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 Germany

time.lex

milieu
Law & Policy Consulting

07.03.2013

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

This report was completed by Prof. Dr. Nikolaus Forgó and Ass. iur. Fritz-Ulli Pieper. The views expressed herein are those of the consultants alone and do not necessarily represent the official views of the Consumers, Health and Food Executive Agency (Chafea) .

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

Executive Summary

This report identifies and examines the national laws of Germany regarding Electronic Health Records (EHRs) and ePrescriptions and identifies legal barriers and good practices for their development as well as for cross-border transfer of data from EHRs within the EU. It provides background information on the stage of development of EHRs in Germany by giving an overview of current EHR systems in place, looking at their general institutional setting and providing a first introduction to the respective legal settings as well as an outlook on prospective future legal developments (Section 1). Furthermore it provides a comprehensive description of the legal requirements applying to EHRs in Germany (Section 2). This information will then be further used to identify potential legal barriers and good practices for the development of EHRs in Germany (Section 3).

1. Stage of development of EHRs in Germany

In Germany, several concepts of electronic records in the (public) health domain exist with different maturity levels. The main focus of this study lies on the Electronic Health Records (EHRs) which are regulated within § 291a SGB V (5th book of the Social Security Code). The provisions therein constitute a basic framework but remain very abstract in terms of specific technical, organizational and content-related requirements.

The lawmaker installed the framework of EHRs within the broader concept of an "Electronic Health Card", which is the basic setup for the implementation of a nationwide, technically mature *telematics infrastructure* for interconnecting roughly 80 million insurants, 270.000 doctors, 2.000 hospitals and 300 health insurance companies. The proceedings in that area serve the goal to create an arrangement of regulations within the German Social Security Code relating to statutory health insurance companies, to enable them to ultimately introduce, foster and maintain the use of information and communication technologies within the public health domain. The most important stakeholders are the German Federal Ministry of Health (BMG), which is responsible for the design of the legal framework of the telematics infrastructure and the German Society for Telematics (gematik), the latter being an umbrella organization formed by the most important stakeholders and unions in the German social security and particularly health insurance area. Gematik is responsible for concrete undertakings in elaborating and implementing the telematics infrastructure.

To date, however, the EHC only transfers the previous functions of the German insurance card to a new card concept. The legislator only set up basic regulations. It will be the task of the German social security institutions to develop the technical features by self-administration. The concept of EHRs according to § 291a SGB V is still in the conceptual phase. Research and individual pilot projects are being conducted. Many projects and initiatives already take into account technical and legal aspects of EHRs.

Some electronic record initiatives aim to push forward the exploitation of electronic case records, which however are limited in scope in comparison to EHRs, because they are limited to a specific medical case of a patient. A privately designed EHR is regulated in § 68 SGB V, setting up only financial rules regarding support from health insurance companies for insurants aiming to make use of the concept.

2. Summary of legal requirements applying to EHRs

The main legal requirements for EHRs are regulated in § 291a SGB V. Further data protection provisions are regulated in the relevant data protection section in §§ 284 – 305b SGB V. Moreover, in some cases, the general data protection regulations of the German Federal Data Protection Act (BDSG) may apply. A range of other provisions dealing with more general scopes might also be applicable to EHRs, such as limitation rules or rules on archiving durations.

There is a legal definition of general content in EHRs, while regulations on health data to be included in EHRs are rather abstract, which complies with the legislator's approach of setting up a general framework and leaving the concrete arrangement of EHRs to the self-governing bodies in a formalised procedure. Consent is an essential requirement for the work with EHRs. The regulations on consent are accompanied by further informational obligations for the involved stakeholders. There are also specific rules on access to EHRs within the setup of the EHC, whereas concrete determinations for different categories of health data are not in place, since only the legal groundwork is regulated. The insurants have access and erasure rights and the access for health professionals is generally connected to further requirements. There are no specific medical negligence rules related to the use of EHRs but various grounds for liability for medical malpractice might apply for the work with EHRs. Archiving durations are only regulated generally in different German acts and do not refer to the use of EHRs. There are no specific rules regulating secondary uses to the use of EHRs. As there is no specific EHR scheme in place yet, it cannot be assessed how the interoperability of EHRs would function. However, the legal setup of a telematics infrastructure in Germany by the legislator shall be "interoperable and compatible", so the basic rules for providing interoperability are laid down in the law. The only relation between ePrescriptions and EHRs is their common regulation within the setup of the EHC, i.e. within the setup of the telematics infrastructure. But they are to be seen as different, independent applications.

3. Good practices and legal barriers

As EHRs have not been established in Germany yet, good practices could not be identified yet. The most important factor governing EHRs and ePrescriptions in Germany at the moment could be seen as both a legal barrier as well as a useful good practice: their implementation in a wider framework of setting a telematics infrastructure to bring healthcare on national level to the next generation within the striving information and communication technologies.

An abstract definition of the concept of an EHR provides for great flexibility for practical undertakings. However, practical testing is needed. This does not necessarily constitute a legal barrier but rather a time constraint. However, an undetermined approach by the German legislator can also be seen as a legal barrier. Ultimately, the complex structure of German social security law, the need to respect data protection requirements and extensive technical feasibility considerations, especially focused on interoperability, form a challenging ground for the development of EHRs and ePrescriptions within a telematics infrastructure in Germany.

Contents

List of abbreviations

BDSG	"Bundesdatenschutzgesetz", Federal Data Protection Act
BÄK	"Bundesärztekammer", Federal Medical Association
BfDI	„Bundesbeauftragter für den Datenschutz und die Informationsfreiheit", German Federal Data Protection Authority
BMG	"Bundesministerium für Gesundheit", German Federal Ministry of Health
BVerfG	"Bundesverfassungsgericht", German Constitutional Court
BZÄK	"Bundeszahnärztekammer", Federal dentists Association
DKG	"Deutsche Krankenhausgesellschaft", German Hospital Federation
DPA	Data Protection Authority/Authorities
eEPA(s)	"Einrichtungsübergreifende elektronische Patientenakte", electronic patient record(s) between different medical institutions
EHC(s)	Electronic Health Card(s)
EHIC	European Health Insurance Card
EHR(s)	Electronic Health Record(s)
gematik	„Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH", Society for telematics
GKV(en)	Gesetzliche Krankenversicherunge(n), National Association of Statutory Health Insurance Funds
GMG	"GKV-Modernisierungsgesetz", the law to modernize the statutory health insurance
HIC	Health Insurance Card
NJW	"Neue Juristische Wochenschrift", a weekly German law journal
NZS	"Neue Zeitschrift für Sozialrecht", a German journal on Social Security Law
KBV	"Kassenärztliche Bundesvereinigung", National Association of Statutory Health Insurance Physicians
KZBV	"Kassenzahnärztliche Bundesvereinigung", German Federal Association of Sick Fund Dentists
MedR	"Medizinrecht", a German journal on medical law
SGB	"Sozialgesetzbuch", German Social Security Code

§ “Signum Sectionis”, Section (of a law)

1. General context

This section will provide background information on the stage of development of EHRs in Germany. It will give an overview of the competent authorities in charge of the implementation of EHRs policies, point out the according distribution of competences and highlight the legal background. This section will therefore focus on current EHR systems in place (Section 1.1), provide an overview of their general institutional setting (Section 1.2) and finally give a first introduction to the respective legal settings as well as an outlook on prospective future legal developments (Section 1.3).

1.1. EHR systems in place

At least eight different systems of "electronic medical records" can be distinguished in Germany.[1] What is internationally known as an "Electronic Health Record" ("*EHR*") can generally be seen as an "electronic patient record for various medical cases between different medical institutions", although terms may differ widely depending on the (for example institutional) background, making it difficult to reach exact, reliable classification.[2]

The idea of EHRs and ePrescriptions in Germany is embedded in the concept of an "electronic health card" ("*elektronische Gesundheitskarte*", "*EHC*"). The legal basis for this card has been set out in the beginning of 2004 within the "*law to modernize the statutory health insurance*" ("*GKV-Modernisierungsgesetz*", "*GMG*"). This law seeks to advance the concept of the former "health insurance card" ("*Krankenversichertenkarte*", "*HIC*"), and adapt its rules to the modern information society as well as establish a telematics infrastructure in the public health domain.[3] The law sets the groundwork for interconnecting roughly 70 million insurants, 200,000 doctors, 20.000 pharmacies, 2,000 hospitals and 130 health insurance companies.[4]

What is internationally seen as an EHR would in Germany correspond with what is defined as an "electronic patient record between different medical institutions" ("*einrichtungsübergreifende Elektronische Patientenakte*", "eEPA"). This record would store the most important data and documents of all treatments of a patient for different medical institutions, guided and moderated by a physician, if necessary with entries by the patient assigned by the physician.[5] It does not exist in Germany yet.

The central piece of legislation regarding EHRs in that context is § 291a of the fifth book of the German Code of Social Security Law (SGB V). § 291a (3) sentence 1 SGB V states that the EHC has to be suited to support several applications. § 291a (3) sentence 1 point 4 SGB V specifies that the card has to support the processing of "*data about medical findings, diagnoses, therapy measures, treatment reports and immunizations for a comprehensive documentation of various medical cases between different medical institutions*". This is a definition by law on what the German legislator considers to be an EHR. Therefore, EHRs in Germany are to be seen as an application model or a function, respectively, of the EHC. There are mandatory and voluntary applications within the usage scenario of the card; EHRs are a voluntary application, the ePrescription is a mandatory application.[6]

It could be argued that the concept of (national) EHRs according to § 291a SGB V cannot be seen as

[1] ZTG Zentrum für Telematik im Gesundheitswesen GmbH, AK EPA/EFA der Initiative eGesundheit@nrw, Elektronische Akten im Gesundheitswesen, Nutzen, Ausprägungen, Datenschutz Elektronische Akten im Gesundheitswesen, Ergebnisse des bundesweiten Arbeitskreises EPA/EFA, p. 16, available at http://egesundheit.nrw.de/wp-content/uploads/2013/08/AKEPA-eFA.pdf.
[2] ZTG Zentrum für Telematik im Gesundheitswesen GmbH, ibid., p. 13, 17.
[3] Lücking in: Sodan, Handbuch des Krankenversicherungsrechts, 2nd ed. 2014, § 41, Rec. 42.
[4] Speth/Koutses, MedR 2005, 493 (493) m. w. N.
[5] ZTG Zentrum für Telematik im Gesundheitswesen GmbH, op. cit. 1, p. 16.
[6] Krauskopf, Soziale Krankenversicherung, Pflegeversicherung, 83. Ergänzungslieferung 2013, SGB V § 291a, Rec.Rec. 19 ff., 32 ff.

fully matching the concept of (national) eEPAs; in EHRs, patients have more access rights and influential possibilities. However, the concepts of EHRs and eEPAs are very similar.[7] Also, the legislator decided to implement the concept of EHRs in the Social Security Code. Hence, for the purpose of this study, the EHR regulated within § 291a SGB V shall be seen as the basic concept of EHRs in Germany.

