 'patient information leaflet' (*brochure d'information patient*). To attest to the delivery of prior information to the patient and consent from the patient when creating a DMP, two possibilities exist: – give back the 'patient information leaflet', and eventually stamp its back with the health institution's stamp, and date it; print and give to the patient the document containing his/her 'connexion credentials' to the DMP scheme, on which prior consent is

[57] Practical guide of the DMP project in health institutions (*Guide pratique du projet DMP en établissement de santé*), available at: http://www.dmp.gouv.fr/documentation/guide-dmp-en-es (last access December 2013).

Questions	Legal reference	Detailed description
		reiterated. Ideally, this information is delivered by the physician as s/he is in a trusting relationship with the patient and is best able to explain the benefits of the DMP support for the patient. This prior information can also be delivered by any trained person, including for example a person at the reception of a health institution or a patients association.
Are there specific national rules on consent from the patient to share data?		See below.
Are there any opt-in/opt-out rules for patient consent with regard to processing of EHRs?	Electronic and liberty law, Art. 40 (last amended in 2004)	The French law does not require consent to be expressed every time data is being processed. However, a patient may ask that certain information be not reported on his/her DMP.
Are there any opt-in/opt-out rules for patient consent with regard to sharing of EHRs?	Electronic and liberty law, Art. 40 (last amended in 2004)	The patient needs to consent to the sharing of data. Once s/he gives his/her consent to a health institution, this consent also applies to the health professionals involved in his/her 'care management'. However, a patient may ask that specific pieces of information are not shared with every health institutions or physicians in private practice.
Are there requirements to inform the patient about the purpose of EHRs and the consequences of consent or withholding consent on the sharing of EHRs?		There are no such requirements per se, apart from that of prior information described above.
Can the patient consent to his/her EHRs being accessed by a health practitioner or health institution outside of the Member State (cross-border situations)?		The DMP scheme is a national initiative: only health physicians and health institutions registered in France and certified with their CPS or 'institution software' may access a patient's DMP. However, as a patient has access to his/her own DMP, s/he may provide access to a health professional by disclosing his/her details or login him/herself directly on a physician's electronic device.
Are there specific rules on patient consent to share data on a cross-border situation?		At present, reliance on the CPS system means that only French professionals can create and update the DMP. The reference to 'other equivalent system' in the law on the DMP may be used at a later stage to consolidate rules on consent and access with regard to transboundary situations.

2.4 CREATION, ACCESS TO AND UPDATE OF EHRS

2.4.1 Main findings

The access to the DMP is granted only to the patient and to health professionals provided they have received the patient's consent. In French law, the notion of health professionals encompasses over 20 different professions, including but not limited to, physicians, nurses and physical therapists whether or not they exercise their activities in public or private practice. Moreover, considering that physicians rarely practice on their own in health institutions, in this case, consent is presumed to have been delivered to the entire 'healthcare team' (*équipe de soins*)[58].

Concerning the patient's access to the DMP, after calculation of the INS and creation of a DMP (see Section 2.3), the patient will receive a DMP login and password, s/he will use for connection. For each connection, in a manner similar to many online banking systems, the patient will create a One Time Password (OTP) using his/her Healthcare Card, DMP login and password, that will allow him/her to access his/her DMP.

Once the patient has given permission to access the DMP, adding document in the DMP can be done by any health professional, a medical secretary or any other person authorised by the health institution, i.e. any person involved in the 'healthcare team'. The physician regularly involved with the patient is also allowed to update the DMP. Finally, each hospital may decide that certain information or categories of documents should be systematically updated to the DMP, subject to a general prior approval by the medical profession at large represented in this institution. In such situations, physicians still retain the right to withhold a piece of information from this systematic update. Three categories of people retain an inalienable right to access a document on the DMP: the patient him/herself, the physician regularly involved with the patient (*médecin traitant*) (bearing in mind several physicians can be considered as the patient's *médecin traitant*), and finally the author of the document.

Health professionals need to be properly authenticated before acceding to DMP. This authentication is done through specifically created and protected CPS cards or software certificates. It should be noted however that two or more medical doctors can exchange information relating to a patient's health under the shared professional secrecy rule (*secret medical partagé*).

Access to the DMP for the conclusion of insurance contract or any other contract is expressly prohibited by the Public Health Code. Furthermore, Article L.1111-18 of the Public Health Code third paragraph provides that occupational physicians cannot have access to the Personal Health record.

