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 the Netherlands

time.lex

milieu
Law & Policy Consulting

1 March 2014

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

This report was completed by Mrs Linda H.M. Eijpe. The views expressed herein are those of the consultant 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

1. Stage of development of EHRs in the Netherlands

In the Netherlands most medical records are updated electronically and are no longer available in paper. A 2013 Survey from the National IT Institute for Healthcare in the Netherlands ('NICTIZ') and the Netherlands Institute for Health Services Research ('NIVEL') shows that 93% of general practitioners and 66% of medical specialists update their records primarily or exclusively electronically.[1] There are several EHR solutions in place, for example the systems offered by ChipSoft, CSC-iSOFT and McKesson.[2]

There are also several systems in place for the electronic exchange of patient data inserted in EHRs. For example at the regional / local level there are systems that connect the information systems of general practitioners, GPs out-of-hours surgery and pharmacists (for example 'OZIS-ring'). There are also systems that connect data of medical specialists or other healthcare providers who are active in the same chain of care (for example for cancer or diabetes).

One of the current initiatives, launched by the Association of Healthcare providers for Health communication (Vereniging van Zorgaanbieders voor Zorgcommunicatie, (VZVZ)) is responsible for a system for the electronic exchange of medical data between healthcare providers. The exchange of medical data between the healthcare providers takes place via a National Switch Point (LSP) which provides a reference index for routing, identification, authentication, authorization and logging. The LSP can be compared to a traffic-control tower which regulates the exchange of patient data between the healthcare providers. At this moment LSP mainly connects general practitioners, GPs out-of-hours surgery, pharmacists and a few hospitals. In January 2014 a spokesman of the VZVZ said that 75% of the general practitioners and 83% of the pharmacists are connected to the LSP.[3] This system has the potential to be a nationwide system, but at the moment it is not. Besides this it should be clear and stated that the gouvernement is not involved in this system.

Legal Framework

The Netherlands rely on general health and data protection law laid down, for example, in the Medical Treatment Contracts Act [*Wet geneeskundige behandelingsovereenkomst*] (WGBO) and the Personal Data Protection Act [*Wet bescherming persoonsgegevens*] (WBP). There are no specific laws/programmes/decisions/ or action plans to regulate EHRs. An analysis was made what additional rules were necessary and the conclusion was that only on a few subjects would need additional regulation. This led to *Proposal on patient's rights with regard to electronic data processing* and administrative regulation with regard to the electronic exchange of data between healthcare providers. For the electronic exchange of medical data, the following legislation is relevant:

Code of Conduct Electronic Data Exchange in Health care (Gedragscode EGiZ)
This is a form of self-regulation by several umbrella health care organisations. The *Gedragscode EGiZ* applies to information systems that are used for exchanging personal data between healthcare providers. It lays down requirements specific to the WBP as well as technical requirements with regard to (i) the rights of the data subject, (ii) informed consent, (iii) authorization of healthcare providers and patients with regard to health data and (iv) information security and logging. This code of conduct is not legally binding. However, supervisory authorities refer to these documents when executing their supervisory responsibilities.

[1] Ehealth monitor 2013, Summary, Nictiz and Nivel, p. 15 and 16.
[2] Interview with Mr J. Krijgsman
[3] Aanmelding LSP groeit fors, Zorgvisie, 23 januari 2014, http://www.zorgvisie.nl/Home/Dossiers/EPD--LSP/

Proposal on patient's rights with regard to electronic data processing (Proposal Patient's rights)[4]

On 4 January 2013, the Minister of Health, Welfare and Sport introduced the Proposal Patient's Rights. This proposal aims at giving clients more rights when electronic records are compiled, when healthcare providers exchange data and when data is requested. The proposal applies to the use of 'electronic exchange systems', i.e. systems which enable healthcare providers to consult records, parts of records or information from records from other healthcare providers, using electronic means. In order to avoid doubt, the proposal does not apply to internal systems used by a healthcare provider to keep an EHR up-to-date.

NEN Standards
NEN standards are issued by the Netherlands Standardization Institute (NEN) and contain voluntary agreements made by market parties on the quality and safety of their products, services and processes. The following NEN standards are important: NEN 7510, NEN 7512, NEN 7513 and NEN7521 (The NEN 7521 is still under development and is not expected to be finalised until end 2014). The NEN 7510 is largely an elaboration of the ISO 27001/ISO 27002 and the European standard SEN 27799.

In November 2013, the Dutch Ministry of Health, Welfare and Sport issued a General administrative regulation with regard to the electronic exchange of data between healthcare providers (*Besluit elektronische gegevensuitwisseling tussen zorgaanbieders*[5]). This general administrative regulation is supplementary to the Personal Data Protection Act and the Proposal on Patient's rights. It lays down functional, technical and organisational measures with respect to the electronic exchange of health data and it explicitly prescribes that the electronic exchange systems[6], the network connections[7], and the logging of the system[8] must comply with NEN 7510, NEN 7512 and NEN 7513.

Institutional setting

There are mainly two supervisory authorities responsible for data processing in EHRs and the exchange of information between EHRs: the Dutch Data Protection Authority (*College bescherming persoonsgegevens* (CBP) is responsible for enforcing privacy regulations, while the Dutch Healthcare Inspectorate (*Inspectie voor de Gezondheidszorg* (IGZ) primarily enforces quality standards for the provision of healthcare.

2. Summary of legal requirements applying to EHRs

Content of EHR's
There is no specific legislation with respect to the type of data that must or may be included in an EHR because the rules can be found in the Medical Treatment Contracts Act (WGBO), the Data Protection Act (WBP) and the Proposal on patient's rights with regard to electronic data processing *(Proposal Patient's rights)*[9]. The exact meaning and the specific details of these general rules are left to code of conducts or guideline of the healthcare organisations. For example guidelines of the Dutch College of General Practitioners (*Nederlandse Huisartsen Genootschap*) (NHG).

[4] Tweede Kamer, Vergaderjaar 2012-2013, Kamerstuk 33509
https://zoek.officielebekendmakingen.nl/dossier/33509/kst-33509-1?resultIndex=30&sorttype=1&sortorder=4
[5] General administrative regulation with regard to additional rules for functional, technical and organisational measures with respect to the electronic exchange of data between healthcare providers (hereafter: 'Besluit elektronische gegevensuitwisseling tussen zorgaanbieders')
Tweede Kamer, Vergaderjaar 2013-2014, Bijlage bij Kamerstuk 33509 nr. 7.
https://zoek.officielebekendmakingen.nl/blg-264784.html
[6] Article 3 of the Besluit elektronische gegevensuitwisseling tussen zorgaanbieders
[7] Article 5 of the Besluit elektronische gegevensuitwisseling tussen zorgaanbieders
[8] Article 7 of the Besluit elektronische gegevensuitwisseling tussen zorgaanbieders
[9] Tweede Kamer, Vergaderjaar 2012-2013, Kamerstuk 33509
https://zoek.officielebekendmakingen.nl/dossier/33509/kst-33509-1?resultIndex=30&sorttype=1&sortorder=4

Requirements on the institution hosting EHR's

There is no specific legislation with respect to the requirements on institutions hosting EHR data. However the general rules and obligations laid down in the Data Protection Act (WBP) are relevant in this respect. For example the obligations laid down in article 13 and 14 of the WBP. If the hosting institution acts as a processor of personal data the responsible party (healthcare provider) has to make sure that this hosting institution implements appropriate technical and organizational measures to secure all personal data against loss or any form of unlawful processing.

Consent

The Medical Treatment Contracts Act (WGBO) makes it mandatory for healthcare professionals to keep a medical record (whether electronically or on paper). The WGBO does not require the patient's explicit consent for this. Access to or copies of documents from the record may only be provided to the patient himself and to third parties with the patient's consent, but this does not apply to the parties who are immediately involved in the execution of the treatment contract and the party who acts as a deputy of the healthcare professional, insofar as the disclosure is necessary for the work that is to be done by those parties within that context.

The Code of Conduct Electronic Data Exchange in Health care *(Gedragscode EGiZ)* determines how patients should be informed and how consent can be obtained. This depends on the method used for the exchange of data. In this context, the Code of Conduct makes a distinction between 'pull traffic' and 'push traffic'[10]. The patient must explicitly grant his or her consent in advance for data processing, i.e. for the disclosure of patient data in case of pull traffic. In case of push traffic, prior consent is not required, although the patient may object to his data being exchanged.