However, it is important to notice that the German legislator has only set out basic regulations that need to be complemented by specific technical developments in a self-administrative manner by social security institutions.[8] Concrete settings and contents of EHRs will have to be elaborated further within the establishment of the telematics infrastructure. The social security institutions are hence obliged by law to create an interoperable and compatible information-, communication- and security infrastructure for the implementation and application of the EHC with special focus on EHRs and ePrescriptions, pursuant to § 291a (7) sentence 1 SGB V. This task is to be administered by an organisation responsible for the telematics applications for the eHealth card, namely the „*gematik*", pursuant to §§ 291a (7) sentence 2, 291b SGB V. It has to be noted though, that although the legislator specifically mentioned EHRs and ePrescriptions as leading applications within the development of the telematics infrastructure, the priorities have been moved to other applications after first appraisals and realignments regarding the implementation planning for a telematics infrastructure.[9]

First of all, the *gematik* has developed specification measures for the card. Furthermore, it gave formal admissions to card producers and health insurance companies as card issuers. Also, admissions for stationary and mobile card reading devices have been issued. Those were seen as basic requirements for the so called "basic rollout" which includes a comprehensive distribution of cards.

However, the wider distribution of the cards to the patients took the responsible health insurance companies until the end of 2011. One possible reason for this might be that § 4 (6) SGB V sets out financial sanctions (only) for the case that health insurance companies do not distribute the cards to at least 10% of their insurants until the end of 2011 and 70% until the end of 2012.[10]

At this moment, the EHC only transfers the previous functions of the insurance card to a new card concept. It is generally acknowledged that further telematics functions as a basis for further medical applications require extensive additional testing procedures.[11] As of now, two applications are in place: the insurants master data, pursuant to § 291a (2) sentence 1 clause 1 SGB V, and the European health insurance card (EHIC), pursuant to § 291a (2)sentence 1 point 2 SGB V. Five more applications are to be introduced in a two-step online rollout.[12] EHRs are not part of it. Apart from that, up until now, ten amendments have been carried out involving § 291a SGB V alone, which leads to the conclusion that the various reformation efforts as well as the complete implementation of the EHC, and therefore also the EHR, is not foreseeable as of yet. In conclusion, a functioning EHR scheme according to § 291a SGB V is not yet in place in Germany.

Apart from the official setup of an EHR within § 291a SGB V, the lawmaker also provided for an alternative, privately organized framework of an EHR: § 68 sentence 1 SGB V states that for the

[7] ZTG Zentrum für Telematik im Gesundheitswesen GmbH, op. cit. 1, p. 41 f.
[8] Speth/Koutses, MedR 2005, 493 (494); more specifically on this see section 1.2 and 1.3.
[9] Scholz, in: Beck'scher Online-Kommentar Sozialrecht, SGB V, § 291a, Rec. 3.
[10] Bales/von Schwanenflügel, Die elektronische Gesundheitskarte, NJW 2012, 2475 (2476).
[11] Lücking in: Sodan, Handbuch des Krankversicherungsrechts, 2. Auflage 2014, § 41, Rec. 45; an example of a project regarding EHR is carried out by the "Fraunhofer Institute for Software and Systems Engineering" with a duration from 2009 until the end of 2014, see https://www.sit.fraunhofer.de/de/angebote/projekte/elektronische-patientenakte/; German stakeholders are also involved in the epSOS-project on EU-level as well.
[12] See http://gematik.de/cms/de/egk_2/anwendungen/vorbereitung/vorbereitung_1.jsp; the *gematik* accordingly took out a call for proposals in 2012, see http://ted.europa.eu/udl?uri=TED:NOTICE:116639-2012:TEXT:DE:HTML; while conducting the desk research, the *gematik* held an official informative meeting as kickoff for the testing of the first of these two steps, see http://gematik.de/cms/de/header_navigation/presse/meldungen_1/Meldungen.jsp# or http://www.e-health-com.eu/service/veranstaltungsberichte/details-veranstaltungsbericht/gematik-informationsveranstaltung-zu-ors1-br-10-februar-2014/b089603ff032ae19855509f68c913b52/.

improvement of quality and cost effectiveness, the health insurance companies can grant financial assistance to their insurants for matters of electronic provision of services of (private) third parties relating to patient health data. This alternative approach therefore opens a second route to establishing EHRs in the medical domain by involving patients on the one hand and private companies which create or handle EHR platforms on the other hand; these EHR platforms therefore are not regulated by the statutory health insurance regulations. The goal is a setup of a personal health management solution completely within the sphere and up to the decision of the patient.[13] It could therefore be called a "personal electronic health record", "PHR" ("*persönliche Elektronische Patientenakte*", "pEPA").[14] However, the further arrangement of the financial support has to be laid down in an association charter of the health insurance company, § 68 sentence 2 SGB V, and may therefore widely vary among the institutions. Moreover, the different solutions of private platform providers may vary in their technical and organizational framework. Finally, it lies within the self-administrative discretion of the health insurance companies to promote these kinds of records; there is no duty to introduce this concept.[15]

Currently, concepts of an inter-institutional electronic case record ("*elektronische Fallakte*", "EFA") are being developed by stakeholders of the medical domain. This record serves a collective treatment of one particular health case of one patient between different institutions and is administered by health professionals. It could therefore be seen as a pre-stage to the EHR. Since this does not include treatment of more than one particular case, it does not match the understanding of a (wider) EHR as described above.

1.2. Institutional setting

The lawmaking process in Germany is governed by the German constitution. The German ***Bundestag***, the Federal State Council ("***Bundesrat***") and the acting German government ("***Bundesregierung***") are allowed to initiate the lawmaking process by presenting draft acts which then need to pass the German Bundestag in a procedure regulated by the German constitution. First and foremost, these three entities therefore mark the starting point for any law, and therefore also legislation concerning EHRs as in §§ 291 sqq. SGB V.

The German Federal Ministry of Health ("***Bundesgesundheitsministerium***", "***BMG***") is part of the Bundesregierung and therefore the central state entity in this context. It is the governing ministry regarding all health related issues at federal level. The legislator reserves several possibilities to steer and impair the practical composition of the telematics infrastructure in Germany.[16] It has several supervisory control rights, especially towards the *gematik* as the responsible entity for the setup of the telematics infrastructure.

The most important stakeholders in the German social security area are obliged by law to form an umbrella organization, which shall be responsible for the creation of the telematics infrastructure, the gematik ("***Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH***"), pursuant to §§ 291a (7), 291b SGB V. It is the key entity regarding the implementation and application of the telematics infrastructure in Germany in general and specifically inter alia responsible for the admission of components and services of the infrastructure. As stakeholders, the law includes the National Association of Statutory Health Insurance Funds ("***GKV-Spitzenverband***"), the National Association of Statutory Health Insurance Physicians ("***Kassenärztliche Bundesvereinigung***", "***KBV***"), the German Federal Association of Sick Fund Dentists ("***Kassenzahnärztliche Bundesvereinigung***", "***KZBV***"), Federal Medical Association ("***Bundesärztekammer***"), Federal Dentists Association ("***Bundeszahnärztekammer***"), German Hospital Federation ("***Deutsche Krankenhausgesellschaft***", "**DKG**") and the Federal Union of German Associations of Pharmacists

[13] Scholz, in: Beck'scher Online-Kommentar Sozialrecht, SGB V, § 68, Rec. 1; Becker/Kingreen, SGB V, § 68, Rec. 1, 2.
[14] ZTG Zentrum für Telematik im Gesundheitswesen GmbH, op. Cit. 1, p. 16.
[15] Becker/Kingreen, SGB V, § 68, Rec. 4.
[16] Bales/von Schwanenflügel, NJW 2012, 2475 (2479).

("Bundesvereinigung Deutscher Apothekerverbände", "ABDA").

The *statutory health insurance companies* themselves play an important role in distributing the EHCs, which is accompanied, for example, by informational duties regarding insurants' data protection rights.

Moreover, the German federal office for information security ("***Bundesamt für Sicherheit in der Informationstechnik***", "***BSI***") plays an important role in the certification procedures regarding the EHC. While the *gematik* is responsible for functionality and interoperability of technical components of the EHC, the BSI is responsible for collaborating with the *gematik* to elaborate guidelines for security certification measures.

Furthermore, the German federal data protection authority ("***Bundesbeauftragter für den Datenschutz und die Informationsfreiheit***", "***BfDI***") is entitled to participate in the advisory board of the *gematik*, which is inter alia supposed to be consulted before decisions of fundamental concerns, pursuant to § 291b (2) point 4 SGB V. Also, the BfDI itself has the opportunity to comment towards the BMG on the decisions of the *gematik* concerning the regulations, implementation and application of the telematics infrastructure, pursuant to § 291b (4) sentence 1 clause 2 SGB V.

Finally, various private companies are involved as stakeholders (mainly) in research activities focusing on the implementation of the EHC and the telematics infrastructure in general and therefore also of EHRs.

1.3. Legal setting and future legal development

The main legal background concerning EHRs and ePrescriptions is provided in the fifth book of the German Code of Social Security Law. Therefore, to better understand this legal background, it is useful to give a very brief[17] overview of the general setup of German social security law.

Social security law in Germany follows the *Social Security Principle* of Art. 20 (1) within the German constitution ("*Grundgesetz*", "GG"). One elementary pillar of this principle, and thus also of social security law as a derivation from the Social Security Principle, is the concept of *social insurance*.[18] Within this pillar, there are five associated branches, one of which is *health insurance*.[19] Each branch is administered by *social security institutions*. Institutions of the health insurance branch are the *health insurance companies*.[20]

The German legislator chose the model of self-administration regarding the organisation of the institutions and hence also the health insurance companies, pursuant to § 29 (1), (3) SGB IV, which means the autonomous realization of public duties, to connect societal and governmental spheres.[21] They are public law bodies with legal capacity, pursuant to § 29 (1) SGB IV and § 4 (1) SGB V. Their practice is however subject to control and steering mechanisms of the government under its federal supervision activities, pursuant to §§ 87 (1), (2), 88 sqq. SGB IV. This factual constraint – the organisation of self-administration within the barriers of the governmental legal framework – leads to a broad influence of union associations and chambers.[22]

Germany follows the dual model between statutory health insurance companies and private health

[17] German social security law is, also in scientific discourse, considered to be extremely complex; this overview intends to point out just the very basic setup to help better understand the legal framework on which EHRs and the ePrescription are based.
[18] von Maydell, in: von Maydell/Ruland/Becker, Sozialrechtshandbuch (SRH), 5. Auflage 2012, § 1, Rec. 3.
[19] Becker, in: von Maydell/Ruland/Becker, Sozialrechtshandbuch (SRH), 5. Auflage 2012, § 13, Rec. 1.
[20] Becker, in: von Maydell/Ruland/Becker, Sozialrechtshandbuch (SRH), 5. Auflage 2012, § 15, Rec. 25.
[21] Becker, in: von Maydell/Ruland/Becker, Sozialrechtshandbuch (SRH), 5. Auflage 2012, § 13, Rec. 4.
[22] Becker, in: von Maydell/Ruland/Becker, Sozialrechtshandbuch (SRH), 5. Auflage 2012, § 13, Rec. 4; the most important stakeholders in the health care domain have also been pointed out to take part in the second part of this report, the interviews.

insurance companies. It is estimated that roughly 90% of all insurants within the health insurance scheme are insured by statutory health insurance companies.[23] The main legal framework regarding the statutory health insurance is the fifth book of the German Social Security Code ("*Sozialgesetzbuch V*", "SGB V"). Health insurance has the goal to preserve, restore or improve the health of the insurants, pursuant to § 1 sentence 1 SGB V. Diagnostic findings, medical reports or therapy recommendations need to adapt to the modern information and communication society to continue reaching this goal. Therefore, the German legislator created an arrangement of regulations within the German social security code relating to statutory health insurance companies, to enable them to introduce information and communication technologies within the public health domain.[24]