Under emergency procedures, a DMP may be accessed without a patient's prior consent but with mandatory full traceability.

Sensitive documents can also be hidden from the patient until a consultation takes places announcing him/her the content of these documents (e.g. oncology documents).

[58] Public Health Code, Article L.1110.4.

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?		According to the DMP practical guide , the creation of a DMP can be made by any health professional or hospital personnel certified by a CPS card or authenticated under the responsibility of the head of this institution (i.e. through a 'software certificate' for legal persons). The creation of a DMP can be organised in any place and at any time (the reception, the admissions office, care unit, etc.), as soon as a face-to-face with the patient is possible and provided that the patient's INS can be calculated on the basis of the Healthcare Card
Are there specific national rules on access and update to EHRs?	Public Health Code, Art. L.1111-15 (last amended in 2009)	The access to the DMP is only allowed to the patient and to health professionals provided they have received the patient's consent.
Are there different categories of access for different health professionals?	Public Health Code, Art. L.1111-16 (last amended in 2009) Social Security Code, Art. L.162-5-3 (last amended in 2009)	Consultation of the DMP is possible, subject to the access authorisation of the patient, by health professionals authenticated individually by CPS. The presence of the patient is not required. Once access has been granted, the health professional can access all information, provided it has not been hidden (*masquage*) by the patient. The patient may exercise his/her right to hide information against several physicians or health institutions. However, in any case, a document is always visible to: – the patient him/herself (see below for further information on exceptions), – the physician regularly involved with the patient (*médecin traitant*) (bearing in mind this denomination can be given to several physicians), and – the author of the document.
Are patients entitled to access their EHRs?		The patient provided with login credentials during the creation of the DMP can access the DMP via the national internet portal, alone at home or with the help of a physician in the physician's office. When connecting on his/her own, the patient will need to create a One Time Password (OTP) using

Questions	Legal reference	Detailed description
		his/her Healthcare Card, DMP login and password, that will allow him/her to access his/her DMP.
Can patient have access to all of EHR content?		In certain situations, the information needs to be first disclosed to the patient in a meeting before being accessible on the DMP. This is for instance the case when a patient has been diagnosed with cancer but still ignores it[59]. Apart from this very specific situation, a patient retains access to all documents on his/her DMP.
Can patient download all or some of EHR content?		Content from a DMP is entirely downloadable[60]. This is however not detailed in the legislation.
Can patient update their record, modify and erase EHR content?	Electronic and liberty law, Art. 40 (last amended in 2004)	Article 40 of the Electronic and liberty law states that any person can requests that their personal information be rectified, completed, updated, locked or erased when this information is no longer correct, complete, or when it is obsolete. As a result, multiple functions are available for management of the DMP (professional blocked, hiding documents, access tracks, closing the DMP, reactivation, etc.). In practice, as stated in the Report from the National Council of Health Professionals[61] erasure of documents may take place in common agreement with a health professional. When the patient requests the deletion of a document, a procedure takes place whereby a medical correspondent will enter in contact with the patient to ascertain the patient's wishes. A form needs to be filled and a delay is respected before deletion is completed. In case of refusal by the patient to update data, modification or erasure of data, the DMP will not indicate to their users that information has been deleted or that a file is incomplete. Note that the IT system keeps track of these actions anyway. This element linked to the concept of 'personalisation' of the DMP scheme raised concerns amongst health professionals and can be

[59] Interview with the CNOM on 22nd January 2014.
[60] Interview with the ASIP Santé of 20th January 2014.
[61] Report of 18 June 2010 the National Council of the Order of Health Professionals, Dematerialiation of medical documents: creating trust to promote information technology (*Rapport du 18 Juin 2012 adopté par le Conseil national de l'ordre des médecins, Dématérialisation des documents médicaux: créér la confiance pour favoriser l'informatisation*), available at: http://www.conseil-national.medecin.fr/sites/default/files/Dematerialisation%20des%20documents%20medicaux.pdf (last access December 2013).

