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 Poland

time.lex

milieu
Law & Policy Consulting

5 March 2014

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

This report was completed by Dariusz Adamski. The views expressed herein are those of the consultants alone and do not necessarily represent the official views of the Executive Agency for Health and Consumers

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

Executive Summary

1. Stage of development of EHRs in Poland

At this point in time there exists no obligation to store and process HRs in an electronic form in Poland. Transition from a voluntary system of EHRs to an obligatory one is, however, ordained by the Act on the System of Information in Healthcare. Accordingly, it should be completed by the end of July 2014. It has turned out, however, that IT systems of healthcare providers are insufficiently developed to allow for the transition by August 2014, as originally planned. The Ministry of Healthcare has thus proposed to postpone the deadline for the obligatory transition to EHRs to 1 August 2017. A central system is currently developed by an agency of the Ministry of Healthcare (CSOIZ) to mediate the exchange of EHRs.

2. Summary of legal requirements applying to EHRs

The Polish system provides for a broad scope of information, especially personal data, to be exchangeable through the SIM. The goal is clearly to improve the system's functionality for both medical and reimbursement purposes, by the general "easy interconnectibility" of the data. Data protection is rather achieved by certain limitations on who may access the system data rather than by limiting the scope of personal information stored in the system in the first place.

Requirements imposed on the institution hosting EHRs data stem, first of all, from Act on Rights of Patients and the Patients' Rights Ombudsman. This piece of legislation first establishes that each provider of medical treatment is obliged to keep and make available health records to authorised institutions and individuals. It is also obliged to protect the data in the records. Second, more specific requirements for the IT system processing the EHRs are established by an executive Ordinance. Third, additional requirements are introduced in the context of exchanging medical data through the SIM. The latter group, however, is primarily imposed on the administrator of the SIM, rather than on institutions hosting EHR data.

No patient's consent is necessary to process HRs in Poland. This also applies to EHRs.

Creating and updating HRs is an obligation of each healthcare provider and should take place immediately after providing each healthcare service. Currently the exchange of HRs (in whatever form) is not mediated by a third party. The recipient of the HRs is thus by default known to the sender, as the exchange occurs in the context of an individual treatment or an administrative procedure. The identification and authorisation are in consequence only rudimentarily determined by law. The exchange of EHRs through the SIM will be different in this respect, which requires more advanced rules on the identification and authorisation processes.

A mismanagement of EHRs would first of all ensue penal liability for failing to secure confidentiality of personal data. An inaccuracy of HRs could not alter the liability for negligence/malpractice, because, according to Act on the professions of a doctor and a dentist medical professionals are obliged to decide about health conditions of a patient after examining her in person. Implicitly this examination should also establish the accuracy of any HR data.

The list of secondary uses for which HRs may be processed is relatively long, which remains rather obvious considering that HRs play a role in contexts other than individual treatments. The corresponding disclosure obligation is justified by the goal of avoiding financial fraud stemming (medical treatment is most often funded from public resources). On the other hand, the institutions obtaining access to HRs for secondary uses are not authorised to process the records for purposes other than established by relevant legislation. Individuals doing otherwise face penal sanctions provided for in the general data protection legislation.

Archiving durations are unambiguously determined by the Act on Rights of Patients.

As a basic principle, until the SIM system is up and running it is up to healthcare providers keeping EHRs to make their EHR systems interoperable. Subsequently they are obliged to use formats and standards allowing for interoperability of their systems.

E-prescriptions have been precluded in Poland by a sub-legislative act requiring that prescriptions be signed with a handwritten signature. E-prescriptions will replace paper ones in 2016, when the SIM allows for necessary functionalities.

3. Good practices

While access to medical e-registers has been advanced recently, the project aimed at establishing a common platform for an exchange of EHRs is still ongoing. An assessment of its efficiency and functionalities is possible only when healthcare gains experience in using it (i.e. not later than late 2017).

4. Legal barriers

Legal barriers for the deployment of EHRs are neither persistent nor difficult to remove in Poland (the process of removing the barriers is ongoing and unendangered, as it involves no controversies).

Contents

List of abbreviations

EHRs	Electronic Health Records
HRs	Health Records
NFZ	Narodowy Fundusz Zdrowia (National Health Fund)
SIM	System Informacji Medycznej (Medical Information System)
CSIOZ	Centrum Systemów Informacyjnych Ochrony Zdrowia (Centre of Health Information Systems)

1. General context

At this point there exists no obligation to store and process HRs in an electronic form in Poland. Individual healthcare providers may choose to do so, however, in which case their IT systems processing EHRs should comply with certain (rather basic, as further discussed in Sec. 2.4) requirements established by the Ordinance of the Minister of Healthcare of 21 Dec. 2010 on types and the scope of health records and on the method of processing them (hereinafter: Ordinance on health records).[1]

A transition from a voluntary system of EHRs to an obligatory one is, however, ordained by the Act of 28 April 2010 on the System of Information in Healthcare[2] (hereinafter: Act on the System of Information in Healthcare). One of its interim provisions (art. 56) explicitly allows for maintaining HRs either in a paper or an electronic form, depending on the choice of the provider, yet no longer than by the end of July 2014. Starting from 1 August 2014, according to art. 11(1) of the same Act "service providers shall keep medical documentation in the electronic form". Simultaneously, another provision of the same Act (art. 50) has introduced a new sentence to art. 24 of the Act of 6 November 2008 on Rights of Patients and the Patients' Rights Ombudsman[3] (hereinafter: Act on Rights of Patients). The latter provision sets general principles for HRs. The new sentence requires that HRs be kept exclusively in an electronic form starting from 1 August 2014.

It has turned out, however, that IT systems of healthcare providers are insufficiently developed to allow for the transition by August 2014, as originally planned. Nor will the SIM project, further discussed especially in Sec. 1.3, be sufficiently developed to allow for the interoperability of the systems by this date. The Ministry of Health has thus proposed to postpone the deadline for the obligatory transition to EHRs. According to its document entitled "Principles of Draft Amendment to the Act on the System of Information in Healthcare"[4] (hereinafter: Amendment Principles), dated 17 January 2014, the obligation to keep EHRs only is delayed by three years, and hence will not become operational before 1 August 2017.

EHR systems in place

As mentioned above, EHR systems are not obligatory in Poland. What is more important, technical requirements for such systems, as provided by the Ordinance on health records, are rather general (see Sec. 2.4). In consequence, EHRs of individual providers may vary significantly, often precluding their interoperability.

A central system for processing data from medical registers (a platform for making on-line services and digital resources of medical registers available to enterprises, Pol. Platforma udostępniania on-line przedsiębiorcom usług i zasobów cyfrowych rejestrów medycznych), known as the P2 project, was launched in January 2013. While the P2 project uses authorisation processes and infrastructure shared in the future with the P1 project (mentioned in Sec. 1.3), otherwise it does not involve aspects relevant for the subject matter of this report.