The basis for this envisaged *telematics infrastructure* is the EHC.[25] Since the EHR and ePrescriptions conceptually are applications of this card, the legislation applicable for the card is generally also applicable for EHRs and ePrescriptions. Other regulations covering more general aspects, namely electronic data processing activities in the health domain,[26] would also apply to the concept of EHRs and ePrescriptions. Furthermore, regulations from other legislation with different scopes might be applicable to electronic records, such as the rules on data protection and minimum archiving durations. Hence, the most important legislation regarding EHRs and ePrescriptions consists inter alia of the following:

- **SGB I** contains basic regulations for the whole complex of social security law. Moreover, general provisions for all social security institutions can be found in the **SGB IV**, which serves as an overall introductory code of law concerning social insurance in general.
- The **SGB V** regulates the statutory health insurance. The main regulations in terms of a legislative basis for the EHC are **§§ 291, 291a, 291b SGB V**. The EHR is specifically mentioned as one envisaged applications of the EHC, **§ 291a (3) point 4 SGB V**; the ePrescription is specifically mentioned in **§§ 291a (2) sentence 1 point 1, 87 (1) sentence 6 SGB V**.
- **291a, 291b SGB V** also include several provisions related to data protection of patient data. Social data protection is also regulated more general in the **SGB X**. Moreover, most general data protection regulations are laid down in the German code for data protection ("**Bundesdatenschutzgesetz**", "**BDSG**"). The relation between the codes and which data protection regulations are applicable need to be investigated individually for each case, they are subject to the rule "*lex specialis derogat legi generali*".[27]
- A "decree on test measures for the implementation of an EHC" was set up and continuously renewed by the German Ministry of Health to test and further develop the telematics infrastructure which is necessary for the introduction and application of the EHC, pursuant to **§§ 1, 2 (1) sentence 1 TestV**.
- **§ 68 SGB V** provides for a setup of patient-owned and -controlled private "EHRs".
- To access data on the EHC, the legislator implemented the need to own a medical profession ID card, "*Heilberufsausweis*". According to **§ 291a (5) sentence 3 SGB V**, this ID needs to be equipped with an advanced electronic signature. Therefore, the state laws for the medical professions as well as the German signature codes "**Signaturgesetz**" and "**Signaturverordnung**" apply.
- **§ 630f** of the German Civil Code, "**Bürgerliches Gesetzbuch**","**BGB**" regulates a documentation duty also concerning electronic records, where the physician has the choice to conduct documentation either on paper or electronically.
- **§ 10 Musterberufsordnung Ärzte**, the Medical Association's professional code of conduct, regulates a documentation duty and archiving rules also concerning (voluntary) electronic records.

[23] Sodan, in: Sodan, Handbuch des Krankenversicherungsrechts, 2. Auflage 2014, § 1, Rec. 13.
[24] Pitschas, NZS 2009, 177 (177).
[25] Bales/von Schwanenflügel, NJW 2012, 2475 (2475).
[26] Bales/von Schwanenflügel, NJW 2012, 2475 (2476).
[27] Where applicable, this relation shall be mentioned in the tables in section 2.

- **§ 203 (1) point 1** of the German Criminal Code, "**Strafgesetzbuch**", "**StGB**" regulates punishments for breaching medical confidentiality.
- The requirement of a written form can in an electronic context be replaced by, for example, advanced electronic signatures; corresponding regulations can be found in **§ 126a BGB**, **§ 3a** of the Administrative Procedure Code, "**Verwaltungsverfahrensgesetz**", "**VwVfG**", and **§ 36a SGB I**.

Finally, many initiatives already take into account technical and legal aspects of EHRs. The e-Health-initiative of the German Federal Ministry of Health has been introduced within the seventh national IT summit in 2013.

The German state North Rhine-Westphalia is a forerunner in research projects, test scenarios and showcases. The private company ZTG, the center for telematics and telemedicine, as a competency center with the goal to develop, implement and spread modern information and communication technologies for the health sector, is based there and coordinates the initiative "eGesundheit.nrw", a state initiative to bring together various projects dedicated to the advancement of information and communication technologies in the health sector. It is therefore to be expected that many projects or initiatives are going to carry out field tests in the near future also involving EHRs and ePrescriptions.

2. Legal requirements applying to EHRs in Germany

This section will give a comprehensive description of the legal requirements applying to EHRs in Germany by answering specific questions on several EHRs related topics. This information will be used to identify potential legal barriers and good practices for the development of EHRs in Germany.

The focus in the context of EHRs and ePrescriptions clearly lies on § 291a SGB V, since it regulates the EHC as the primary structure for the implementation of EHRs and ePrescriptions. Where necessary, other relevant legislation shall be observed within the comprehensive descriptions in the tables. In order to put the answers to the questions into a broader context, a short introduction to the setup of the SGB V as the main piece of legislation relevant for EHRs and especially the provisions specifically dealing with EHRs is given.

The SGB V contains various chapters and mainly regulates the correlations between the health insurance companies and the insurants, as well as the various care providers.[28] There is a general conflict between the general right to self-determination and the corresponding right to social data protection on the one hand, and the advancement of the health sector to fit the information society as well as according cost-effectiveness motivations on the other hand.[29] Therefore, § 291a (1) SGB V states the goal of the EHC: to improve the cost effectiveness, quality and transparency of medical treatment. At the same time, patient sovereignty and individual responsibility of an insured person shall be strengthened.[30] § 291a SGB V is located in the tenth chapter, "Insurance and benefit data, data protection, data transparency". It contains general principles of data usage, regulations concerning the processing of data, data transparency, erasure and duties to give information.

Transmissible data are hence regulated under an own, detailed, sector specific social data protection law regime.[31] This sector-specific law usually supersedes the more general regulations of the BDSG.[32] The BDSG is only applicable where no other regulations govern personal data, pursuant to § 1 (3) sentence 1 BDSG.

Where deemed necessary or applicable, an apportionment between the two acts is being carried out. However, since the regulations on the setup of the telematics infrastructure, and therefore also the ones taking into account data protection measures, are still rather broad and do not yet stand in relation to a functioning §291a-EHR scheme, the relationship between the sector specific SGB V and the BDSG remains yet to be fully ascertained.

Since the EHR and the ePrescription in Germany are rooted within the setup of an EHC, it is also advisable to give an overview of the clauses regulating this card. Most of the general regulations also apply to EHRs and the ePrescriptions, since they are a applications of the EHC. A very basic example: An insurant's master data (like for example the name, sex and date of birth) must be stored on the card, pursuant to §§ 291 (2a) sentence 3, 291a (2) sentence 1 SGB V. These data would then also be available to serve as master data when working with the EHR of the insurant. However, since there is no functioning EHR scheme in place in relation to the regulations within the SGB V, the concrete setup of EHRs might as well be a completely separate one within the EHC framework, where all applications function completely independantly. The explanations in this study partly need to take into account hypothetical or anticipatory principles.

[28] Detailed overview by Ingwer Ebsen, in: von Maydell/Ruland/Becker, Sozialrechtshandbuch (SRH), 5. Auflage 2012, § 15, Rec. 56 ff.
[29] Pitschas, NZS 2009, 177 (178).
[30] BT-Drucks. 15/1525, 72.
[31] Pitschas, NZS 2009, 177 (178)
[32] Binne/Rixen, in: von Maydell/Ruland/Becker, Sozialrechtshandbuch (SRH), 5. Auflage 2012, § 10, Rec. 15.

This report shall keep a focus on EHR and ePrescriptions (and therefore the EHC) regarding data protection regulations. Even though there might be regulations according to the Cross-Border Healthcare Directive 2011/24/EU, this report therefore only takes into account the relevant legislation concerning EHRs and the ePrescription, mainly the SGB and partially the BDSG.

The basic setup of § 291a features 16 subparagraphs (§ 291a (1) - § 291a (8)). Subparagraph 1 stipulates the objectives and purposes of the advancements towards the EHC. Subparagraph 1a foresees that most provisions are applicable also to private health insurance schemes, should these envisage to implement a similar card concept. Subparagraph 2 states the mandatory applications of the card, Subparagraph 3 the voluntary applications as well as information and consent duties. Subparagraph 4 regulates the access rights of different persons to the card. Subparagraph 5 statutes further data protection requirements and further technical necessities for access. Subparagraph 5a is tailored to specific applications of the EHC not including EHRs or ePrescriptions. Subparagraph 5b stipulates specific duties for the gematik. Subparagraph 5c obliges the German states to determine the centres responsible for acknowledgement of the validity and permission to conduct a medical profession as well as the handout of special professional ID cards. Subparagraph 6 states a right to erasure and logging obligations for data protection purposes. Subparagraphs 7 to 7e constitute the groundwork for the setup of the gematik as well as important financial provisions for its undertakings and also regulative measures for the supervisory body, the German Federal Ministry of Health. Subparagraph 8 finally states a protection right of the card holder regarding forbidden disadvantages for denial of access to the card.

2.1. Health data to be included in EHRs

2.1.1. Main findings

The rules on which health data are to be included in EHRs are rather vague. That complies with the lawmaker's approach of setting up a general framework and leaving the concrete arrangement of EHRs to the self-governing bodies in a formalised procedure. However, the content clearly focuses on medical data only. Furthermore, the lawmaker stipulates a legal definition of what an EHR actually is within the law, which can serve as an important classification criterion where needed. It should be noted, however, that, as explained in Section 1 and 2 above, an EHR within the meaning of an interoperable system where different health service providers share the data on the respective patient is not in place in Germany yet.

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?)	§ 291a (3) Sentence 1 point 4 SGB V	The German legislator provided for the groundwork of EHRs, which includes a legal definition of the term itself. This definition refers to "*medical findings, diagnoses, therapy measures, treatment reports and immunizations"* as content of an EHR.
Are these data restricted to purely medical information (e.g. physical or mental health, well-being)?	§ 291a (3) sentence 1 point 4 SGB V	"*Medical findings, diagnoses, therapy measures, treatment reports and immunizations*" solely refer to medical (treatment) data.
Is there a definition of EHR or patient's summary provided in the national legislation?	§ 291a (3) sentence 1 point 4 SGB V	EHR (in the SGB referred to as 'electronic patient record') is defined as a n application that supports the collection, processing and utilization of data concerning medical findings, diagnoses, therapy measures, treatment reports and vaccinations for a comprehensive documentation of various medical cases [of one patient] between different medical institutions.
Are there any requirements on the content of EHRs (e.g. detailed requirements on specific health data or general reference to health data)?	§ 291a (3) sentence 1 point 4 SGB V	The legal definition in § 291a (3) sentence 1 point 4 SGB V is wide (see above first question). A statement from the German Medical Association from mid-July furthermore states that with regard to the *eHealth-Governance-Initiative* guidelines for EHRs, a collocation of a non-exhaustive list of specific EHR content "is not reasonable at this point in time".[33]
Are there any specific rules on the use of a common terminology or coding system to identify diseases, disorders, symptoms and others?	-	Since the legislator has only set out ground rules and EHRs are not part of the basic rollout procedures, no specific rules exist. In any case, there is the obligation laid down in the law to design the EHC in an interoperable and compatible way (see below 2.7.2).
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)?	-	The definition of EHRs contains only a general statement about content: "*medical findings, diagnoses, therapy measures, treatment reports and immunizations"* are part of it. Even though access is regulated in an own section of § 291a SGB V (see below 2.4.2), a differentiation between different kinds of data is not provided by law.
Are there any specific rules on identification of patients in EHRs?	-	-

[33] Stellungnahme der Bundesärztekammer zu den geplanten Inhalten einer elektronischen Patientenakte auf Basis des epSOS-Datensatzes vom 16.07.2013, available at http://www.bundesaerztekammer.de/downloads/BAeK-Stellungnahme_zu_den_geplanten_Inhalten_einer_elektronischen_Patientenakte_auf_Basis_des_epSOS-Datensatzes_16.07.2013.pdf.