Questions	Legal reference	Detailed description
		indicated as a reason for the lack of success of the scheme. In contrast, the initiative of pharmaceutical record (*Dossier pharmaceutique*) (see Section 2.8) will bear the mention 'file incomplete' whenever a patient wishes information to be withheld from the updating and sharing process.
Do different types of health professionals have the same rights to update EHRs?	Public Health Code, Art. L.1111-16 (last amended in 2009) Social Security Code, Art. L.162 -5-3 (last amended in 2009)	Once the patient has given permission to access the DMP, adding document in the DMP can be done by: – any health professional carrying a CPS card or indirect authentication (using a software certificate) ; – a medical secretary or any other person authorised by the hospital and authenticated through indirect authentication (i.e. through software certificate, under the responsibility of the head of the institution). The physician regularly involved with the patient (*médecin traitant*) is allowed to update the DMP as specified in Article L.162-5-3 of the Social Security Code. As the law allows, the patient may designate several such physicians. The update of the DMP can be systematised by default for certain categories of documents (health professionals retain the possibility to withdraw a given document from this systematic update). This update needs to be defined by the rules of the health institution. These rules are subject to validation by the medical profession.
Are there explicit occupational prohibitions? (e.g. insurance companies/occupational physicians…)	Public Health Code, Art. L.1111-18 (last amended in 2009)	Pursuant to Article L.1111-18 of the Public Health Code, subject to the authorisation of patients, only health professional in line with the rules of deontology can have access to the DMP. This Article expressly denies access to the DMP for the conclusion of insurance contract or any other contract (e.g. loan) that require a health assessment. Article L.1111-18 of the Public Health Code third paragraph provides that occupational physicians cannot have access to the Personal Health record.
Are there exceptions to the access requirements (e.g. in case of emergency)?	Public Health Code, Art. L.1111-17 (last amended in 2010)	A document may be hidden for the patient pending prior announcement through a consultation. This is the case of sensitive documents (e.g. psychiatric or oncologic). This restriction is lifted once the consultation took

Questions	Legal reference	Detailed description
		place. The document then becomes visible to the patient. If the person is unable to express his will and if circumstances require, emergency physician authenticated through their CPS may decide, in the interest of the patient, to access to the DMP without obtaining prior consent. This mode of access called 'ice-breaker' (*bris-de-glace*) is subject to a written reasoned opinion and with mandatory full traceability. This access without patient consent is governed by Article L.1111-17 of the Public Health Code. The patient may object to such access prior to such emergency cases. This information is then registered on the DMP and in this case, access through the 'ice breaker' functionality will be rejected by the system. The physicians who receive calls for emergency medical assistance (ambulance) may, without prior opposition of the patient, consult the DMP of a person seeking their service. As access to the patient's Healthcare Card is by definition impossible in this case, these physicians have a particular certification system, allowing them to examine the DMP database and consult the relevant DMP.
Are there any specific rules on identification and authentication for health professionals? *Or are they aggregated?*		According to the DMP practical guide[62], CPS certificates are issued by the ASIP Santé and function as professional ID cards. They are required to establish secure connections with the DMP, allowing professionals to log on to the system and update data. Certificates of individuals are confined to cards within a smart card of the CPS type. There are also 'software certificates' allowing identification and authentication of a legal person such as a health institution. These certificates are distributed in the form of files to be installed and maintained by the legal person in a containment device software or hardware.
Does the patient have the right to know who has accessed to his/her EHRs?		Every access to the DMP is traced and the patient can obtain this information from the DMP interface without the need to fill in a specific request[63].

[62] Practical guide of the DMP project in health institutions (*Guide pratique du projet DMP en établissement de santé*), available at: http://www.dmp.gouv.fr/documentation/guide-dmp-en-es (last access December 2013).
[63] Interview with the ASIP Santé of 20th January 2014

Questions	Legal reference	Detailed description
Is there an obligation on health professionals to update EHRs?	Public Health Code, Art. L.1111-15 (last amended in 2011)	Article L.1111-15 of the Public Health Code requires that each health professional must report in the DMP during each act or consultation diagnostic and therapeutic elements necessary for the coordination of health-related care given to the care recipient. In addition during the stay of a patient in a health establishment, health professionals must report on the DMP, the summaries of the key elements of the stay.
Are there any provisions for accessing data on 'behalf of' and for request for second opinion?	Public Health Code, Art. L.1110-4 (last amended in 2011)	These provisions are not specific to the DMP scheme but general to the French medical organisation. Pursuant to Article L.1110-4 of the Public Health Code, two or more health professionals can, unless the patient duly informed opposes, exchange information relating to this patient's health to ensure continuity of care or to determine the best 'care management' possible. When the person is under the care of a team in a health institution, the information about him/her is deemed assigned by the patient to the whole team.
Is there in place an identification code system for cross-border healthcare purpose?		At present, reliance on the CPS system means that only French professionals can create and update the DMP. The reference to 'other equivalent system' in the law on the DMP may be used at a later stage to consolidate rules on consent and access with regard to transboundary situations.
Are there any measures that consider access to EHRs from health professionals in another Member State?		This has not been a consideration during the deployment of the DMP scheme, the main objective being a generalised deployment and use of the scheme in France.

