

Federal Act, which enacts a Health Telematics Act 2012 and amends the General Social Insurance Law, the Act on Social Security for Persons engaged in Industry, the Act on Social Security for Farmers, the Act on Health and Accident Insurance for Civil Servants, the Gene Technology Act and the Criminal Code (Electronic Health Records Act – EHRA)

The National Council adopted:

Table of Contents

Art. Subject

- 1 Health Telematics Act 2012
- 2 Amendment of the General Social Insurance Law
- 3 Amendment of the Act on Social Security for Persons Engaged in Industry
- 4 Amendment of the Act on Social Security for Farmers
- 5 Amendment of the Act on Health and Accident Insurance for Civil Servants
- 6 Amendment of the Gene Technology Act
- 7 Amendment of the Criminal Code

Article 1

Federal Act on Data Security Measures when using personal electronic Health Data (Health Telematics Act 2012 – HTA 2012)

Table of contents

Sect. Headline

1st Part: General Provisions

- 1 Scope of Application
- 2 Definitions

2nd Part: Data Security in Electronic Transfer of Health Data

- 3 Principles of Data Security
- 4 Identity
- 5 Role
- 6 Confidentiality
- 7 Integrity
- 8 IT-Security Concept

3rd Part: Information Management

- 9 Organization of the Electronic Health-Directory Service (EHDS)
- 10 Data of the Electronic Health Directory Service
- 11 Monitoring
- 12 Basics of Cross-Border Healthcare

4th Part: Electronic Health Records (EHR)

- 13 General Requirements for EHR
- 14 Principles on the Usage of Data
- 15 Principles on the participation in EHR
- 16 Fundamental Rights of EHR-Participants
- 16a E-Medication
- 17 EHR-Ombudsman
- 18 Authorization of EHR-Participants
- 19 Authorization of EHR-Healthcare Providers and the EHR-Ombudsman
- 20 Storage of EHR-Health Data

- 21 Access Control Centre
- 22 Logging System
- 23 e-Health Access Point
- 24 Right to Use the EHR Infrastructure

5th Part: Final Provisions

- 25 Administrative Penalties
- 26 Entry into Force
- 27 Transitional Provisions
- 28 Regulatory Powers
- 29 Enactment and Entry into Force of Ordinances
- 30 References
- 31 Enforcement

First Part

General Provisions

Scope of Application

Section 1. (1) Subject of this Federal Act is the usage (sect. 4 no. 8 of the Data Protection Act 2000 [[DPA 2000](#)], Federal Law Gazette I No. 165/1999, [German: “*Datenschutzgesetz 2000 (DSG 2000)*”]) of personal electronic Health Data by Healthcare Providers pursuant to sect. 2 no. 2 of this Federal Act.

(2) Objectives of this Federal Act are:

1. to foster and extend data security, when using electronic Health Data in directed or undirected communication by setting up uniform federal minimum standards and avoiding abuse of data (2nd Part),
2. to provide and broaden the information basis necessary for the steering and development of e-health [translator’s note: *in Austria*] (3rd Part) as well as
3. to create uniform rules for undirected communication of electronic Health Data, especially in the context of EHR (sect. 2 no. 6), where special attention shall be drawn on:
 - a) the rights of the participants (sect. 16), in particular the self-determination of the EHR-Participants,
 - b) the verification of the identity of participants (sect. 18),
 - c) the verification of the identity of EHR-Healthcare Providers (sect. 19),
 - d) the individual and general access authorizations (sect. 21) and
 - e) the logging of the usage of EHR-Health Data (sect. 22) (4th Part).

(3) If not stated otherwise in this Federal Act, provisions of other laws shall remain unaffected.

Definitions

Section 2. For the purpose of this Federal Act the following terms shall have their respective meaning:

1. “Health Data” [German: “*Gesundheitsdaten*”]: personal data pursuant to sect. 4 no. 1 [DPA 2000](#) on the physical or psychological state of a person, including data collected to examine this state, as well as data collected for the purposes of preventive medicine or healthcare provision, for diagnosis, treatment or care methods, for provision of care, prescribed or taken medicines (“medication data”), medical aids or aids, for the charging of healthcare services, or for data collected for the insurance of health risks.
2. “Healthcare Providers” (“HCP”) [German: “*Gesundheitsdiensteanbieter (GDA)*”]: controllers or processors as set forth in sect. 4 [DPA 2000](#) who use electronic Health Data in one of the Roles set forth in the ordinance based upon sect. 28 para. 1 no. 1, on a regular basis for the following purposes:
 - a) medical treatment or healthcare or
 - b) nursing care or
 - c) charging of health services or
 - d) insurance of health risks or
 - e) exercising rights of patients.
3. “IT-Security Concept” [German: “*IT-Sicherheitskonzept*”]: sum of all data security measures of a Healthcare Provider, necessary and reasonable according to sect. 14 [DPA 2000](#), in order to protect personal data, in particular sensitive data.
4. “Registration Bodies” [German: “*Registrierungsstellen*”]: authorities, that keep records according to sect. 9 para. 3 no. 1 or are referred to in sect. 9 para. 3 nos. 2 and 3.
5. “Role” [German: “*Rolle*”]: classification of Healthcare Providers according to the type of their area of responsibility, their employment, their business object or their range of services.

6. “Electronic Health Record (EHR)” [German: “*Elektronische Gesundheitsakte (ELGA)*”]: an information system providing all authorized EHR-Healthcare Providers (no. 10) and EHR-Participants with Health Data (no. 9) in electronic form, without reference to location and time (undirected communication).
7. “Repository” [German: “*Datenspeicher*”]: technical infrastructure serving as storage for EHR-Health Data.
8. “Electronic References to EHR-Health Data” [German: “*elektronische Verweise auf ELGA-Gesundheitsdaten*”]: electronic information in EHR regarding type and memory location of EHR-Health Data.
9. “EHR-Health Data” [German: “*ELGA-Gesundheitsdaten*”]: the following personal data, that could be essential for further treatment, care or the assurance of healthcare continuity of EHR-Participants and may legally be used in EHR:
 - a) medical documents, including any image data in a standardized format according to sect. 28 para. 2 no. 1, those contain Health Data pursuant to no. 1, except data, which are exclusively related to the accounting of health services or health-related insurance services, such as:
 - aa) hospital discharge reports pursuant to sect. 24 para. 2 of the Hospitals and Sanatoriums Law (HSL) [German: “*Krankenanstalten- und Kuranstaltengesetz (KAKuG)*”], Federal Law No. 1/1957,
 - bb) laboratory findings,
 - cc) results of diagnostic imaging and
 - dd) other medical reports structured and formatted according to sect. 28 para. 2 no. 3 lit. a,
 - b) medication data pursuant to no. 1 regarding prescription as well as non-prescription drugs (“E-Medication”),
 - c) living wills (sect. 2 para. 1 of the Living Wills Act, Federal Law Gazette I No. 55/2006),
 - d) powers of attorney (sect. 284f of the Civil Code, Collection of Laws No. 946/1811),
 - e) data from the registers pursuant to sects. 73 and 73a of the Medical Devices Act (MDA), Federal Law Gazette No. 657/1996 and
 - f) data of patients according to art. 14 para. 2 lit. b sublit. i of Directive 2011/24/EU on the application of patients' rights in cross-border health care (“patient summary”),
whereas secrets pursuant to sect. 10 para. 4 HSL, data of this kind, if used by other Healthcare Providers as well as records of results pursuant to sect. 71a para. 2 of the Gene Technology Act (GTA), Federal Law Gazette No. 510/1994, must not be regarded EHR-Health Data.
10. “EHR-Healthcare Providers (EHR-HCP)” [German: “*ELGA-Gesundheitsdiensteanbieter (ELGA-GDA)*”]: are the following Healthcare Providers (no. 2):
 - a) members of the medical profession pursuant to sect. 3 of the Doctors Code 1998 (DC 1998) [German: “*Ärztegesetz 1998 (ÄrzteG 1998)*”], Federal Law Gazette I No. 169/1998, also when exercising their medical profession in form of a collaboration as an independent authorized group practice, except:
 - aa) physicians, when acting as chief physicians for the Social Insurance Carriers,
 - bb) physicians, evaluating the constituent parts of insurance contracts or resulting claims,
 - cc) occupational health physicians (sect. 81 of the Employee Protection Act, Federal Law Gazette No. 450/1994),
 - dd) medical officers (sect. 41 DC 1998),
 - ee) physicians being involved in the determination of suitability for military service as well as
 - ff) school doctors (sect. 66 of the School Education Act, Federal Law Gazette No. 472/1986).
 - b) members of the dental profession (sect. 5 of the Dental Act [German: “*Zahnärztegesetz (ZÄG)*”], Federal Law Gazette I No. 126/2005), also when exercising their medical profession in form of a collaboration as an independent authorized group practice, except:
 - aa) dentists, who are not authorized to treatment, that requires general anaesthetic [German: “*Dentisten*”] (sect. 60 of the Dental Act),
 - bb) dentist officers (sect. 32 of the Dental Act),
 - cc) dentists, when acting as chief dentists for the social insurance carriers as well as
 - dd) dentists, evaluating the constituent parts of insurance contracts or resulting claims,
 - c) pharmacies pursuant to sect. 1 of the Pharmacy Act, Federal Law Gazette No. 5/1907,
 - d) hospitals according to sect. 1 HSL other than independent outpatient clinics (sect. 2 para. 1 no. 5 HSL) in the field of occupational healthcare and
 - e) healthcare institutions whose operation is subject to a notification or permission requirement according to federal or state laws as well as governmental supervision and control.