Questions	Legal reference	Detailed description
Is there a specific identification number for eHealth purposes?	§§ 291a (2) sentence 1 Clause 1, 291 (2) sentence 1 point 6 SGB V	The EHC has to contain the insurant's master data, pursuant to §§ 291a (2) sentence 1 Clause 1 SGB V, which consists of the data which was also foreseen to be available on the old health insurance card (HIC), under § 291 (2) point 6 SGB V. Therefore, the health identification number was originally not designed for eHealth purposes. But as the EHC is supposed to fully replace the old card and will function as the pioneer practice for telematics in the health sector also containing an individual identification number, it can be argued that this number serves a specific function for eHealth purposes. Since this number is unique and potentially easily relatable to a certain person, this number would have to be regarded as (under certain circumstances even sensitive) personal data. There are no specific rules on constraints of usage because of, for example, a potential easy interoperability. However, § 290 (2) sentence 2 SGB V states that the identification number has to be issued by a centre of trust, separated spatially, organisationally and regarding staff from the card-issuing health insurance companies. Furthermore, § 291 (1) sentences 3, 4, 5 SGB V state that the health insurance identification number may not be the same as the separate pension insurance identification number, or that if the pension insurance identification number is used to create a health insurance identification number, when according to the state-of-the-art of science and technology it is not possible to draw conclusions about the person behind the numbers from the interconnection of the two.

2.2. Requirements on the institution hosting EHRs data

2.2.1. Main findings

Since a fully functioning EHR scheme is not yet in place, requirements on the institutions hosting EHRs data only exist in a broader sense. Institutions, however, will have to comply with specific autorisation requirements.

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?	-	Since the German legislator laid down only the basic rules of the development of a telematics infrastructure and the gematik has until now only begun with the basic rollout which does not include EHRs and the ePresciption, no specific rules exist. Specifically, § 291a (2) SGB V does not provide for rules regarding the storage location of data on EHCs.[34] It hence also remains unclear whether hospitals, physicians or health insurance companies would have to provide the hosting and management infrastructure. However, there is an obligation to store emergency data, which is another application of the EHC, on the card itself, § 291a (3) sentence 1 SGB V so that they can be accessed without network access. In reverse, this would mean that there is at least no obligation to store data (other than emergency data) on the EHC itself. In any case, this would not be very likely as these data can easily sum up to large amounts of memory size.
Is there a need for a specific authorisation or licence to host and process data from EHRs?	-	Services and provider have to be authorised by gematik (§291b, 1b).
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)?	-	Services and provider have to be authorised by gematik (§291b, 1b).
In particular, is there any obligation to have the information included in EHRs encrypted?	-	No specific legal regulations. However encryption of data or equivalent measures to prevent unauthorized data access might be required by gematik for authorisation of EHR Services and providers
Are there any specific auditing requirements for institutions hosting and	-	No specific legal regulations. However auditing might be required by gematik for authorisation of EHR Services and providers

[34] Pitschas, NZS 2009, 177 (182) indicates that the German legislator only provided for the basic groundwork in that matter to be able to conduct the concrete setup of new applications according to the current technical state-of-the-art and also implement new findings. On the other hand, this would lead to serious safety hazards, especially regarding the ePrescription, which would pose high demands towards the availability of the system, which could be contradicted by for example server timeouts. An open implementation scheme would not help in that matter, since only realtime exploitation would show implications beyond testing measures.

Questions	Legal reference	Detailed description
processing EHRs?		

2.3. Patient consent

2.3.1. Main findings

The German legislator made consent an essential requirement for the use of the EHC (which includes the future use for EHRs). There are specific rules on consent not only for the initial use of the EHC but also for the use of specific applications, meaning that there has to be a first consent to use the card and another, second consent for the specific use of different applications on the card. The regulations on consent are accompanied by further informational obligations for the involved stakeholders, such as the card distributing institutions or institutions working with applications of the EHC. The answers provided in the following tables refer to the EHC.

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?	§ 291a (3) sentences 4, 5 SGB V	Persons with authorized access may only start data processing when the patient has given his or her consent.. There is a general obligation to cooperate in social security law in order to claim benefits, § 60 SGB I. It has been argued that a denial of consent therefore might lead to the denial of benefits also in relation to EHRs.[35] However, since the consent rules for EHRs are more specific and provide for the right to revoke it, no disadvantages may derive from not consenting. Furthermore, the legislator clearly states that the patient can decide whether or not he wants to use the different applications. Finally, § 291a Abs. 8 SGB V suggests that patients should suffer no disadvantages in case they do not want specific stakeholders to access their EHC.
Is a materialised consent needed?	§ 291a (3) sentence 4 SGB V	Patient consent is to be documented on the card (electronically) at the first time of usage of the EHC for the EHR and other medical applications..
Are there requirements to inform the patient about the purpose of EHRs and the consequences of the consent or withholding consent to create EHRs?	§ 291a (3) sentence 3 SGB V	Before the first use of the EHC the patient has to be informed in a comprehensive manner and in a generally understandable way about the functionality of the EHC, including the possible data to be collected and processed by it. Furthermore, § 291a (3) sentence 7 SGB V states that also § 6c BDSG is applicable, which stipulates further rules on information duties. However, it can be seen as problematic that EHR functionality was not in place when the EHC was introduced, making it questionable how comprehensive and understandable information can be given out to the patient, because the original information duties have already been fulfilled when the EHC was delivered to the insurants, potentially making it necessary to inform separately about the EHR as soon as a functioning scheme is in place.
Are there specific national rules on consent from the patient to share data?	§ 291a Abs. 3 S. 3, Abs. 5 S. 1 SGB V	Data on the EHC may only be processed if the patient has generally given his consent, § 291a Abs. 3 S. 3 SGB V. Moreover, every single access or processing measure, and this would include sharing ("Erheben, Verarbeiten, Nutzen" in the German terminology seeks to cover every possible act of working with the data), needs to be done in accordance with the patient, § 291a Abs. 5 S. 1 and 2 SGB V.

[35] Pitschas, NZS 2009, 177 (182)

Questions	Legal reference	Detailed description
Are there any opt-in/opt-out rules for patient consent with regard to processing of EHRs?	§ 291a (3) sentence 3SGB V	By using the EHC data may only be collected, processed and used if the patient has generally given his consent, pursuant to § 291a (3) sentence 3 SGB V.
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?	§ 291a (3) sentence 7 in conjunction with § 6c of the Federal Data Protection Act	§ 291a (3) sentence 7 SGB V provides that § 6c of the Federal Data Protection Act is applicable The latter prescribes that data controllers need to inform, inter alia, on the functionality of the system.
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)?	§ 291a (3) sentence 3 SGB V, §§ 4 (1), 4a, 4b, 4c (1) point 1 BDSG	There is no restriction of the right to consent in § 291a (3) sentence 3 SGB V. The general rules for sharing data outside the EU, namely §§ 4b, 4c BDSG, also allow for cross-border sharing within the EU when a patient has given his or her consent, § 4c (1) point 1 BDSG. Please note that the patient needs his/her EHC, a PIN code and the doctor a health professional card in order to access a EHR based on §291 a, which means that currently it is not possible for a foreigner doctor to have access to the system.
Are there specific rules on patient consent to share data on a cross-border situation?		No.

2.4. Creation, access to and update of EHRs

2.4.1. Main findings

The German legislator provides for specific rules on access to EHRs within the setup of the EHC. However, concrete determinations for different categories of health data are not in place yet, since only the legal groundwork is regulated. The insurants have access and erasure rights. Access for health professionals is generally connected to further requirements, e.g. ensuring they only get access via a health professional ID card secured by electronic signature measures.

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?	§ 291a (4) sentence 1 point 2 lit. a) - lit. f) SGB V	EHRs based on §291a can be created by the following professions if it is necessary for the medical care of the patient: • doctors (lit. a), • dentists (lit. b), • pharmacists, pharmacist assistants, pharmacy engineers, pharmacy assistants (lit. c), • persons that work under a professional mentioned in lit a) - lit c) or in a hospital as assistants or in preparation for their assisting occupation, insofar as this is permissibly required for their occupational tasks and their access is being carried out under supervision of the persons mentioned in lit a) to lit c). • psychotherapists (lit. f) .
Are there specific national rules on access and update to EHRs?	§ 291a (4) sentence 1 point 2 lit. a) - lit. f) SGB V	Access is allowed for the following professions as long as it is necessary for the medical care of the patient: • doctors (lit. a), • dentists (lit. b), • pharmacists, pharmacist assistants, pharmacy engineers, pharmacy assistants (lit. c), • persons that work under a professional mentioned in lit a) - lit c) or in a hospital as assistants or in preparation for their assisting occupation, insofar as this is permissibly required for their occupational tasks and their access is being carried out under supervision of the persons mentioned in lit a) to lit c). psychotherapists (lit. f)
Are there different categories of access for different health professionals?	§ 291a (4) sentence 1 point 1, point 2 SGB V	The clause regulating access rights lists different types of health professionals (see above) but does not set limitations for different categories concerning EHRs (but does so for other applications of the EHC).
Are patients entitled to access their EHRs?	§ 291a (4) sentence 2 SGB V	§ 291a (4) sentence 2 SGB V specifically states that insurants have the right to access their "data according to Abs. 2 S. 1 und Abs. 3 S. 1" [(2) sentence 1 and (3) sentence 1], which includes EHR data.