2.5 LIABILITY

2.5.1 Main findings

The national legislation does not set specific medical liability requirement related to the use of the DMP. As a result, the general rules on medical liability (*responsibilité médicale / hospitalière*) apply.

Health professionals can be held liable for breach of their professional secrecy under the Criminal Code. One condition to engage their criminal liability is subject to harm being caused by the medical team or physician, or the hospital public administration authority).

This situation has been assessed as a potential obstacle of the DMP development in France[64].

[64] Interview with the CNOM on 22nd January 2014.

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?	Medical Deontology Code, Art. 69 (also Public Health Code, Art. R.4127-69) (last amended in 2004) Criminal Code, Art. 226-13 (last amended in 2000) and 226-14 (last amended in 2007)	The national legislation does not set specific medical liability requirement related to the use of the DMP. As a result, the general rules on medical liability (*responsibilité médicale / hospitalière*) would be applicable. First of all, health professionals can be held liable for breach of their professional secrecy under the Criminal Code. The Public Health Code in its part containing the Medical Deontology Code provides that each physician is responsible for his/her decisions and acts. In order to engage this liability, harm needs to have been caused by the medical team or physician, or the hospital (public administration authority). - A fault causing harm; The responsibility of the medical team, physician or hospital can be engaged in case of physical or psychological harm that includes, *inter alia*, lack of consent or lack of information leading to an informed consent (*défaut d'information*), wrong appreciation as to the emergency of a situation and disrespect of religious beliefs. - The medical team, physician, or health institution; The issue of liability will fall under the competency of the common civil jurisdictions (whether in a civil or criminal court) if it can be proven that the medical team, or a specific physician, that did/did not perform the medical acts in question, operated outside of their functions (*faute détachable à la fonction*). Otherwise, the responsibility of the hospital will be engaged under the Medical Liability regime (*régime de la responsabilité hospitalière*) in the administrative jurisdictions. - Causality; Depending on the jurisdictions, the harm suffered needs to be directly

Questions	Legal reference	Detailed description
		connected to the medical team, specific physician, or to public administration authority's fault. When these three elements are reunited, damages can be obtained by the victim on various bases – in particular, loss of chance (*perte de chance*) and moral harm (*préjudice moral*). Depending on the fault, damages for breach of privacy rights may also be invoked (see below). Moreover, depending on the jurisdictions, imprisonment terms may also be ordered.
Can patients be held liable for erasing key medical information in EHRs?		Patients cannot be held liable for erasing key information, however, in such instances; the patient will not be able to prove a fault from the health professional and hence loses any chance to sue the professional. This is further the case considering that the DMP does not indicate that a file is incomplete or that information has been withheld or hidden.
Can physicians be held liable because of input errors?		Inputting information necessary for the coordination of health-related care given to the care recipient in an erroneous way (whether this input was negligent, reckless, or intentional) could be considered a professional fault triggering medical liability as explained above.
Can physicians be held liable because they have erased data from the EHRs?		Withholding information necessary for the coordination of health-related care given to the care recipient could be considered a professional fault triggering medical liability as explained above.
Are hosting institutions liable in case of defect of their security/software systems?	Electronic and liberty law, Art. 45 and 47 (last amended in 2011) Criminal Code, Art. 226-16 to 226-24 (last amended in 2004, 2009, 2011, and	The CNIL may issue a formal notice (*mise en demeure*) against a person processing data ('*la personne responsible d'un traitement*') that do not respect the Electronic and liberty law. If this person does not rectify its action, the CNIL may order a 'warning' (*avertissement*) bearing the nature of a sanction to this person. This sanction may also be directly ordered without the need for a formal notice to be first issued. This sanction can consist of a proportionate fine (up to EUR 300,000 in case of repeated misbehaviour) and the CNIL may also withdraw the authorisation to process data delivered to this person/company as well as refer the matter to the Prime Minister or the Court. Additional criminal sanctions (fines and imprisonment terms) may also be ordered by the courts for e.g. processing personal data without respecting formalities, diverting personal data from their true purposes, etc.

