Current and Future Settings of Austrian Legislation Regarding Electronic Health Records (EHR)

Sebastian Reimer[1]

[1]CEO Intelligent Law and Internet Applications, Wien, Austria

Abstract

In the context of the European large-scale pilot on e-health ("epSOS") numerous discussions on the implementation of a pan-European e-health infrastructure have been held. They all proved that differences among the national e-health legislations pose serious obstacles to the European-wide exchange of personal health data. Even if it is very difficult to meet all requirements of the involved countries, this is an absolute pre-condition for a smooth exchange of patient data. The unlawful usage of personal health data can result in the loss of reputation, administrative fines and the need to restructure internal workflows at high costs. Being aware of the current legal framework avoids such. To know about future innovations to the legal framework facilitates strategic decisions and enables to take over leadership in the innovative process.

Recognising this, the aim of this paper is to provide a better understanding of the current Austrian e-health legislation and the innovations to come, inspired by national and European projects. As development is still ongoing at national and European level, the information provided, especially regarding the outlook, is to be understood as of April 2012.

Keywords

computer security, epSOS, electronic health records, health telematics, personal identifiers

Correspondence to:

Sebastian Reimer
CEO Intelligent Law and Internet Applications
Address: A-1030 Wien, Rasumofskygasse 30/1/8
E–mail: office@ilia.ch

EJBI 2012; 8(2):11–28
recieved: June 20, 2011
accepted: February 20, 2012
published: June 15, 2012

1 Status Quo of Austrian E-Health Legislation

The main legal provisions, relevant for the use of personal electronic health data and therefore the establishment of electronic health records (EHR), are to be found in:

- the Data Protection Act 2000 (DPA 2000) [1],
- the Health Telematics Act (HTA) [2],
- the E-Government Act (EGovA) [3],
- the Doctors Code 1998 (DC 1998) [4],
- the General Social Insurance Law (GSIL) [5],
- the Insurance Agreement Act (IAA) [6] and
- the Genetic Engineering Act (GEA) [7].

As these acts are all ordinary statutory law, they have to meet the requirements of higher-ranking law as for example national constitutional law or European law.

1.1 Austrian Constitutional Law Framework

The constitutional provisions of Austria are the highest ranked national provisions and for two reasons of interest: on the one hand they define the binding regulatory framework for future EHR provisions at ordinary law level. On the other hand some of them lay down directly applicable rights, that protect citizens, foreigners and even private law bodies against improper government action ("fundamental rights").

Usually these fundamental rights grant protection solely against infringements by acts of public authorities, as for example rulings, ordinances or ordinary statutory laws. However, there is one fundamental right in Austria – the right to privacy – that also protects against infringe-

ments by private law entities ("third party effect") as for example medical doctors, other healthcare providers or companies. They can be both: plaintiffs and defendants due to privacy infringements. Being informed about basic rights strengthens argumentation, especially when arguing with official authorities. The following fundamental rights are the most relevant ones for e-health:

- the fundamental right to privacy (Sect. 1 DPA 2000 [1]),
- the fundamental right to private and family life (Art. 8 European Convention on Human Rights – ECHR [8]),
- the principle of equality (Art. 2 Basic Law on the General Rights of Nationals – BLGRN [9], Art. 7 FCL [10]) and
- the protection of property (Art. 5 BLGRN [9]).

The **fundamental right to privacy** requires that the use of personal data is proportional, i.e. not excessive. Furthermore the use must:

- serve vital interests of the data subject or third persons or
- serve others' overriding legitimate interests or
- be based upon consent of the data subject.

Laws on EHR need to be legitimated by one of these rationales in order to be compliant with the fundamental right to privacy. The **principle of equality** ensures for example that all patients may receive healthcare under the same conditions regardless whether they opted out of an EHR system or not ("anti-discrimination"). Equal treatment of healthcare providers (HCP) requires that all healthcare providers face the same deadlines for adaption of their systems (hardware, software, organisation, ...) or financial burdens. The **protection of property** prevents that unreasonable financial burdens and risks are imposed on healthcare providers, e.g. high IT infrastructure investments in a short period of time.

Infringements of fundamental rights entitle the persons affected to constitutional legal suits against the government, that enacted the law, in front of the Austrian Constitutional Court. If the court finds in favour of the plaintiff, he can be reimbursed and the contested unconstitutional parts of the law, ordinance, treaty or decision are to be repealed. *Constitutional claims are often the last chance for private companies to avoid unjust burdens, especially financial burdens!*

1.2 Data Protection Law

Sect. 9 DPA 2000 [1] on the usage of sensitive data transposes Art. 8 of the Data Protection Directive (DPD) [11] into Austrian national law. Sensitive data is „data relating to natural persons concerning their racial or ethnic origin, political opinion, trade-union membership, religious or philosophical beliefs, and data concerning health or sex life" (Sect. 4.2 DPA 2000 [1]).

According to the current legal situation in Austria a specialised law as legal base for the usage of personal health data in the context of EHR does not exist. As a consequence a national EHR, with mandatory participation of all national healthcare providers, is missing. For this reason, only legal entities, that do not perform governmental tasks, as for example medical doctors, hospitals or other healthcare providers according to Art. 3.g of the Patients' Rights Directive (PRD) [12] may take the initiative and introduce or participate in existing EHR systems.

Usage of EHR systems can legally be based upon explicit consent of the patients (Sect. 9.6 DPA 2000 [1]) or medical necessity, especially regarding treatment purposes (Sect. 9.12 DPA 2000 [1]). Some of the healthcare providers, as for example medical doctors may – due to special professional duties – communicate personal data of patients only with their consent (Sect. 51.2 Doctors' Code 1998 [4]).