[1] Pol. *rozporządzenie Ministra Zdrowia z dnia 21 grudnia 2010 r. w sprawie rodzajów i zakresu dokumentacji medycznej oraz sposobu jej przetwarzania* (Dz.U. 2010 nr 252 poz. 1697, with further amendments).
[2] Pol. *ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia* (Dz. U. 2011 r., Nr 113, poz. 657, with further amendments).
[3] Pol. *ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta* (Dz. U. 2009, Nr 52, poz. 417, with further amendments).
[4] Pol. Założenia do projektu ustawy o zmianie ustawy o systemie informacji w ochronie zdrowia oraz niektórych innych ustaw, available at http://www2.mz.gov.pl/wwwfiles/ma_struktura/docs/projzalust_sioz_20140120.pdf.

Institutional setting

Pursuant to art. 24(1) of the Act on Rights of Patients, in order to make the patients' right to access health records possible each provider of medical treatment is obliged to keep and make available health records of individual patients, as well as to protect their confidentiality. The obligation of keeping HRs thus falls on each provider of medical treatment. Another important institutional actor is the NFZ, in charge of reimbursing medical treatments of the patients insured in the state-owned health insurance scheme. Both the state insurance and the structure of the NFZ are currently highly centralised, though a decentralisation is contemplated by the Ministry of Healthcare.

HRs may also be accessed by various oversight bodies, essentially depending on the ownership structure of medical healthcare providers (which may be highly diverse, from purely private to owned by local communes to owned by regions or by the state).

Furthermore, as HRs are devised in the Polish legal system as patient rights, the Patients' Rights Ombudsman[5] is authorised to oversee whether/how healthcare providers abide by the right. The general data protection framework also applies, as are powers of the Data Protection Authority.[6]

Legal setting and future legal development

One of main goals of the Act on the System of Information in Healthcare is to establish the legal tissue for an overarching IT infrastructure allowing for the interoperability of EHRs (which the act treats essentially as tantamount to individual medical data) systems kept by individual providers. To that end the Act provides (art. 3(1)) that the information on:

- medical treatments provided and planned;
- service providers and
- service recipients

should form one information system (called Healthcare Information System).

While the Healthcare Information System is disentangled from the technological context (it is entirely preoccupied with the informational aspect), the Act on the System of Information in Healthcare provides that the information system be technologically enabled by the SIM: a tele-informatic system for processing data on provided and planned medical treatments, patients' personal data and medical data, information on providers, on payers, on medical employees, as well as on costs and other data necessary to exchange electronic documents (art. 10(1) Act on the System of Information in Healthcare). Some of the abovementioned data is derived from various central registers, and in particular from:

- the Central Register of Service Recipients (Pol. Centralny Wykaz Usługobiorców);
- the Central Register of Service Providers (Pol. Centralny Wykaz Usługodawców);
- the Central Register of Medical Employees (Pol. Centralny Wykaz Pracowników Medycznych).

To allow for matching the registry data with EHRs, as well as to enable the interoperability of the latter, the CSOIZ – an agency affiliated to the Ministry of Health and specialised in IT issues - has developed a project called Electronic Platform for Collecting, Analysing and Sharing Digital Medical Records (Pol. *Elektroniczna Platforma Gromadzenia, Analizy i Udostępniania zasobów cyfrowych o Zdarzeniach Medycznych*), more commonly known as „P1 Project".[7] It corresponds to two legal

[5] Pol. *Rzecznik Praw Pacjenta*.
[6] Pol. *Generalny Inspektor Ochrony Danych Osobowych*.
[7] According to the information obtained from the Respondent No. 4, the P1 project should be fully functional by December 2014, while some of its functionalities (e-Prescription, e-Request) should be available by May/June 2014.

provisions established in the Act on the System of Information in Healthcare. First, pursuant to its art. 11(2), each service provider should be able to gain access, through the SIM/P1 project, to data, including personal data and individual HRs, from EHRs stored in another provider's IT system, if this is necessary to continue treatment or for a diagnostic procedure. Each provider is also obliged – according to art. 11(3) – to give access, through the SIM, to data necessary for another healthcare provider or a pharmacist. The P1 Platform should allow for both of the actions.

2. Legal requirements applying to EHRs in Poland

2.1. Health data to be included in EHRs

The Act on the System of Information in Healthcare (art. 2(6)) defines EHRs as:

a) an electronic document entitling a service recipient to obtain medical treatment of a given type, in respect to providers of orthopaedic items or pharmacies;
b) in other cases: HRs generated in an electronic form, containing data on provided and planned medical treatments, including electronic documents allowing the healthcare provider to obtain medical treatment of a given type.

The Polish legal system does not directly determine the specific data to be included in EHRs. It does so, however, indirectly, by – on the one hand – establishing the scope of the HR data (irrespective of the medium on which it is stored) and – on the other hand – determining the range of HR data processed in the SIM.

As to the first of the two aspects, art. 25 Act on Rights of Patients provides that HRs cover *at least* (i.e. the list is non-exclusive):

1) Personal data identifying the patient:
   a) surname and first name(s);
   b) date of birth;
   c) gender;
   d) place of abode;
   e) personal identification number (PESEL);
   f) name of legal representative (in respect to legally incapacitated individuals).
2) Indication of the treatment provider;
3) Description of the patient's health condition or the treatment provided;
4) Date of producing the record.

As to the second aspect, the SIM system should process data on provided and planned medical treatments, patients' personal data and medical data, information on providers, on payers, on medical employees, as well as on costs of the treatment and data necessary to exchange electronic documents (art. 10(1) Act on the System of Information in Healthcare). Contrary to the scope of personal data included in HRs, the range of personal data to be processed by the SIM system is closed, even though it is broad. According to art. 4(3) Act on the System of Information in Healthcare it includes, in addition to the list provided in the Act on Rights of Patients, the following personal data:

- family name;
- citizenship;
- marital status (processed for statistical purposes only);
- education (processed for statistical purposes only);
- ID or passport number in respect to individuals who have not been assigned a PESEL number;
- place of residence of those who do not have their abode in Poland;
- mailing address and e-mail address;
- insurance numbers;
- type of healthcare entitlements, numbers and dates of expiry of documents certifying the healthcare entitlements of a given type or the date of those entitlements' expiry;
- identification numbers assigned by the payer or the healthcare provider;
- level of disability;
- the date and reason of demise.