Questions	Legal reference	Detailed description
Can patient have access to all of EHR content?	§ 291a (4) sentence 2 SGB V	See above. There is no restriction to certain kinds of data.
Can patient download all or some of EHR content?		Since a functioning EHR system is not yet in place, the question where the data should be stored is also not (yet) answered (by law). However, the law regulates the right to access the data for an insurant, § 291a Abs. 4 S. 2 SGB V.
Can patient update their record, modify and erase EHR content?	§§ 291a (3) sentence 6, 291a (6) sentence 1, sentence 2 SGB V	Patients cannot modify or update the content of an EHR based on §291a. § 291a (6) sentence 1 SGB V states data relating to EHRs have to be deleted when so required by the insurant, indicating that not the insurant himself can delete but only express the request. This interpretation is backed by § 291a (6) sentence 2 SGB V, which states that data from particular applications on the EHC mentioned in § 291a (2) sentence 1 point 1 and (3) sentence 1 point 5, point 7, point 8, point 9 (so not point 4 which regulates EHRs) can be deleted independantly by insurants. In any case, data relevant for accounting purposes must be kept, § 291a (6) 1.
Do different types of health professionals have the same rights to update EHRs?	§ 291a (4) sentence 1 point 2 lit. a) - lit. f) SGB V	See row 2.
Are there explicit occupational prohibitions? (e.g. insurance companies/occupational physicians…)	§ 291a (8) sentence 1 SGB V	Even though there are no specific restrictions to explicit occupations, § 291a Abs. 8 S. 1 SGB V states that it is not allowed to demand from the owner of the EHC to give access to other professionals than the ones mentioned in § 291a Abs. 4 S. 1 Nr. 2 lit. a) - lit. f) SGB V (see above). An agreement between the patient and other persons than the ones listed therein to provide access to the data is prohibited by law.
Are there exceptions to the access requirements (e.g. in case of emergency)?	§ 291a (4) sentence 1 point 2 lit. e) SGB V	No, there are no exceptions. However, there are plans for a separate emergency data set with special rules of access in case of emergency..
Are there any specific rules on identification and authentication for health professionals? *Or are they aggregated?*	§ 291a (5) sentence 3 SGB V	See table 2.2.2, row 2: Access to EHRs may only be concluded in conjunction with an electronic health profession ID card, § 291a (5) sentence 3 SGB V, which has to provide for secure authentification measures and have the technical infrastructure of qualified electronic signatures available.
Does the patient have the right to know who has accessed to his/her EHRs?	§ 291a (6) sentence 3 SGB V	See table 2.6.1, row 1: It is to be ensured by technical measures that at least the last 50 access activities on the EHC are logged in a protocol for purposes

Questions	Legal reference	Detailed description
		of data protection monitoring. The access right of § 291a (4) sentence 2 SGB V is limited to specific EHR data, not protocol data. § 291a (6) does not statute an independent access right. But since the protocol duty specifically refers to "data protection monitoring" purposes, it can be argued that also the patient needs to be enabled to carry out this control.
Is there an obligation on health professionals to update EHRs?	-	There is no specific obligation to update data in EHRs
Are there any provisions for accessing data on 'behalf of' and for request for second opinion?	-	No
Is there in place an identification code system for cross-border healthcare purpose?	-	No
Are there any measures that consider access to EHRs from health professionals in another Member State?	-	There are no specific regulations on cross-border access within EHRs. However, the general data protection rules of the BDSG state in relation to data transmission (which would imply access) that the regular permissive regulations apply, § 4b BDSG. In addition, the general rules of the law on electronic signatures on cross-border usage apply, in particular § 23 BDSG. Please note that the patient needs his/her EHC, a PIN code and the doctor a health professional card in order to access a EHR based on §291 a, which means that currently it is not possible for a foreigner doctor to have access to the system.

2.5. Liability

2.5.1. Main findings

There are no specific medical negligence rules related to the use of EHRs. More generally, there are various grounds for liability for medical malpractice. Patient and physician usually conclude a treatment contract, out of which the breach of duties by the physician can constitute medical liability. Furthermore, medical negligence can lead to compensational duties according to tort law. Since there are no specific regulations regarding medical negligence related to the use of EHRs and neither are there any functioning EHR systems in place which would be needed to specifically point out obligations and duties of the treating physician, statements on a possible liability would be highly speculative and therefore should not deemed to be conclusively feasible at this time.

2.5.2. Table on liability

Liability		
Questions	**Legal reference**	**Detailed description**
Does the national legislation set specific medical liability requirements related to the use of EHRs?		General liability legislation (e.g. under the German Civil Code) may apply, for example, in cases where doctors who directly supervise and control staff members (e.g. nurses, assistants) entitled to fill EHRs, are liable for injuries associated with inaccurate or deficient summary reports provided by these staff members (see also § 291a (4) sentence 1 point 2 mentioned above in 2.4.2, row 2). However, there is no specific liability legislation relating to EHRs in place. § 7 BDSG sets out a standard rule for compensation covering misuse of personal data: "*If a controller harms a data subject through collection, processing or use of his or her personal data which is unlawful or improper under this Act or other data protection provisions, the controller or its supporting organization shall be obligated to compensate the data subject for damage suffered. The obligation to provide compensation shall be waived if the controller exercised due care in the case*". This regulation specifically takes into account "other data protection provisions", which would also cover the data protection regulations within the setup of the telematics infrastructure. Since a functioning EHR scheme is not yet in place, it remains open what would be considered improper use of data and how "*due care in the case"* would be defined. As electronic health profession IDs imply the usage of qualified electronic signatures, also the general liability rules of the laws on electronic signatures, in particularar § 11 of the law, can apply.
Can patients be held liable for erasing key medical information in EHRs?	§ § 291a (6) sentence 1 SGB V; § 291a (3) sentence 4, 5 SGB V	Patient has an explicit right to erasure, § 291a (6) sentence 1 SGB V. A further argument against liability would be that all key medical information in EHRs would only be available on the EHR following the consent of the patient (§ 291a (3) sentence 4 SGB V). This consent may be revoked at any time (§ 291a (3) sentence 5 SGB V), which indicates that data may only be stored for EHR purposes as long as there is valid consent. Therefore, if there is no consent, the data may not be used anymore. Liability for the "erasure" would therefore contradict this basic right of the patient.
Can physicians be held liable because of input errors?		Since there is no specific liability legislation in place relating to EHRs, these questions can only be answered hypothetically. It is questionable if an originally

Liability		
Questions	**Legal reference**	**Detailed description**
Can physicians be held liable because they have erased data from the EHRs?		recording party could be held liable if input or erasure lead to treatment errors of another physician working with the EHR file. Regarding data protection liability, see row 1.
Are hosting institutions liable in case of defect of their security/software systems?	-	See above; if treatment on the basis of an EHR is to be seen as a specific contractual obligation of the treating party, a non-functioning record could potentially lead to contractual liability or liability following tort law. Regarding data protection liability, see row 1.
Are there measures in place to limit the liability risks for health professionals (e.g guidelines, awareness-raising)?	-	No
Are there liability rules related to breach of access to EHRs (e.g. privacy breach)?	-	No
Is there an obligation on health professionals to access EHRs prior to take a decision involving the patient?	§ 291a (5) sentence 1, 2, 5 SGB V	See table 2.8.2, row 4: On the contrary, each access to a single application on the EHC has to be approved by the patient. Furthermore, each access has to be authorised by the patient with support from technical measures.
Are there liability rules related to the misuse of secondary use of health data?	-	Regarding general data protection liability, which would also cover data usage under secondary use aspects, see row 1.

2.6. Secondary uses and archiving durations

2.6.1. Main findings

Archiving durations are only regulated generally in different German acts and do not reflect on the use of EHRs. There are no specific rules regulating secondary uses to the use of EHR data.

2.6.2. Table on secondary uses and archiving durations

Questions	Legal reference	Detailed description
Are there specific national rules on the archiving durations of EHRs?	§ 291a (6) sentence 3 SGB V	There are no specific archiving duration rules regarding EHRs. However, it is to be ensured by technical measures that at least the last 50 access activities on the EHC are logged in a protocol for purposes of data protection monitoring. However, this should not be seen as an archiving requirement; this is rather to be seen as a technical measure for ensuring data protection rights and information for the insurant.[36]
Are there different archiving rules for different providers and institutions?	-	§ 291a (6) sentence 3 SGB V refers to all data and applications stored on the EHC and in that context does not specifically differentiate between users of the card. However, different archiving specifications may be applicable according to various other archiving regulations concerning medical professionals. For example, § 630f (3) of the German Civil Code and § 10 of the Model Professional Code for Physicians ("Musterberufsordnung Ärzte") establish a general obligation to store basic medical treatment documentation for ten years. This seems to contradict the patients' right to erasure provided in § 291a Abs. 6 SGB V, but since the EHR is just a voluntary application of the EHC, the obligation concerns two different instruments of documentation, meaning that documentation obligations in these areas differ and the right to erasure in the EHC could always be observed. The basic medical documentation and the EHR documentation are two different areas of documentation duties. It is therefore likely that these durations do not apply to EHRs.
Is there an obligation to destroy (…) data at the end of the archiving duration or in case of closure of the EHR?	§ 291 (4) sentence 5, 6 SGB V	The redemption of the EHC leads to the duty of the health insurance company to assure that the further use of the stored data is possible for and by the insurant. Before the actual redemption, the health insurance company has to give out information about the options of erasure of the data. A specific obligation to destroy the data is not foreseen in the law. However, according to the more general § 20 (2) point 2 BDSG, data have to be deleted as soon as the knowledge of these data is no longer necessary for the undertakings of the responsible controller.

[36] Becker/Kingreen, SGB V, § 291a, Rec. 16.

Questions	Legal reference	Detailed description
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?	-	See above.
Can health data be used for secondary purpose (e.g. epidemiological studies, national statistics...)?	§ 28 (7) sentence 1 BDSG	No, this is not possible (§291a, data can only be used, if they are necessary for the medical care of the patient.
Are there health data that cannot be used for secondary use?	-	See above
Are there specific rules for the secondary use of health data (e.g. no name mentioned, certain health data that cannot be used)?	-	See above
Does the law say who will be entitled to use and access this data?	§ 28 (7) sentence 1 BDSG	Under the general rules, the usage is restricted to health professionals who are subject to the obligation of professional secrecy or by other persons also subject to an equivalent obligation of secrecy.
Is there an opt-in/opt-out system for the secondary uses of eHealth data included in EHRs?	-	No

2.7. Requirements on interoperability of EHRs

2.7.1. Main findings

As there is no specific EHR scheme in place yet, it cannot be assessed how the interoperability of EHRs is regulated. However, the legal setup of a telematics infrastructure in Germany by the legislator shall be "interoperable and compatible", which leads to the conclusion that whenever supporting research is being conducted and ultimately first implementation steps are executed, it could be argued that full interoperability (e.g. between health institutions, health practitioners, different geographical areas in Member States and between Member States, as Germany is also involved in epSOS and the followup project EXPAND), would be aimed for.

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?	§ 291a Abs. 7 S. 1 SGB V	The telematics infrastructure that stakeholders need to create in the long term for the introduction and application of the EHC specifically needs to be "interoperable and compatible". This interoperability and compatibility has to be applicable especially to EHRs and the ePrescription, since these are each mentioned as examples of that infrastructure.
Are there any specific rules/standards on the interoperability of EHR?	-	There are no specific rules/standards on the interoperability of EHR within the law itself. However, most initiatives are aware of the necessity of interoperability and therefore take this into account in their research.
Does the law consider or refer to interoperability issues with other Member States systems?	-	No

2.8. Links between EHRs and ePrescriptions

2.8.1. Main findings

There is a relation between ePrescriptions and EHRs since they are related within the setup of the EHC, i.e. within the setup of the telematics infrastructure. However, EHRs and ePrescriptions are to be seen as two different applications of the EHC. Hence, they both will function independently.

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?	§§ 291a Abs. 2 S. 1 Nr. 1, Abs. 3 S. 1 Nr. 4 SGB V	EHR and ePrescription are two different applications within the EHC and are planned to exist and function independently.
Can an ePrescription be prescribed to a patient who does not have an EHR?	§§ 291a Abs. 2 S. 1 Nr. 1, Abs. 3 S. 1 Nr. 4 SGB V	Since the ePrescription is mentioned individually and constitutes a unique application within the EHC, it can be used without having the EHR application in place.

- ***Access***

Questions	Legal reference	Detailed description
Do the doctors, hospital doctors, dentists and pharmacists writing the ePrescription have access to the EHR of the patient?	§ 291a Abs. 5 S. 1, 2, 5 SGB V	Each access of a single application on the EHC has to be approved by the patient. Furthermore, each access has to be authorised by the patient with support from technical measures. Therefore, each access happens separately and can be controlled by the patient. § 291a Abs. 5 S. 5 even constitutes a unique rule for the access to the ePrescription, which in reverse leads to the conclusion that separate access scenarios must be possible.
Can those health professionals write ePrescriptions without having access to EHRs?	§§ 291a Abs. 2 S. 1 Nr. 1, Abs. 3 S. 1 Nr. 4 SGB V	Since the ePrescription is an individual application on the EHC, its functions can be used without having access to EHRs (see above).