Working parties on national and European level have been contesting the view, that Sect. 9.12 DPA 2000 [1] on national level or Art. 8.3 DPD [11] on European level could legitimate EHR systems. The Austrian STRING Commission (Kommission für Standards und Richtlinien für den Informatikeinsatz im österreichischen Gesundheitswesen) for example, set up by the Federal Minister for Health and Women (now: Federal Minister for Health) is convinced that Sect. 9.12 DPA 2000 [1], which transposes Art. 8.3 DPD [11] into Austrian law, cannot legitimate the use of EHR, because EHR systems have not yet been in use, when Art. 8 DPD [11] was drafted and therefore cannot cover EHR systems [13].

This argument is false, as it can be verified, that EHR systems have already been discussed in the USA during the 80's of the last century [14]. A similar opinion is shared by the Art. 29 Data Protection Working Party[1] in its Working Paper 131 (WP 131) on EHR systems [16] and its Working Paper 189 (WP 189) on epSOS [17] regarding the non-applicability of Art. 8.3 DPD [11]. Both statements [13, 16] lack detailed explanations of the underlying legal grounds for the non-applicability of Art. 8.3 DPD [11]. They are discussed in more detail below in chapter 2.2.1.

[1]The Art. 29 Data Protection Working Party is an independent advisory body, composed of national representatives of each national Supervisory Authority (Art. 28 DPD [11]) and of two EU representatives. The working party regularly adopts opinions on recent data protection topics [15], among them document WP 131 [16], that deals with EHR issues.

In fact a special law on EHR systems is not necessary from the data protection point of view[2], as both of the above cited general provisions of the DPA 2000 [1], would qualify as valid legal bases for EHR systems. The Viennese Hospital Association (Wiener Krankenanstaltenverbund) – for example – has been operating a network of medical reports since 2008 [21]. Even service providers, as for example in the field of information and communication technologies (ICT), could legally introduce and operate EHR systems based upon either Sect. 9.12 DPA 2000 [1] or Art. 8.3 DPD [11], if the personal health data is decrypted available only to medical staff for treatment purposes or other persons, who are subject to a special obligation of secrecy.

1.3 Health Telematics Law

The Health Telematics Act (HTA) [2] is the most relevant EHR related law, as it explicitly deals with personal health data communicated by electronic means. It is the only Austrian law, to determine the conditions of communicating electronic personal health data in more detail. The HTA [2] is in fact a more specialised and precise part of the Austrian data protection legislation. At the current state the HTA [2] does not provide the legal basis for processing personal electronic health data, but only governs the data security requirements for lawful communication of electronic personal health data. The Austrian Health Telematics Act [2] consists of:

1. general provisions on scope and definitions, e.g. definitions of healthcare provider or health data (Part 1 HTA [2]),
2. special **data security requirements** with regard to e-health (Part 2 HTA [2]),
3. detailed regulations regarding the **e-health directory** (Part 3 HTA [2]),
4. general guidelines for **e-health information governance** (Part 3 HTA [2]) and
5. final provisions, e.g. regarding administrative offences and transitional provisions (Part 4 HTA [2]).

Hereafter the main provisions of the HTA [2] – the core e-health law in Austria – shall be described in more detail.

1.3.1 Personal Scope of the Health Telematics Act: the healthcare providers

The HTA [2] applies to healthcare providers (Gesundheitsdiensteanbieter), who are defined as „data controllers and processors for whom the regular usage of health data is part of their business“ (Sect. 2.2 HTA [2]). The Austrian definition of healthcare providers builds upon the terms of data controllers (Sect. 4.4 DPA 2000 [1])[3] and data processors (Sect. 4.5 DPA 2000 [1])[4] , which are themselves derived from the European Data Protection Directive. Not only medical doctors and their staff are regarded as healthcare providers, but also lawyers specialised on health law or even more important IT companies using personal health data are regarded as healthcare providers in the terms of the HTA [2]. Unfortunately, such a wide definition referring to the regular usage of health data as part of one's business leads to complex discussions what can be deemed "a regular usage of health data" and whether civil servants or public authorities shall also be regarded as healthcare providers or not. Due to data protection the term healthcare provider should be interpreted in an extensive manner: the wider the definition of healthcare provider, the more data controllers and processors are covered and consequently have to comply with the HTA's [2] specialised data security rules, which – in the end – would increase the level of data protection in the health sector. This notion also corresponds with the Austrian legislation on regularity in the context of the legal definition of business according to which "even a singular activity is

[2]If public authorities want to use personal data, they need an accurately formulated legal base at least at statutory law level (Sect. 1.2 DPA 2000 [1]), to be legitimated. Private law entities are regarded too as public authorities in the meaning of Sect. 1.2 DPA 2000 [1], if they can unilaterally determine others' legal positions, in a way typical for public authorities. Based upon a draft of an Austrian EHR law, Mayer [18] argued, that ELGA healthcare providers, as for example medical doctors, will have to enforce the usage of data against the will of the patients and must therefore be regarded as public authorities. Such would require a statutory law in accordance with Art. 8.2 ECHR [8, 17]. This belief is false for the following reasons:

- Medical doctors have always been obliged by law to record medical histories of their patients – in former times by means of paper files – and never have been deemed public authorities, except of course for the public health officers (Sect. 41.1 DC 1998 [4]), who decide, according to specialised provisions of statutory law, for example on the fitness of persons to hold driving permits.
- Patients are entitled to **opt out at any time**, starting one and a half year before ELGA shall be started. Such a possibility to autonomously define one's own legal position does not exist for administrative decisions, that unilaterally define one's legal position, as for example tax assessment notices. Because such decisions were enacted with power of the state (Hoheitsgewalt) it is not possible to rescind or "opt-out". The Austrian Constitutional Court ruled that the ability to issue binding instructions or perform coercive measures is a mandatory requirement for public authorities [19].
- The Austrian Constitutional Court ruled also that the legal relations among citizens are typically regarded civil law matters [20].