According to the Ordinance of the Minister of Healthcare of 11 April 2013 on the method of identifying service recipients, medical employees and service providers as well as the method of transmitting information by service providers about medical employees providing healthcare[8], both healthcare recipients and medical employees using the SIM system are identified in the SIM system with their PESEL numbers. Foreigners are identified either by the identification number used in their country of origin or by the number of their ID or passport when they have not been assigned an identification number.

2.1.1 Main findings

The Polish system provides for an open list of HR data and a broad scope of information, especially personal data, to be exchangeable through the SIM. The goal is clearly to improve the system's functionality for both medical and reimbursement purposes, by the general "easy interconnectibility" of the data. Data protection is rather to be achieved by certain limitations on who may access the data rather than by limiting the scope of personal information stored in the system in the first place.

[8] Pol. *Rozporządzenie Ministra Zdrowia z dnia 11 kwietnia 2013 r. w sprawie sposobu identyfikacji usługobiorców, pracowników medycznych i usługodawców oraz sposobu i trybu przekazywania przez usługodawców informacji o pracownikach medycznych udzielających świadczeń opieki zdrowotnej*, (Dz.U. 2013, poz. 502).

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?)	Act on the Rights of Patients	As long as EHRs are not covered by the SIM system, general rules on HRs apply. When the SIM system becomes fully functional, the scope of EHRs it processes will be determined by the requirements for the data to be exchanged through the SIM.
Are these data restricted to purely medical information (e.g. physical or mental health, well-being)?	Art. 25 Act on Rights of Patients	Purely medical information is a part of HRs, but the latter is contextualised by including other information (primarily identifying the patient).
Is there a definition of EHR or patient's summary provided in the national legislation?	Art. 2 Act on the System of Information in Healthcare	The Act on the System of Information in Healthcare (art. 2(6)) defines EHRs as: • an electronic document entitling a service recipient to obtain medical treatment of a given type, in respect to providers of orthopaedic items or pharmacies; • in other cases: HRs generated in an electronic form, containing data on provided and planned medical treatments, including electronic documents allowing the healthcare provider to obtain medical treatment of a given type.
Are there any requirements on the content of EHRs (e.g. detailed requirements on specific health data or general reference to health data)?	Art. 25 Act on Rights of Patients	Art. 25 Act on Rights of Patients only states that the HR should contain "a description of the patient's health condition or the treatment provided" without further details.
Are there any specific rules on the use of a common terminology or coding system to identify diseases, disorders, symptoms and others?	§ 7 Ordinance on health records	The International Statistical Classification of Diseases and Related Health Problems, Tenth Revision, is used for names and statistical numbers of diseases diagnosed.
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)?		n/a
Are there any specific rules on identification of patients in EHRs?	Art. 25 Act on Rights of Patients + art. 4 Act on the System of Information in Healthcare	Art. 25 Act on Rights of Patients provides that HRs cover *at least* (i.e. the list is non-exclusive) the following personal data identifying the patient: • surname and first name(s); • date of birth;

Questions	Legal reference	Detailed description
		• gender; • place of abode; • personal identification number (PESEL); • name of legal representative (in respect to legally incapacitated individuals). According to art. 4(3) Act on the System of Information in Healthcare it includes, in addition to the list provided in the Act on Rights of Patients, the following personal data: - family name; - citizenship; - marital status (processed for statistical purposes only); - education (processed for statistical purposes only); - ID or passport number in respect to individuals who have not been assigned a PESEL number; - place of residence of those who do not have their abode in Poland; - mailing address and e-mail address; - insurance numbers; - type of healthcare entitlements, numbers and dates of expiry of documents certifying the healthcare entitlements of a given type or the date of those entitlements' expiry; - identification numbers assigned by the payer or the healthcare provider; - level of disability; - the date and reason of demise.
Is there is a specific identification number for eHealth purposes?		The general identification (PESEL) number is used as a reference. No specific safeguards to avoid "easy interconnectibility" of data are provided.

2.2. Requirements on the institution hosting EHRs data

Pursuant to art. 24(1) Act on Rights of Patients each provider of medical treatment is obliged to keep and make available health records to authorised institutions and individuals, as well as to protect the data in the records.

Specific rules relevant for EHRs are furthermore laid down in the Ordinance on health records. According to its § 4(1) HRs must be updated immediately after an individual healthcare service is provided. Furthermore, according to 80 §HRs may be kept in an electronic form, if the system in which they are stored allows to:

- prevent the HRs from loss or damage;
- maintain their integrity and credibility;
- provide constant access of authorised individuals and prevent access by unauthorised individuals;
- identify individuals providing healthcare and updating HRs;
- make individual HRs available, including by an export of electronic documents, in XML or PDF files;
- allow for an export of all the data in the XML format, so that the HRs may be retrieved in another IT system;
- print the HRs.

The Ordinance of the Minister Of Healthcare of 28 March 2013 on requirements for the Healthcare Information System[9] (hereinafter: the Ordinance on requirements for the HIS) provides for a set of additional requirements imposed on the administrator of the SIM and healthcare providers in the context of the exchange of data through the system.

According to its § 10, minimum requirements for the security of processing and disclosure of electronic data should allow for:

1) access of the service provider to protected information stored in the SIM;
2) implementation of mechanisms for audits of the exchange of data related to an electronic SIM document;
3) authorisation and identification of the individuals attempting to access electronic SIM documents;
4) implementation of mechanisms for obtaining, registering and updating the service recipient's consent to have either all or a part of the data processed in the SIM accessed, including the purpose of obtaining the data;
5) determination, modification or revocation of the rights to access all or some of the data processed in the SIM.

Furthermore, pursuant to § 11 Ordinance on requirements for the HIS, EHRs and other data processed in the system should be "highly protected". In practice this means that protection measures ought to, first, allow for controlling information flows between the SIM and the public Internet network and for controlling actions initiated from the public Internet network and the SIM. Second, administrators of personal data exchanged through the SIM (healthcare providers) should apply cryptographic protection of the authorisation data. Finally, according to § 12 Ordinance, the administrator of the SIM (CSIOZ) is obliged to deploy and constantly improve the information security management system used to guarantee confidentiality, accessibility and integrity of the exchanged information. The security management system should be compliant with the following standards: PN-EN 14484:2005, PN-EN 14485:2005, PN-EN ISO 27799:2010, or standards replacing them.

[9] Pol. *Rozporządzenie Ministra Zdrowia z dnia 28 marca 2013 r. w sprawie wymagań dla Systemu Informacji Medycznej, Dz. U. 2013, poz. 463*.

2.2.1. Main findings

Requirements imposed on institutions hosting EHR data stem, first of all, from Art. 24(1) Act on Rights of Patients, which provides that each healthcare provider is obliged to keep and make available health records to authorised institutions and individuals, as well as to protect the data. Second, requirements for IT systems in which EHRs are processed derive from the Ordinance on health records. Third, additional requirements are introduced in the context of exchanging medical data through the SIM. The latter group, however, is primarily imposed on the administrator of the SIM, rather than on institutions hosting EHR data.