The Proposal on patient's rights with regard to electronic data processing *(Proposal Patient's rights)* also stipulates that the healthcare provider may only exchange patient data via the electronic exchange system if it has determined that the patient has given its consent to do so.[11]

Creation, access to and update

Pursuant to the Code of Conduct Electronic Data Exchange in Health care *(Gedragscode EGiZ)* the party responsible for the electronic exchange system has to (i) adopt an 'authorisation policy'[12], (ii) take measures in order to avoid access of the personal / health data by third parties which do not have a medical treatment relationship with the data subject,[13] (iii) introduce a logging system[14] and (iv) take technical measures to limit the access to all personal / health data. On request, the patient has the right to access or copy all his/her personal and health data, which the healthcare provider makes available through an electronic exchange system, in an electronic way.[15]

The Proposal on patient's rights with regard to electronic data processing *(Proposal Patient's rights)* also stipulates that medical data, available via the electronic exchange system, may only be accessed after prior consent of the client. This consent is not necessary if the access takes place by a healthcare provider who is directly involved in the treatment of the patient and who replaces the healthcare provider who made the medical data.[16]

The NEN standards (NEN 7510, NEN 7512, NEN 7513 and NEN 7521) provide requirements with regard to authorization, exchange of patient data, consent protocols, information security and logging.

[10] See paragraph 2.3.1 for a definition of 'pull traffic 'and 'push traffic'.
[11] Proposal Patient's Rights, Article I, paragraph D, article 23a sub a. and Article II, paragraph B, article 15a sub 1.
[12] Article 6 of the Gedragscode EGiZ
[13] Article 7 of the Gedragscode EGiZ
[14] Article 8 of the Gedragscode EGiZ
[15] Proposal Patient's Rights, Article I, Paragraph D, Article 23c sub 1 and Article II, Paragraph B, Article 15d sub 1
[16] Proposal Patient's Rights, Article II, Paragraph B, Article 15b sub 2

Security
Pursuant to the Regulation on the Use of the Citizen Service Number in Health Care ('*Regeling BSN in de zorg*') and several reports of the Dutch Data Protection Authority (*College Bescherming Persoonsgegevens)*[17], the processing of health data and the use of Citizen Service Number must comply with the NEN 7510 standard of the Netherlands Standardization Institute[18]. Furthermore, the General administrative regulation with regard to the electronic exchange of data between healthcare providers (*Besluit elektronische gegevensuitwisseling tussen zorgaanbieders*) lays down functional, technical and organisational measures with respect to the electronic exchange of health data and it explicitly prescribes that the electronic exchange systems[19], the network connections[20], and the logging of the system[21] must comply with the NEN 7510, NEN 7512 respectively NEN 7513.

Liability
Medical professionals may be held liable for professional errors, including errors in an EHRs, under Civil Law, Criminal Law and Disciplinary Rules. The general regulation of respectively, Civil Law, Criminal law and Disciplinary Rules apply in cases of professional error, including errors in EPDEHR's. There are is no specific regulations with respect to liability for the use or errors of the EHR.

Secondary uses and archiving durations
Pursuant to the Medical Treatment Contracts Act (WGBO), medical files must be kept for a period of fifteen years after they have been created, or as long as is necessary for the treatment by a good healthcare professional. This provision is applicable to both physical and digital medical files. There are no specific legal obligations to destroy data in EHRs at the end of the archiving duration.

Interoperability of EHR's
There are no legal requirements regarding the interoperability of national EHRs with other Member States' EHR systems.

Links between EHR and ePrescription
Pursuant to article 67 of the Medicines Act (*Geneesmiddelenwet*) is forbidden to prescribe medications over the Internet to persons whom the prescribing physician has never met in person, who the prescriber does not know or from who the prescriber does not have a medical history available.

The definition of "prescription" (Dutch: *recept)* in the Medicines Act *(Geneesmiddelenwet*) takes account of prescriptions by means of electronic information carriers. It is required that the prescription is secured in such a way that the prescribing physician (issuing the prescription) will be recognised on the basis of agreements made with the intended receiving party (pharmacist) as the party with whom such agreements have been made. The document may be signed using an electronic signature. A new aspect of this is that the prescribing physician indicates on the prescription a unique identification of the patient, i.e. distinguishing the patient from other patients in such a way that no confusion is possible.

Furthermore, the KNMG Guideline on electronic prescriptions (*KNMG Richtlijn Elektronisch voorschrijven*) entered into force on 1 January 2014. The guideline requires prescribers to use an electronic prescription system that provides possibilities to monitor unsafe situations and meet requirements with regard to (1) their functionality and (2) the exchange of information between

[17] Access to digital patient files within care institutions (*Toegang tot digitale patiëntdossiers binnen zorginstellingen*), survey of CBP of June 2013
[18] See for example:
http://www.nen.nl/NEN-Shop/Norm/NEN-75102011-nl.htm?gclid=CLWgj5HNqb4CFYXItAodDU0AAA
[19] Article 3 of the Besluit elektronische gegevensuitwisseling tussen zorgaanbieders
[20] Article 5 of the Besluit elektronische gegevensuitwisseling tussen zorgaanbieders
[21] Article 7 of the Besluit elektronische gegevensuitwisseling tussen zorgaanbieders

healthcare providers. Also, electronic prescription systems should allow for the copying of data from other automated systems or for the manual registration of data.

3. Good practises and legal barriers

Good practices
In the Netherlands there are several EHR solutions in place, for example the systems offered by ChipSoft, CSC-iSOFT and McKesson.[22]There are also several systems in place for the electronic exchange of patient data inserted in EHRs. At regional/local level there are systems that connect the information systems of general practitioners, GPs out-of-hours surgery and pharmacists (for example 'OZIS-ring'). There are also systems that connect medical specialists or other healthcare providers who are active in the same chain of care (for example the chain of care with respect to cancer or diabetes).

Finally, there is a nationwide system for the electronic exchange of medical data between healthcare providers. This system is based on a National Switch Point (LSP). The exchange of medical data between the healthcare providers takes place via this LSP.

Legal barriers
Stakeholders mainly observe (legal) barriers in the situation that the EHRs are being used for the electronic exchange of health / personal data. These barriers for example are related to (i) the lack of uniform (technical) standards and language, (ii) the strict security measures laid down in the NEN standards, (iii) questions with respect to interpretation of the legislation, (iv) concerns of healthcare providers with respect to liability, and (v) the rules with respect to the verification of healthcare providers and the obstacles in the practise to comply with such rules.[23]

[22] Interview with Mr J. Krijgsman
[23] Interview with stakeholders

Contents

List of abbreviations

Besluit elektronische gegevensuitwisseling tussen zorgaanbieders	General administrative regulation with regard to the electronic exchange of data between healthcare providers
CBP	The Dutch Data Protection Authority (*College Bescherming Persoonsgegevens*)
EHRs	Electronic Health Records
Gedragscode EGiZ	Code of Conduct Electronic Data Exchange in Healthcare
GmW	Medicines Act (*Geneesmiddelenwet*) *IGZ* The Dutch Healthcare Inspectorate (*Inspectie voor de Gezondheidszorg*)
LSP	National Switch Point
NEN	Netherlands Standardization Institute
NHG	The Dutch College of General Practitioners (*Nederlandse Huisartsen Genootschap)*
KNMG	Royal Dutch Medical Association (*Koninklijke Nederlandsche Maatschappij tot bevordering der Geneeskun*st)
Proposal Patient's Rights	The proposal on patient's rights with regard to electronic data processing
Regeling BSN in de zorg	Regulation on the Use of the Citizen Service Number in Health Care
Wet BIG	Individual Health Care Act
Wet publieke gezondheid	Public Health Act
WBP	Personal Data Protection Act (*Wet Bescherming Persoonsgegevens*)
WGBO	Medical Treatment Contracts Act (*Wet geneeskundige behandelingsovereenkomst*)
Wgbsn-z	Act on the Use of the Citizen Service Number in Health Care (*Wet gebruik burgerservicenummer in de zorg*)

1. General context

1.1. EHR systems in place

In the Netherlands, most of the medical records are updated electronically and are no longer available in paper. A Survey from the National IT Institute for Healthcare in the Netherlands ('NICTIZ') and the Netherlands Institute for Health Services Research ('NIVEL') shows that 93% of general practitioners and 66% of medical specialists update their records primarily or exclusively electronically. There are several EHR solutions in place, for example the systems offered by ChipSoft, CSC-iSOFT and McKesson.[24]