11. “EHR-System Partners” [German: “*ELGA-Systempartner*”]: the Federal Government, the States and the Federation of the Austrian Social Security Carriers (hereinafter: Federation).
12. “EHR-Participants” [German: “*ELGA-Teilnehmer/innen*”]: natural persons, that meet the requirements for participation according to sect. 15 and for whom, accordingly, electronic references to their EHR-Health Data (no. 9) may be stored.
13. “Registry” [German: “*Verweisregister*”]: a register of electronic references to EHR-Health Data (no. 9) in the context of EHR.
14. “EHR-Ombudsman” [German: “*ELGA-Ombudsstelle*”]: institution, advising and supporting EHR-Participants in the perception and enforcement of their rights in matters of EHR and in matters of data protection as well as supporting EHR-System Partners in further developing participants’ rights and data protection.
15. “Opt-out Offices” [German: “*Widerspruchstellen*”]: bodies, that general objections of participating in EHR can be declared to in written form.

Second Part

Data Security in Electronic Transfer of Health Data

Principles of Data Security

Section 3. (1) This section applies to all forms of electronic transfer of personal Health Data (directed and undirected communication) by health care providers (sect. 2 no. 2).

(2) Para. 4 no. 3 to 6 and sects. 5 to 7 do not apply to electronic transfer of Health Data within a Healthcare Provider, if unauthorized third parties could be excluded from accessing Health Data by means of data security and control measures that are effective and state-of-the-art.

(3) The legitimacy of using Health Data has to be represented by means of Roles. Healthcare Providers have to technically ensure that Health Data are not used beyond the legitimate Roles.

(4) Healthcare Providers may disclose health information only if

1. the transfer is legitimated according to one of the purposes determined in sect. 9 [DPA 2000](#),
2. the identity (sect. 4) of the persons whose Health Data shall be disclosed has been confirmed,
3. the identity (sect. 4) of the Healthcare Providers being involved in the transfer has been confirmed,
4. the Roles (sect. 5) of the Healthcare Providers being involved in the transfer are demonstrated,
5. confidentiality (sect. 6) of the shared Health Data is guaranteed and
6. integrity (sect. 7) of the shared Health Data is guaranteed.

Identity

Section 4. (1) When transferring Health Data the identity (sect. 2 no. 1 of the E-Government Act [E-GovA], Federal Law Gazette I No. 10/2004) [German: “*E-Government-Gesetz (E-GovG)*”] of those individuals whose Health Data are disclosed has to be determined.

(2) In the event of undirected communication additionally the unique identity (sect. 2 no. 2 E-GovA) of the persons, whose Health Data shall be transferred, needs to be proven and verified.

(3) The Patient Index pursuant to sect. 18, may legitimately be used for verifying the unique identity (sect. 2 no. 2 E-GovA) of individuals, whose health information shall be disclosed, even beyond the scope of EHR (Part 4).

(4) Proof and verification of the unique identity (sect. 2 no. 2 E-GovA) of Healthcare Providers shall be done

1. by using electronic signatures that have to be traceable to qualified certificates, as well as sector-specific personal identifiers (sect. 9 E-GovA) or
2. by matching of the identification data with the data of the eHealth Directory Service (sect. 9) or
3. by matching of the identification data with the data of the Healthcare Provider Index (sect. 19).

(5) For reasons of patients’ safety the unique identity

1. of individuals whose Health Data shall be disclosed and
2. of Healthcare Providers

has to be stored by means of the unique electronic identifiers according to sect. 8 E-GovA.

(6) To facilitate the identification in the health area (sect. 9 para. 1 E-GovA) sects. 14 and 15 E-GovA on the usage of the citizen card function in the private sector are not applicable. Instead the provisions of the E-GovA, applicable for the public sector controllers, in particular the sects. 8 to 13 E-GovA, shall be applied accordingly. Thus the Healthcare Providers are entitled to have their data applications equipped with sector specific sourcePINs [translator’s note: the source Personal Identification Number (sourcePIN) is a personal

identifier according to art.8 para.7 of the Data Protection Directive 95/46/EC] (ssPINs) [German: “bereichsspezifisches Kennzeichen (bPK)”] by the sourcePIN Register Authority [German: “Stammzahlenregisterbehörde” - cf. <http://www.stammzahlenregister.gv.at>] according to sect. 10 para. 2 E-GovA.

Role

Section 5. (1) Proof and verification of the Role of Healthcare Providers shall be performed according to sect. 4 para. 4.

(2) The Federal Minister of Health shall lay down the Roles to use by means of ordinance according to sect. 28 para. 1 no. 1.

Confidentiality

Section 6. (1) The confidentiality of electronically transferred personal Health Data has to be ensured either

1. by performing the electronic transfer of personal Health Data via networks, that are secured against unauthorized intrusion, compliant to the state of the art in network security, by at least providing
 - a) the protection of the data transfer by cryptographic or physical measures,
 - b) access to the network only for a closed or definable group of users as well as
 - c) the authentication of usersor
2. by using protocols and methods, that
 - a) provide full encryption of Health Data and
 - b) whose cryptographic algorithms are enlisted in the ordinance based upon sect. 28 para. 1 no. 2.

(2) In the course of electronic transfer of Health Data in accordance with para. 1 no. 2 information that are possibly excluded from the encryption, must neither refer to any of the data subjects (sect. 4 no. 3 [DPA 2000](#)), whose Health Data are communicated, nor to any authentication data.

(3) Health Data may only be saved in storages, that are provided based on the needs of clients ("cloud computing"), if the Health Data have been encrypted state-of-the-art (para. 1 no. 2).

Integrity

Section 7. (1) Proof and verification of the integrity of electronic Health Data shall be provided by the application of advanced or qualified electronic signatures pursuant to sect. 2 no. 3 of the Digital Signature Act [German: “*Signaturgesetz*”], Federal Law Gazette I No. 190/1999.

(2) Para. 1 shall not be applied on the electronic transfer of Health Data between Healthcare Providers, if a state-of-the-art secured network pursuant to sect. 6 para. 1 no. 1 is used and the access to this network is restricted to Healthcare Providers known in advance.

IT-Security Concept

Section 8. (1) On the basis of an IT-security concept Healthcare Providers have to document all data security measures taken in accordance with sect. 14 [DPA 2000](#) and the provisions of this Act. This documentation shall give evidence that both access and disclosure of the data are performed in accordance with the law and that data are not accessible to unauthorized persons.

(2) The legal entities of hospitals as well as the regulatory or supervisory authorities of institutions of care, the Austrian Medical Chamber, the Austrian Dental Association, the Austrian Midwives Board, the Austrian Chamber of Pharmacists, the Austrian Economic Chamber and the Federation of Austrian Social Insurance Carriers, may provide standardized forms and fill-ins for the documentation according to para. 1 as assistance to these Healthcare Providers to whom they act as Registration Bodies pursuant to sect. 2 no. 4.

(3) Upon request of the Federal Minister of Health the documentation according to para. 1 shall be submitted to the Federal Minister of Health.

Third Part

Information Management

Organization of the Electronic Health-Directory Service (EHDS)

Section 9. (1) The Minister of Health has to operate an Electronic Health-Directory Service (EHDS) [German: “*eHealth-Verzeichnisdienst*”] to

1. support the legitimate use of Health Data in electronic form,
2. improve information about health-related services and
3. support planning activities and reporting (sect. 11).