[3]Data controller: "natural or legal person, group of persons or organ of a territorial corporate body [German: Gebietskörperschaft] or the offices of these organs, if they decide alone or jointly with others to use data (subpara. 8), without regard whether they use the data themselves (sub-para. 8) or have it done by a service provider (sub-para. 5). They are also deemed to be controllers when the service provider instructed to carry out an order (sub-para. 5) decides to use data for this purpose (sub-para. 8) except if this was expressly prohibited or if the contractor has to decide under his own responsibility, on the basis of rules of law or codes of conduct".

[4]Data processor: "natural or legal person, group of persons or organ of a federal, state and local authority [German: Gebietskörperschaft] or the offices of these organs, if they use data only for a commissioned work".

regarded a regular activity, if one usually would expect a repetition of that activity or the activity takes more time" (Sect. 1.4 Industrial Code – IC [22]).

The national term of healthcare provider differs significantly from the Patients' Rights Directive's (PRD) [12] definition of healthcare provider[5] according to Art. 3.g PRD [12]. The more narrow PRD-term refers only to entities, that factually provide healthcare[6] (Art. 3.a PRD [12]), whereas the Austrian term refers to all entities, that use personal health data. This should be kept in mind, when applying the legal e-health framework in Austria. Medical scientists – for example – dealing with personal health data would qualify as healthcare providers according to Austrian law and would therefore be subject to the national health telematics law. However, they would never qualify as healthcare providers according to the Patients' Rights Directive [12].

1.3.2 Material Scope of the HTA: personal health data

The HTA [2] applies to the communication of **personal health data**, which is according to Sect. 4.1 DPA 2000 [1] defined as personal data about the physical and mental condition of a person, the condition and function of his/her body or parts of it, including data collected during anamnesis, for purposes of preventive medicine or medical treatment, care, settlement of healthcare services or insuring health risks, including but not limited to information:

- about health relevant lifestyle or environmental influences,
- about prescribed or applied medication,
- about methods of diagnosis, treatment or care or
- necessary for the billing of healthcare services.

If such data is communicated by healthcare providers the rules of the HTA [2] apply. Mere processing without communicating data does not entail applicability of the HTA [2] (Part 2 of the HTA [2]). The definition of health data has been heavily criticised during the parliamentary process by privacy institutions [23, 24, 25] but not regarded unconstitutional. So did, however, the Austrian Medical Association years later (sic!) during the preparation of an Austrian EHR law in April 2012 [26]. Allegedly the definition of personal health data is according to the AMA not accurate enough [26]. The AMA is convinced, that the definition does not conform to relevant judgments of the Austrian Constitutional Court on accuracy of legal terms. According to these judgements the terms "severe breach of duty" [27], "excellent job performance" [28], "important service interests" [29] or the "economically justified price" [30] are sufficiently determined. Contrary "usually" for example has not been found sufficiently determined [31]. In these premises, the allegation of the AMA appears unsupported.

1.3.3 Special Laws on Data Security

Part 2 of the HTA [2] specifies concrete data security measures, which prevail over the more general data security measures laid down in Sect. 14 DPA 2000 [1]. In contrast to the DPA 2000 [1] the HTA's [2] data protection provisions are limited to data security. Other aspects of data protection, as for example the legitimacy of data usage, are not governed by the HTA [2]. Even more detailed provisions than the provisions of the HTA [2] on data security are laid down in the Health Telematics Ordinance [32], that itself is based upon the HTA [2]. The HTO's [32] special data protection rules concern:

- proof of identity and role as precondition for communication of electronic personal health data (Sect. 3 HTA [2] and Sect. 1 HTO [32]),
- verification and proof of the involved healthcare providers' identities and roles (Sect. 4 and 5 HTA [2], Sect. 1 and 2 HTO [32] and Annex 1 HTO [32]),
- protection of confidentiality and integrity of the communicated health data (Sect. 6 and 7 HTA [2], Sect. 3 and 4 HTO [32] and annex 2 HTO [32]),
- documentation of the applied data security measures (Sect. 8 HTA [2] and Sect. 5 HTO [32]),
- administrative penalties of up to EUR 5.000 EUR[7] to ensure compliance with the HTA's [2] data security requirements (Sect. 17 HTA [2]) and
- transitional provisions to balance the interests of data and investment protection (Sect. 19 HTA [2]).

1.3.4 Verification and Proof of Identity

The identity of healthcare providers has to be proven primarily (Sect. 4.1 HTA [2]) by means of certificates[8] (Sect. 2.8 Electronic Signature Act [33]) and identity data. These identity data must be collected in a way compliant to the Austrian E-Government Act (EGovA) [3], i.e. by means of the citizen card (Sect. 2.10 and Sect. 4 et sqq. EGovA [3]) and/or the e-government registers (Sect. 6.2 and 6.3 EGovA [3]). Subsidiary proof of identity may also be carried out:

[5] Healthcare provider: "any natural or legal person or any other entity legally providing healthcare on the territory of a Member State".

[6] Healthcare: "health services provided by health professionals to patients to assess, maintain or restore their state of health, including the prescription, dispensation and provision of medicinal products and medical devices".