2.9. Other requirements

None identified.

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

3.1. Introduction

This section will provide an overview of the potential legal barriers and good practices for the development of EHRs in Germany and for their cross-border transfer in the EU. Therefore, first, conclusions from the findings of the desk research are presented. The most important findings from the conducted interviews are outlined and finally legal barriers and good pratices of specifically targeted areas within the questionnaires are presented.

When deciding upon the designated interview partners, first of all the recommendations within the background information accompanying this study have been taken into account. Therefore, four definite interviewees were pointed out, i.e. a hospital association, a health practitioner association, a national authority in charge of the implementation of EHR systems and finally a national data protection supervisory authority.

Since the German social security landscape is extremely diversified and the developments of EHRs and ePrescriptions are still in their infancy, many other stakeholders have been addressed to prepare a comprehensive overview of the views of different interest group involved in the process.[37]

However it has turned out that many different factors lead to a rather low participation rate. In most of the cases, the stakeholders raised concerns whether the study is being conducted at a premature state at least concerning the current legal and factual background in Germany. Moreover, since all relevant stakeholders are also engaged in the setup of the gematik (mainly as associated partners as regulated within the contract of association), many separate institutions or unions referred to their involvement in the setup of a telematic infrastructure within their participatory role in the gematik, which would make it either unnecessary or contradictory to also participate in their role as a separate unit. It has to be further noted that seemingly also administrative or other, undetermined factors lead to a refusal of participation.[38] Ultimately, the participants only came from areas indirectly linked to the implementation of EHRs.

In any case, the presentation of the final results within this study depend also largely on the stakeholders who did take part in the interviews, and provided useful background information and continuative updates and indications on the status of EHRs and ePrescriptions in Germany.

The most important factor governing EHRs and ePrescriptions in Germany at the moment could be seen as both a grave legal barrier as well as a useful good practice: their implementation in a wider framework of setting a telematics infrastructure to bring healthcare on national level to the next generation within the striving information and communication technologies.

On the one hand, this wider goal features setting up only basic groundwork in terms of legislation, leaving out specific questions regarding the technical and contentual setup. On the other hand, this leaves flexible development opportunities for the involved stakeholders of the self-administrating community.

The administrative fundament of the German healthcare system might also be seen as hindering the process of EHR and ePrescription application development. There are many stakeholders with different interests; reform processes generally evolve slowly and have to take into account various concerns. Furthermore, the size of the German population and the hence complex infrastructure of the

[37] See Section 3.2, detailed list of interviewees.
[38] The exact status of participation or refusal is also being presented in Section 3.2, detailed list of interviewees.

German healthcare system seems to increase the likelihood of slowing down legal and technical progress. Adding this to the fact that the implementation of the EHC in Germany is seen as potentially one of the biggest IT-projects worldwide[39] gives an apprehensible picture for understanding the various issues within the development process.

In any case, even though the German approach might seem to allow only slow developments and a fully functioning EHR scheme is not yet in place, it provides for a sound, comprehensible and equitable approach without leaving feasibility out of the picture. Accompanying the view that the organizational, technical and administrative setup implies challenging tasks, it has always been recognized that also data protection and privacy interests of the patient need to be observed in the best way possible and moreover play an outstanding role interlinking roughly 80 million patients within the setup of a telematics infrastructure.[40]

Therefore, a study[41] within the eHealth initiative by the German state of North Rhine-Westphalia (see also above section 1.3) suggests that within the concept of an EHR not only functional but also data protection aspects need to be respected. From a constructional perspective it was hence deemed useful first to determine functional requirements and basic conditions. When a system has been specified in that matter, a further analysis should assess and incorporate data protection requirements. The synthesis of functional and data protection requirements would then form the basis for specifying the technical and organizational system and security structure.[42]

3.2. Detailed list of interviewees

(Requested) Interviewee	Function	Status (if declined with reason)
Bundesärztekammer, BÄK	German Medical Association; central organisation in the system of medical self-administration in Germany, joint association of the State Chambers of Physicians	Declined (17/02/14); missing direct involvement in EHR projects
Bundeszahnärztekammer, BZÄK	German Dental Association; professional representation of all dentists in Germany, joint association of the dental chambers of the German federal states	No feedback (06/03/14); final feedback regarding a possible participation in the interview announced for the first week of March; however the timeframe was exceeded even beyond an extension of the reporting deadline so that an interview could not be conducted
Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, BfDI	German Federal Data Protection Authority; independent controlling body for the safeguarding of data protection in federal authorities and private companies in Germany	Participated
Bundesministerium für Gesundheit, BMG	German Federal Ministry for Health; responsible for a variety	Declined (19/02/14); premature state of the study, EHRs do not

[39] Krauskopf, Soziale Krankenversicherung, Pflegeversicherung, 83. Ergänzungslieferung 2013, SGB V, § 291a, Rec. 11.
[40] Speth/Koutses, MedR 2005, 493 (493).
[41] ZTG Zentrum für Telematik im Gesundheitswesen GmbH, AK EPA/EFA der Initiative eGesundheit@nrw, Elektronische Akten im Gesundheitswesen, Nutzen, Ausprägungen, Datenschutz, op. cit. 1.
[42] ZTG Zentrum für Telematik im Gesundheitswesen GmbH, ibid., p. 30.

(Requested) Interviewee	Function	Status (if declined with reason)
	of policy areas, with a focus predominantly on the drafting of bills, ordinances and administrative regulations	have priority in the implementation of the telematics infrastructure and the EHC
Deutsche Krankenhausgesellschaft, DKG	German Hospital Federation; Federation of national and state associations of hospital owners	Declined (13/02/14); premature state of the study, dialogue within the *gematik* needs to be prioritized before participating as a singular body in the questionnaire
Fraunhofer FOKUS	Fraunhofer Institute for Open Communication Systems; independent research body focused on developing solutions for future communication systems, particular focus on the implementation of EHRs	Participated
Gesellschaft für Telematik, *gematik*	Society for telematics; umbrella organization responsible for the creation of the telematics infrastructure, especially through the EHC	No feedback (06/03/14); final feedback regarding a possible participation in the interview could not be obtained at all after various contacting inquiries at different institutional areas (such as the pressoffice or different representatives of various departments)
Beirat der Gesellschaft für Telematik	Advisory board of the *gematik*; to be consulted before decisions of fundamental concerns within the *gematik*	Participated
GKV-Spitzenverband	National Association of Statutory Health Insurance Funds; Federal Joint Committee of the National Association of Statutory Health Insurance Physicians, the National Association of Statutory Health Insurance Dentists and the German Hospital Federation	Declined (03/03/14); currently existing EHR schemes are not part of the statutory health provision and within a competition framework of health insurance companies, where the GKV-Spitzenverband does not want to intervene; the telematics infrastructure is a future topic of the GKV-Spitzenverband which is not even in the conceptual phase yet
Kassenärztliche Bundesvereinigung, KBV	National Association of Statutory Health Insurance Physicians and the regional Associations of Statutory Health Insurance Physicians	Declined (06/03/14); via telephone, short explanatory Email was promised but never sent
Kassenzahnärztliche Bundesvereinigung, KZBV	National Association of Statutory Health Insurance Dentists; special interest group of statutory health insurance dentists	Declined (18/02/14): missing direct involvement in questions and contemporary developments of EHRs on European level; premature state of the study,

(Requested) Interviewee	Function	Status (if declined with reason)
		current European projects within the *gematik* (epSOS and EXPAND) form basis for future projects within the national telematics infrastructure
Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V.	Technology and methodological platform for connected medical research; integrated platform for the medical research community	Declined (17/02/14): heavy focus on research activities, which does not fit the aim of the study/questionnaire

3.3. General Interview findings

The interviews generally showed that precise awareness of EHRs exists within the public health domain and surrounding areas. Mostly, the rather abstract setup of regulations was seen as a sound basis for an implementation scheme which can be suited to any according circumstances that might appear in the development of the technical aspects and possible content of the EHC and EHRs.
A widespread examination of different institutions and projects is taking place, all working towards a step-by-step implementation of a telematics infrastructure. There is widespread knowledge and understanding of issues surrounding the implementation of EHRs. A heavy focus should be put however on actual use cases and prototypic scenarios to elaborate the most efficient solutions regarding technical and data protection implications.

3.4. Concrete legal barriers and good practices

It has been pointed out by all interviewees that the most effective features should depend on the final environment of EHRs, which is not in place yet. Anyhow, regarding concrete measures, as far as possible, the following legal background regulations, initiatives, studies, research activities etc. could be seen as either legal barriers or good practices in the respective domain. The following findings arise from the desk-research carried out under section 2 and 3 of this report and also from the interviews conducted with the stakeholders.

- Health data to be included in EHRs
    - An abstract definition of EHR content was generally seen as sufficient
    - Concrete findings were hard to think of because the basic framework is generic
    - Data security should be considered when deciding upon which specific data needs to be included
    - It needs to be investigated what requirements there are for specific usage scenarios are and how they can be re-used in different contexts in practice, which is not feasible as long as there is only legal groundwork in place.

- Requirements on the institutions hosting EHRs data
    - Certificate authorization is an established and sufficient control mechanism for institutions working with EHR data
    - Practical implementation needs further development
    - Strict measures enforcing strong data protection with however feasible technical realization are regulated

- Patient consent
    - Consent is an effective measure for safeguarding patient rights and not to be seen as a barrier
    - The concept is important but should not be overstretched; different solutions for different

types of medical records might need to be developed and applied

- Creation, access to and update of EHRs
  - Working with certificates as well-established technical groundwork for authentication; they have to take into account institution based authorization measures
  - Practical testing needed
  - No cross-reference between different social security regulations allowing or not allowing cross-border data processing
  - Voluntary applications and patient approval need to go hand in hand

- Liability
  - Directive 2011/24/EU on the application of patients' rights in cross-border healthcare enforces liability regulations; a regulation at EU level offers a holistic approach
  - Open questions on commitment of processing party and hence which liability conclusions might be applicable

- Secondary use and archiving duration
  - Quite different legal requirements for duration of archiving of medical recortds exist; they are not applicable to EHRs according to §291a SGBV
  - Paper documents and digital data shall be handled the same – which is the current situation

- Requirements on interoperability of EHRs
  - Setup of interoperability already within basic legal groundwork as strong factor for effective development of interoperable infrastructure

- Links between EHRs and ePrescriptions
  - No real links available
  - ePrescription needs further priorization towards other applications within EHC

- Other requirements
  - Most effective: Setting up the telematic infrastructure with all necessary safety mechanisms, clear use-case benefits must be worked out, medical applications must show the ultimate benefit.
  - Strong focus needs to be practically be put on interoperability
  - Restricted usage of the EHC to specific person groups might make it difficult to ultimately imply areas as old-age care or rehabilitation and adjacent areas of health provision, where not necessarily only physicians are involved
  - Restrictive handling of EHR implementation provisions concerning direct access of the insurant

1 Annexes – Questionnaires

1.1 German Federal Data Protection Authority

A) Background information

- *How would you describe the stage of development of eHealth legislation in Germany, in particular that covering EHRs?*

Currently, there are two main regulations covering electronic health records. § 630f BGB allows the electronic administration of a patient record. It has been introduced by the law on patient rights in 2013. The record must be administered in a complete and accurate manner. The treating entity is obliged to use tamper-proof software to secure the patient data.
§ 291a Abs. 3 Nr. 4 SGB V provides for a legal definition of what is an electronic health record. It is a voluntary application within the electronic health card.
Electronic records are being introduced to different areas, for example also human resources management, where similar rules apply with in order to treat paper and electronic records alike. Keeping the legal requirements abstract and in a general manner helps to fulfill this purpose.