(2) Healthcare Providers are registered with the EHDS by the Registration Bodies.

- (3) The record of data according to sect. 10 para. 1 and their removal from the EHDS is provided:
 1. by continuous electronic transmission of:
 - a) the list of doctors pursuant to sect. 27 of the Doctors Code 1998,
 - b) the list of dentists pursuant to sect. 11 of the Dental Act,
 - c) the midwives register pursuant to sect. 42 of the Midwives Act, Federal Law Gazette No. 310/1994 [German: “*Hebammengesetz*”],
 - d) the pharmacies directory pursuant to sect. 2 para. 4 no. 12 of the Pharmacists Chamber Act 2001, Federal Law Gazette I No. 111/2001 [German: “*Apothekerkammergesetz*”],
 - e) the list of the clinical psychologists and health psychologists pursuant to sect. 16 of the Psychologists Act, Federal Law Gazette No. 360/1990 [German: “*Psychologengesetz*”],
 - f) list of psychotherapists pursuant to sect. 17 of the Psychotherapy Act, Federal Law Gazette No. 361/1990 [German: “*Psychotherapiegesetz*”],
 - g) the list of music therapists in accordance with section 19 of the Music Therapy Act, Federal Law Gazette I No. 93/2008 [German: “*Musiktherapiegesetz*”] and
 - h) the list of perfusionists pursuant to section 19 of the Perfusionists Act, Federal Law Gazette I No. 96/1998 [German: “*Kardiotechnikergesetz*”] or
 2. due to electronic notification of
 - a) Healthcare Providers, already registered with the EHDS, about exclusively subordinated organization units,
 - b) governors or district authorities
 - aa) on permits for Healthcare Providers issued, amended or cancelled in their state resp. district or
 - bb) otherwise in their state resp. district indicated activities of Healthcare Providers,
 - c) the Federation [German: “*Hauptverband*”] of the Austrian Insurance Carriers and
 - d) the legal entities of healthcare institutions for government employees [German: “*Krankenfürsorgeanstalten*”] or
 3. by the Federal Minister of Health for all other Healthcare Providers.
- (4) Simplified notification according to para. 3 no. 2 lit. a may only be used by Healthcare Providers other than natural persons, if their organizational structure is stored internally and it is ensured that:
 1. the organizational structure is available in the currently valid form,
 2. for all generated Health Data at least one natural person can be held responsible,
 3. the stored organization data can subsequently not be changed without a trace and
 4. the time of storage of organizational data remains detectable and can also subsequently not be changed without a trace.
- (5) The Registration Bodies have to provide the technical and organizational requirements for
 1. registration according to para. 3 and
 2. clearing in cases of doubt with regard to the data quality.

Data of the Electronic Health Directory Service

Section 10. (1) The following information must be included with the EHDS:

1. name and academic degrees or designation of the Healthcare Provider,
2. the name of the legal entity, if the Healthcare Provider is not a natural person,
3. identifiers of the Healthcare Provider including unique electronic identifiers pursuant to sect. 8 E-GovA,
4. information on the professional, postal and electronic availability of the Healthcare Provider,
5. the Role(s) and special powers or attributes of the Healthcare Provider,
6. the unique identifier (OID [translator’s note: Object IDentifier as jointly developed by ITU-T and ISO/IEC]) and the symbolic identifier,
7. the nationality of the Healthcare Provider,
8. information essential for the encryption of Health Data or the electronic address at which this information can be found,
9. information on the EHR-Healthcare Provider status,
10. information on the geographic location of the Healthcare Provider,
11. information about the services offered by the Healthcare Provider,
12. the name of the Registration Body pursuant to sect. 2 no. 4, that was responsible for registration as well as the name of the data source, provided that such information is available as well as
13. the date of registration with the EHDS and the date of the last amendment.

(2) Notwithstanding para. 1 information on the electronic availability (para. 1 no. 4) and information pursuant to para. 1 nos. 8 and 11 shall only be registered with the EHDS, as such information is transmitted by the Registration Bodies.

(3) Information about special powers or properties pursuant to para. 1 nos. 5, 6, 9, 10, 12 and 13 shall be supplemented by the Federal Minister of Health.

(4) For the unique electronic identification of Healthcare Providers (para. 1 no. 3) that are natural persons, the Registration Bodies have to use sector-specific Personal Identification Numbers (ssPINs). If the Registration Bodies do not provide ssPINs, the date of birth, the sex and the birthplace of the relevant Healthcare Providers, shall be forwarded to the Federal Minister of Health in addition to the data pursuant to para. 1. The information transfer on the place of birth shall only take place if this information is available and necessary for identification purposes.

(5) The unique identifiers pursuant to para. 1 no. 6 (OID and symbolic identifier) shall be derived from the ÖNORM A 2642, "Information Technology - Open Systems, Methods for Registration of information objects in Austria" as of January 1st 2011 from the identifier (OID) of the Federal Ministry of Health. If necessary the Minister of Health may transmit the data referred to in para. 1 nos. 1 to 7, 12 and 13 to systems established for assigning and managing object identifiers.

(6) Apart from identifiers, the nationality of the Healthcare Providers (para. 1 nos. 3 and 7) and data excluded from publication due to existing legislation, the data of the EHDS shall be publicly available and – where necessary – be provided in English.

(7) If necessary the Federal Minister of Health may transmit the data pursuant to para. 1 nos. 1 to 6, 8, 12 and 13 to Healthcare Providers or their service providers. Recipients may use these data exclusively for purposes laid down in sect. 9 para. 1 no. 1.

Monitoring

Section 11. (1) The Minister of Health may establish a nationwide reporting system to evaluate the usage and impact of information and communication technologies in healthcare. Based on standardized requirements this system shall in accordance with the requirements from European level, facilitate the provision of information in particular about

1. the availability of technical infrastructure, including communication infrastructure,
2. the nature and scale of e-health applications and procedures as well as
3. the economic conditions of e-health.

(2) Depending on role-specific characteristics the nature and extent of the incurred data collection may be determined according to the necessary degree of detail.

(3) The Federal Minister of Health has to submit the report pursuant to para. 1 to the National Assembly. Furthermore he is entitled to use these results for purposes of reporting to the European Union or other international organizations.

(4) Healthcare Providers, and all other entities that have information on the use of information and communication technologies in healthcare at their disposal, are obliged to provide the information needed for the preparation of a report pursuant to para. 1 or to provide the required documentation.

Basics of Cross-Border Healthcare

Section 12. The Federal Minister of Health shall support the continuity of care and the patients' cross-border security and therefore create the necessary, especially technical basis.

Fourth Part

Electronic Health Records (EHR)

General Requirements for EHR

Section 13. (1) The use of the Electronic Health Records satisfies an important public interest pursuant to art. 8 para. 4 of the Directive 95/46/EC on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data, OJ No. L 281, 23.11.1995 p. 31. This important public interest in the use of EHR results in particular from:

1. an improved and faster availability of medical information leading to a quality improvement of diagnostic and therapeutic decisions as well as treatment and care,
2. the increase of the process and result quality of health services,
3. the development of integrated care and a cross-sector interface management in public health,
4. the maintenance of a balanced, high-quality and generally accessible healthcare,
5. the strengthening of patients' rights, especially the right to information and the legal protection under the [DPA 2000](#) in accordance with the use of personal data and

6. a contribution to the financial maintenance of the social security system.

(2) In order to fulfil the purposes mentioned in sect. 14 para. 2 EHR-Healthcare Providers have the right to store EHR-Health Data in EHR. According to their professional obligations (e.g. sect. 49 para. 1 DC 1998, sect. 10 of the Pharmacy Operations Regulations [German: “*Apothekenbetriebsordnung*”], Federal Law Gazette II No. 65/2005) they also have the right to collect EHR-Health Data from EHR, unless otherwise provided in this Federal Act due to for example the exercise of EHR-Participants’ rights in accordance with sect. 16.