A significant proportion of general practitioners (48%) and medical specialists (42%) are interested in having further options available, such as the ability to correspond with other healthcare providers.[25] Furthermore, many doctors exchange patient data electronically. Nearly all (83 – 90 %) of the general practitioners (GPs) exchange patient data electronically with public pharmacies, emergency general practitioner services and hospitals. Almost half (46%) of medical specialists exchange patient data electronically with general practitioners.[26]

There are also several systems in place for the electronic exchange of patient data inserted in EHRs. For example on local/regional level there are systems that connect the information systems of general practitioners, GPs out-of-hours surgery and pharmacists (for example 'OZIS-ring') who work together in a certain region. Other regional solutions are, for example:

- Zorgdomein (a solution for the exchange of patient data between general practitioners and hospitals in case the general practitioner refers the patient for further examination to a specialist in the hospital);
- POINT (a solution for the exchange of information between the hospitals and the institutions for care and homecare in the event that a patient leaves the hospital and has to be treated at home or in a nursing home); and
- EDIFACT (a solution for the exchange of patient data between general practitioners, hospitals and pharmacists that is used for the exchange of prescriptions and results of the laboratories).[27]

There are also systems which connect medical specialists or other healthcare providers who are active in the same chain of care (for example for cancer or diabetes). These systems will not be accessible for healthcare providers who are active outside the region (as defined by the involved parties) or outside the chain or specialism.

National Switch Point (LSP)
The Dutch Ministry of Health, Welfare and Sport worked with several stakeholders in the health care sector to build a nationwide system for the safe and reliable electronic exchange of medical data between healthcare providers. Since 2011, the exchange of medical data between healthcare providers can take place via a National Switch Point (LSP) which provides a reference index for routing, identification, authentication, authorization and logging. The LSP can be compared to a traffic-control tower which regulates the exchange of patient data between healthcare providers. Authorized care providers can consult these data to obtain a clear picture of a patient's medical history or medication use.

The Association of Healthcare providers for Health communication (*Vereniging van Zorgaanbieders voor Zorgcommunicatie* (VZVZ)) is since 2012 responsible for the LSP. The Dutch government is not

[24] Interview with Mr J. Krijgsman
[25] Ehealth monitor 2013, Summary, Nictiz and Nivel, p. 15 and 16.
[26] Ehealth monitor 2013, Summary, Nictiz and Nivel, p. 16.
[27] Interview with Mr. D Ormel

involved anymore. Healthcare providers have the freedom whether or not to connect their healthcare information systems to LSP. At this moment LSP mainly connects general practitioners, GPs out-of-hours surgery, pharmacists and a few hospitals (75% - 80% of the general practitioners and 83% of the pharmacists are connected to the LSP).[28] This high percentage is mainly caused by the fact that the health insurance companies gave a subsidy to the general practitioners and pharmacists for the connection. Nevertheless, the connection of these healthcare providers does not actually mean that they really use the LSP, since there are quite a few barriers, such as:[29]

- Only a few patients have given their consent for the exchange of their health data through the LSP and by lack of any useful patient data the LSP is not very useful for the healthcare providers.
- In order to access and use the LSP, a healthcare provider has to own and use an UZI Card[30]. Healthcare providers initially were of the opinion that the card was too expensive, the procedure to order the card too difficult and the use of the card not efficient. The price of the Card has recently been lowered to 255 EURO for three years.
- The information systems of the healthcare providers which have to be connected to the LSP do not comply with all imposed standards and requirements.

As above, in order to access and use the LSP, a healthcare provider has to own and use an UZI Card. Only professional practitioners who are registered in conformance with the so-called BIG registration (as set out in article 3 or article 34 of the Individual Health Care Act (*Wet BIG*)[31] are entitled to receive and use an UZI Card, meaning: doctors, dentists, pharmacists, healthcare psychologists, psychotherapists, midwifes and nurses. At this moment an increasing number of healthcare providers and pharmacists use the UZI Card. In order to have access to the LSP a healthcare provider based outside the Netherlands need to be registered in the BIG-registration and need to have a UZI-card in order to able to access the LSP.

1.2. Institutional setting

There are mainly two supervisory authorities responsible for data processing in EHRs and the exchange of information between EHRs: the Dutch Data Protection Authority (*College bescherming persoonsgegevens)* (CBP) is responsible for enforcing privacy regulations, while the Netherlands Healthcare Inspectorate (*Inspectie voor de Gezondheidszorg*) (IGZ) primarily enforces quality standards for the provision of healthcare.

The CBP

The CBP monitors the observance and application of the Personal Data Protection Act (*Wet bescherming persoonsgegevens*, WBP) and a number of other laws that regulate the use of personal information.

The CBP is authorised to, either on its own initiative or at the request of an affected party, start an inquiry into the way in which personal information is processed. The responsible party, to whom the inquiry is directed, is obliged to allow the inspection of data and systems insofar as it is necessary. Within the context of its supervision, the CBP may request to inspect the data processing of healthcare providers, of the administrator of an EHR and of ICT service companies. Consequently, the responsible party may not invoke its obligation of secrecy in response to the CBP's request.

[28] Aanmelding LSP groeit fors, Zorgvisie, 23 januari 2014, http://www.zorgvisie.nl/Home/Dossiers/EPD--LSP/ and Interview with Mr. A. Jaoenathmisier

[29] Interview with Mr. A. Jaoenathmisier

[30] With the help of an UZI card, healthcare providers can provide authentication, meaning they can prove their identity. The UZI card certifies that the pass holder is a healthcare provider and indicates whether he or she provides treatment on behalf of a healthcare institution.

[31] Individual Health Care Act (Wet op de beroepen in de individuele gezondheidszorg) http://wetten.overheid.nl/BWBR0006251/geldigheidsdatum_14-05-2014

If a party fails to comply with the aforementioned regulations, the CBP is authorised to impose an order subject to a penalty or to enforce an administrative order. Imposing an order subject to a penalty means that a command ('order') to comply with a statutory obligation is issued to the offender. If the order is not executed on time, a penalty becomes due. An order subject to a penalty is intended to reverse a violation of a regulation or to prevent more violations. An administrative order – in short – applies to cases in which the CBP actually takes measures against actions in breach of the law or failures to observe the law.

The IGZ

The IGZ enforces the regulations pertaining to the quality of the provision of healthcare. The IGZ supervises the use of EHRs and other systems for information exchange pursuant to laws such as the Care Institutions Quality Act (*Kwaliteitswet zorginstellingen)* (KWZi) and the Individual Healthcare Professions Act (*Wet op de beroepen in de individuele gezondheidszorg*) (Wet BIG).

Healthcare providers are obliged to disclose all information and data – including personal medical information – necessary for monitoring the use of the citizen service number to enable the IGZ to carry out its task. Besides inspection of patient records, this includes inspection of things like central and local log data. In addition, the IGZ has a statutory right to inspect patient records.

The IGZ has the competence to take corrective measures such as remedial and punitive sanctions, which means that the IGZ may take measures such as imposing fines on healthcare providers that fail in their healthcare provision. Furthermore, the IGZ, like the CBP, has the option of imposing an order subject to a penalty.

1.3. Legal setting and future legal development

The Netherlands rely on general health and data protection legislation. There are no specific laws/programmes/decisions/ or action plans to regulate EHRs and ePrescriptions. For the purposes of this study, the following legislation is relevant:

- Medical Treatment Contracts Act [*Wet geneeskundige behandelingsovereenkomst*] (WGBO)

The WGBO applies to the provision of care by healthcare providers as defined in the WGBO, which are both individual professionals and care institutions. The WGBO sets out requirements, among other things, on (i) professional confidentiality, (ii) the duty to maintain and save medical records and (iii) patients' rights.

The WGBO requires healthcare providers to keep a medical file with regard to the treatment of the patient (art. 454 lid 1 WGBO). The medical file must contain notes regarding the health of the patient and the medical proceedings as well as documents containing such data, to the extent necessary for the treatment of the patient. The obligation to keep a medical file can be met by means of a paper file or a digital file. The WGBO does not make any distinction in this regard.