[7] The abusive use of the e-health directory's data is fined up to 50.000 EUR.

[8] Certificate: "an electronic confirmation, that assigns signature-verification data [German: Signaturprüfdaten] to a particular person and confirms her identity".

- via access of the e-health directory (Sect. 4.2 HTA [2]),
- by means of server certificates (Sect. 4.3 HTA [2]),
- via login details, if the use of certificates or the e-health directory appears inappropriate from either the technical or the economical point of view (Sect. 4.4 HTA [2]),
- in form of personal or phone contact, contractual agreement or via electronic professional registers access, if proof of identity according to Sect. 4 HTA [2] is unreasonable due to inappropriate technical expenditure (Sect. 19.1 HTA [2]) or
- in any other form, provided that
- confidentiality of data transfer is assured,
- the link between identity data of the healthcare providers and transferred health data cannot be changed without a trace and
- confusion between the involved healthcare providers can be ruled out (Sect. 1.2 HTO [32]).

1.3.5 Verification and Proof of Roles

Basically the same rules apply to verification and proof of roles: primarily they have to be proven by means of certificates (Sect. 5.2 HTA [2]). Healthcare providers choose their roles out of the 46 roles[9], defined in the HTO [32] and have them confirmed by so called registration bodies, which are according to Sect. 2.2 HTO [32] the Austrian Medical Association, the Austrian Dental Association, the Austrian Chamber of Pharmacists, the Austrian Midwives Committee as well as the Federation of the Austrian Social Security Institutions (Hauptverband der österreichischen Sozialversicherungsträger) and the Austrian Federal Minister for Health. Evidence that the correct roles are used may be given:

- via access of the e-health directory (Sect. 5.3 HTA [2] or Sect. 2.5 HTO [32]),
- via login details (Sect. 5.5 HTA [2]) or
- in the form of personal or phone contact, contractual agreement or via electronic professional registers access, if proof of roles according to Sect. 5 HTA [2] is unreasonable due to inappropriate technical overhead (Sect. 19.1 HTA [2]).

In case of automated exchange of data, evidence must be given basically only prior to the first use of health data (Sect. 5.4 HTA [2]). Roles other than those provided for in Annex 1 HTO [32] must not be used (Sect. 1.1 HTO [32]).

1.3.6 Confidentiality: Legitimacy of Fax and E-Mail

The confidentiality of communicated personal health data has to be ensured by means of encryption. The procedures and algorithms applied must resist attacks, that can be performed with economically acceptable effort (Sect. 6.1 HTA [2]). According to Annex 2 of the HTO [32] the procedures and algorithms laid down in the Electronic Signature Ordinance [34] as well as the symmetric encryption algorithms AES[10] and TripleDES[11] may be used for ehealth purposes. For performance reasons the obligation to encrypt the data is limited to identifiers or any other information, allowing to track down the data subject, as well as any login details (Sect. 3.2 HTO [32]).

Unencrypted mailing of personal health related data is forbidden by law[12]. Faxing is nonetheless permitted according to Sect. 19.3 HTA [2], provided that:

- the fax is access-restricted,
- the phone numbers are verifiably kept up-to-date,
- automatic forwarding and remote maintenance functions are deactivated and
- the device's security features are activated.

Until December 31st 2015 the requirements of the HTA [2] regarding confidentiality do not apply to wireless communication of rescue services (Sect. 19.7 HTA [2]). This exemption is the last and now only transitional provision with a fixed deadline. This is owed to the fact, that former transitional provisions regarding the technical pre-requisites needed continuous amendment[13], because technical development and dissemination of innovations

[9] These roles comprise: all kinds of medical doctors (Annex [Anx] 1.1 to 1.5 HTO [32]), all kinds of therapists (Anx. 1.6 to 1.9 and 1.11 HTO [32]), midwives (Anx. 1.10 HTO [32]), nursing staff (Anx. 1.18 to 1.20 HTO [32]), various legal entities, as for example hospitals, penal institutions (Anx. 1.24 HTO [32]), pharmacies (Anx. 1.26 HTO [32]), tissue banks (Anx. 1.27 HTO [32]), patient transport (Anx. 1.36 HTO [32]), health administration (Anx. 1.44 HTO [32]), patient advocacy (Anx. 1.45 HTO [32]) and – due to the wide definition of the term "healthcare provider" according to Sect. 2.2 HTA [2] – a general role called "health service provider" (Anx. 1.46 HTO [32]).

[10] Advanced Encryption Standard (AES) is an encryption procedure published in 2000.

[11] Data Encryption Standard (DES) is an encryption procedure officially confirmed by the US government in 1976 and the predecessor of AES.

[12] The prohibition of unencrypted mailing can be drawn from Sect. 19.1 HTA [2], that is a transitional provision for all data security requirements except confidentiality according to Sect. 6 HTA [2]. Sect. 19.3 HTA [2] again limits the strict confidentiality requirement of Sect. 6 HTA [2] only with regard to faxing, but not with regard to mailing. Hence no exemption from confidentiality is stipulated, that would allow unencrypted mailing.

[13] All amendments to the HTA [2], from 2008 to 2010 [35], have been driven by the idea to extend the fixed deadlines of the transitional provisions. The underlying problem is still hard to resolve, because the conflicting interests of data protection on the one hand and cost awareness of the healthcare providers ("investment protection") on the other hand need to be balanced. Based on risk assessment the last amendment [36] introduced a completely revised version of transitional provisions.

were not and still are not predictable. For this reason a "smooth" deadline, depending on the factual deployment of privacy enhancing technologies has been introduced in 2010 (Sect. 19.5 HTA [2]). As a result the Federal Minister of Health may terminate the transitional phase by means of ministerial ordinance, if the data security requirements can be met by commonly available and affordable technology, after having heard the relevant stakeholders[14].