(3) To achieve the objectives referred to in para. 1 the following data shall not be stored prior to the dates laid down in sect. 27 para. 2 to 6 and not later than laid down in sect. 28 para. 2 no. 4:

1. clinical discharge reports (sect. 2 no. 9 lit. a sub lit. aa) from hospitals (sect. 2 no. 10 lit. d),
2. laboratory findings (sect. 2 no. 9 lit. a sub lit. bb) by members of the medical profession (sect. 2 no. 10 lit. a) provided that they are specialized in “medicinal chemistry laboratory diagnostics” or “hygiene and microbiology”, as well as laboratory findings by hospitals (sect. 2 no. 10 lit. d) in the context of outpatient treatment,
3. findings of diagnostic imaging by members of the medical profession (sect. 2 no. 10 lit. a) provided that they are specialized in radiology, as well as laboratory findings by hospitals (sect. 2 no. 10 lit. d) in the context of outpatient treatment,
4. medication data (sect. 2 no. 9 lit. b), in so far as they relate to trade name or active ingredient, by members of the medical profession (sect. 2 no. 10 lit. a) at prescription,
5. medication data (sect. 2 no. 9 lit. b), in so far as they relate to trade name or active ingredient, by pharmacies (sect. 2 no. 10 lit. c) or drug dispensing doctors at dispensation as well as
6. other findings (sect. 2 no. 9 lit. a sub lit. dd) pursuant to sect. 28 para. 2 no. 3 and 4.

(4) Image data (sect. 2 no. 9 lit. a) shall only be stored in EHR if and to the extent necessary according to the EHR-Healthcare Providers.

(5) The EHR-System Partners have to provide EHR in a way compliant to the necessary security requirements, that allows for a user-friendly integration of EHR for EHR-Participants and EHR-Healthcare Providers, especially with easy to use, effective and for medical criteria optimized search and filter functions.

(6) As far as they are concerned, EHR-System Partners and EHR-Healthcare Providers respectively their legal representation bodies, shall jointly determine in accordance with economic justifiability and the state of technical possibilities the relevant parameters of usability. Prior to this determination, the relevant technical issues and parameters need to be agreed with the Austrian Economic Chamber.

(7) If, for reasons beyond the EHR-Healthcare Provider’s responsibility, in a specific case, the use of EHR is technically impossible or the life or health of the EHR-Participant is due to the time necessary for search seriously at risk, the EHR-Healthcare Provider is not obliged to collect EHR-Health Data from EHR.

Principles on the Usage of Data

Section 14. (1) The usage (storing and collection) of EHR-Health Data is only legitimate, if

1. EHR-Participants (sect. 15 para. 1) were unambiguously identified pursuant to sect. 18,
2. EHR-Healthcare Providers or the EHR-Ombudsman pursuant to sect. 19 were unambiguously identified and
3. EHR-Healthcare Providers or the EHR-Ombudsman are entitled to use EHR-Health Data according to sect. 21.

(2) EHR-Health Data made accessible by EHR may used in a personally identifiable manner exclusively

1. for health purposes in accordance with sect. 9 no. 12 [DPA 2000](#), except for the administration of health services, by
 - a) EHR-Healthcare Providers treating EHR-Participants,
 - b) EHR-Healthcare Providers, to whom EHR-Participants have been referred to for treatment or healthcare by EHR-Healthcare Providers pursuant to lit. a as well as
 - c) persons, that support EHR-Healthcare Providers referred to in lit. a and b in the performance of their activities, and were in the specific case instructed to do so or
2. for the protection of the participants’ rights pursuant to sect. 16 of
 - a) EHR-Participants,
 - b) their legal or authorized representatives as well as
 - c) the EHR-Ombudsman (sect. 2 no. 14).

(2a) From the age of fourteen (mature minors) the responsibility for the protection of the participants’ rights pursuant to sect. 16 resides exclusively with the EHR-Participants.

(3) The request of, the access to and the use of EHR-Health Data made available by EHR is in any case prohibited for:

1. persons or entities that are neither EHR-Healthcare Providers (sect. 2 no. 10) nor EHR-Ombudsman (sect. 2 no. 14),
2. EHR-Healthcare Providers who are not involved in treatment or healthcare of an EHR-Participant,
3. EHR-Healthcare Providers, if the requirements of para. 1 are not satisfied,
4. the EHR-Ombudsman, if it is not involved in the advice or assistance of an EHR-Participant,
5. employers and personnel consultants,
6. insurance companies,
7. statutory social insurance carriers and institutions for health- and accident insurance, unless they are involved in the treatment or healthcare of an EHR-Participant pursuant to para. 2 and 3a,
8. administrative authorities and courts and
9. other natural or legal persons, who are not expressly authorized under this Federal Act, and for any other purpose not expressly specified to be admissible according to this Federal Act.

(3a) EHR-Healthcare Providers, who are employers and are involved in the treatment or healthcare of EHR-Participants, who are their employees or employed by them, may use their EHR-Health Data only if they

1. have explicitly informed in advance the EHR-Participants about their participants' rights under sect. 16 and
2. have ensured by technical means, that only these people of EHR-Healthcare Providers have access to EHR-Health Data, who are involved in the specific treatment or healthcare process of the particular EHR-Participant.

(4) EHR-Healthcare Providers, the EHR-Ombudsman and its service providers and employees – these are employees and people in an employee-related (similar service contractor) relationship – have to keep secret EHR-Health Data, that were entrusted or made accessible to them because of their professional employment, without prejudice to any other legal obligations of secrecy.

(5) The Federal Minister of Health assumes the registration duty of the EHR-Healthcare Providers according to sect. 17 [DPA 2000](#).

Principles on the Participation in EHR

Section 15. (1) EHR-Participants are all natural persons who

1. are registered with the Patient Index pursuant to sect. 18 and are therefore at least those people who are registered with the data applications of the Federation of the Austrian Social Insurance Carriers pursuant to sect. 31 para. 4 no. 3 lit. a of the General Social Insurance Law (GSIL) or in the Supplementary Register pursuant to sect. 6 para. 4 E-GovA and
2. have not opted out from EHR (para. 2).

(2) The participation in EHR may be generally objected at any time (Opt-out). Objecting EHR-Participants have to indicate, whether this objection relates to all or just some kinds of EHR-Health Data (sect. 2 no. 9). The general objection may be given

1. in writing to Opt-out Offices according to sect. 28 para. 7 no. 2 or
2. electronically via the e-Health Access Point (sect. 23),

provided, that both the unique identity of the person, not willing to participate in EHR, and the authenticity of the declaration can be checked. The declaration of objection needs to be confirmed. The Federal Minister of Health shall establish Opt-out Offices by ordinance according to sect. 28 para. 2 no. 7, whereas more detailed rules on their responsibilities and to ensure the participants' rights shall be given.

(3) All references and EHR-Health Data including medication data, already stored in the registries at the time of objection (para. 2) and subject of this objection, need to be deleted; if deleting is prohibited by statutory documentation requirements or sect. 22 para. 5 no. 1, the references shall be rendered inaccessible for EHR.

(4) General objection (Opt-out) pursuant to para. 2 may be revoked at any time. During valid objection, references that make EHR-Health Data accessible to EHR must not be stored according to sect. 20 para. 2 first sentence. EHR-Participants are not entitled to have references to their EHR-Health Data stored for periods of valid objection pursuant to para. 2 and sect. 16 para. 2 no. 2.

Fundamental Rights of EHR-Participants

Section 16. (1) EHR-Participants are entitled either electronically by way of the e-Health Access Point (sect. 23) or by written statement to the EHR-Ombudsman (sect. 17), to

1. obtain information concerning their EHR-Health Data as well as their log data according to sect. 22 para. 2 and
2. set individual access rights pursuant to sect. 21 para. 3 by

- a) hiding or displaying electronic references and EHR-Health Data including medication data for EHR-Healthcare Providers or deleting these data; if deleting is prohibited by statutory documentation requirements or sect. 22 para. 5 no. 1, the references shall be rendered inaccessible for EHR or
 - b) reducing the access periods pursuant to sect. 18 para. 6 or
 - c) nominating according to sect. 18 para. 7 an especially trusted EHR-Healthcare Provider, provided that the EHR-Healthcare Provider agreed to this nomination.
- (2) In relation to their treating or supervising EHR-Healthcare Providers EHR-Participants are entitled to:
1. demand the recording of medication data (sect. 2 no. 9 lit. b) as well as of references to EHR-Health Data (sect. 2 no. 9 lit. a) pursuant to sect. 20 para. 2 first sentence, in conjunction with sect. 13 para. 3 and 4, as well as
 2. object the inclusion of references and EHR-Health Data including individual medication data for a concrete treatment or care case unless this is prohibited by other statutory documentation requirements. The EHR-Participants have to be informed about this right, particularly in case of EHR-Health Data related to
 - a) HIV infections,
 - b) mental illnesses,
 - c) data according to sect. 71a para. 1 of the Gene Technology Act or
 - d) abortions.
- (3) Persons
1. objecting their participation in EHR pursuant to sect. 15 para. 2 or
 2. exercising their participants' rights,
- must neither experience disadvantages regarding the access to healthcare nor in terms of cost apportionment. However, responsibility resides with them, if for this reason a due diligent EHR-Healthcare Provider is not aware of essential circumstances concerning the treatment or care. EHR-Healthcare Providers are not obliged to ask EHR-Participants about their exercise of participants' rights.
- (4) EHR-Healthcare Providers have to inform about the provisions of para. 1 to 3 by means of easily readable, visible and accessible posters in their premises. As part of their conferred powers, the statutory representation bodies for freelance Healthcare Providers have to provide the EHR-Healthcare Providers with such posters.
- (5) The Minister of Health has to continually publish information about the current state of EHR and to inform the persons concerned about their rights.