- Data Protection Act [*Wet bescherming persoonsgegevens*] (WBP)

The most important rules for processing personal data have been set forth in the WBP. This act implements the provisions of the European Directive 95/46/EC. Generally speaking the WBP is very similar to the European directive. The WBP limits the processing of personal data concerning a person's health and stipulates that responsible parties must implement appropriate technical and organizational measures to secure all personal data against loss or any form of unlawful processing

- Act on the Use of the Citizen Service Number in Health Care [*Wet gebruik burgerservicenummer in de zorg*] (Wgbsn-z)

The Wgbsn-z requires healthcare providers to use the Citizen Service Number (BSN) of the individual concerned and to establish the client's BSN when processing personal data in providing care. This requirement applies to all care provided in the Netherlands. The Wgbsn-z sets out certain requirements

that healthcare providers must comply with when processing BSN, such as identification of the patient and security measures.

- Regulation on the Use of the Citizen Service Number in Health Care [*Regeling gebruik burgerservicenummer in de zorg*]

Under this regulation the processing of the BSN by healthcare providers must comply with NEN 7510.

- Medicines Act [*Geneesmiddelenwet*] (Gmw)

The Gmw prohibits the online prescription of medicinal products to persons who the prescriber has not personally met, or who the prescriber does not know of or of whom the prescriber does not have a medication history available. The Gmw also requires explicit consent of the individual concerned for the electronic application, consultation and storing of laboratory results. It furthermore follows from the Gmw that electronic prescriptions must be provided with an electronic signature.

- Public Health Act [*Wet publieke gezondheid*]

When recording patient data in the context of youth health care, the municipal executive must use digital data storage.

Future legislation

- Proposal on Patient's Rights with regard to electronic data processing [*Wetsvoorstel cliëntenrechten bij elektronische verwerking van gegevens*](Proposal Patient's Rights)

The proposal was introduced by the Minister of Health, Welfare and Sport on 4 January 2013 and aims at giving patients more rights when electronic records are compiled, when healthcare providers exchange data and when data is requested.

The proposal applies to the use of 'electronic exchange systems in general (i.e. al kind of systems that enable healthcare providers to allow other healthcare providers to consult records, parts of records or information from records, using electronic means, not including a system used by a healthcare provider to keep an electronic record up-to-date).

The proposal introduces, among other things:

- definitions of the terms 'record', 'electronic exchange system', 'treatment relationship' and 'healthcare professional';
- the healthcare provider's obligation to only disclose the client's details by means of an electronic exchange system insofar as the client has explicitly granted consent;
- the client's right to grant, at the client's discretion, general consent for all healthcare providers connected to the electronic exchange system, or specified consent to disclose all or specific information to a certain healthcare provider or categories of healthcare providers to be specified by the client;
- the condition that explicit consent for consulting information or making a copy of it has been granted by the client within the context of the treatment relationship in question;
- the disclosure of information by the healthcare provider to the client about the client's rights in the event of electronic information exchange and how the client can exercise those rights;
- offering the client inspection, by electronic means or by means of a copy of the records and/or of the client information that have been disclosed;
- a right of the data subject to request access to log data;
- an access injunction of the electronic exchange systems against healthcare insurance companies, company medical doctors, insurance companies' medical advisors and medical examiners.

Codes of Conduct and Guidelines

A number of codes of conduct, guide and guidelines are applicable to the use of EHRs. These documents are not legally binding. However, supervisory authorities refer to these documents when executing their supervisory responsibilities.

- Code of Conduct Electronic Data Exchange in Health care (*Gedragscode EGiZ*)

This is a form of self-regulation by several umbrella health care organizations. The *Gedragscode EGiZ* applies to information systems that are used for exchanging personal data between healthcare providers. It lays down requirements specific to the Data Protection Act (WBP) as well as technical requirements with regard to (i) the rights of the data subject, (ii) informed consent, (iii) authorization of healthcare providers and patients with regard to health data and (iv) information security and logging. In short, the rights of the data subject are:

- right to information;
- right to give or withhold consent for the processing of health data or, where applicable, the right to object;
- right to access, correction and transcript of data;
- right of access to log records;
- right to erasure of data;
- right to be informed about abuse of data.

- Online Doctor Patient Contact Guideline (Royal Dutch Medical Association (KNMG) 2007)

This guideline addresses healthcare providers and regulates all online doctor – patient contacts in which doctors have indicated that they can be contacted online by patients and (i) provide patients with advice tailored to their specific situations or (ii) start (pharmaco)therapy or (iii) give out repeat prescriptions. It requires, among other things that (i) sufficient reliable and relevant information concerning the patient is available, (ii) the doctor takes reasonable measures to identify the patient, and (iii) the patient is informed about the circumstances in which online medical advice is given.

- NEN Standards

NEN standards are issued by the Netherlands Standardization Institute (NEN) and contain voluntary agreements made by market parties about the quality and safety of their products, services and processes.

a. NEN 7510: NEN 7510 is largely an elaboration of ISO 27001/ISO 27002 and the European standard SEN 27799. This standard lays down general guidelines and basic principles for determining, instituting and maintaining measures to be taken by health care organizations to safeguard the information supply. Any instance of data processing using the citizen service number must comply with NEN 7510. The IGZ and CBP use NEN 7510 as a framework for review.
b. NEN 7512: This standard lays down the minimum requirements for the safe exchange of data. This standard is directed specifically at electronic communication in health care. This means communication between healthcare providers and communication with patients, care insurers and other parties involved in health care.
c. NEN 7513: This standard provides for the systematic, automated registration of actions in electronic patient files (logging). This registration makes it possible to check whether access to the patient file is lawful. This standard is currently still in the design phase.
d. NEN 7521: This standard lays down authorisation protocols and consent profiles for access to and electronic inspection and exchange of patient data (notifications, images, files) between healthcare providers, care institutions and patients. This standard is still under development and is not expected to be finalised until end 2014.

2. Legal requirements applying to EHRs in the Netherlands

2.1. Health data to be included in EHRs

2.1.1. Main findings

There is no specific legislation with respect to the type of data that must or may be included in an EHR. However, some general rules with respect to medical records can be found in the Medical Treatment Contracts Act (WGBO), the Data Protection Act (WBP) and the Proposal on Patient's Rights with regard to electronic data processing (Proposal Patient's Rights).

Pursuant to article 454 WGBO, healthcare providers are obliged to keep medical records – whether electronically or on paper. In this medical record, the healthcare provider has to keep a record and notes with respect to the health of the patient, the treatments of the patient and other data and information necessary in respect of the provision of good care services to the patient. On request of the patient, the healthcare provider will add comments of the patient in the medical records as well.

Another general rule with respect to personal or medical records is laid down in article 11 WBP, stating that personal data shall only be processed where, given the purposes for which they are collected or subsequently processed, they are adequate, relevant and not excessive. As a consequence hereof, an EHR may not contain more personal data (including medical data) than necessary for the purpose of such EHR.

In accordance with article 11 WBP, the Proposal Patient's Rights limits the access and use of medical records through the electronic exchange system. The Proposal Patient's Rights explicitly stipulates that a healthcare provider who may have access to a medical record through the electronic exchange system only has permission to access personal and medical data necessary for the fulfilment of his obligations with respect to the treatment.[32]

The WGBO, WBP and Proposal Patient's Rights provide only general standards and basic principles. The meaning and the specific details of these general standards and principles are not laid down in legislation itself and are left to code of conducts or guidelines of the healthcare organizations. Examples are the guidelines of the Dutch College of General Practitioners ('NHG'):

1) The Guideline Adequate record administration with regard to the Electronic Patient Record [*de Richtlijn Adequate dossiervorming met het Elektronisch Patiënten Dossier* (ADEHR)]
   This guideline provides directions with respect to the methods of the documentation of relevant health data and information in the EHR. The purpose of this guideline is to ensure that all relevant patient data will be documented in an unambiguous and structured way in order to make data easily accessible and exchangeable between the healthcare providers.
2) The Guideline Exchange of information between General Practitioner and the GP out-of-hours surgery (*de Richtlijn gegevensuitwisseling huisarts en centrale huisartspost*)
   This second guideline provides directions with respect to the exchange of data in case of a substitution of GP out-of-hours surgery. For example it lays down the (kind of) patient/health data that should be inserted in the Professional Summary (*professionele samenvatting*) in the EHR.

An example of specific legislation can also be found in the Public Health Act [*Wet publieke gezondheid*]. This Act states, for example, that the municipal executive must use digital data storage when recording patient data in the context of youth health care.