Questions	Legal reference	Detailed description
	2012)	
Are there measures in place to limit the liability risks for health professionals (e.g guidelines, awareness-raising)?		The national legislation does not set specific medical liability requirement related to the use of the DMP, and therefore no measures are in place to limit the liability risk of health professionals in relation to the DMP.
Are there liability rules related to breach of access to EHRs (e.g. privacy breach)?	Public Health Code, Art. L.1111-18 (last amended in 2009) Criminal Code, Art. 226-13 (last amended in 2000)	Any breach of legal provisions and requirements relating to DMP is punishable by a year's imprisonment and a fine of EUR 15,000
Is there an obligation on health professionals to access EHRs prior to take a decision involving the patient?		No such obligation could be found in the French law. It is important to note that the DMP is not compulsory in France and is, as of now, only used by a small part of the French population (less half a million for a population of over 65 Million, i.e. approximately less than 1%).
Are there liability rules related to the misuse of secondary use of health data?	Electronic and liberty law, Art. 45 (last amended in 2011) Criminal Code, Art. 226-16 to 226-24 (last amended in 2004, 2009, 2011, and 2012)	The CNIL may pronounce a 'warning' (*avertissement*) bearing the nature of a sanction to a person processing data ('*la personne responsible d'un traitement*'). This sanction can consist of a proportionate fine (up to EUR 300,000 in case of repeated misbehaviour) and the CNIL may also withdraw the authorisation to process data delivered to this person/company as well as refer the matter to the Prime Minister or the Court. Additional criminal sanctions (fines and imprisonment terms) may also be ordered by the courts for e.g. processing personal data without respecting formalities, diverting personal data from their true purposes, etc.

2.6 SECONDARY USES AND ARCHIVING DURATION

2.6.1 Main findings

Pursuant to Article L.1111-18 of the Public Health Code, the DMP must be kept for a period of ten years after its closure. The term closure is not explicitly defined in the law, but one stakeholder described it as the last time the DMP was used[65].

It should be noted that other Health Records are subject to different rules. For instance, health institutions are required to keep their records for twenty years from the date of the last stay or external consultation of the patient in the institution (except for minors).

There are no specific rules on the secondary use of DMP health data (e.g. scientific research). The general rules on the secondary use of health data are set under Chapter IX and X of the Electronic and liberty law.

Chapter IX regulates how personal health data can be used for research. This secondary use must be authorised by the CNIL after consultation of an expert committee. These data must be anonymised when submitted to research institutes and non-identifiable in the research result.

Chapter X regulates how personal health data can be used for health assessment of medical practices and prevention. This secondary use must be subject to authorisation of the CNIL. The key condition for the secondary use of health data for assessment of medical practices and prevention is that they must be anonymised and must be communicated through aggregated statistics or in such a way that persons concerned cannot be identified.

It is worth mentioning that France has set in place an important database, the national information system of the health insurance scheme (*Système national d'information inter-régime de l'assurance maladie)* that collects a number of data including all physicians treatment forms (i.e. forms filled by doctors so that their patients can ask reimbursements), as well as 'medical-administrative' information (e.g. number of hospital days and costs), and date of death and cause of death, but no health data as such. Data under this database are anonymised prior to being consulted for secondary use. This data is archived for 3 years. Access to this information is strongly regulated and mainly administrative bodies can have access to aggregated data without authorisation. Scientific research institutes and universities must apply for an authorisation to have access to these data. Private entities (e.g. pharmaceutical industries) cannot have access to these data.

Discussions are on-going at the national level for reforming the system for authorising secondary use of health data. These discussions are also interrelated with the discussions on the development of the DMP2 scheme as the DMP offers a unique visibility into French health and its architecture could be adapted for a systematic extraction of data for secondary use in certain situations (e.g. oncology)[66]. This requires further work on semantics and interoperability, and needs to be done in a manner consistent with confidentiality of data and without hindering the deployment of the DMP nation-wide.

In any case, different stakeholders[67] were of the opinion that the procedure as it stands is heavy and could be simplified with regard to some of its formalities and repetitive nature.

[65] Interview with the ASIP Santé on 20th January 2014.
[66] Interview with the ASIP Santé on 20th January 2014.
[67] Interviews with the ASIP Santé on 20th January 2014 and CNOM o 22nd January 2014.