E-Medication

Section 16a. (1) Until December 31st 2014 and under the responsibility of the Federal Minister of Health ("scope of conferred powers") the Federation of Austrian Social Insurance Carriers shall establish and operate from this date on an information system on prescribed and dispensed medication ("e-Medication") as EHR-application. The information system shall provide an overview of the medication prescribed and dispensed to EHR-Participants and EHR-Healthcare Providers pursuant to sect. 2 no. 10, while respecting the participants' rights under sect. 16. To this end EHR-Healthcare Providers must – in accordance with their obligations defined in this Federal Act – store EHR-Health Data according to sect. 2 no. 9 lit. b in this information system, unless otherwise excluded due to the exercise of participants' rights. EHR-Healthcare Providers are in charge of adverse drug reaction testing, which is not subject of the information system.

(2) The operation of the e-Medication system may not interfere with the provision of treatment or healthcare services for EHR-Participants, particularly the doctors' freedom of therapy.

(3) In case that EHR-Participants are identified according to sect. 18 para. 4 no. 4, the recording of medication data is the only legitimate use of these data.

EHR-Ombudsman

Section 17. (1) The EHR-Ombudsman (sect. 2 no. 14) has to be established by ordinance of the Federal Minister of Health (sect. 28 para. 2 no. 8), whereas more detailed rules on the performance of the duties under para. 2, and to ensure the EHR-Participants' rights shall be laid down.

(2) The Federal Minister of Health shall operate the EHR-Ombudsman. The object of the EHR-Ombudsman is to inform, advise and assist persons concerned in matters of EHR, especially regarding the enforcement of participants' rights and in matters of data protection. To this end, the EHR-Ombudsman must – as a focal point for the EHR-Participants – grant any requested information necessary to determine the data controller, who is responsible for the data processing in EHR within two weeks. While exercising their duties especially regarding information, advice and support, employees of the EHR-Ombudsman are free from instructions of the Federal Minister of Health. Access to EHR-Health Data by the EHR-Ombudsman shall be

logged. The responsibilities of the Data Protection Commission [German: “*Datenschutzkommission*” – cf. <http://www.dsk.gv.at>] remain unaffected of this provision.

(3) The EHR-Ombudsman shall support the EHR-System Partners in the development of participants’ rights and data protection.

(4) Persons who are working on behalf of the EHR-Ombudsman may at the EHR-Participants’ request act as representatives for them in accordance with sect. 5 para. 3 E-GovA. At the request of the persons working on behalf of the EHR-Ombudsman the sourcePIN Register Authority shall provide ssPINs instead of sourcePINs of the person represented.

Authorization of EHR-Participants

Section 18. (1) Under the responsibility of the Federal Minister of Health (“scope of conferred powers”) the Federation of Austrian Social Insurance Carriers shall establish and operate a Patient Index. This serves:

1. the verification of the unique identity (sect. 2 no. 2 E-GovA) of natural persons in the context of EHR or other e-health-applications and
2. the localization of Registries, in which references to EHR-Health Data of these individuals can be found.

(2) The following data of natural persons shall be processed in the Patient Index:

1. name information:
 - a) first name (s)
 - b) family name or surname
 - c) birth name
 - d) academic degrees
2. personal characteristics:
 - a) date of birth
 - b) place of birth, if available
 - c) gender
 - d) date of death, if available
 - e) nationality
3. address data
4. identity data:
 - a) social security number
 - b) local patients’ IDs
 - c) ssPIN of the health area
 - d) data of the European Health Insurance Card (EHIC) not enlisted in nos. 1 to 3
 - e) other public identifiers.

(3) The data referred to under para. 2 shall mainly be collected from the data applications of the Federation of Austrian Social Insurance Carriers pursuant to sect. 31 para. 4 no. 3 lit. a GSIL and from the Supplementary Register pursuant to sect. 6 para. 4 E-GovA.

(4) The EHR-Participants’ (sect. 14 para. 1 no. 1) identity shall be verified in electronic form and through their participation. Therefore the identity data registered with the Patient Index needs to be compared with the identity data collected during identification. The identity data can be collected by

1. electronically verifying the validity of the e-card and reading data from the e-card via the e-card system (sects. 31a et sqq. GSIL) or
2. using a citizen card (sect. 2 no. 10 E-GovA) or
3. using identity data of a unambiguously identified natural person according to sect. 4 para. 2, which are stored at a EHR-Healthcare Provider pursuant to sect. 2 no. 10 lit. d and e, provided that the IT-Security Policy according to sect. 8 technically assures, that EHR-Health Data is only used for purposes laid down in sect. 14 para. 2 no. 1 and identification of EHR-Participants is verified or
4. using data of a electronic or otherwise unique prescription or referral (sect. 14 para. 2 no. 1 lit. b), if the identity data are not collected according to nos. 1 to 3.

(5) Cases of objection pursuant to sect. 16 para. 2 shall be documented in the same step of the procedure as collecting the identity data via the e-card system (sects. 31a et sqq. GSIL), but technically separated from its data flows.

(6) The verification of the EHR-Participants’ identities (para. 4) must for reasons of accessing and using their EHR-Health Data for the purposes of sect. 14 para. 2 not be more than

1. 28 days ago, with regard to EHR-Healthcare Providers pursuant to sect. 2 no. 10 lit. a, b, d and e and the EHR-Ombudsman pursuant to sect. 2 no. 14 and
2. two hours ago, with regard to EHR-Healthcare Providers pursuant to sect. 2 no. 10 lit. c.

(7) Notwithstanding para. 6 EHR-Participants may grant to one or several especially trusted EHR-Healthcare Providers pursuant to sect. 2 no. 10 lit. a, b, c, and e, a period of up to 365 days (sect. 21 para. 2), provided that the EHR-Healthcare Providers agreed to this.

(8) Powers of representations for EHR-Participants may – except for the cases of sect. 17 para. 4 – electronically be only registered according to sect. 5 para. 1 E-GovA, whereas:

1. the respective ssPIN of the EHR-Participant shall be used instead of his/her sourcePIN and
2. the permission to access EHR needs to be registered separately.

(9) Ten years after knowledge of the date of death of an EHR-Participant the Federation of Austrian Social Insurance Carriers has to automatically delete the patient data stored in the Patient Index.

Authorization of EHR-Healthcare Providers and the EHR-Ombudsman

Section 19. (1) To verify the identity of EHR-Healthcare Providers and the EHR-Ombudsman the Federal Minister of Health has to set up and operate a Healthcare Provider Index [German: “*Gesundheitsdiensteanbieterindex (GDA-Index)*”]. The data recorded in the Healthcare Provider Index shall be collected from the EHDS and has to include the information pursuant to sect. 10 para. 1 no. 1 to 8.

(2) The identity of EHR-Healthcare Providers and the EHR-Ombudsman shall be determined by collecting the data pursuant to sect. 10 para. 1 no. 1 to 8, whereas these data is to be collected

1. from appropriate identification cards of the e-card system (sect. 31a et sqq. GSIL) or
2. by using a citizen card (sect. 2 no. 10 E-GovA) or
3. by using electronic signatures, which must be traceable to qualified certificates.

(3) The identity determined according to para. 2 shall be verified electronically by comparing the data collected according to para. 2 with the data registered with the Healthcare Provider Index.

Storage of EHR-Health Data

Section 20. (1) Unless sects. 15 para. 2 and 16 para. 2 no. 2 regulate otherwise, EHR-Healthcare Providers shall save (sect. 13 para. 3) EHR-Health Data in storages according to sect. 28 para. 2 no. 5, which need to be located in the territory of the European Union. Already saved EHR-Health Data may not be altered. If circumstances emerge, that could cause significant changes in the course of treatment, updated versions have to be saved additionally. EHR-Healthcare Providers are controllers [translator’s note: data controllers according to sect. 4 no. 4 [DPA 2000](#)] of the storage.