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?	§ 80 Ordinance on health records; § 10, 11 Ordinance on requirements for the HIS	Specific rules relevant for EHRs are laid down in the Ordinance on health records. According to its § 80 HRs may be kept in an electronic form, if the system in which they are stored allows to: - prevent the HRs from loss or damage; - maintain their integrity and credibility; - provide constant access of authorised individuals and prevent access by unauthorised individuals; - identify individuals providing healthcare and updating HRs; - make individual HRs available, including by an export of electronic documents, in XML or PDF files; - allow for an export of all the data in the XML format, so that the HRs may be retrieved in another IT system; - print the HRs. According to § 10 Ordinance on requirements for the HIS, minimum requirements for the security of processing and disclosure of electronic data should allow for: 1) access of the service provider to protected information stored in the SIM; 2) implementation of mechanisms for audits of the exchange of data related to an electronic SIM document; 3) authorisation and identification of the individuals attempting to access electronic SIM documents; 4) implementation of mechanisms for obtaining, registering and updating the service recipient's consent to have either all or a part of the data processed in the SIM accessed, including the purpose of obtaining the data; 5) determination, modification or revocation of the rights to access all or some of the data processed in the SIM. Furthermore, pursuant to § 11 Ordinance on requirements for the HIS, EHRs and other data processed in the system should be "highly protected". In practice this means that protection measures ought to, first, allow for controlling information flows between the SIM and the public Internet network and for controlling actions initiated from the public Internet network and the SIM. Second, administrators of personal data exchanged through the SIM (healthcare providers) should apply

Questions	Legal reference	Detailed description
		cryptographic protection of the authorisation data. Finally, according to § 12 Ordinance, the administrator of the SIM (CSIOZ) is obliged to deploy and constantly improve the information security management system used to guarantee confidentiality, accessibility and integrity of the exchanged information. The security management system should be compliant with the following standards: PN-EN 14484:2005, PN-EN 14485:2005, PN-EN ISO 27799:2010, or standards replacing them.
Is there a need for a specific authorisation or licence to host and process data from EHRs?		n/a
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)?	§ 80 Ordinance on health records; § 10, 11 Ordinance on requirements for the HIS	Specific rules relevant for EHRs are laid down in the Ordinance on health records. According to its § 80 HRs may be kept in an electronic form, if the system in which they are stored allows to: - prevent the HRs from loss or damage; - maintain their integrity and credibility; - provide constant access of authorised individuals and prevent access by unauthorised individuals; - identify individuals providing healthcare and updating HRs; - make individual HRs available, including by an export of electronic documents, in XML or PDF files; - allow for an export of all the data in the XML format, so that the HRs may be retrieved in another IT system; - print the HRs. According to § 10 Ordinance on requirements for the HIS, minimum requirements for the security of processing and disclosure of electronic data should allow for: 1) access of the service provider to protected information stored in the SIM; 2) implementation of mechanisms for audits of the exchange of data related to an electronic SIM document; 3) authorisation and identification of the individuals attempting to access electronic SIM documents; 4) implementation of mechanisms for obtaining, registering and updating the service recipient's consent to have either all or a part of the data processed in the SIM accessed, including the purpose of obtaining the data;

Questions	Legal reference	Detailed description
		5) determination, modification or revocation of the rights to access all or some of the data processed in the SIM. Furthermore, pursuant to § 11 Ordinance on requirements for the HIS, EHRs and other data processed in the system should be "highly protected". In practice this means that protection measures ought to, first, allow for controlling information flows between the SIM and the public Internet network and for controlling actions initiated from the public Internet network and the SIM. Second, administrators of personal data exchanged through the SIM (healthcare providers) should apply cryptographic protection of the authorisation data. Finally, according to § 12 Ordinance, the administrator of the SIM (CSIOZ) is obliged to deploy and constantly improve the information security management system used to guarantee confidentiality, accessibility and integrity of the exchanged information. The security management system should be compliant with the following standards: PN-EN 14484:2005, PN-EN 14485:2005, PN-EN ISO 27799:2010, or standards replacing them.
In particular, is there any obligation to have the information included in EHRs encrypted?	§ 11 Ordinance on requirements for the HIS	Administrators of personal data exchanged through the SIM (healthcare providers) should apply cryptographic protection of the authorisation data.
Are there any specific auditing requirements for institutions hosting and processing EHRs?		No as long as EHRs are not accessible through the SIM. Afterwards the SIM is audited. Audits by the Data Protection Authority and/or IT audits in the context of fulfilling minimum technical requirements by public bodies (the latter based on general framework of informatisation of public bodies) may take place, on an ad hoc basis, when HRs are processed in an IT system.

2.3. Patient consent

Processing of personal data contained in HRs is not based on a patient's consent in Poland, in compliance with art. 8(3) Directive 95/46. The latter lifts the ban on processing data concerning health or sex life "where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy". In principle, therefore, no patient's consent is required to process any of the data included in HRs, whether processed on paper or in an electronic form.
Similarly, neither the content nor the ability to exchange HRs through the SIM is dependent on the patient's consent. One exception refers to processing data in the payment and statistical modules of the SIM. According to art. 35(5) Act on the System of Information in Healthcare patients may refuse access to individual medical data stored in this module. Even this objection may, however, be overcome in a number of cases (e.g. for purposes of improving access to medical treatments and its equality, of financial management, etc.).

2.3.1. Main findings

No patient's consent is necessary to process HRs in Poland. This also applies to EHRs.

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?		n/a
Is a materialised consent needed?		n/a
Are there requirements to inform the patient about the purpose of EHRs and the consequences of the consent or withholding consent to create EHRs?		n/a
Are there specific national rules on consent from the patient to share data?	Art. 35(5) Act on the System of Information in Healthcare	Patients may refuse access to individual medical data stored in the payment and statistical module of the SIM. This objection may, however, be overcome in a number of cases (e.g. for purposes of improving access to medical treatments and its equality, of financial management, etc.).
Are there any opt-in/opt-out rules for patient consent with regard to processing of EHRs?		n/a
Are there any opt-in/opt-out rules for patient consent with regard to sharing of EHRs?		n/a
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?		n/a
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)?		n/a
Are there specific rules on patient consent to share data on a cross-border situation?		n/a

2.4. Creation, access to and update of EHRs

Pursuant to art. 24(2) Act on Rights of Patients doctors, nurses and midwifes are authorised to obtain and process HR data.
As a basic principle, providers of medical treatment should render HRs available to the patient or her legal representative and to individuals otherwise authorised by the patient (art. 26(1)). HRs are, however, also available to a closed list of institutions enumerated in art. 26(3) Act on Rights of Patients, the most important among which are:

- healthcare providers, if HRs are necessary to secure continuity of treatment;
- public authorities, the NFZ, vocational associations (compulsory organisations) of medical professionals, as well as certain other advisory and auditing bodies, as far as revealing HRs is necessary for fulfilling their tasks, referring in particular to control and oversight;
- the minister in charge of healthcare, courts, public prosecutors, medical consultants in court proceedings and agents of vocational responsibility, in connection to their individual proceedings;
- separate institutions and bodies, if they have ordered a given examination;
- pension authorities, in connection to their individual proceedings;
- insurance companies, when authorised by the patient.