2.6.2 Table on secondary uses and archiving duration

Questions	Legal reference	Detailed description
Are there specific national rules on the archiving durations of EHRs?	Public Health Code, Art. L.1111-18 (last amended in 2009)	Pursuant to Article L.1111-18 of the Public Health Code the DMP must be kept for a period of ten years after its closure.
Are there different archiving rules for different providers and institutions?		The rules with regard to the DMP for the different actors concerned are similar. However, other Health Records (including EHRs) are subject to different rules. For instance, health institutions are required to keep their records for twenty years from the date of the last stay or external consultation of the patient in the institution (except for minors)[68].
Is there an obligation to destroy (…) data at the end of the archiving duration or in case of closure of the EHR?		According to a stakeholder, ten years after the last use of the DMP, the file would be archived provided the person concerned by the DMP has agreed to this archiving[69]. As the DMP scheme has been formally launched in 2011, such a situation has not occurred yet, and is moreover not legally regulated.
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...)?	Electronic and Liberty Law, Chapters IX and X (last amended in 2004)	There are no specific rules on the secondary use of DMP health data. The general rules on the secondary use of health data are set under Chapter IX and X of the Electronic and Liberty Law. According to Chapter IX of this law, the use of health data for research purposes is subject to authorisation by the CNIL and consultation by a committee composed of relevant persons in the field of health, epidemiology, genetics and biostatistics. This committee delivers an opinion on the research methodology, the need for use of personal data and the relevance of these in relation to the objective of the research. In case health personal data allow the identification of patients they must be

[68] Public Health Code, Article R.1112-7
[69] Interview with the ASIP Santé on 20th January 2014.

Questions	Legal reference	Detailed description
		codified prior to be submitted for research purposes. The result of health data processing for research purposes must not allow the direct/indirect identification of persons concerned. According to Chapter X of this law, the use of personal health data for health assessment of medical practices and prevention is subject to authorisation from the CNIL. For each application, the CNIL verifies the guarantees provided by the applicant for the purposes of these provisions and , where appropriate, the conformity of the application to its mission or purpose. It checks the need of the applicant to use personal data and the appropriateness of treatment in relation to its stated purpose of evaluation or analysis of medical practices and prevention. It verifies that the personal data whose processing is envisaged does not include the name of the persons concerned, or their Number of Inscription to the Registry. In addition, if the applicant does not provide sufficient evidence to demonstrate the need for certain information from all personal data whose processing is considered, the CNIL may prohibit the disclosure of such information.
Are there health data that cannot be used for secondary use?	Electronic and Liberty Law, Chapters IX and X (last amended in 2004).	All personal health data can be used for secondary use subject to requirements set under the Electronic and Liberty Law.
Are there specific rules for the secondary use of health data (e.g. no name mentioned, certain health data that cannot be used)?	Electronic and Liberty Law, Chapters IX and X (last amended in 2004).	Non-anonymised data cannot be used for secondary purpose apart under very specific circumstances. Furthermore the result of the use of these data must be presented in such a way (e.g. aggregated data) that individuals concerned cannot be identified.
Does the law say who will be entitled to use and access this data?		No, this is subject to authorisation by the CNIL on a case by case basis. Discussions are however on-going to modify the current authorisation system, especially in light of EHRs initiatives such as the DMP where extraction of data could be systematically provided for in the architecture.
Is there an opt-in/opt-out system for the secondary uses of eHealth data included in EHRs?	Electronic and Liberty Law, Chapters IX and X (last amended in 2004).	Not really but Article 56 of the Electronic and Liberty Law states that any person has the right to oppose that the professional secrecy is lifted for the use of his/her personal health data in health research.

2.7 REQUIREMENTS ON INTEROPERABILITY OF EHRS

2.7.1 Main findings

The DMP is a response to difficulties frequently encountered in computerisation projects. It provides a national infrastructure based on a set of national standards developed based on international standards such as ISO recognised standards (Health Level 7 (HL7), including 'Clinical Document Architecture' (CDA), and Digital imaging and communications in medicine (DICOM) standards) based on the Logical Observation Identifiers Names and Codes (LOINC) database and universal standard..

This interoperability framework provides a unique structure conducive to breaking down barriers between health information systems. The framework relies both on technical and semantic interoperability.