[32] Proposal Patient Rights, Article II, Paragraph D, Article 15B

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?)		No
Are these data restricted to purely medical information (e.g. physical or mental health, well-being)?		No
Is there a definition of EHR or patient's summary provided in the national legislation?		However the Proposal Patient's Rights provides a definition of 'electronic exchange system': '*a system by means of which healthcare providers can send information from records to other healthcare providers linked to the system, by means of which healthcare providers can share information from records with each other, or by means of which a healthcare provider can gain access to a record or parts of a record of which it is the administrator, not including a system used by a healthcare provider as intended in part c, under 1°, for keeping an electronic record up-to-date*.'[33]
Are there any requirements on the content of EHRs (e.g. detailed requirements on specific health data or general reference to health data)?		No
Are there any specific rules on the use of a common terminology or coding system to identify diseases, disorders, symptoms and		However, there are some guidelines from the NHG to ensure that all relevant patient data will be documented in an unambiguous and structured way in order to make data easily accessible and exchangeable between the

[33] Proposal Patient's Rights, Article II paragraph A.

Questions	Legal reference	Detailed description
others?		healthcare providers and between the healthcare provider and the GP out-of-hours surgery.[34]
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)?		No
Are there any specific rules on identification of patients in EHRs?		There are no specific rules on the identification of patients in an EHR. However pursuant to the Wgbsn-z, healthcare providers are obliged to verify if a Citizen Service Number (BSN) belongs to a certain patient (for example with an identification document) and thereafter record and use the BSN in order to identify that patient. They must register this number in administration / records.
Is there is a specific identification number for eHealth purposes?		Wgbsn-z regulates the use of the BSN in the health care sector. See the information above.

[34] See the Guideline Adequate record administration with regard to the Electronic Patient Record [*de Richtlijn Adequate dossiervorming met het Elektronisch Patiënten Dossier*] and the Guideline Exchange of information between General Practitioner and the GP out-of-hours surgery (*de Richtlijn gegevensuitwisseling huisarts en centrale huisartspost*).

2.2. Requirements on the institution hosting EHRs data

2.2.1. Main findings

There is no specific legislation with respect to the requirement on institutions hosting EHR data. However the general rules and obligations laid down in de data Protection Act (WBP) are relevant in this respect. An important obligation is laid down in article 13 WBP. Pursuant to this article the responsible party (for example healthcare provider) must implement appropriate technical and organizational measures to secure all personal data against loss or any form of unlawful processing. These measures shall guarantee an appropriate level of security, taking into account the state of the art and the costs of implementation, and having regard to the risks associated with the processing and the nature of the data to be protected. These measures shall also aim at preventing unnecessary collection and further processing of personal data. If the responsible party (healthcare provider) appoints a third party (for example an institution hosting the EHR data) to process the personal data (for example the EHR) it needs to make sure that such party (the processor) provides adequate guarantees concerning the technical and organizational security measures for the processing of the personal data and the healthcare provider has to make sure that these measures are complied with (article 14 WBP).

Article 13 WBP provides only general standards and basic principles. The concrete meaning and details of the these standards and principals are not laid down in the WBP itself but can be found in the standards with respect to information security in the health sector issued by the Netherlands Standardisation Institute (NEN 7510, NEN 7512 en NEN 7513). See Chapter 1.3 above.

Pursuant to the Regulation on the Use of the Citizen Service Number in Health Care ('*Regeling BSN in de zorg*') and several reports of the Dutch Data Protection Authority (CBP)[35], the processing of health data and the use of Citizen Service Number (BSN) must comply with NEN 7510. The Citizen Service Number is used in the EHR's to identify the patients.

Furthermore, in November 2013 the Dutch Ministry of Health, Welfare and Sport issued a general administrative regulation with regard to the electronic exchange of data between healthcare providers ('*Besluit elektronische gegevensuitwisseling tussen zorgaanbieders*'). This general administrative regulation lays down functional, technical and organisational measures with respect to the electronic exchange of health data and it explicitly prescribes that the electronic exchange systems,[36] the network connections[37] and the logging of the system[38] must comply with the NEN standards (NEN 7510, NEN 7512 respectively NEN 7513). The date of entry into force is linked to the effective date of the Proposal Patient's Rights.

[35] *Toegang tot digitale patiëntdossiers binnen zorginstellingen,* survey of CBP of June 2013
[36] Article 3 of the Besluit elektronische gegevensuitwisseling tussen zorgaanbieders
[37] Article 5 of the Besluit elektronische gegevensuitwisseling tussen zorgaanbieders
[38] Article 7 of the Besluit elektronische gegevensuitwisseling tussen zorgaanbieders

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?		No
Is there a need for a specific authorisation or licence to host and process data from EHRs?		No
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)?		However, pursuant to 13 and 14 WBP an institution has to provide adequate guarantees concerning the technical and organizational security measures for the processing of the personal and health data. These measures should comply with the regulation laid down in the NEN 7510, NEN 7512 en NEN 7513 standardizations (see above).
In particular, is there any obligation to have the information included in EHRs encrypted?		No
Are there any specific auditing requirements for institutions hosting and processing EHRs?		No

2.3. Patient consent

2.3.1. Main findings

- Data Protection Act (WBP)

Pursuant to Section 16 of the WBP, the processing of personal data pertaining to a person's health is prohibited, save for a number of statutory exceptions. A general exception applies if data is processed with the explicit consent of the person involved (Section 23, paragraph 1(a) of the WBP).

Furthermore, the prohibition of processing personal information pertaining to a person's health does not apply if the processing is done by care providers, institutions or amenities for health care or social services insofar as it is necessary for the adequate treatment or care of the person involved or necessary for the administration of the institution or professional practice in question (Section 21, paragraph 1, under a of the WBP). Accordingly, the WBP does not require explicit consent for compiling an EHR.

- Medical Treatment Contracts Act (WGBO)

The WGBO makes it mandatory for healthcare professionals to keep a medical record (Section 454 of the WGBO, see § 1.3). The WGBO does not require the patient's explicit consent for this. Nonetheless, access to or copies of documents from the record may only be provided to the patient him/herself or third parties if with the patient's consent (Section 457, paragraph 1 of the WGBO), but this does not apply to the parties who are immediately involved in the execution of the treatment contract and the party who acts as a deputy of the healthcare professional, insofar as the disclosure is necessary for the work that is to be done by those parties within that context (Section 457, paragraph 2 of the WGBO).

- Code of Conduct Electronic Data Exchange in Health care (Gedragscode EGiZ)

The Gedragscode EGiZ further elaborates the current standards of the WBP and the WGBO for the exchange of information between healthcare providers and healthcare institutions. The Gedragscode EGiZ applies to every system that connects different institutions (or practices) to each other or by which means personal data can be shared or exchanged between healthcare providers. The Gedragscode EGiZ uses the term 'Electronic Exchange System' to describe such systems.

The Gedragscode EGiZ determines how patients should be informed and how consent can be obtained. This depends on the method used for the exchange of data. In this context, the Code of Conduct makes a distinction between 'pull traffic' and 'push traffic'.

The term 'pull traffic' is used if a healthcare provider discloses data from his medical file to a group of healthcare providers. In general, it is not usually clear in advance which particular healthcare providers will consult that data. The healthcare provider who needs the data for the treatment takes the initiative to consult the data. This healthcare provider is called the 'record consultor'. If pull traffic is involved, information about this type of data exchange must be given to the person in question personally or under the responsibility of the source record coordinator. Furthermore, the person in question must explicitly grant his or her consent in advance for the data processing, i.e. for the disclosure of patient data by the source record coordinator for consultation.

'Push traffic' involves the sending of personal data by the source record coordinator to one or several particular healthcare provider(s) who has (have) a treatment relationship with the person in question, or with whom a treatment relationship is intended. In that case, the party disclosing the data takes the initiative. The recipient healthcare provider will receive the data without having to take the initiative or without having to undertake any additional action. Push traffic does not require the disclosure of

information [about the electronic data exchange] personally [to the person in question] but such information must be permanently disclosed via public communication channels. Nor is prior consent required, although the person in question may object to his data being exchanged.