The abovementioned rules apply, of course, also to EHRs.
Furthermore, according to § 83(1) Ordinance on health records the disclosure of HRs may take a form of:

- transfer of a physical carrier with the recorded data;
- electronic transmission;
- disclosure of paper printouts.

In each case the transmission should guarantee integrity of data and protection of personal data (§ 83(2)).

Furthermore, according to § 86 Ordinance on health records, EHRs are deemed protected if the following requirements are fulfilled on a continuous basis:

1. they are accessible by authorised individuals only;
2. they are protected from accidental or unauthorised destruction;
3. effectiveness of methods and means of protection is universally recognised at the time of their application;

The abovementioned protection requires in particular that:

1) security threats involved are systematically analysed;
2) security procedures and processing systems, including access and storage procedures, are developed and applied;
3) security measures are adequate to the threats involved;
4) all organisational and technological means of protection are controlled systematically and ascertained periodically;
5) plans of keeping records in a longer perspective, including transferring them to new data carriers and new data formats are developed and implemented, if this is necessary to secure continuity of access to the documents.

A new layer of issues analysed in this section will become relevant when the SIM becomes fully operational. Particularly the question of the EHRs' accessibility and the interoperability of the systems in which they are stored will become a serious issue at this point. The Act on the System of Information in Healthcare and the Ordinance on requirements for the HIS thus sets up specific rules on

the issues. The first establishes a list of purposes for which the data may be disclosed (art. 12(1)), including, among others:

- improving access to medical treatment funded from public resources;
- monitoring of equal access to the treatment funded from public resources;
- analysing financial flows;
- monitoring by healthcare recipients of the waiting periods on waiting lists;
- exchanging EHRs between healthcare providers when necessary to secure continuity of healthcare provision.

Furthermore, art. 12(2) Act on the System of Information in Healthcare stipulates that the access to the SIM data is dependent on functions and legal entitlements of individual users. Some categories of users may explicitly gain access to medical and personal data (healthcare recipients, payers, medical employees, healthcare providers and entities keeping medical registers – art. 12(3-4, 6-7). Other categories (regional representatives of the state government and local communes, both of which are involved in monitoring or providing healthcare) are simply mentioned as authorised to access SIM data (art. 12(5), (8)). It could thus be argued that the latter categories are not entitled to gain access to individual medical and personal data (as accessing HR data by this category is not, contrary to the former ones, explicitly mentioned in the Act).

Furthermore, the Ordinance on requirements for the HIS provides detailed rules on more technical aspects related to the exchange of medical information through the SIM. First, EHRs should be exchanged as XML files or multimedia files, with their logical structure further determined by the administrator of the SIM system (§ 3). The exchange of data should be compliant with the XML/XSD format and the DICOM format (§ 4(3)). EHRs may be disclosed after the user is identified either with a qualified certificate or the so-called "trusted profile" provided by the Electronic Platform of Public Administration Services (ePUAP) (§ 4(1)). According to the same Ordinance, accessing the EHRs via the SIM consists of the following steps (§ 5):

1. sending a request for EHRs by the recipient and receiving it by the SIM;
2. verifying the recipient's authorisation by the administrator of the SIM;
3. in case the verification is positive: transmitting the request to the provider originating the EHRs;
4. preparing the communication to be transmitted by a medical employee of the provider;
5. signing the communication by the medical employee of the provider either with a secure electronic signature verified with a qualified certificate, or with a signature verified with the so-called "trusted profile" of the ePUAP;
6. sending the EHRs by the provider and receiving it by the recipient;
7. confirming the receipt of the EHRs by the recipient both in the SIM and the EHR system of the provider.

2.4.1. Main findings

Creating and updating HRs is an obligation of each healthcare provider and should take place immediately after providing each healthcare service. Currently the exchange of HRs (in whatever form) is not mediated by a third party. The recipient of HRs is thus by default known to the sender, as the exchange occurs in the context of an individual treatment or an administrative procedure. The identification and authorisation are in consequence only rudimentarily determined by law. The exchange of EHRs through the SIM will be different in this respect, which requires more advanced rules on the identification and authorisation processes.

2.4.2.Table on creation, access to and update of EHRs

Questions	Legal reference	Detailed description
Are there any specific national rules regarding who can create and where can EHRs be created?	Art. 24 Act on Rights of Patients	Creation and updating of HRs is an obligation of each healthcare provider. Doctors, nurses and midwifes are authorised to obtain and process HR data (including the creation of EHRs).
Are there specific national rules on access and update to EHRs?	§ 83 Ordinance on health records, art. 12 Act on the System of Information in Healthcare	According to § 83(1) Ordinance on health records the disclosure of HRs may take a form of: - transfer of a physical carrier with the recorded data; - electronic transmission; - disclosure of paper printouts. In each case the transmission should guarantee integrity of data and protection of personal data (§ 83(2)). A new layer of issues analysed in this section will become relevant when the SIM becomes fully operational. Particularly the question of the EHRs' accessibility and the interoperability of the systems in which they are stored will become a serious issue at this point. The Act on the System of Information in Healthcare and the Ordinance on requirements for the HIS thus sets up specific rules on the issues. The first establishes a list of purposes for which the data may be disclosed (art. 12(1)), including, among others: - improving access to medical treatment funded from public resources; - monitoring of equal access to the treatment funded from public resources; - analysing financial flows; - monitoring by healthcare recipients of the waiting periods on waiting lists; - exchanging EHRs between healthcare providers when necessary to secure continuity of healthcare provision.
Are there different categories of access for different health professionals?		n/a
Are patients entitled to access their EHRs?	Art. 26 Act on Rights of Patients	According to Art. 26(1) Act on Rights of Patients providers of medical treatment should render HRs available to the patient or her legal representative and to individuals otherwise authorised by the patient.
Can patient have access to all of EHR content?	Art. 26 Act on Rights of Patients	No restrictions in the scope of access provided by the Act on Rights of Patients
Can patient download all or some of EHR content?	Art. 26 and Act on Rights of Patients and § 83 Ordinance on	Such a conclusion may be inferred from the obligation to provide access to patients and from the possibility to transmit EHRs electronically. Some