- *In case Germany relies on paper-era legislation to regulate EHR would you consider it as a legal barrier to the development of EHRs?*

Paper-era legislation is not necessary a barrier for the development of EHRs. The telematic infrastructure is being setup and continuously developed. Hence, at the moment the barriers are rather of practical than of legal nature.

- *Are you aware of any cross-border cooperation projects on EHRs in your country apart from the epSOS project?*

There is the eHealth-governance initiative, in which Germany participates. In this context, the European Commission Guidelines on patient summary set of data for electronic exchange under the cross border directive have been discussed.

B) Possible barriers for the development of EHRs

a. *Health data to be included in EHRs*

- *Do the requirements on EHRs information content allow an efficient use of EHRs within Germany and for cross-border exchanges?*

The abstract regulation of EHR content within § 291a SGB V is sufficient, the concrete content should depend, i.e., on which institution hosts the data. At the moment, this is difficult to foresee since there are few EHR scenarios in place.

- *Would you add any other elements that should be included in the EHRs?*

The conference of data protection authorities on federal and state level in Germany worked out an orientation manual for usage of hospital information systems compliant to data protection regulations. This paper sets out requirements for data security which should be considered when data is included in EHRs in hospital information systems.

- *Are there any elements currently included in the EHRs that you think should not be covered?*

None identified.

b. *Requirements on the institution that host the data from EHRs*

- *Are the authorisation requirements on the institution that host the data from EHRs simple enough to foster the development of EHRs? Or does the complexity or length of the procedure*

prevent the interest of host institutions to implement this system? Is the procedure easy enough for a host of e-health data to be authorised?

The health professional ID card ("Heilberufsausweis") is a sufficient measure to secure safe authorization procedures, since it enables only authorized personnel to work with the applications. The practical implementation needs further development. In any case, these authorization measures are usual procedures in various domains and proved not to be too complex.

c. *Consent*

- *Do the requirements on patient consent allow an efficient development of EHRs? If not, what are the consent requirements that impede the development of EHRs?*

It is indispensable that revocable consent needs to be in action at any time, which is not to be seen as a barrier in the introduction of EHRs.

- *Do the consent requirements adequately protect the patients' right to confidentiality?*

The consent requirements in § 291a Abs. 3 S. 4, 5 SGB V are sufficient. The German Federal Commissioner for Data Protection and Freedom of Information was involved in the lawmaking process as a consulting entity and therefore also in terms of patient consent. Moreover, the German Federal Commissioner for Data Protection and Freedom of Information according to the bylaws of the German government ("Bundesregierung") needs to be consulted in due time regarding new legislation involving personal data.

d. *Access, authentication and authorisation*

- *Do the requirements on access, authentication and authorisation allow an adequate development of EHRs? If not could you specify where improvement is needed?*

Requirements on access, authentication and authorisation are yet to be put to the practical test. Generally, the basic access, authentication and authorization rules allow for an appropriate development.

- *Can health practitioners in Germany have access to other foreign EHR systems? If yes, do they face any problems to access those? Please describe Can health practitioners in another Member State access and enter information on an EHR hosted in your Member State? If yes, how is access granted? (e.g. on case by case basis)*

A differentiation has to be made between legal and technical approaches. epSOS aimed to provide for a common technical environment which turned out to be difficult. From a legal point of view, consent would make cross-border access possible, while §§ 4b, 4c BDSG would need to be observed, if no specific rules are being put in place by the German legislator.

Other areas of social security law (for example the pension insurance scheme) provide for regulations allowing transmission of data in other countries. However, there is no cross reference between these regulations and the regulations concerning EHRs. Therefore, the question arises if there is a particular need to regulate cross-border exchange for EHRs specifically.

e. *Liability*

- *Are there liability issues not resolved related to the use of EHRs?*

N/A for being answered by the German Federal Authority for Data Protection and Information Freedom.

- *Is it considered as a legal barrier for the deployment of EHRs?*

N/A for being answered by the German Federal Authority for Data Protection and Information Freedom.

f. *Archiving durations and other uses of data in EHR*

- *Do you think that the current archiving durations for EHRs are adequate to allow a proper use of EHRs?*

There is no differentiation between electronic and paper records according to § 10 of the Medical Association's professional code of conduct, the archiving duration for physicists is 10 years. Same goes for EHRs from health insurance companies, § 304 SGB V.
Log files are not classified as sensitive health data. It remains unclear, whether they have to be archived as well. However, they would have to be deleted earlier.

- *Are the current data protection requirements on e-health data a constraint for their adequate use for academic and research purpose?*

A differentiation between electronic records in hospitals and panel doctors on the one hand and health insurance companies on the other hand is necessary. The latter are governed by § 75 SGB X, which governs "social data" in general. There is an urgent need to reform this regulation since it dates from the early 90s. Hence, the current technological developments were not taken into account at that time.
However, the high level of data protection guaranteed in the German Social Code, i.e. also in § 75 SGB X, should be kept. Likewise, the duty of health insurances to get formal approval by the relevant supervisory authority before data transfer for research purposes should be upheld.

g. *Links between EHRs and ePrescriptions*

- *Is the EHRs system coordinated enough with the ePrescription system?*

Both are planned applications on the EHC, the concrete arrangement is still open; therefore, a specific common coordination cannot yet be determined.

h. *Any other legal barriers*

- *Are you aware of any other legal barriers that impede the development of EHR system ?*

No.

C) Possible good practices

- *In your view, what are the most effective features of the legal framework in your country in relation to:*
    - *Health data to be included in EHRs*
    - *Requirements on the institution that host the data from EHRs*
    - *Consent*
    - *Access, authentication and authorisation*
    - *Liability issues*
    - *Archiving durations and other uses of data in EHRs*
    - *Links between EHRs and ePrescriptions*
    - *Any other legal good practice*

The most effective features shall be depending on the final environment of EHRs, which is not in place yet.

Annex 1 – Summary of interviews with targeted stakeholders

INTERVIEW NO 1					
Name of the interviewee:Mr. Bertram Raum					
Profession/role of the interviewee:Head of division, Social Security and Health, Employee Data Protection					
*Type and name of organisation represented:*German Federal Commissioner for Data Protection and Freedom of Information					
Location of the interview: -					
Date of the interview: Feb 19th, 2014					
Duration of the interview:	*<45'*	*X*			
	45'-60'				
	60'- 75'				
	>75'				
Interview conducted:	*Face to face*			*By telephone*	*X*
Summary of the interview: *Please identify any key themes and then summarize the discussion under each section.* The concept of electronic records is not new. There are other areas where they have been successfully implemented; the medical domain needs to adapt best practices and also elaborate own effective features tailored to the specific needs of patients and caretakers working with sensitive personal data.					

1.2 Advisory board of the Society for Telematics

A) Background information

- *How would you describe the stage of development of eHealth legislation in Germany, in particular that covering EHRs?*

There is a high need on the part of the patients for electronic records. Hospitals aim for implementing the electronic case record (ECR). On the other hand, the general public is not yet set for differentiating between the multiple variations of different records. But people will express an increased demand for using them. There are however still many open questions that need to be addressed.

- *In case Germany relies on paper-era legislation to regulate EHR would you consider it as a legal barrier to the development of EHRs?*

SGB V generally regulates EHRs, however quite different regulations apply for electronic or telematic purposes: Beside §§ 291a and 291b there are § 67 for electronic communication, §§ 140a, 140b for the concept of integrated healthcare provision, § 63 for model schemes, § 295 for data exchange, and numerous others that deal with telematics or telemedicine questions. These regulations are rather unstructured which complicates their application. Not all derive from the law to modernize the statutory health insurance ("GKV-Modernisierungsgesetz", GMG"). Many of the regulations have even been amended but there has been no significant change in the general setup. This is to be seen as a legal barrier.

- *Are you aware of any cross-border cooperation projects on EHRs in your country apart from the epSOS project?*

No.

B) Possible barriers for the development of EHRs

a. *Health data to be included in EHRs*

- *Do the requirements on EHRs information content allow an efficient use of EHRs within Germany and for cross-border exchanges?*

For the purposes of getting a telematic infrastructure started, yes.

- *Would you add any other elements that should be included in the EHRs?*

No.

- *Are there any elements currently included in the EHRs that you think should not be covered?*

No. Undetermined legal terms give the possibility of further exegesis, they can be concretized. What specific terminology, if any, is really necessary needs to be figured out in practice. The discussion about emergency data underlines this.

b. *Requirements on the institution that host the data from EHRs*

- *Are the authorisation requirements on the institution that host the data from EHRs simple enough to foster the development of EHRs? Or does the complexity or length of the procedure*

prevent the interest of host institutions to implement this system? Is the procedure easy enough for a host of e-health data to be authorised?

The current foreseen measures are necessary for the effective protection of personal data. Germany will stress the necessity of strong data protection rules continuously in the future. The current measures allow for an efficient access and use of the system. The most important issue at stake however is interoperability. We need to figure out how to best establish interoperable structures. German patients will ultimately demand for strong security standards also in foreign countries.

c. *Consent*

- *Do the requirements on patient consent allow an efficient development of EHRs? If not, what are the consent requirements that impede the development of EHRs?*

Consent requirements do not hinder the efficient development.

- *Do the consent requirements adequately protect the patients' right to confidentiality?*

Yes.

d. *Access, authentication and authorisation*

- *Do the requirements on access, authentication and authorisation allow an adequate development of EHRs? If not could you specify where improvement is needed?*

The voluntary applications on the EHC are bound to only be used with approval of the patient, this is an important necessity. Since EHRs as in § 291a are administered by physicians, patients need to be informed and be able to let changes only happen with their approval.

- *Can health practitioners in Germany have access to other foreign EHR systems? If yes, do they face any problems to access those? Please describe Can health practitioners in another Member State access and enter information on an EHR hosted in your Member State? If yes, how is access granted? (e.g. on case by case basis)*

To the best of my knowledge, they cannot.

e. *Liability*

- *Are there liability issues not resolved related to the use of EHRs?*

Since Directive 2011/24/EU on the application of patients' rights in cross-border healthcare enforces liability regulations there are none as of now.

- *Is it considered as a legal barrier for the deployment of EHRs?*

NA.

f. *Archiving durations and other uses of data in EHR*

- *Do you think that the current archiving durations for EHRs are adequate to allow a proper use of EHRs?*

The German civil code provides for limitations up to 30 years. Storing 50 accesses on the EHC is also quite a lot.

- *Are the current data protection requirements on e-health data a constraint for their adequate use for academic and research purpose?*

NA.

g. *Links between EHRs and ePrescriptions*

- *Is the EHRs system coordinated enough with the ePrescription system?*

No. They are two different, seperate applications within the EHC. § 291a might be changed in the nearer future for the sake of the seamless introduction of the ePrescription and hence a better coordination of ePrescription and EHRs.

h. *Any other legal barriers*

- *Are you aware of any other legal barriers that impede the development of EHR system ?*

An increased focus must be put on interoperability. Current reformation activities concentrate too much on domestic processes, a more European approach needs to be the ultimate goal. The German lawmaker should be more concerned about this and create rules that take this into account more effectively.