1.3.7 The E Health Directory: a Register of Healthcare Providers

The e-health directory is a register of healthcare providers to promote the electronic exchange of health data, to increase information on healthcare services and to improve policy making in the field of e-health (Sect. 9.1 HTA [2]). Healthcare providers exercising their profession in Austria – including of course foreign healthcare providers – can be registered regardless of their citizenship. Registration is free of costs, voluntary (Sect. 11.1 HTA [2]) and accomplished by registration bodies (Sect. 13 HTA [2]). For the purposes of the e-health directory the following data are collected and processed (Sect. 10.1 HTA [2]):

- name and unique identification according to Sect. 8 EGovA [3] of the healthcare provider,
- contact details (postal and electronic),
- Object Identifier (OID) according to ISO[15]/IEC[16] 9834 respectively DIN[17] 66334,
- role(s) of the healthcare provider,
- information on geographic localisation of the healthcare provider,
- uniform resource locator (URL) of the public key[18] for encryption of health data,
- name of the registration body,
- date of registration and latest amendment to registration as well as name of the performing registration body.

The data of the e-health directory must not be published, but may only be used by the healthcare providers concerned, the registration bodies and government bodies competent in public health (Sect. 9.3 HTA [2]).

1.3.8 E-Health Information Governance

The HTA's [2] provisions on e-health related information governance were introduced in 2004, with unfortunately remaining some of them without considerable practical impact up to now. One of these provisions deals with the reporting system on health telematics (Sect. 14 HTA [2]), that would in fact cover very interesting information on:

- the availability of technical infrastructure for health telematics,
- the nature and scope of applications and procedures employed in the field of health telematics,
- the type and amount of personal health data, that has been electronically communicated as well as
- the general economic conditions of health telematics.

For the purpose of this monitoring, data of the e-health directory may be used (Sect. 14.2 HTA [2]).

Furthermore, the Federal Minister of Health is entitled to issue guidelines regarding the quality of health-related online information [37]. These guidelines shall include provisions on complaints management and be published – together with the results of the complaints management – in the Information Centre (Sect. 16 HTA [2]), which is online at [38]. Main objective of this publicly available Information Centre is to raise awareness in the field of health telematics, e.g. by informing about new procedures and methods of health telematics ("best practices") or national or international standards as for example ICD-10[19].

1.4 Austrian E-Government Law: Data Protection Compliant Identification

Main goal of the Austrian E-Government Act (EGovA) [3] is to provide a data protection compliant and accurate way of identification of entities[20] by means of personal identifiers.

Accurate identification creates trust and is therefore an essential pre-requisite for electronic communication of delicate personal data, as for example health data or legal relevant information. Unambiguous identification of both patients and healthcare providers is necessary to ensure quality of e-health services: health information assigned to the right patients prevents maltreatment, whereas correct identification of healthcare providers allows traceabi-

[14] E.g.: Austrian Medical Association, representatives of hospital operators or advocates for patients.

[15] International Organisation for Standardisation.

[16] International Electrotechnical Commission.

[17] German Institute for Standardisation (Deutsches Institut für Normung).

[18] Public keys are used in asymmetric encryption, the function of which is based upon two different keys: one for encryption and one for decryption. If information shall be hid the encryption is done with the public key, published by the potential recipient of encrypted data. If information shall be electronically signed the encryption is done with the private key. The public key is usually published in the certificate of the signatory and can be used by any recipient to decrypt the transmitted information. Thereby the recipient verifies that it could have been only the holder of the private key, who encrypted the information.

[19] ICD-10 (International Classification of Diseases version 10) is an international standard issued by the World Health Organisation (WHO) "for all general epidemiological, many health management purposes and clinical use" [39].

[20] Entities according to EGovA [3] include natural and legal persons, as well as other entities.

lity and quality control, especially relevant in cases of law suits.

Nonetheless, personal identifiers are often regarded as harmful[21], as they can be used for profiling of people. To overcome this problem the accurateness of a unique identifier is combined with a structure representing the different fields of activity. Public services are divided into at least 35 sectors and private services into sectors for each data controller.

This separation guarantees that activities of one data subject cannot be traced over different sectors, because the different unique identifiers of one and the same person can – due to encryption – not be derived from each other. The central register of residents number – CRRN (Zentrale Melderegister-Zahl) serves as the before mentioned unique identifier. It is strongly[22] encrypted to generate the so called sourcePIN (Stammzahl) according to Sect. 2.8 EGovA [3].

Then this sourcePIN is concatenated with individual tokens for each sector and the resulting term is hashed with a one-way hash algorithm[23] to calculate the sector specific personal identifier – ssPIN (bereichsspezifisches Personenkennzeichen) according to Sect. 9 EGovA [3]. The use of such one-way functions assures that ssPINs can only be derived from the sourcePIN of a data subject but not from other ssPINs of the data subject. As the sourcePIN is the only means to calculate ssPINs, the usage of the sourcePIN is subject to strict limitations. sourcePINs must not be used directly for identification purposes (Sect. 12 EGovA [3]) or stored outside the data subjects' citizen cards.

Solely the ssPINs may lawfully be kept by data controllers. The citizen card does not need to be a smart card in the common understanding, but can be any technical device, as for example a mobile phone. The only pre-condition is that the device provides an electronic signature function and allows the storage of an identification data set (identity link) that is electronically signed by the sourcePIN Register Authority[24].