Questions	Legal reference	Detailed description
	health records	providers deliver such a functionality.
Can patient update their record, modify and erase EHR content?		Patients are not authorised to single-handedly alter contents of any HRs.
Do different types of health professionals have the same rights to update EHRs?		No differentiation in this respect provided by the legislation.
Are there explicit occupational prohibitions? (e.g. insurance companies/occupational physicians…)	Art. 26 Act on Rights of Patients, art. 12 Act on the System of Information in Healthcare	Except for patients and physicians HRs are available to a closed list of institutions enumerated in art. 26(3) Act on Rights of Patients, the most important among which are: - healthcare providers, if HRs are necessary to secure continuity of treatment; - public authorities, the NFZ, vocational associations (compulsory organisations) of medical professionals, as well as certain other advisory and auditing bodies, as far as revealing HRs is necessary for fulfilling their tasks, referring in particular to control and oversight; - the minister in charge of healthcare, courts, public prosecutors, medical consultants in court proceedings and agents of vocational responsibility, in connection to their individual proceedings; - separate institutions and bodies, if they have ordered a given examination; - pension authorities, in connection to their individual proceedings; - insurance companies, when authorised by the patient. Furthermore, art. 12(2) Act on the System of Information in Healthcare stipulates that the access to the SIM data is dependent on functions and legal entitlements of individual users. Some categories of users may explicitly gain access to medical and personal data (healthcare recipients, payers, medical employees, healthcare providers and entities keeping medical registers – art. 12(3-4, 6-7). Other categories (regional representatives of the state government and local communes, both of which are involved in monitoring or providing healthcare) are simply mentioned as authorised to access SIM data (art. 12(5), (8)). It could thus be argued that the latter categories are not entitled to gain access to individual medical and personal data (as accessing HR data by this category is not, contrary to the former ones, explicitly mentioned in the Act).
Are there exceptions to the access		No temporary or extraordinary exceptions provided.

Questions	Legal reference	Detailed description
requirements (e.g. in case of emergency)?		
Are there any specific rules on identification and authentication for health professionals? *Or are they aggregated?*	§ 4 Ordinance on requirements for the HIS	§ 4(1) Ordinance provides that EHRs may be disclosed after the user is identified either with a qualified certificate or the so-called "trusted profile" provided by the Electronic Platform of Public Administration Services (ePUAP).
Does the patient have the right to know who has accessed to his/her EHRs?		According to general data protection principles (in particular art. 32 Act on the Protection of Personal Data).
Is there an obligation on health professionals to update EHRs?	§ 4 Ordinance on health records	According to § 4(1) Ordinance on health records HRs must be updated immediately after an individual healthcare service is provided.
Are there any provisions for accessing data on 'behalf of' and for request for second opinion?	Art. 24 and 26 Act on Rights of Patients	Accessing the data "on behalf of" has been provided for explicitly, in respect to legal representatives. The right to access HRs (irrespective of the form) for second opinion is a consequence of the right of medical professional to access it when necessary to guarantee continuity of treatment.
Is there in place an identification code system for cross-border healthcare purpose?	§ 7 Ordinance on health records	The International Statistical Classification of Diseases and Related Health Problems, Tenth Revision, is used for names and statistical numbers of the diagnosed diseases.
Are there any measures that consider access to EHRs from health professionals in another Member State?		But access to HRs (irrespective of the form) for health professionals in other Member States may be inferred from the right of a medical professional to access them when necessary to guarantee a continuity of treatment.

2.5. Liability

Liability for negligence/malpractice is governed by general civil law rules on either contractual or non-contractual liability. In any case, the liability arises if the damage is done by a violation of due diligence, which in turn takes the professional character of treatment provision into account. The aggrieved party can also request a compensation if her personal non-pecuniary rights (e.g the right to dignity) is violated by a medical negligence/malpractice.

There are no medical liability requirements related to the use of EHRs in Poland. It is, furthermore, rather improbable that the civil law proceedings would ever be instituted for mismanagement of the HRs, as a causality between it and the damage would be difficult to prove. On the other hand, in case of such a mismanagement art. 51 and art. 52 Act of 29 August 1997 on the Protection of Personal Data[10] would apply. Art. 51(2) provides that the administrator who unintentionally allows an unauthorised person to access personal data is subject to a fine, partial or outright imprisonment for the period of up to one year. The same sanctions are provided by art. 52 for the administrator who – even unintentionally – violates the obligation to protect data from interception, damage or destruction by a third person.

Furthermore, art. 49(1) Act on the Protection of Personal Data provides that whoever processes personal data in a filing system without legal basis is subject to a fine, partial or outright imprisonment for the period of up to two years. This provision may apply to secondary users processing HRs covering personal data outside eligible purposes.

No further specific documents on the issue (no position papers, guidelines, or recommendations) have been developed in Poland.

2.5.1. Main findings

A mismanagement of EHRs would first of all ensue penal liability for failing to secure confidentiality of personal data. An inaccuracy of HRs could not alter the liability for negligence/malpractice, because, according to art. 42 Act of 5 Dec. 1996 on the professions of a doctor and a dentist[11] medical professionals are obliged to decide about the patient's health condition after examining her in person. Implicitly this examination should also establish the accuracy of any HR data, thus the latter may not alter medical liability.

[10] Pol. *ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 1997, Nr 133, poz. 883, with further ammendments).*

[11] Pol. *ustawa z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty, Dz. U. 2011, Nr 277, poz. 1634, with further ammendments).*