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?		The French EHR initiative, the DMP, is a national scheme and is therefore by definition offering a national infrastructure system using national standards developed based on international standards that avoid any interoperability problems within France.
Are there any specific rules/standards on the interoperability of EHR?		No
Does the law consider or refer to interoperability issues with other Member States systems?		No

2.8 LINK BETWEEN EHRS AND EPRESCRIPTIONS

2.8.1 Main findings

The law n°2007-127 of January 2007 amending Article L.161-36-4-2 of Code of Social Security provides that each person covered by the national healthcare can have a pharmaceutical record (*dossier pharmaceutique*) (DP) based on his/her consent. All pharmacists must consult and complete this file based on the medicines they provide, the patient may still withdraw his/her consent punctually with regard to certain medicines. The DP is therefore a record on the distribution of medicine (*dispensation de médicaments*) rather than the prescription of medicine per se (*prescription de médicaments*). It does not include prescription of other types of care which, by definition, should be updated to the DMP as they relate to the coordination of health-related care.

The DMP and the DP were designed to work together, although at the current stage of implementation they are not inter-connected. The DP has been developed at the initiative of the National Council of the Order of Pharmacists (*Conseil national de l'ordre des pharmaciens*) in consideration of the needs surrounding a single medical act. Deployment of the DP has been gradual since its launch in 2006, and as of end of 2012, every pharmacists is legally required to feed into the DP system[70].

In the near future, information in the DP would feed in the DMP in order for the health professional to:

- Identify the treatment of the patient;
- Identify problems with compliance or redundancy;
- Improve the delivery of prescription.

[70] Public Health Code, Article L.1111-23.

2.8.2 Table on the links between EHRs and ePrescriptions

- ***Infrastructure***

Questions	Legal reference	Detailed description
Is the existence of EHR a precondition for the ePrescription system?		The DMP and the DP were designed to work together although at the current stage of implementation they are not inter-connected. In the near future, information in the DP will feed in the DMP in order for health professional to: - identify the treatment of the patient, - identify problems with compliance or redundancy, - improve the quality of prescriptions[71].
Can an ePrescription be prescribed to a patient who does not have an EHR?		The two systems are completely independent.

- ***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?		The DP is therefore a record on the distribution of medicine (*dispensation de médicaments*) rather than its prescription per say (*prescription de médicaments*). For instance, doctors, hospital doctors, and dentists do not feed into the system. Members of the healthcare team in a health institution, as well as private physicians, have access to DMPs whilst pharmacists do not have access to DMPs. Pharmacists have access to the DP. A pilot is currently on-going to ensure that nurses and chemists in health institutions can feed in the DP system[72].
Can those health professionals write ePrescriptions without having access to EHRs?		Access to the DMP or other electronic health record is not a prerequisite to prescription of medicines. Bearing in mind that the DP is a tool recording the distribution of medicine

[71] Information retrieved from the presentation of January 2010: http://unt-ori2.crihan.fr/unspf/2010_Nancy_Poitiers_Paulus_Seguin_DossierPharmaceutique/co/DMP.html (last access January 2014).
[72] Interview with the CNIL on 24th January 2014.

Questions	Legal reference	Detailed description
		and not its prescription, pharmacists working in private practice do not have access to DMPs.

2.9 OTHER REQUIREMENTS

None identified.

3 LEGAL BARRIERS AND GOOD PRACTICES FOR THE DEVELOPMENT OF EHRS IN FRANCE AND FOR THEIR CROSS-BORDER TRANSFER IN THE EU

- ***Good practices for the development of EHRs in France***

The French EHRs initiative has been launched since 2011 after nearly a decade of negotiations and different pilot phases. Since 2013, every pharmacist is required to feed into the French ePrescription scheme.

The implementation of the DMP architecture is very thorough and more stringent than existing EU law on data privacy. In this sense, the DMP is in many ways considered and designed to be under the control of the patient rather than to be the health professionals' file[73]. The patient can in particular update, download, delete or hide documents from the DMP. Moreover, safeguards have been set up with regard to this extensive control, ensuring continuity of care. For instance, when a patient wishes to erase information from the DMP, s/he is contacted by a medical correspondent who will inform the patient of the consequences, ensure erasure is the patient's will, provide the patient with a deletion form, and, finally, deletion will only happen after the expiry of a delay[74]. Other solutions exist and have been implemented, for instance the DP has been designed to bear a mention 'file incomplete' when information is removed. Moreover, the content of the DMP is open-ended and at the moment has not been regulated upon, as a result any document considered necessary for the coordination of health-related care can be updated to the DMP. If maintained unregulated, this practical approach grants flexibility and discretion to health professionals, as well as an approach based on the patient's needs rather than legal requirements[75].