National personal identifiers, that are at the same time accurate and data protection compliant, will be extremely important for patients, as such identifiers allow patients to manage their health data online, for example via a national health portal. Entities without residence in Austria can also participate in the Austrian identity management by applying for registration in the supplementary register [44]. Even powers of attorney can be managed [45].

1.5 Doctors' Code 1998: the Medical Secrecy

Fundamental provisions, whether data may be used or not, are laid down in the Doctors Code 1998 (DC 1998) [4], in particular Sect. 51.2 DC 1998 [4]. According to this provision medical doctors may process personal health data necessary for the patients' treatment and communicate this data to other healthcare providers, if patients have agreed to such, or social security institutions.

Secret information that has been revealed to medical doctors in the course of their professional activities must not be communicated ("medical secrecy[25]"), except for the following:

1. other laws require the communication of health data (Sect. 54.2.1 DC 1998 [4]),
2. communication of health data is necessary for sickness insurance institutions to perform their duties (Sect. 54.2.2 DC 1998 [4]),
3. the data subject gave consent (Sect. 54.2.3 DC 1998 [4]),
4. communication is necessary to protect prevailing public interests regarding public health or jurisdiction (Sect. 54.2.4 DC 1998 [4]),
5. communication is necessary for settlement of medical costs and costs for drugs or medical aids (Sect. 54.3 DC 1998 [4]) or
6. in cases of serious crimes, e.g.: sexual abuse, maltreatment or neglect of minors or incapacitated persons or bodily harm leading to serious injury or death (Sect. 54.4 to 54.6 DC 1998 [4]).

A similar provision for dentists is Sect. 21 Dentists' Code [46], which differs from the general medical secrecy of Sect. 54 DC 1998 [4] in particular in the absence of legitimating communication in cases of serious crime. Both secrecies also protect third persons [47] – e.g. information about the spouse's mental illness – and do not presume a valid treatment contract [47], but are directly effective due to the cited law provisions.

[21] According to Art. 8.7 DPD [11] "Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed".

[22] The strong encryption is required by law (Sect. 6.2 EGovA [3]) and currently achieved using Triple DES [40] in CBC (Cipher Block Chaining) mode [41, 42].

[23] A one-way hash algorithm allows to compute a digital fingerprint (hash-value) that represents the original data. This hash-value is usually a fixed-digit number, that changes after re-calculation, if the original data has been altered. Whereas the hash-value can always be calculated if the original data is known, the inversion, i.e. the calculation of the original data from the hash value, does not work.

Hashing can be used to generate checksums for data. An example for a one-way hash function is the MD5 algorithm, that creates 128 bit hash values.

[24] According to Sect. 7 EGovA [3] the Austrian Data Protection Agency acts as the sourcePIN Register Authority [43].

[25] The term "secrecy" in the Austrian legal language refers to the duty of persons to not actively communicate data, whereas "confidentiality" refers to the obligation to prevent even passive, i.e. accidental, communication or loss of data, e.g. by using encryption techniques and checksums.

1.6 General Social Insurance Law

1.6.1 The Electronic Management System ELSY

In 1999 an amendment to Sect. 31a [48] of the Austrian General Social Insurance Law (GSIL) [5] introduced the electronic management system "ELSY", to support the administrative processes among insurance holders, employers, contractual partners and insurance carriers. Part of the ELSY are the e-cards for patients, the a-cards for pharmacists and the o-cards for physicians. All these cards are key cards, meaning that by default no data except for identification and authentication purposes are stored on these cards. Additionally the citizen card can be used as e-card (Sect. 31a.2 GSIL [5]). Till December 31st 2010 all cards should have been access protected by use of passwords or biometrics, which did not happen till now [49]. As a result issues of liability could be raised in cases of loss and misuse of e-cards.

The patients' health card, called e-card, is an electronic health insurance certificate and replaces the former paper version. Thereby red tape is cut, as a defined goal of ELSY (Sect. 31a.1 GSIL [5]). According to Sect. 31a.3 GSIL [5] the e-card may exclusively hold the following data:

1. name, date of birth and sex of the card holder,
2. insurance number,
3. card number, date of issuance and name of card issuer as well as
4. any other data, that shall be stored on the e-card by law.

Patients may also have their emergency data[26] written on their e-cards (Sect. 31a.5 GSIL [5]). Strict rules on the usage of data guarantee a high level of data protection, e.g.: the ban to link patients' claims to the fact whether patients agreed upon the use of their e-cards or not (Sect. 31a.4a GSIL [5]) or the restriction of purposes, for which ELSY may be used (Sect. 31a.4 GSIL [5]). As an additional safeguard, the misuse of emergency data stored on e-cards is fined up to 18 890 EUR.

1.6.2 The Obligation to Cooperate in ELGA Affairs

Sect. 31d GSIL [5] obliges the Federation of the Austrian Social Security Institutions (FASSI – Hauptverband der österreichischen Sozialversicherungsträger) to engage in the conception and implementation of a national EHR, called ELGA. The FASSI is one of the three shareholders of the "ELGA-GmbH", which shall introduce and implement ELGA. The other two shareholders are the federal government and all state governments together. The division into three shareholders is owed to the constitutional law fact, that the distribution of competences among the federal and states governments is not absolutely clear. The main competence "health affairs" resides with the federal level. However, it is to a large extent restricted by the state governments competences regarding infrastructure and operation of hospitals. Due to this lack of clarity the federal and state level need to closely co-operate.