2.5.2. Table on liability

Questions	Legal reference	Detailed description
Does the national legislation set specific medical liability requirements related to the use of EHRs?		n/a
Can patients be held liable for erasing key medical information in EHRs?		Patients are not authorised to alter contents of HRs.
Can physicians be held liable because of input errors?		As no decision on treatment may be taken only on the basis of HRs, the damage (if any) would rather be caused by neglecting an actual examination of the patient before taking a decision on treatment, rather than by a HR input error.
Can physicians be held liable because they have erased data from the EHRs?		According to § 4(3) Ordinance on health records HRs ought not to be erased. But as no decision on treatment may be taken only on the basis of HRs, the damage (if any) would rather be caused by neglecting an actual examination of the patient before taking a decision on treatment, rather than by an erasure of HR data.
Are hosting institutions liable in case of defect of their security/software systems?	Art. 51 and 52 Act on the Protection of Personal Data	Art. 51(2) Act on the Protection of Personal Data provides that the administrator who unintentionally allows an unauthorised person to access personal data is subject to a fine, partial or outright imprisonment for the period of up to one year. The same sanctions are provided by art. 52 for the administrator who – even unintentionally – violates the obligation to protect data from interception, damage or destruction by a third person.
Are there measures in place to limit the liability risks for health professionals (e.g guidelines, awareness-raising)?		n/a
Are there liability rules related to breach of access to EHRs (e.g. privacy breach)?	Art. 51 and 52 Act on the Protection of Personal Data	Art. 51(2) Act on the Protection of Personal Data provides that the administrator who unintentionally allows an unauthorised person to access personal data is subject to a fine, partial or outright imprisonment for the period of up to one year. The same sanctions are provided by art. 52 for the administrator who – even unintentionally – violates the obligation to protect data from interception, damage or destruction by a third person.
Is there an obligation on health professionals to access EHRs prior to take a decision involving the patient?		It is a rudimentary professional standard, even if not clearly provided by law. Proving that a defendant doctor in malpractice liability proceedings did not consult HRs (which may be easier to prove in respect to EHRs) would be an evidence in favour of the plaintiff.
Are there liability rules related to the	Art. 49 Act on the Protection	Art. 49(1) Act on the Protection of Personal Data provides that whoever processes

Questions	Legal reference	Detailed description
misuse of secondary use of health data?	of Personal Data	personal data in a filing system without legal basis is subject to a fine, partial or outright imprisonment for the period of up to two years.

2.6. Secondary uses and archiving durations

As mentioned in Sec. 2.4, HRs are available for a set of secondary users, the most important among which are:

- public authorities, the NFZ, vocational associations (compulsory organisations) of medical profe
- ssionals, as well as to certain other advisory and auditing bodies, as far as revealing HRs is necessary for fulfilling their tasks, referring in particular to control and oversight;
- the minister in charge of healthcare, courts, public prosecutors, medical consultants in court proceedings and agents of vocational responsibility, in connection to their individual proceedings;
- separate institutions and bodies, if they have ordered a given examination;
- pension authorities, in connection to their individual proceedings;
- insurance companies, when authorised by the patient.

Furthermore, according to art. 26(4) Act on Rights of Patients HRs may be disclosed to an institution of higher education or a research institute for scientific purposes, without however disclosing any relevant personal data.

Any other uses than established by the two provisions of the Act on Rights of Patients would be tantamount to illegal processing of sensitive personal data, which can trigger sanctions established in art. 51(1) Act on the Protection of Personal Data. According to it, whoever – as an administrator of a filing system or one obliged to protect personal data – discloses the data or gives an access thereto to unauthorised individuals - is subject to a fine, partial or outright imprisonment for a period of up to 2 years (or 1 year for unintentional actions).

Pursuant to art. 29 Act on Rights of Patients medical records should be stored for a period of 20 years since the end of the year of the last insert, except for:

1. HRs about a patient demised due to an injury or a poisoning, in which case the archiving duration is extended to 30 years;
2. X-ray pictures kept outside HRs of the patient, archived for 10 years;
3. laboratory orders, archived for 5 years;
4. HRs of children to 2 years old, archived for 22 years.

After the archiving periods the healthcare providers keeping the HRs are obliged to anonymise the HRs.

2.6.1. Main findings

The list of secondary uses for which HRs may be processed is relatively long, which should be rather obvious considering that HRs play a role in contexts other than individual treatments. The fact that for many of the uses personal data may be disclosed as well is justifiable by the goal of avoiding financial fraud, in turn stemming from the fact that medical treatment is primarily funded from public resources. On the other hand, the institutions with an access to HR data for secondary uses are not authorised to process the records for purposes other than established by the applicable legislation. Individuals doing otherwise face penal sanctions provided for in the general data protection legislation.

Archiving durations are unambiguously determined by the Act on Rights of Patients.

2.6.2. Table on secondary uses and archiving durations

Questions	Legal reference	Detailed description
Are there specific national rules on the archiving durations of EHRs?	Art. 29 Act on Rights of Patients	Medical records should be stored for a period of 20 years since the end of the year of the last insert, except for: 1. HRs about a patient demised due to an injury or a poisoning, in which case the archiving duration is extended to 30 years; 2. X-ray pictures kept outside HRs of the patient, archived for 10 years; 3. laboratory orders, archived for 5 years; 4. HRs of children to 2 years old, archived for 22 years.
Are there different archiving rules for different providers and institutions?		No, but there are different archiving durations for different types of HRs.
Is there an obligation to destroy (…) data at the end of the archiving duration or in case of closure of the EHR?	Art. 29 Act on Rights of Patients	After the archiving periods healthcare providers keeping the HRs are obliged to anonymise the HRs.
Are there any other rules about the use of data at the end of the archiving duration or in case of closure of the EHR?		n/a
Can health data be used for secondary purpose (e.g. epidemiological studies, national statistics...)?	Art. 26 Act on Rights of Patients	HRs are available for a set of secondary users, the most important among which are: - public authorities, the NFZ, vocational associations (compulsory organisations) of medical professionals, as well as to certain other advisory and auditing bodies, as far as revealing HRs is necessary for fulfilling their tasks, referring in particular to control and oversight; - the minister in charge of healthcare, courts, public prosecutors, medical consultants in court proceedings and agents of vocational responsibility, in connection to their individual proceedings; - separate institutions and bodies, if they have ordered a given examination; - pension authorities, in connection to their individual proceedings; - insurance companies, when authorised by the patient. Furthermore, HRs may be disclosed to an institution of higher education or a research institute for scientific purposes, without however disclosing any relevant personal data.
Are there health data that cannot be used for secondary use?		n/a

Questions	Legal reference	Detailed description
Are there specific rules for the secondary use of health data (e.g. no name mentioned, certain health data that cannot be used)?	Art. 26 Act on Rights of Patients	Disclosure to an institution of higher education or a research institute for scientific purposes (no personal data may be disclosed).
Does the law say who will be entitled to use and access this data?	Art. 26 Act on Rights of Patients	Educational and research institutions.
Is there an opt-in/opt-out system for the secondary uses of eHealth data included in EHRs?	Art. 35 Act on the System of Information in Healthcare	Patients may refuse access to individual medical data stored in the payment and statistical module of the SIM. This objection may, however, be overcome in a number of cases (e.g. for purposes of improving access to medical treatments and its equality, of financial management, etc.).

2.7. Requirements on interoperability of EHRs

The issue is discussed in Sections 1 and 2.4, in the context of general requirements for the HIS and requirements for the systems storing EHRs.

2.7.1. Main findings

As a basic principle, until the SIM system is up and running, it is up to healthcare providers keeping EHRs whether they wish to make their EHR systems interoperable. Subsequently they are obliged to use formats and standards allowing for the interoperability of their systems.