(2) Unless sects. 15 para. 2 and 16 para. 2 no. 2 regulate otherwise, EHR-Healthcare Providers have to save (sect. 13 para. 3) [translator’s note: “Electronic References to EHR-Health Data” was missing in the original text] in Registries that are located in the territory of the European Union. This does not apply, when EHR-Participants have objected the registration of references. EHR-Healthcare Providers are controllers [translator’s note: data controllers according to sect. 4 no. 4 [DPA 2000](#)] of the storage.

(3) Regardless of other statutory documentation requirements, EHR-Health Data as well as electronic references to it shall be stored decentralized for ten years. Thereafter the electronic references and EHR-Health Data shall be deleted by the operators of the appropriate data storages pursuant to sect. 28 para. 2 no. 5 and Registries; if deleting is prohibited by statutory documentation requirements or sect. 22 para. 5 no. 1, the references shall be rendered inaccessible for EHR.

(4) Notwithstanding paras. 2 and 3 medication data pursuant to sect. 2 no. 9 lit. b shall be

1. stored centrally in EHR without registering electronic references and
2. deleted automatically by the entity in charge of the technical operation one year from dispensation.

(5) Electronic references shall be created automatically and shall contain:

1. data relating to the EHR-Participants:
 - a) the ssPIN of the health area of the EHR- participant or
 - b) local patients identifiers,
2. data relating to the EHR-Healthcare Providers:
 - a) the unique identifier of the EHR-Healthcare Provider being responsible for the registration of the EHR-Health Data,
 - b) the natural person, who saved the EHR-Health Data to EHR,
3. data relating to the EHR-Health Data:
 - a) the storage location of the EHR-Health Data,
 - b) the unique identifier of the EHR-Health Data,

- c) the date and time of the creation of the EHR-Health Data,
- d) if needed, a reference to earlier versions of this EHR-Health Data,
- e) if applicable, a structured reference to the medical name of the EHR-Health Data as well as
- f) the date and time at which the electronic reference to EHR-Health Data was registered with a Registry.

Access Control Centre

Section 21. (1) The Access Control Centre shall be set up and operated by the EHR-System Partners. The Access Control Centre shall facilitate the administration of access authorizations and the access itself to EHR-Health Data. Without access authorization neither EHR-Health Data nor references to such may be displayed.

(2) According to the general access authorizations, that determine which standard requests shall be allowed, access is granted to:

1. members of the medical profession (sect. 2 no. 10 lit. a) for all EHR-Health Data (sect. 2 no. 9),
2. members of the dental profession (sect. 2 no. 10 lit. b) for EHR-Health Data according to sect. 2 no. 9 lit. a and b,
3. pharmacies (sect. 2 no. 10 lit. c) for medication data according to sect. 2 no. 9 lit. b,
4. hospitals (sect. 2 no. 10 lit. d) for all EHR-Health Data (sect. 2 no. 9),
5. nursing institutions (sect. 2 no. 10 lit. e) for all EHR-Health Data (sect. 2 no. 9),
6. representatives pursuant to sect. 14 para. 2 no. 2 lit. b for all EHR-Health Data (sect. 2 no. 9) as well as
7. employees of the EHR-Ombudsman for all EHR-Health Data (sect. 2 no. 9).

(3) EHR-Participants are allowed by means of individual access authorizations to:

1. hide or display as well as to delete electronic references and EHR-Health Data including medication data for EHR-Healthcare Providers within the limits of the general access authorizations; if deleting is prohibited by statutory documentation requirements or sect. 22 para. 5 no. 1, the references shall be rendered inaccessible for EHR or
2. shorten the periods for existing access rights pursuant to sect. 18 para. 6 or
3. nominate according to sect. 18 para. 7 an especially trusted EHR-Healthcare Provider, provided that the EHR-Healthcare Provider agreed to this nomination.

Logging System

Section 22. (1) The Logging System shall be set up and operated by the EHR-System Partners. The Logging System serves the documentation and traceability of the use of EHR-Health Data.

(2) Any use of EHR-Health Data in the context of EHR has to be logged according to sect. 14 [DPA 2000](#), including the following information:

1. date and time of use,
2. the unique log-transaction number,
3. type of the use process,
4. the unique electronic identity of the EHR-Healthcare Provider or the EHR-Ombudsman that has triggered the process,
5. the name of the natural person, who has actually used the EHR-Health Data,
6. the unique identifier of the used EHR-Health Data,
7. the query criteria as well as
8. the error messages for queries, that result in error messages.

(3) The log data pursuant to para. 2 shall be stored, kept readable and available for three years from access.

(4) According to sect. 16 para. 1 no. 1 EHR-Participants are entitled to access and use the log data relating to them. The log data shall be presented in a simple and clearly arranged manner.

(5) The log data according to para. 2 must not be used in a personally traceable way, except:

1. for administrative or judicial enforcement and defence of asserted legal claims or
2. for ensuring the use according to the Roles (sect. 5) or
3. for information about updated EHR-Health Data or
4. for any technical necessity or
5. in an indirect personal way for optimization and evaluation of EHR.

(6) EHR-Healthcare Providers pursuant to sect. 2 no. 10 lit. a and c are entitled to access and use log data that refers to their EHR usage.

(7) The EHR-System Partners shall implement EHR in such a way, that changes to EHR-Health Data, that could cause a significant change in treatment or care (sect. 20 para. 1, third sentence), shall, in accordance with

sect. 21 para. 3, be made available in EHR to the EHR-Healthcare Providers, who have accessed the EHR-Health Data in the non-updated version.

e-Health Access Point

Section 23. (1) The Minister of Health shall operate a publicly accessible health portal for the provision of quality-assured health-related information to the public.

(2) This health portal shall serve as access point to EHR (e-Health Access Point) and has to

1. ensure the verification of the unique identity of EHR-Participants according to sect. 18 para. 4 no. 2 and
2. offer functions to protect the participants' rights according to sect. 15 and 16.

(3) EHR-Healthcare Providers may access health information related to EHR-Participants via the e-Health Access Point only in compliance with the provisions of this Federal Act.

(4) The health portal may also offer access to other health-related electronic services.

Right to Use the EHR-Infrastructure

Section 24. (1) In order to maintain the financial balance of the social security system the use of the following EHR-components

1. Patient Index (sect. 18),
2. Healthcare Provider Index (sect. 19),
3. Registry (sect. 20),
4. Data Storage (sect. 20),
5. Access Control Centre (sect. 21),
6. Logging system (sect. 22) and
7. E-Health Access Point (sect. 23)

is free for the collection of EHR-Health Data that are made available by EHR, according to sect. 14 para. 2.

(2) Regardless of their legal status, operators of data storages and Registries must not be excluded as service providers for EHR, provided that they meet the requirements of sect. 28 para. 2.

Fifth Part

Final Provisions

Administrative Penalties

Section 25. (1) Anyone who

1. fails contrary to sect. 3 para. 3 to technically ensure that Health Data can only be used in legitimate Roles, or
2. fails contrary to sect. 4 to identify the Healthcare Providers or individuals whose health information should be disclosed, or
3. fails contrary to sect. 5 para. 1 to verify or proof the Role(s) of Healthcare Providers, or
4. fails contrary to sect. 6 to ensure the confidentiality of Health Data by data security measures, or
5. fails contrary to sect. 7 to verify or proof the integrity of electronic Health Data, or
6. places persons contrary to sect. 16 para. 3 at a disadvantage regarding the access to healthcare or in terms of cost apportionment, or
7. makes use of the facilitated conditions as laid down in sect. 27 para. 10 or 12, without meeting their requirements, or
8. in his role as an EHR-Healthcare Provider intentionally uses EHR-Health Data, without being entitled to,

commits an administrative offense and shall be subject to a financial penalty of up to EUR 10 000, provided that the deed does not fulfil the conditions for a criminal offence or is subject under a legal specification to the threat of penalty of greater severity.

(2) Provided that the deed does not fulfil the conditions for a criminal offence or is subject under a legal specification to the threat of penalty of greater severity, similar punishment shall be imposed on anyone who

1. intentionally uses EHR-Health Data as a staff member of the EHR-Ombudsman without being entitled to, or
2. uses EHR-Health Data as a servant of the Federal Ministry of Health without being entitled to.