Consent with regard to the creation or access to a DMP is dematerialised, and arises after information has been delivered by a health professional. However, in emergency situations, the DMP may still be accessed using the 'ice-breaker' procedure: subject to a written reasoned opinion and in the interest of the patient, an emergency physician can access a DMP without obtaining prior consent. Consent is further considered delivered to an entire team in the context of health institutions.

Each health data hosting institution must be approved ensuring security and confidentiality of DMP storage. France involves different stakeholders in the authorisation procedure, ensuring the technical (medicine), legal (privacy and medical law), and operational (IT) are all taken into account.

The authorisation procedure in France includes a control of the finances of the applicant, ensuring continuity of service. Each secondary use of health data must also be approved following a strict procedure whereby confidentiality of data is ascertained[76].

France is working towards the maintenance of register with every French health professionals. Moreover, France is involved in international negotiations for the establishment of health-related semantics that are planned to be incorporated in the DMP scheme[77].

- ***Potential legal barriers for the development of EHRs in France***

Extensive control on EHRs by the patient can potentially void the aim of EHRs as a professionals' information tool, in particular the EHR does not indicate if a file is incomplete. This has lead health professionals to distrust the system and not promote its use[78].

[73] Interview with the CNIL on 24th January 2014.
[74] Interview with the ASIP Santé on 20th January 2014.
[75] Interview with the CNOM on 22nd January 2014.
[76] Interview with the CNIL on 24th January 2014.
[77] Interview with the ASIP Santé on 20th January 2014.
[78] Interview with the CNOM on 22nd January 2014.

The current situation whereby the content of the DMP is potentially open-ended, yet the law foresees the adoption of a Decree detailing what health data should be included, leads to uncertainty of the DMP and its use[79]. An obstacle can arise in case of lack of harmonised content and categorisation requirements.

The notion of 'healthcare team' can be seen as restrictive and only arise in health institutions situations[80], therefore the modalities surrounding consent only concern the authorised health professionals involved with the patient (namely private practitioners and healthcare team). This situation therefore ignores the cross-sectorial element often present in relation to medical care (e.g. ambulatory, medico-social, health and safety), and poses issues with regard to shared medical secrecy[81].This is subject to enlargement in the upcoming new law under preparation.

With regard to the consent on the creation of DMPs, stakeholders[82] have recommended using a general opt-out procedure, whereby all the persons covered under the National Healthcare would have a DMP created. These persons could then expressly opt-out of the scheme. Indeed, at present, DMPs are created during consultations, therefore their creation is entirely left to health professionals on an individual basis, which slows down the deployment of the scheme. Furthermore, France has not regulated whether creating or updating a DMP can be considered part of the notions of 'medical act' or 'medical consultation', yet DMP activities subtract time out of medical practice. Issues of remuneration or financial incentives in this regard have not been addressed, as a result this time subtraction can be done at the expense of the patient, who still pays the full cost of a consultation, or at the expense of the professional who will take the necessary time out of his/her schedule. This means health professionals may not be willing to spend an appropriate time to feed into the system and can block the deployment of the scheme[83].

Both the procedure for approval of health data institution or secondary use of data are seen as repetitive and complex, potentially altering the progress of public health[84].

The national legislation does not set specific medical liability requirement related to the use of the DMP. As a result, the general rules on medical liability apply which has been described by stakeholders as fostering reluctance of health professionals to use and develop the system[85].

Work on a register of health professionals and health-related semantics are on-going. They are therefore not yet implemented and it remains to be seen how they will be. Whilst the DMP system is completely interoperable throughout France, it is not yet interoperable with the French ePrescription file, despite the law providing for their coordinated use. This should have been clarified at the outset of the development of each system[86].

[79] Interview with the CNOM on 22nd January 2014.
[80] Interview with the CNOM on 22nd January 2014.
[81] Interviews with the ASIP Santé on 20th January 2014 and CNOM on 22nd January 2014.
[82] Interviews with the ASIP Santé on 20th January 2014 and CNOM on 22nd January 2014.
[83] Interview with the CNOM on 22nd January 2014.
[84] Interviews with the ASIP Santé on 20th January 2014 and CNOM on 22nd January 2014.
[85] Interview with the CNOM on 22nd January 2014.
[86] Interview with the CNIL on 24th January 2014.