As further discussed in Sec. 2.4, while the Ordinance on health records sets general requirements of interoperability, the Ordinance on requirements for the HIS defines specific standards to be implemented by the providers when they use the SIM.

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?	Act on the System of Information in Healthcare	The obligation will come into force when the SIM is up and running
Are there any specific rules/standards on the interoperability of EHR?	Ordinance on requirements for the HIS	Ordinance on requirements for the HIS provides detailed rules on more technical aspects related to the exchange of medical information through the SIM. First, EHRs should be exchanged as XML files or multimedia files, with their logical structure further determined by the administrator of the SIM system (§ 3). The exchange of data should be compliant with the XML/XSD format and the DICOM format (§ 4(3)). EHRs may be disclosed after the user is identified either with a qualified certificate or the so-called "trusted profile" provided by the Electronic Platform of Public Administration Services (ePUAP) (§ 4(1)). According to the same Ordinance, accessing the EHRs via the SIM consists of the following steps (§ 5): 1. sending a request for EHRs by the recipient and receiving it by the SIM; 2. verifying the recipient's authorisation by the administrator of the SIM; 3. in case the verification is positive: transmitting the request to the provider originating the EHRs; 4. preparing the communication to be transmitted by a medical employee of the provider; 5. signing the communication by the medical employee of the provider either with a secure electronic signature verified with a qualified certificate, or with a signature verified with the so-called "trusted profile" of the ePUAP; 6. sending the EHRs by the provider and receiving it by the recipient; confirming the receipt of the EHRs by the recipient both in the SIM and the EHR system of the provider.
Does the law consider or refer to interoperability issues with other Member States systems?		n/a

2.8. Links between EHRs and ePrescriptions

The issue is irrelevant in Poland, as e-prescriptions are precluded by requirements of a sub-legislative act determining the form and content of prescriptions: the Ordinance of the Minister of Healthcare of 8 March 2012 on medical prescriptions.[12] According to its § 2(1), the issuance of a prescription consists of :

- writing legibly and durably, on the face side of the prescription, the information required by the Ordinance;
- placing a handwritten signature of the person issuing the prescription.

Furthermore, each alteration of the prescription's content requires a handwritten signature and a stamp of the person inserting the alteration (§ 2(1)).
These legal restraints have not been eliminated so far, despite one of major goals of the Act on the System of Information in Healthcare was to allow for interoperability of EHRs and for issuing e-Prescriptions. The Ministry of Health now intends to amend the abovementioned Ordinance and thus to eliminate barriers both to EHRs and e-Prescriptions.

2.8.1. Main findings

E-prescriptions have been precluded in Poland by a sub-legislative act requiring that prescriptions be signed with a handwritten signature. E-prescriptions are scheduled to replace paper ones in 2016, when the SIM allows for their interoperability with EHRs available through the SIM.

[12] Pol. *rozporządzenie Ministra Zdrowia z dnia 8 marca 2012 r. w sprawie recept lekarskich*, Dz.U. 2012, poz. 260, with further amendments.

2.8.2. Table on the links between EHRs and ePrescriptions

- ***Infrastructure***

Questions	Legal reference	Detailed description
Is the existence of EHR a precondition for the ePrescription system?		The issue is irrelevant in Poland so far, as e-prescriptions are precluded by requirements of a sub-legislative act determining the form and content of prescriptions: the Ordinance of the Minister of Healthcare of 8 March 2012 on medical prescriptions. E-prescriptions are scheduled to replace paper ones in 2016, when the SIM allows for their interoperability with EHRs available through the SIM.
Can an ePrescription be prescribed to a patient who does not have an EHR?		The issue is irrelevant in Poland so far, as e-prescriptions are precluded by requirements of a sub-legislative act determining the form and content of prescriptions: the Ordinance of the Minister of Healthcare of 8 March 2012 on medical prescriptions. E-prescriptions are scheduled to replace paper ones in 2016, when the SIM allows for their interoperability with EHRs available through the SIM.

- ***Access***

Questions	Legal reference	Detailed description
Do the doctors, hospital doctors, dentists and pharmacists writing the ePrescription have access to the EHR of the patient?		The issue is irrelevant in Poland so far, as e-prescriptions are precluded by requirements of a sub-legislative act determining the form and content of prescriptions: the Ordinance of the Minister of Healthcare of 8 March 2012 on medical prescriptions. E-prescriptions are scheduled to replace paper ones in 2016, when the SIM allows for their interoperability with EHRs available through the SIM.
Can those health professionals write ePrescriptions without having access to EHRs?		The issue is irrelevant in Poland so far, as e-prescriptions are precluded by requirements of a sub-legislative act determining the form and content of prescriptions: the Ordinance of the Minister of Healthcare of 8 March 2012 on medical prescriptions. E-prescriptions are scheduled to replace paper ones in 2016, when the SIM allows for their interoperability with EHRs available through the SIM.

2.9. Other requirements

One additional important future requirement concerns the use of so called "Cards of Healthcare Insurance". Those cards, according to art. 49 Act of 27 August 2004 on healthcare financed from public resources[13], have a double function of, first, acknowledging the insured person's right to healthcare treatment and, second, allowing for an acknowledgement that an individual treatment has been completed. The latter function has not been practically possible so far, as necessary accompanying elements (cards of medical professionals in particular) have not been implemented so far. The Amendment Principles define necessary legal adaptations required to establish the infrastructure. Ultimately, however, the process will predominantly depend on whether the underlying IT system (SIM) is technologically capable of providing sufficient technological capacity. This is particularly important, considering that the number of people with public insurance exceeds 35 million in Poland.

[13] Ustawa z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych, Dz. U. z 2008 r. Nr 164, poz. 1027, with further amendments.

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

Legal barriers for the deployment of EHRs are neither persistent not difficult to remove in Poland (the process of removing the barriers is ongoing and unendangered, as it involves no controversies). Instead, difficulties stem primarily from other three factors:

1) financial limitations;
2) the level of awareness and acceptance of the transition to EHRs, considering in particular its costs;
3) organisational and technological legacy issues: individual EHR systems (implemented either locally or regionally) have been developed within only general technological framework so far and hence are often incompatible.

Those findings have been corroborated during the interviews, especially No. 1 and 4.

It can also be further conjectured that advancements in cross-border transfer of EHRs within the EU can hardly be achieved through soft coordination based on dissemination of good practices in particular. Necessary interoperability will not be achieved unless relevant European projects (e.g. EU eHealth Governance Initiative, Translational Research and Patient Safety in Europe (TRANSFoRm) project, Advancing eHealth Interoperability (Antilope) project, or their future successors) are able to develop necessary technological standards and unless their implementation is secured by national authorities. Otherwise national authorities will pursue their technological solutions independently (as the Polish example corroborates).