- Proposal on Patient's Rights with regard to electronic data processing (Proposal Patient's Rights)

With respect to 'consent', the Proposal Patient Rights introduces:
- the healthcare provider's obligation to only disclose the client's details by means of an electronic exchange system insofar as the client has explicitly granted consent;
- the client's right to grant, at the client's discretion, general consent for all healthcare providers connected to the electronic exchange system, or specified consent to disclose all or specific information to a certain healthcare providers or categories of healthcare providers to be specified by the client;
- the condition that explicit consent for consulting information or making a copy of it has been granted by the client within the context of the treatment relationship in question.

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?		No
Is a materialised consent needed?		No
Are there requirements to inform the patient about the purpose of EHRs and the consequences of the consent or withholding consent to create EHRs?		There are no specific requirements other than the general obligations, based on general data protection law.
Are there specific national rules on consent from the patient to share data?	Art. 457, section 1, WGBO.	Based on this article, as a general rule, explicit consent is required for sharing data by healthcare practitioners with third parties, unless there is a 'treatment relation'. Proposal Patient's Rights and the Gedragscode EGiZ further specify how and when such consent should be obtained when data are shared by means of an electronic system.
Are there any opt-in/opt-out rules for patient consent with regard to processing of EHRs?		The rules mentioned above qualify as 'opt-in'.
Are there any opt-in/opt-out rules for patient consent with regard to sharing of EHRs?		The rules mentioned above qualify as 'opt-in'.
Are there requirements to inform the patient about the purpose of EHRs and the consequences of consent or withholding consent on the sharing of EHRs?		There are no specific requirements other than the general obligations, based on general data protection law.
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)?		There are no legal obstacles to do so. However, the authorization of such health practitioners or institutions may cause practical problems.
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

- Data Protection Act (WBP)

With respect to the creation, access and update of EHR's the following articles of the WBP are relevant.

Pursuant to article 16 WBP it is prohibited to process personal data concerning a person's health except as otherwise provided. According to article 21, paragraph 1 WBP this prohibition does not apply where the processing is carried out by medical professionals, healthcare institutions or facilities or social services, provided that this is necessary for the proper treatment and care of the data subject (the patient), or for the administration of the institution or professional practice concerned. Furthermore, the prohibition on processing data concerning a person's health does not apply where this is carried out with the express consent of the data subject (article 23 WBP).

Pursuant to article 13 WBP the healthcare provider must implement appropriate technical and organizational measures to secure all personal data against loss or against any form of unlawful processing. These measures shall guarantee an appropriate level of security, taking into account the state of the art and the costs of implementation, and having regard to the risks associated with the processing and the nature of the data to be protected. These measures shall also aim at preventing unnecessary collection and further processing of personal data.

Furthermore, the WBP states that all personal data shall be processed in accordance with the law and in a proper and careful manner[39] and shall be collected for specific, explicitly defined and legitimate purposes[40]. Article 9 WBP stipulates that the personal data shall not be further processed in a way that is incompatible with the (original) purposes for which they have been obtained. As a consequence thereof the access and use of the personal data or EHR is limited to the original purpose.

Pursuant to article 11 WBP, the personal data shall only be processed where they are adequate, relevant and not excessive. Furthermore, the responsible party (for example healthcare provider) shall take the necessary steps to ensure that personal data, given the purposes for which they are collected or subsequently processed, are correct and accurate. As a consequence hereof a healthcare provider has to take measures to make sure that the content of the EHR is of good quality and accurate and updated if necessary.

- Medical Treatment Contracts Act (WGBO)

Pursuant to article 457 WGBO a healthcare provider is not allowed to inform a third party on patient's data without his consent. The article stipulates that a third party does not refer to a person (healthcare provider) who is directly involved in the treatment of the patient and the fulfilment of the medical treatment contract or who replaces the healthcare provider. Such a person may have access to the health record insofar this is necessary for the fulfilment of his obligations.

- Code of Conduct Electronic Data Exchange in Health care (Gedragscode EGiZ)

The *Gedragscode EGiZ* provides directions with respect to the general rules inserted in the WBP. The code provides some specific requirements as well as technical requirements with regard to the authorization of healthcare providers and patients with regard to health data, information security and logging. Pursuant to the *Gedragscode EGiZ* the party responsible for the electronic exchange system has to:

[39] Article 6 of the WBP
[40] Article 7 of the WBP

- adopt an 'authorisation policy' that stipulates who may have access to which personal and health data[41]
- take measures in order to avoid access of the personal / health data by third parties that do not have a medical treatment relationship with the data subject[42]
- introduce an electronic registration of all actions (updates, access, revisions etc.) in the electronic patient records (logging). Such registration should make it possible to check whether access to the patient file was lawful[43].
- take technical measures to limit access to personal / health data to:[44]
    - the healthcare provider who is the source of all health data regarding the patient;
    - the healthcare provider who is allowed to have access to the personal and health data, however only if the permissions criteria are fulfilled (meaning for example that there is a medical treatment contract or that the data subject has given its consent)
    - the data subject (patient itself)
    - the responsible party (only for management purposes)

- Proposal on Patient's Rights with regard to electronic data processing (Proposal Patient's Rights)

With respect to 'access' or 'disclosing' of information of the patient through an electronic exchange system , the proposal introduces, among other things:
- the condition that explicit consent for consulting information or making a copy of it has been granted by the client within the context of the treatment relationship in question;
- the disclosure of information by the healthcare provider to the client about the client's rights in the event of electronic information exchange and how the client can exercise those rights;
- offering the client inspection, by electronic means or by means of a copy of the records and/or of the client information that have been disclosed;
- a right of the data subject to request access to log data;
- an access injunction of the electronic exchange systems against healthcare insurance companies, company medical doctors, insurance companies' medical advisors and medical examiners.

- General administrative regulation with regard to the electronic exchange of data between healthcare providers (Besluit elektronische gegevensuitwisseling tussen zorgaanbieders)

This a general administrative regulation that prescribes that the electronic exchange systems must comply with the NEN standards (NEN 7510, NEN 7512 respectively NEN 7513) (See chapter 2.2.1).

[41] Article 6 of the Gedragscode EGiZ
[42] Article 7 of the Gedragscode EGiZ
[43] Article 8 of the Gedragscode EGiZ
[44] Article 8 of the Gedragscode EGiZ

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?		No
Are there specific national rules on access and update to EHRs?		There are only 'general rules' laid down in the Data Protection Act. See for example paragraph 2.4.1. However, the *Gedragscode EGiZ* provides some specific requirements and technical requirements with regard to the authorization of healthcare providers and patients with regard to health data, information security and logging. The NEN standards (NEN 7510, NEN 7512, NEN 7513 and NEN 7521) provide requirements with regard to authorization, exchange of patient data, consent protocols, information security and logging.
Are there different categories of access for different health professionals?		No
Are patients entitled to access their EHRs?	456 WGBO	Pursuant to this article 456, the patient has the right to have access to and a transcript of his medical records. The healthcare provider supplies the information he possesses on the patient's request, with the exception of information that might be disadvantageous to the patient. The doctors personal work-notes are not open to access or transcript as well as data possibly violating the privacy of a third party.
Can patient have access to all of EHR content?		However, the Proposal Patient's Rights stipulates that:

Questions	Legal reference	Detailed description
		on request, the patient has the right to access or copy all data, which the healthcare provider makes available through an electronic exchange system, in an electronic way;[45] and if medicines are being supplied by a pharmacist, the patient has the right to have access to its medication record in an electronic way.[46]
Can patient download all or some of EHR content?		No
Can patient update their record, modify and erase EHR content?		Yes (right to erase)
Do different types of health professionals have the same rights to update EHRs?		No
Are there explicit occupational prohibitions? (e.g. insurance companies/occupational physicians…)		However, the Proposal Patient's Rights introduces an access injunction of the electronic exchange systems against healthcare insurance companies,[47] company medical doctors, insurance companies' medical advisors and medical examiners.[48]
Are there exceptions to the access requirements (e.g. in case of emergency)?		However, the Proposal Patient's Rights stipulates that a healthcare provider who must act directly to avoid serious harm for the patient, while it is impossible to ask consent at that time, is authorised to access the data of the client in question that are available by means of an electronic exchange system, insofar as

[45] Legislative Proposal 33 509, Article I, Paragraph D, Article 23c sub 1 and Article II, Paragraph B, Article 15d sub 1
[46] Legislative Proposal 33 509, Article I, Paragraph D, Article 23c sub 2 and Article II, Paragraph B, Article 15d sub 2
[47] Proposal Patient's Rights, Article I, Paragraph F, Article 25a sub 1 and Article II, Paragraph B, Article 15f sub 1.
[48] Proposal Patient's Rights, Article I, Paragraph F, Article 25a sub 2and Article II, Paragraph B, Article 15f sub 2.