1.6.3 Electronic Exchange of Data

Data between hospitals and insurance carriers must be exchanged electronically (Sect. 148.6 GSIL [5]) as well as the settlement of accounts needs to be done by electronic means of communication (Sect. 340a, 342a, 348g and 349a GSIL [5]). The social insurance number (SIN) may be used as personal identifier for purposes of social and unemployment insurance (Sect. 460d GSIL [5]).

In case that personal details, e.g.: SIN, name, birth date, sex or citizenship, need to be changed or updated, these changes have to be communicated to the matching table[27] of the Federal Minister of the Interior (Sect. 460d GSIL [5]).

Although this matching table does not hold health related information, it is an important pre-requisite to calculate the ssPINs for the health sector, as it eases the transformation from SINs to CRRNs, which are the mathematical base for calculating the ssPINs. For statistical purposes the Federal Minister of the Interior is legitimated to match the CRRNs against the SINs by comparing sets of personal data from the central register of residents and the FASSI's central partner database (Zentrale Partnerverwaltung).

1.7 Insurance Agreement Act: Usage of Insurance Data

The Austrian Insurance Agreement Act (IAA) [6] provides a framework for e.g. conclusion, rights and duties, pre-requisites of validity and termination of insurance agreements or the profession of insurance brokers. Addressees of the IAA [6] are insurers under private law. Public insurers as for example the Regional Health Insurance Fund of Vienna (Wiener Gebietskrankenkasse) are not subject to the IAA [6] but to the GSIL [5]. According to the HTA's [2] definition of healthcare providers (Sect.

[26] Unfortunately there is no explicit definition of the term emergency data, which was introduced by the 59th amendment [50] to the GSIL [5], although Sect. 31a.5 GSIL [5] empowers the Federal Minister for Social Security and Generations (now: Federal Minister for Labour, Social Affairs and Consumer Protection) to specify by ministerial ordinance the use of emergency data in more detail. The only hint, what can be referred to by "emergency data", gives Sect. 31a.5 GSIL [5] itself, by referring to the data "being of vital interest for the data subject in case of medical emergency". This does not specify the data types as for example, blood group, drug intolerances or status of vaccination, but remains on a very abstract and thus open level, which could be necessary for example for people with rare diseases. For them specific emergency data could insofar be relevant as the knowledge of these data could have decisive influence on the ongoing treatment.

[27] The legal foundation of the so called matching table (Gleichsetzungstabelle) is laid down in Sect. 16b of the Registration Act 1991 [51].

2.2 HTA [2]), insurers are regarded healthcare providers, and hence subject to the special data protection requirements set forth in the HTA [2].

Sect. 11a IAA [6] is the most relevant IAA-provision with regard to e-health. It determines how health data may be used by insurers. The only valid purposes for which insurers may use personal health data are:

1. assessment whether and subject to which conditions insurance agreements are entered into or amended (Sect. 11a.1.1 IAA [6]),
2. administration of valid insurance agreements (Sect. 11a.1.2 IAA [6]) and
3. assessment and settlement of claims arising from insurance agreements (Sect. 11a.1.3 IAA [6]).

All methods of data collection are limited to methods, that involve the data subjects and take into account their will (Sect. 11a.2.1 to 11a.2.4 IAA [6]) or concern otherwise lawfully collected data, provided that the data subjects are informed about this way of collection (Sect. 11a.2.5 IAA [6]). As a consequence, any collection of personal health data by insurers requires in some way or another the data subjects' involvement.

Health data may only be kept as long as necessary (Sect. 11a.5 IAA [6]) with the statutory limitation period as an upper limit. The general civil law limitation periods of three respectively thirty years, are altered by Sect. 12.1 IAA [6] to three years after termination of the agreement, at the latest ten years, if third-parties are beneficiaries and not aware of their contractual entitlements.

1.8 Genetic Engineering Act: Usage of Personal Genetic Data

Another relevant provision regarding the usage of personal health data is Sect. 67 of the Genetic Engineering Act (GEA) [7]. It absolutely bans the usage of personal data related to human genetic data by employers and insurers. The provision reads as follows:

„Ban on enquiry and use of genetic analyses' results for particular purposes

§67. Employers and insurers including their appointees and employees must not enquire, require, receive or otherwise use the results of genetic analyses relating to their employees, job-seekers, insurance holders or prospective insurance holders. According to this ban it is also prohibited by law to ask for or accept body substances for purposes of genetic analyses."

All other persons, not mentioned in Sect. 67 GEA [7], may – subject to the provisions of the DPA 2000 [1], HTA [2], HTO [32] and EGovA [3] – use genetic data, also in electronic form.

2 Outlook

In the next few years Austria is facing some fundamental improvements to its e-health sector. Some innovations are nationally inspired, as for example the national EHR, called ELGA (Elektronische Gesundheitsakte), while others, as for example the European Patients Smart Open Services (epSOS) [52] large scale pilot or the voluntary networks according to Art. 14 PRD [12], are European initiatives.

2.1 Expected National Innovations: ELGA and Telemedicine

Since several years an amendment to the HTA [2] has been under discussion. The new provisions shall introduce a legal framework for ELGA. This will be the most important step ever taken regarding Austrian e-health legislation.