C) Possible good practices

- *In your view, what are the most effective features of the legal framework in your country in relation to:*

  - *Health data to be included in EHRs*

  Undetermined legal terms for health data to be included are a good starting point for the effective development of EHRs.

  - *Requirements on the institution that host the data from EHRs*

  Strict measures enforcing strong data protection with however feasible technical realization are regulated.

  - *Consent*

  The general need to consent underlines the importance of the right to privacy.

  - *Access, authentication and authorisation*

  Voluntary applications and patient approval need to go hand in hand.

  - *Liability issues*

  A regulation on EU level offers a holistic approach.

  - *Archiving durations and other uses of data in EHRs*

  However necessary, archiving needs to take into account the protection of personal data.

  - *Links between EHRs and ePrescriptions*

  NA.

- *Any other legal good practice*

NA.

Annex 1 – Summary of interviews with targeted stakeholders

INTERVIEW NO 1					
Name of the interviewee:Brigitte Schmidt-Jaehn					
Profession/role of the interviewee: Deputy Spokeswoman					
Type and name of organisation represented: Advisory board of the Society for Telematics (Beirat der "Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH", "gematik")					
Location of the interview: -					
Date of the interview:28.02.2014					
Duration of the interview:	*<45'*	*X*			
	45'-60'				
	60'- 75'				
	>75'				
Interview conducted:	*Face to face*			*By telephone*	*X*
Summary of the interview:					

An aggregation of the most important regulations should be achieved. Legal appellation should be changed, the focus should rather lie on developing a telematic infrastructure as a whole that on an electronic health card in the centre of efforts. More differentiated emphases are necessary.

1.3 Fraunhofer Institute for Open Communication Systems

A) Background information

- *How would you describe the stage of development of eHealth legislation in Germany, in particular that covering EHRs?*

Probably better than commonly noticed by the general public. Electronic records are the basis of many research projects, such as for example the eBusiness health platform in North Rhine-Westphalia, the project epa2015, the health region "Rhine Neckar" or within several university or statutory clinical centres.

The electronic case record ("Elektronische Fallakte", "EFA"), is being used tailored to regional networks since 2008; the municipal clinical centre Munich uses it regularly; the university clinic of Aachen provides networks for physicians and the responsible manufacturers union has actively participated in developing new according specifications, which are now being used within full-product solutions.
The German Federal Ministry for Health supports a research project for the development of an EHR according to § 291a SGB V concerning prototypic implementation. There is a prototypic realization in place which is being tested together with real patients. The German union of health-IT companies (Bundesverband Gesundheits-IT", "BVITG") has presented solutions such as an IHE-Cookbook for standardization of electronic records. Proceedings regarding the EFA reached rollout step 2, while this topic has special precedence within the *gematik*.

Regarding the EHR as regulated within § 291a SGB V, there is quite a long list of failed activities from other countries and commercial providers, which might relate to interface, usability, usefulness or compatibility issues. Admittedly, this is not really a valid argument, since developments rather lack a clear philosophy. When data are collected and physicians work with that data, a corresponding legal framework needs to be in place and observed. A patient needs according authorization methods. Permissions management is a big barrier, where arbitrary functionalities can be designed. Another problem in that field would be central data storage. The concept of data storage needs to be isolated from fixed memory options, because data might be stored on servers, notebooks or even USB sticks alike.

In conclusion, extensive research activities and practical examples exist. An EFA should cover urgent scenarios, for long-term developments the EHR will solve the current necessities.

- *In case Germany relies on paper-era legislation to regulate EHR would you consider it as a legal barrier to the development of EHRs?*

There are no barriers because of potential paper-era legislation. The focus is rather whether reimbursement schemes allow for a smooth development of EHRs. The German SGB V opens the possibility for health care benefactors to implement own EHRs, which is not administered in practice. § 291a SGB V sets up less barriers as insurants generally control the regulation of their record.

- *Are you aware of any cross-border cooperation projects on EHRs in your country apart from the epSOS project?*

The university clinical centre of Aachen tried to cooperate with Dutch partner clinics for quite some time. Hospitals generally have a big interest in conducting cross-border activities, especially since the Netherlands have an under-supply of clinics. The current status of this project is however unknown to me.

B) Possible barriers for the development of EHRs

a. *Health data to be included in EHRs*

- *Do the requirements on EHRs information content allow an efficient use of EHRs within Germany and for cross-border exchanges?*

The main question is: How do I strategically address the implementation and use of EHRs? There needs to be an agreement on a specific standard. National bodies need to agree on fundamental questions (as for example within three initiatives concerning medication planning). Focus needs to be on the bigger picture, where certain modules need to be reused.
The description of specific drugs is not necessary, whereas an approach based on more generic modules is the right one. Within a practical context it needs to be pointed out what requirements for specific usage scenarios are and how they can be re-used in different contexts.

- *Would you add any other elements that should be included in the EHRs?*

Scenarios involving physicians have priority: medication planning or rather more general approaches where insurants themselves benefit should be the foremost priority. Simplifying health bureaucracy can be steered by an electronic record platform (e.g. regarding repetitive prescriptions). Records kept and mainly controlled by insurants would help to form an assessable development.

- *Are there any elements currently included in the EHRs that you think should not be covered?*

Getting started is difficult, but long term exploitation will provide for solutions. The ePrescription should be put in a definite context as it can hardly be reflected in isolation. A definite context and a strategic line, a roadmap, need to be recognizable.

b. *Requirements on the institution that host the data from EHRs*

- *Are the authorisation requirements on the institutions that host the data from EHRs simple enough to foster the development of EHRs? Or does the complexity or length of the procedure prevent the interest of host institutions to implement this system? Is the procedure easy enough for a host of e-health data to be authorised?*

Authorization based on certificates is a valid, well known and established technology also to foster the development of EHRs.

c. *Consent*

- *Do the requirements on patient consent allow an efficient development of EHRs? If not, what are the consent requirements that impede the development of EHRs?*

Consent is generally the right concept. It seems questionable whether it is really necessary to ask for consent with every access activity. This is not the case for the EFA, since there is a strong purpose appropriation; this is however not the case for the (lifelong) EHR. In any case, it doesn't hinder efficiency. Whoever is responsible for implementing a functioning EHR scheme will have to take into account how to best implement the consent possibilities.

- *Do the consent requirements adequately protect the patients' right to confidentiality?*

Yes. However, it depends on how the consent is designed in practice.

d. *Access, authentication and authorisation*

- *Do the requirements on access, authentication and authorisation allow an adequate development of EHRs? If not could you specify where improvement is needed?*

Authorization procedures need to be administered by institutions rather than singular persons. This can be executed in a reasonable way also taking into account fundamental data protection rules. Person based authorization granting is a "show stopper" (unless it is ad-hoc mediated when the patient is present); the electronic profession ID for medical institutions could serve as a starting point for effective authorization.

- *Can health practitioners in Germany have access to other foreign EHR systems? If yes, do they face any problems to access those? Please describe Can health practitioners in another Member State access and enter information on an EHR hosted in your Member State? If yes, how is access granted? (e.g. on case by case basis)*

To the best of my knowledge, they cannot.

e. *Liability*

- *Are there liability issues not resolved related to the use of EHRs?*

Yes, there are. The question here is: Which commitment does the processing/recording party incur? The problem is that the recording party does not know what a third party also processing data does with the already existing data. The EFA shows good practice, that while recording information the purpose of usage needs to be defined; an all-in approval is difficult. If the user clears the data he recorded for further use and something goes wrong, also the original recording party could be liable. A classification into different categories is problematic. A usage constraint needs to yield from the recorded data.
Hence, whoever works with record data has to see it as informative data, not as a basis for treatment purposes. A qualified electronic signature is not yet fully in place in Germany. It might however serve as a guarantor for security and safety also regarding recorded data in the future.

- *Is it considered as a legal barrier for the deployment of EHRs?*

It is difficult to find an adequate solution. Some concepts of conversion are taken from other countries but they do not fully match the German framework.

f. *Archiving durations and other uses of data in EHR*

- *Do you think that the current archiving durations for EHRs are adequate to allow a proper use of EHRs?*

Archiving duration range from 10 to potentially 100 years (regarding radiological reports of children). A connecting factor is also the limitation of 30 years from the German civil code. Archiving is always to be seen partly as risk management. In the worst case scenario, physicians have to deal with a reversal of evidence; a documentation for protecting the treating persons and as proof of evidence helps in potential law suits. The protocol regulations within § 291a however serve data protection and transparency purposes only.

- *Are the current data protection requirements on e-health data a constraint for their adequate use for academic and research purpose?*

Hospitals generally complain about narrow data protection regulations regarding the conduction of research projects. However, there are diverse guidelines regarding measures to undertake research

with medical data conforming with current data protection legislation. The frame conditions are in place, it might just become difficult in the practical conversion.

g. *Links between EHRs and ePrescriptions*

- *Is the EHRs system coordinated enough with the ePrescription system?*

No. ePrescriptions are not in the focus of the current efforts to implement a telematic infrastructure anymore. Changes in government involved a change and a new prioritization towards other applications.

h. *Any other legal barriers*

- *Are you aware of any other legal barriers that impede the development of EHR system ?*

§ 291a Abs. 8 SGB V might be seen as a legal barrier. It restricts usage of the EHC to specific person groups and hence excludes others, which might make it difficult to ultimately imply areas as old-age care or rehabilitation and adjacent areas of health provision, where not necessarily only physicians are involved.
§ 291a SGB V is also rather restrictive concerning direct access of the insurant. MoH comment on that law suggests this as a reasonable measure, since a first restrictive handling is necessary while opening this up within further developments would be the most proper procedure. However, self-determined access by the insurant can be an important feature and should not be regulated too restrictively.

C) Possible good practices

- *In your view, what are the most effective features of the legal framework in your country in relation to:*

  - *Health data to be included in EHRs*

    Rather abstract legal definition allows for effective development of standards

  - *Requirements on the institution that host the data from EHRs*

    Working with certificates as well-established technical groundwork for authorization

  - *Consent*

    Strong consent regulations in general help safeguarding data protection rights and can at the same time provide for an efficient development of EHRs.

  - *Access, authentication and authorisation*

    Working with certificates as well-established technical groundwork for authentication – they have to take into account institution based authorization measures.

  - *Liability issues*

    NA

  - *Archiving durations and other uses of data in EHRs*

    Not a sole EHR issue; paper documents and digital data shall be handled the same – which is the recent situation.

  - *Links between EHRs and ePrescriptions*

    NA

  - *Any other legal good practice*

Most effective: Setting up the telematic infrastructure with all necessary safety mechanisms, clear use-case benefits must be worked out, medical applications must show the ultimate benefit.

Annex 1 – Summary of interviews with targeted stakeholders

INTERVIEW NO 1					
Name of the interviewee:Jörg Caumanns					
Profession/role of the interviewee: Fraunhofer FOKUS Leiter Kompetenzzentrum eHealth					
Type and name of organisation represented:					
Location of the interview:					
Date of the interview:					
Duration of the interview:	*<45'*				
	45'-60'	X			
	60'- 75'				
	>75'				
Interview conducted:	*Face to face*		*By telephone*		
Summary of the interview: *Please identify any key themes and then summarize the discussion under each section.* There is widespread knowledge and understanding of issues surrounding the implementation of EHRs. A heavy focus must be put on actual use cases and prototypic scenarios to elaborate the most efficient solutions regarding technical and data protection implications. However, there are a few legal barriers that might hinder the progress, for example by focusing EHR use on specific types of professions or limiting direct access possibilities for the insurant.					