Questions	Legal reference	Detailed description
		the consultation is necessary for him to perform acts in respect of the client in those circumstances.
Are there any specific rules on identification and authentication for health professionals? *Or are they aggregated?*		However, pursuant to the *Gedragscode EGiZ* the party responsible for the electronic exchange system has to take measures with respect to identification, authentication and authorisation of the healthcare provider (see above in chapter 2.4.1).
Does the patient have the right to know who has accessed to his/her EHRs?	*Gedragscode EGiZ*	Such right is inserted in the *Gedragscode EGiZ* and the Proposal Patient's Rights. For example: On request, the patient has the right to have a copy of all information regarding: - Who has made information available through the electronic exchange system and when - Who has accessed the information and when.[49]
Is there an obligation on health professionals to update EHRs?	454 WGBO	Pursuant to this article, healthcare providers are obliged to keep medical records.
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

[49] Proposal Patient's Rights, Article I, Paragraph D, Article 23d and Article II, Paragraph B, Article 15e.

Questions	Legal reference	Detailed description
Are there any measures that consider access to EHRs from health professionals in another Member State?		No

2.5. Liability

2.5.1. Main findings

Medical professionals may be held liable for professional errors, including errors in an EHR, under Civil Law, Criminal Law and Disciplinary Rules. There are no specific regulations with respect to liability for the use or errors of the EHR.

If a healthcare provider causes injury to a patient, he may be sued on the grounds of default or tort. Default consists of the failure to fulfil a contract; the patient is assumed to enter into a medical treatment contract with his healthcare provider on the basis of which he can sue the healthcare provider for default at the latter's failure to fulfil the medical treatment contract (see article 446 of the Medical Treatment Contracts Act (WGBO)).

Pursuant to article 453 WGBO, the 'reasonably competent physician' is the norm in judging a healthcare provider's actions. This means that a healthcare provider's actions, for example with respect to his use of the EHR, are tested by the actions of a reasonably competent physician in equal circumstances. In judging whether the criterion of 'a reasonably competent physician' has been met, the judgement of experts is of major importance. The obligation a healthcare provider enters into with a patient is usually regarded as an obligation of effort and not as an obligation of a certain result; the result itself need not be guaranteed.

Healthcare providers can be attached to a hospital in various ways; they are either employed by the hospital or they are admitted by contract. The matter of attachment to an institution decides the way in which a healthcare provider may be held liable for errors made during the treatment. When a healthcare provider is employed by a hospital, the hospital may be held liable for default and the healthcare provider for tort if an error has been committed. When a healthcare provider works in a hospital on the basis of an admittance contract, problems may arise when an error has been made during the treatment. It may not be clear who entered into a contract with the patient concerned, and in what way the hospital's as well as the healthcare provider's liability has been limited. Article 462 WGBO introduced a central liability of the hospital. The hospital may be held liable as 'if it were a party to the contract'. Besides the hospital the healthcare provider remains liable for his own actions all the same.

Pursuant to article 463 WGBO, medical practitioners and hospital are not entitled to restrict or exonerate their liability for failures / error.

If a patient suffers damages as a consequence of a fault in the medical records and the healthcare provider complied with all stipulations set out in the relevant legislations and additional rules with respect to the electronic exchange of patient information and the NEN standards (and therefore complies with 'the actions of a reasonably competent physician in equal circumstances'), the healthcare provider might not be held liable under Criminal Law or Disciplinary Rules. However, he might be liable under Civil Law, for example in the event that the mistake is caused by his employees or his ICT-provider.

The healthcare provider may be liable for mistakes in the treatment caused by missing or incorrect health data in medical records. However, if the fault in the health data is caused by another healthcare provider (the source of the medical record) that provides access to his medical records through (for example) a system for electronic exchange of patient data, the healthcare provider who is the source of the medical record may be liable as well (depending on the circumstances).

If there is a mistake in the software or hardware of an EHR, the ICT provider might be liable towards the healthcare provider. However it's likely that the liability of the ICT provider will be limited by the agreement between the healthcare provider and the ICT provider.

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?		No
Can patients be held liable for erasing key medical information in EHRs?		It is not likely that a patient can erase key medical information in the EHR / medical records. Pursuant to the WGBO, patients have the right to request the healthcare provider to correct, supplement, delete or block some data. However the healthcare provider will always be responsible for its decision to agree to such request.
Can physicians be held liable because of input errors?		There is no specific regulation on this. General rules on liability are applicable.
Can physicians be held liable because they have erased data from the EHRs?		Idem
Are hosting institutions liable in case of defect of their security/software systems?		Idem
Are there measures in place to limit the liability risks for health professionals (e.g. guidelines, awareness-raising)?		Idem
Are there liability rules related to breach of access to EHRs (e.g. privacy breach)?		Idem
Is there an obligation on health professionals to access EHRs prior to take a decision involving the patient?		Idem
Are there liability rules related to the misuse of secondary use of health data?		Idem

2.6. Secondary uses and archiving durations

2.6.1. Main findings

Pursuant to the Medical Treatment Contracts Act (WGBO) medical files must be kept for a period of fifteen years after they have been created or as long as is necessary for the treatment by a good healthcare professional. This provision is applicable to both physical and digital medical files.

There are no specific legal obligations to destroy data in EHRs at the end of the archiving duration.

The WGBO allows for the use of information in medical files for statistical or scientific research as part of the execution of the treatment contract between the healthcare provider and the patient or, under certain conditions, without the consent of the patient.

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. 454, section 3 WGBO	Pursuant to this article medical files must be kept for a period of fifteen years after they have been created, or as long as is necessary for the treatment by a good healthcare professional. This provision is applicable to both physical and digital medical files.
Are there different archiving rules for different providers and institutions?		No
Is there an obligation to destroy (…) data at the end of the archiving duration or in case of closure of the EHR?		There are no specific legal obligations to destroy data in EHRs at the end of the archiving duration.
Are there any other rules about the use of data at the end of the archiving duration or in case of closure of the EHR?		No
Can health data be used for secondary purpose (e.g. epidemiological studies, national statistics...)?	Art. 458 WGBO	This article allows for the use of information in medical files for statistical or scientific research as part of the execution of the Treatment Contract or, under certain conditions, without the consent of the patient.
Are there health data that cannot be used for secondary use?		No
Are there specific rules for the secondary use of health data (e.g. no name mentioned, certain health data that cannot be used)?		No
Does the law say who will be entitled to use and access this data?		No
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

The Netherlands does not have one centralised database for the storage of medical data. Nevertheless there is a nationwide system for the electronic exchange of medical data between healthcare providers (the National Switch Point (LSP)). Several information systems are connected to this national system.

Furthermore, there are no legal requirements regarding the interoperability of national EHRs with other Member States' EHR systems.

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?		No
Are there any specific rules/standards on the interoperability of EHR?		No
Does the law consider or refer to interoperability issues with other Member States systems?		No

2.8. Links between EHRs and ePrescriptions

2.8.1. Main findings

- Medicines Act (*Geneesmiddelenwet*)

In July 2007, the new Medicines Act came into force. Article 67 of this Medicines Act introduced a ban on the prescription of medications over the Internet to persons (i) who the prescribing physician has never met in person, or (ii) who the prescriber does not know or (iii) from whom the prescriber does not have a medical history available.

In view of this ban, the Royal Dutch Medical Association (KNMG) changed its guideline and ruled that prescribing medication over the Internet for patients who you do not know is no longer allowed.

The definition of "prescription" (Dutch: *recept)* in the new Medicines Act takes account of prescriptions by means of electronic information carriers. The requirement is imposed on these information carriers that the document is secured in such a way that the prescribing physician issuing it will be recognised on the basis of agreements made with the intended receiving party (pharmacist) as the party with whom such agreements have been made. The document may be signed using an electronic signature. A new aspect of this is that the prescribing physician indicates on the prescription a unique identification of the patient, i.e. distinguishing the patient from other patients in such a way that no confusion is possible.