(3) In the cases of para. 1 no. 8 and para. 2, also the attempt is punishable.

Entry into Force

Section 26. (1) This Federal Act shall enter into force on January 1st 2013.

(2) The Health Telematics Act, Federal Law Gazette I No. 179/2004, as amended by the Federal Law, Federal Law Gazette I No. 36/2010, shall expire with effect from December 31st 2012.

Transitional Provisions

Section 27. (1) Until December 31st 2013 the Federal Minister of Health shall set up and provide the e-Health Access Point (sect. 23), the Opt-out Offices (sect. 28 para. 2 no. 7) and the EHR-Ombudsman (sect. 17) according to the technical availability so that the exercise of the participants' rights is guaranteed and can be done in a timely manner. From that time on, EHR may be used.

(2) Unless an ordinance based upon sect. 28 para. 2 no. 4 specifies a later date, sect. 13 para. 3 shall apply from January 1st 2015 on, for

1. hospitals pursuant to sect. 3 para. 2b of the Hospitals and Sanatoriums Law, whose costs are settled by regional health funds,
2. the General Accident Insurance Institution, as far as it operates hospitals according to sect. 24 para. 2 GSIL and
3. institutions of care pursuant to sect. 2 no. 10 lit. e,

insofar as the use of EHR-components (sect. 24) for the usage of EHR-Health Data is technically possible.

(3) Unless an ordinance based upon sect. 28 para. 2 no. 4 specifies a later date, sect. 13 para. 3 shall apply from July 1st 2016 on, for

1. pharmacies pursuant to sect. 1 of the Pharmacy Act,
2. freelance doctors,
3. group practices and
4. independent clinics pursuant to sect. 3a HSL,

insofar as the use of EHR-components (sect. 24) is technically possible for the usage of EHR-Health Data. This does not apply to self-employed physicians, group practices and independent outpatient clinics (sect. 3a HSL) with regard to the obligation according to sect. 13 para. 3 no. 4 and 6, if those EHR-Healthcare Providers are not in a contractual relationship to any statutory social insurance carrier.

(4) Unless an ordinance based upon sect. 28 para. 2 no. 4 specifies a later date, sect. 13 para. 3 shall apply from July 1st 2017 on, for private hospitals pursuant to sect. 1 para. 2 of the Private Hospitals Financing Fund Act (PHFFA), Federal Law Gazette I No. 165/2004, insofar as the use of EHR-components (sect. 24) for the usage of EHR-Health Data is technically possible.

(5) From January 1st 2017 on,

1. living wills,
2. powers of attorney and
3. the data of the medical registers according to sect. 2 no. 9 lit. e

have to be provided in the EHR, according to technical availability.

(6) Unless an ordinance based upon sect. 28 para. 2 no. 4 specifies a later date, sect. 13 para. 3 shall apply from July 1st 2022 on, for

1. freelance dentists,
2. dental group practices and
3. independent dental clinics.

(7) Unless an ordinance based upon sect. 28 para. 2 no. 4 specifies a later date, a search in the document metadata by means of the document register has to be possible in any case at the latest by January 1st 2015. This shall be regarded a standard according to sect. 28 para. 2 no. 1 lit. a to c.

(8) Unless an ordinance based upon sect. 28 para. 2 no. 4 specifies a later date, either a uniform structure and organization of content, so that content can be included in medical information systems, or at least a standardization of the structure of content has to be ensured at the latest by January 1st 2015. This shall be regarded a standard according to sect. 28 para. 2 no. 1 lit. a to c.

(9) Unless an ordinance based upon sect. 28 para. 2 no. 4 specifies a later date, the information made available by EHR has to be encoded according to standardized criteria, that are jointly developed by the EHR-System Partners together with the legal interest groups, insofar as they would be affected in performing their tasks, at the latest by January 1st 2018. This shall be regarded a standard according to sect. 28 para. 2 no. 1 lit. a to c.

(10) If proof or verification of identity, Roles and integrity are not feasible in accordance with the provisions of the second part (directed and undirected communication), in particular due to the absence of existing technical infrastructure, Health Data may only be transferred if at least the identities and the relevant Roles of the parties involved in the transfer are mutually confirmed by

1. personal contact or

2. contact by telephone or
3. contractual provisions or
4. queries of electronic directories
 - a) of the Austrian Medical Association or
 - b) of the Austrian Dental Association or
 - c) of the Austrian Midwives Board or
 - d) of the Austrian Chamber of Pharmacists or
 - e) of the Federation of Austrian Social Insurance Carriers or
 - f) of the Federal Ministry of Health.

(11) In the events of para. 10 no. 1 and 2 and prior to the first transfer of Health Data between the participating Healthcare Providers, the following data shall be logged:

1. date and type of contact,
2. the full names and relevant Roles of the Healthcare Providers involved in the transfer,
3. the contact details of the involved Healthcare Providers as well as
4. the details of the natural persons being involved in the contacting.

The contact details need to be kept up to date.

(12) The transfer of Health Data may exceptionally be performed by fax, provided that the requirements of para. 10 no. 1 to 3 are met, and if

1. the fax ports (including printer to fax connections) are protected from unauthorized access and use,
2. the numbers, particularly the saved numbers, are regularly checked for being up-to-date, especially after changes in technical equipment and reinstalling of fax devices,
3. automatic forwarding to others than the Healthcare Providers themselves, is disabled,
4. the security mechanisms, supported by the device, are used and
5. if available, remote maintenance functions are only activated for the agreed duration of the remote maintenance.

(13) The facilitated conditions under para. 10 and 12 cannot be taken advantage of, if the use of Health Data in accordance with the provisions of the second part is reasonable from the level of technical possibilities and economic acceptability (sect. 14 para. 1 [DPA 2000](#)).

(14) When communicating Health Data the facilitated conditions pursuant to para. 10 or 12 apply to all participating Healthcare Providers if these conditions can be applied to at least one of the participating Healthcare Providers.

(15) Until June 30th 2016 sect. 6 shall not be applied to the transmission of Health Data via radio for the purpose of emergency organization at emergency services.

Regulatory Powers

Section 28. (1) The Minister of Health shall determine by means of ordinance based upon this Act:

1. the Roles of Healthcare Providers, whereas the requirements for establishing additional Roles have to be forwarded to the Federal Minister of Health by the respective Registration Body, including
 - a) a description of the nature and scope of the activities carried out,
 - b) the conditions that must be met for the pursuit of such activities,
 - c) the name of the legal basis from which the authorization for professionalism results as well as
 - d) the body, that has to decide on these authorizations,
2. after having heard a confirmation authority pursuant to sect. 19 of the Digital Signature Act, which cryptographic algorithms according to the current state of network security are suitable for encryption pursuant to sect. 6 as well as
3. the details of the registration process pursuant to sect. 9, in particular the technical requirements, the data formats, the periodicity of the data update and the safety requirements that have to be observed.

(2) With regard to the Fourth Part of this Act (EHR), the Federal Minister of Health shall further specify by means of ordinance based upon this Act:

1. the structure, format and standards pursuant to sect. 27 paras. 7, 8 and 9, to be used for
 - a) clinical discharge reports pursuant to sect. 2 no. 9 lit. a sublit. aa,
 - b) laboratory findings pursuant to sect. 2 no. 9 lit. a sublit. bb,
 - c) results of diagnostic imaging, including any image data pursuant to sect. 2 no. 9 lit. a sublit. cc and
 - d) medication data according to sect. 2 no. 9 lit. b

in EHR, whereas internationally recognized standards, the economic justifiability as well as the state of technical possibilities of the EHR-Healthcare Provider shall be considered regarding the level of detail of the structures,

2. which interaction-relevant, non-prescription drugs pursuant to sect. 2 no. 9 lit. b should be registered with EHR,
3. the structure and the format, for
 - a) the following types of findings (sect. 2 no. 9 lit. a sublit. dd):
 - aa) pathology findings by specialists for pathology and hospitals in the course of outpatient care,
 - bb) other medical reports in the course of outpatient care (outpatient department, independent outpatient clinics, settled medical specialist area) and
 - cc) outpatient care reports as well as
 - b) data automatically generated according to art. 14 para. 2 lit. b sublit. i of the Directive 2011/24/EU on the application of patients' rights in cross-border health care (sect. 2 no. 9 lit. f) [translator's note: "patient summary"],

that shall be used in the context of EHR, whereas structure and format shall be determined according to the criteria of no. 1 and based on a uniform standardization process with the participation of the EHR-System Partners as well as statutory representation bodies, to the extent they are concerned in perceiving their assigned tasks,

4. the date from which on the data referred to in no. 1 lit. a to d and in no. 3 lit. a and b shall be stored in and collected from EHR according to sect. 13 paras. 2 and 3 in conjunction with para. 1 no. 1,
5. standards for the search function pursuant to sect. 13 para. 5, the times of availability, the security requirements and access protection of the EHR-components, while it must be guaranteed, that maintenance is logged and allows personal data only to be displayed encrypted or in accordance with a four-eye-principle,
6. scope and level of detail of the information and minimum requirements for the content of the posters pursuant to sect. 16 para. 4,
7. the bodies, to which the objection pursuant to sect. 15 para. 2 needs to be declared and which support EHR-Participants in exercising their participants' rights, sufficiently early to allow for the objection prior to the initial operation of EHR,
8. the establishment of an EHR-Ombudsman according to sect. 17,
9. the establishment of terminals with portal functionality (sect. 23) and of service centres by the EHR system partners,
10. the date from which on a standardized nomenclature must be used for EHR-Health Data (sect. 2 para. 9),
11. the operator [translator's note: "pursuant to sect. 50 [DPA 2000](#)"] of the Access Control Centre pursuant to sect. 21 and the operator of the Logging System pursuant to sect. 22 and
12. the beginning and end of test phases for EHR in conjunction with nos. 1, 3 and 4 as well as an independent evaluation, if necessary.

- (3) Prior to issuing an ordinance according to para. 2

[translator's note: the following enumeration is not included in the German original]

1. the legal entities of hospitals pursuant to sect. 3 para. 2b of the Hospitals and Sanatoriums Law, whose costs are settled by regional health funds,
2. the General Accident Insurance Institution, as far as it operates hospitals according to sect. 24 para. 2 GSIL,
3. the Austrian Medical Association,
4. the Austrian Pharmacists' Chamber,
5. the Austrian Dental Chamber,
6. the Chamber of Commerce Austria,
7. the Federation of Austrian Social Insurance Carriers,
8. the Association of patient advocates and
9. the states

shall be heard.

(4) The Federal Minister of Health shall determine by means of ordinance the date from which on the transfer of Health Data at the facilitated conditions of sect. 27 para. 10 and 12 is definitely prohibited by law, after having heard the affected statutory representation bodies by taking into consideration sect. 27 para. 13.

(5) With regard to the enforcement of the sect. 16a and 18 the Federation of Austrian Social Insurance Carriers is subject to the instructions of the Federal Minister of Health.

Enactment and Entry into Force of Ordinances

Section 29. Ordinances based upon this Federal Act may already be adopted from the day on following the promulgation of executed laws provisions, but they may not come into force prior to the executed statutory provisions.

References

Section 30. Unless explicitly otherwise provided, provisions of other Federal Acts referred to by this Federal Act shall apply as amended.

Enforcement

Section 31. Enforcement of this Act shall be entrusted to the Federal Minister of Health.

Article 2

Amendment of the General Social Insurance Law

The General Social Insurance Law, Federal Law Gazette No. 189/1955, as amended by the Federal Law Gazette I No. 89/2012 is amended as follows:

1. In sect. 31d the term "planning" is omitted.

2. Sect. 81 para. 1 is extended by the following sentence:

“This information shall also inform the insured and their relatives, that EHR-Participants may generally opt-out from EHR at any time according to sect. 15 para. 2 of the Health Telematics Act 2012 (HTA 2012), Federal Law Gazette I No. 111/2012, inspect their Health Data processed in EHR at any time (sect. 16 para. 1 no. 1 HTA 2012), demand the recording of personal Health Data in the context of EHR (sect. 16 para. 2 no. 1 HTA 2012), refrain from using personal Health Data in the concrete treatment encounter (sect. 16 para. 2 no. 2 HTA 2012), determine the individual access control lists for Healthcare Providers and EHR-Health Data (sect. 16 para. 1 no. 2 HTA 2012) and use the services of an EHR-Ombudsman (sect. 17 HTA 2012).”

Article 3

Amendment of the Act on Social Security for Persons Engaged in Industry

The Act on Social Security for Persons Engaged in Industry, Federal Law Gazette No. 560/1978, as amended by Federal Law Gazette I No. 76/2012 is amended as follows:

1. Sect. 43 para. 1 is extended by the following sentence:

“This information shall also inform the insured and their relatives, that EHR-Participants may generally opt-out from EHR at any time according to sect. 15 para. 2 of the Health Telematics Act 2012 (HTA 2012), Federal Law Gazette I No. 111/2012, inspect their Health Data processed in EHR at any time (sect. 16 para. 1 no. 1 HTA 2012), demand the recording of personal Health Data in the context of EHR (sect. 16 para. 2 no. 1 HTA 2012), refrain from using personal Health Data in the concrete treatment encounter (sect. 16 para. 2 no. 2 HTA 2012), determine the individual access control lists for Healthcare Providers and EHR-Health Data (sect. 16 para. 1 no. 2 HTA 2012) and use the services of an EHR-Ombudsman (sect. 17 HTA 2012).”

Article 4

Amendment of the Act on Social Security for Farmers

The Act on Social Security for Farmers, Federal Law Gazette No. 559/1978, as amended by Federal Law Gazette I No. 76/2012 is amended as follows:

1. Sect. 41 para. 1 is extended by the following sentence:

“This information shall also inform the insured and their relatives, that EHR-Participants may generally opt-out from EHR at any time according to sect. 15 para. 2 of the Health Telematics Act 2012 (HTA 2012), Federal Law Gazette I No. 111/2012, inspect their Health Data processed in EHR at any time (sect. 16 para. 1 no. 1 HTA 2012), demand the recording of personal Health Data in the context of EHR (sect. 16 para. 2 no. 1 HTA 2012), refrain from using personal Health Data in the concrete treatment encounter (sect. 16 para. 2 no. 2 HTA 2012), determine the individual access control lists for Healthcare Providers and EHR-Health Data (sect. 16 para. 1 no. 2 HTA 2012) and use the services of an EHR-Ombudsman (sect. 17 HTA 2012).”

Article 5

Amendment of the Act on Health and Accident Insurance for Civil Servants

The Officials' Health and Accident Insurance Act, Federal Law Gazette No. 200/1967, as amended by Federal Law Gazette I No. 35/2012 is amended as follows:

1. Sect. 27 para. 1 is extended by the following sentence:

“This information shall also inform the insured and their relatives, that EHR-Participants may generally opt-out from EHR at any time according to sect. 15 para. 2 of the Health Telematics Act 2012 (HTA 2012), Federal Law Gazette I No. 111/2012, inspect their Health Data processed in EHR at any time (sect. 16 para. 1 no. 1 HTA 2012), demand the recording of personal Health Data in the context of EHR (sect. 16 para. 2 no. 1 HTA 2012), refrain from using personal Health Data in the concrete treatment encounter (sect. 16 para. 2 no. 2 HTA 2012), determine the individual access control lists for Healthcare Providers and EHR-Health Data (sect. 16 para. 1 no. 2 HTA 2012) and use the services of an EHR-Ombudsman (sect. 17 HTA 2012).”

Article 6

Amendment of the Gene Technology Act

The Gene Technology Act, Federal Law Gazette No. 510/1994, as amended by Federal Law Gazette I No. 13/2006, is amended as follows:

1. In sect. 71 para. 2 the term "Health Telematics Act, Federal Law Gazette I No. 179/2004" is replaced by the term "Health Telematics Act 2012, Federal Law Gazette I No. 111/2012".

2. Below sect. 112 the following sect. 113, including heading, shall be inserted:

"Entry into Force

Section 113. Sect. 71 para. 2 as amended by the Electronic Health Records Act, Federal Law Gazette I No. 111/2012 shall enter into force by January 1st 2013."

Article 7

Amendment of the Criminal Code

The Criminal Code, Federal Law Gazette No. 60/1974, as amended by Federal Law Gazette I No. 61/2012, is amended as follows:

1. In sect. 121 para. 1 the phrase "or other Healthcare Provider (sect. 2 no. 2 of the Health Telematics Act 2012, Federal Law Gazette I No. 111/2012)" is inserted after the phrase "of a hospital".

2. Below section 121 para. 1 the following para. 1a is inserted:

"(1a) Similar penalties shall be imposed on anyone, who unlawfully asks for the revelation (inspection or exploitation) of personal health secrets while intending to harm or at least endanger the income or career advancement of the data subject in the event of refusal."