- KNMG Guideline on electronic prescriptions [*KNMG Richtlijn Elektronisch voorschrijven*]

In September 2013 this new guideline regarding electronic prescriptions was published by several umbrella healthcare organisations. This guideline entered into force on 1 January 2014. The guideline requires prescribers to use an electronic prescription system that provides possibilities to monitor unsafe situations. According to the Guideline on electronic prescriptions, systems have to meet current requirements with regard to (1) their functionality and (2) the exchange of information between healthcare providers. Also, electronic prescription systems should allow for the copying of data from other automated systems or for the manual registration of data.

The guideline is not legally enforceable. However in the event that a healthcare provider does not comply with such guideline and an error occurs, he might be liable because of the fact that he didn't met the criterion of 'a reasonably competent physician' as laid down in article 453 WGBO. Pursuant to article 453, the actions of a healthcare provider for example with respect to electronic prescription are tested by the actions of a reasonably competent physician in equal circumstances. In judging whether the criterion of 'a reasonably competent physician' has been met, the judgement of experts is of major importance and they might check whether or not the healthcare provider acted in accordance with the guideline of the Royal Dutch Medical Association (KNMG).

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?		An ePrescription can be prescribed to a patient who does not have an EHR.
Can an ePrescription be prescribed to a patient who does not have an EHR?		There is no specific regulation stating that an EHR is obliged for a ePresciption.

- ***Access***

Questions	Legal reference	Detailed description
Do the healthcare providers, hospital doctors, dentists and pharmacists writing the ePrescription have access to the EHR of the patient?		This is possible, but not legally required.
Can those health professionals write ePrescriptions without having access to EHRs?		There is no general legal obligation to consult the EHR before writing an ePrescription

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

Good practices

In the Netherlands most medical records are updated electronically and are no longer available in paper. A 2013 Survey from the National IT Institute for Healthcare in the Netherlands ('NICTIZ') and the Netherlands Institute for Health Services Research ('NIVEL') shows that 93% of general practitioners and 66% of medical specialists update their records primarily or exclusively electronically.[50] There are several EHR solutions in place, for example the systems offered by ChipSoft, CSC-iSOFT and McKesson.[51]

There are also several systems in place for the electronic exchange of patient data inserted in EHRs. At regional/local level there are systems that connect the information systems of General Practitioners, GPs out-of-hours surgery and pharmacists (for example 'OZIS-ring') who work together on local or regional level. There are also systems that connect medical specialists or other healthcare providers who are active in the same chain of care (for example the chain of care with respect to cancer or diabetes).

Finally, there is a nationwide system for the electronic exchange of medical data between healthcare providers. The Association of Healthcare providers for Health communication (Vereniging van Zorgaanbieders voor Zorgcommunicatie, (VZVZ)) is responsible for this nationwide system. This system is based on a National Switch Point (LSP). The exchange of medical data between the healthcare providers takes place via this LSP. The LSP provides a reference index for routing, identification, authentication, authorization and logging. The LSP can be compared to a traffic-control tower which regulates the exchange of patient data between the healthcare providers.

At this moment LSP mainly connects general practitioners, GPs out-of-hours surgery, pharmacists and a few hospitals. In January 2014 a spokesman of the VZVZ said that 75% of the general practitioners and 83% of the pharmacists are connected to the LSP.[52]

Legal barriers

Stakeholders[53] observe barriers for the electronic exchange of patient data inserted in the EHR. The regulation, guidelines and standards with respect to the electronic exchange of medical data do not support but rather cause a delay in the development and use of electronic exchange systems. These barriers are related to (i) the lack of uniform (technical) standards and language, (ii) the strict security measures laid down in the NEN standards, (iii) questions with respect to interpretation of the legislation, (iv) concerns of healthcare providers with respect to liability, and (v) the rules with respect to the verification of healthcare providers and the problems to comply with such rules.[54]

(i) Lack of uniform (technical) standards and language
An important barrier is caused by the lack of uniform (technical) standards. Therefore, The Dutch Healthcare Inspectorate ('IGZ') has requested the market parties to develop a standardisation and (international) classification for the electronic exchange of patient data and records.[55]

The NEN standards are a good example of such standardisations. However many information systems used for the electronic exchange of health data do not comply with these standards.[56]

[50] Ehealth monitor 2013, Summary, Nictiz and Nivel, p. 15 and 16.
[51] Interview with Mr J. Krijgsman
[52] Aanmelding LSP groeit fors, Zorgvisie, 23 januari 2014, http://www.zorgvisie.nl/Home/Dossiers/EPD--LSP/
[53] Interviews with stakeholders
[54] Interviews with stakeholders
[55] Interview with Mr T. Kliphuis

Furthermore, there are some initiatives to ensure that all relevant patient data will be documented in EHRs in an unambiguous and structured way so that the data will be easy to access and easily exchangeable between the healthcare providers. Examples of these initiatives are: 'Eenheid van Taal' and 'Snowmed'.[57]

In the event that EHRs would be accessible to healthcare providers based in other Member States, the lack of any standard with respect to the language will be a barrier as well.[58]

(ii) Strict security measures laid down in the NEN standards
Although the NEN standards are a good example of the standardisations, these standards are considered too strict. At this moment there is a (major) gap between the security measures currently used in the electronic exchange systems and the security requirements laid down in the NEN standards. For example some electronic exchange systems still work with a Login based on a UserID and Password. This Login does not comply with the security measures suggested in the NEN standards (those are based on to so-called Stork 4).[59]

(iii) Questions with respect to interpretation of the regulation
Information from stakeholders shows that the current regulations lead to a lot of questions with respect to the interpretation of the stipulations.[60] For example:

- *Verification of the medical treatment relationship*

Pursuant to the regulation[61], the electronic exchange system should verify if there is a treatment relationship between the healthcare provider, who wishes to have access to an EHR, and the relevant patient, in order for the healthcare provide to be provided access to information in the EHR. However, the regulation does not provide an answer on the question how this verification process should look like and which specific requirements should apply. In the current practise this verification takes place by verifying the appointment database or agenda of the healthcare providers. This appointment database or agenda is not linked to the EHR and this means that the verification information needs to be inserted manually, which of course is time-consuming and not user-friendly.[62]

- *Consent*

Pursuant to the regulation[63] the consent of the patient will not be necessary in the event of an exchange of data in case of substitution by GP out-of-hours surgery. However the Dutch Data Protection Authority ('CBP') ruled that if the exchange of data in case of substitution by GP out-of-hours surgery takes place through the LSP, consent is still necessary. If the general practitioner and the GP out-of-hours surgery use another electronic exchange system, the consent is not necessary. This means that the same exchange of information through several exchange systems may lead to other interpretations of the legislation. This of course leads to many questions.[64]

(iv)Concerns of healthcare providers with respect to liability[65]

[56] Interviews with stakeholders
[57] Interview with J. Krijgsman
[58] Interview with J. Krijgsman
[59] Interview with Mr J. Krijgsman
[60] Interviews with stakeholders
[61] For example the Code of Conduct Electronic Data Exchange in Health care (Gedragscode EGiZ)
[62] Interview with D. Ormel
[63] For example the Code of Conduct Electronic Data Exchange in Health care (Gedragscode EGiZ)
[64] Interview with Mr J. Krijgsman
[65] Interviews with stakeholders

There aren't any specific rules with respect to the liability for mistakes with respect to EHR's or the electronic exchange of data. The general regulation with respect to liability applies. The healthcare providers are concerned about their liability in the event of, for example:

- mistakes in the information they receive from other healthcare providers through the electronic exchange system.
- mistakes caused by the fact that the healthcare provider didn't make use of information of a patient that is inserted in a EHR of another healthcare provider and that was accessible through the exchange system.
- mistakes caused by faults in the EHR of other healthcare providers and accessible through the exchange system.

(v) Verification of the healthcare provider

An important barrier for electronic exchange of patient data (both national and cross border) relates to verification and authorisation issues. For example pursuant to the regulation[66] the following information has to be verified:

- the identity of the healthcare provider
- the specialism of the healthcare provider
- the existence of a medical treatment relationship between the healthcare provider and the patient
- the consent of the patient[67]

In the daily practise it is difficult to collect and verify all such information. Complying with these verification obligations might lead to systems that are not practical, workable and time consuming.

[66] For example the Code of Conduct Electronic Data Exchange in Health care (Gedragscode EGiZ)

[67] Interviews with Mr T. Kliphuis, Mr. D. Ormel and Mr. A. Jaoenathmisier