2.1.1 ELGA in a Nutshell

ELGA is designed as an IT-infrastructure, that is made up of centralised and decentralised components (figure 1). The centralised components will be the Master Patient Index, the ELGA Healthcare Provider (HCP) Index, the Access Control Centre (ACC – Berechtigungssystem), the logging system and the internet portal. The decentralised components are the document registries and the document repositories. Both **indexes** shall guarantee valid identification of ELGA participants[28] and ELGA healthcare providers. One of their features will be to convert internal identifiers, e.g. of a local hospital in Vienna, into nation-wide valid ssPINs, as provided by the EGovA [3]. The **Access Control Centre** enables the ELGA participants to define individual rules, which data can be accessed by which ELGA healthcare providers. Functionality of the Access Control Centre is provided to the ELGA participants either online, by means of the ELGA portal, or offline via the ELGA ombudsmen. The **logging system** logs every single processing step of data usage in the context of ELGA, as for example access of the indexes, registries or repositories. The **document registries** are collections of links to the actual health data, which is stored in **document repositories**. The reasons and advantages of this decentralised approach are explained below in chapter 2.1.3.

If a request is sent to the ELGA system, the IDs of the ELGA participant and the ELGA healthcare provider are checked against the indexes. According to the rules stored in the Access Control Centre the request is either forwarded to the document registries or not. The registries determine which of them holds the necessary information

[28] As patients are not obliged to participate in ELGA, the ones, who did not opt out are called ELGA participants to distinguish them from other patients, that opted out of ELGA.

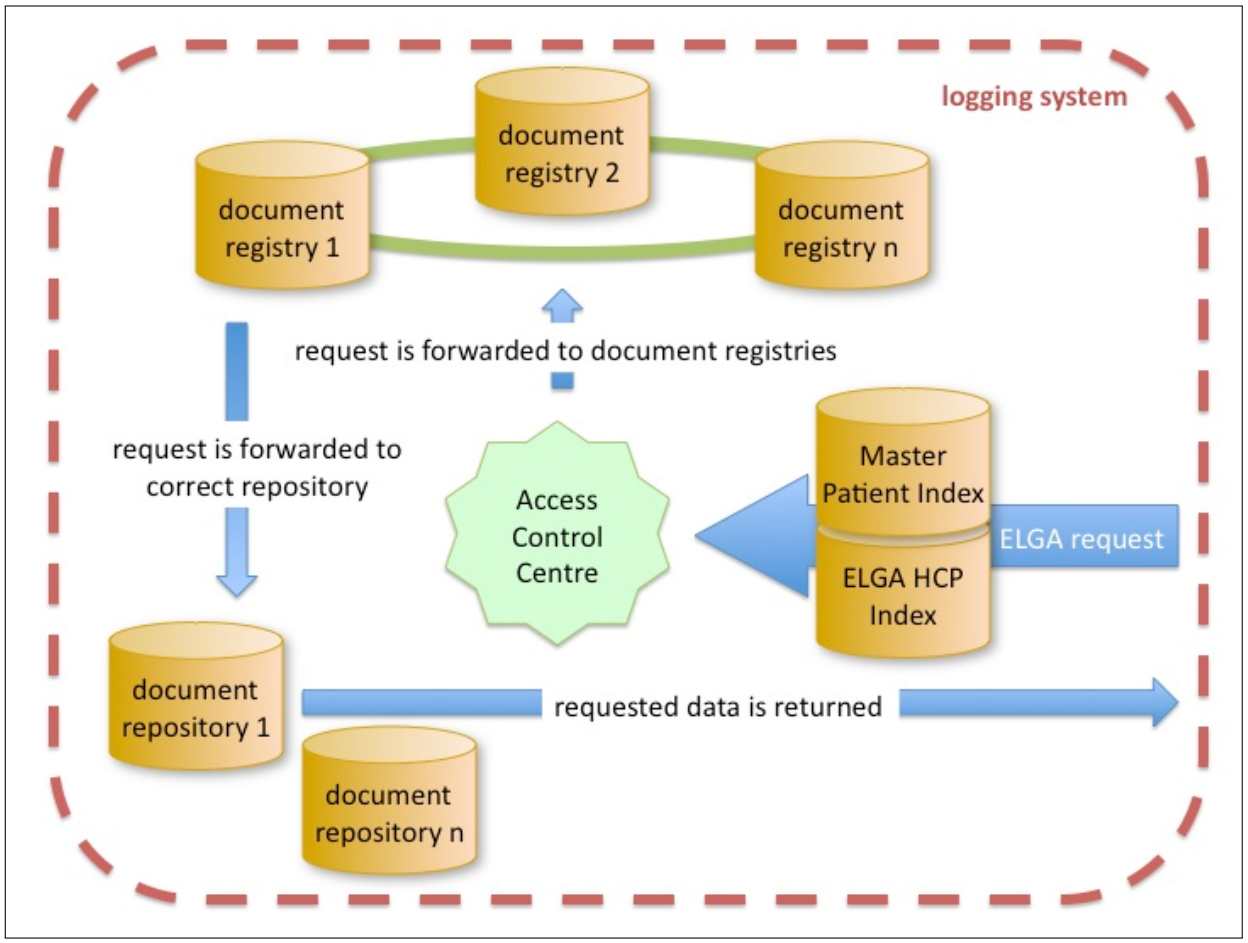

Figure 1: Fundamental structure of ELGA.

and then forwards the request accordingly to the right document repository, from where the requested data is retrieved and returned.

The document registries are linked databases of links. As already mentioned, they do not hold any health data, but only technical information about the documents, as for example addresses and IDs of the document repositories, where the health data are saved, keywords, IDs of ELGA healthcare providers, IDs of ELGA participants or versioning information. The decentralised approach reduces vulnerability of ELGA, as the data of ELGA participants is not stored at one central place, but at many different places.

2.1.2 Main Principles of ELGA

ELGA is based upon the following principles:

1. the legitimate usage of ELGA is exclusively granted to the ELGA participants and their representatives, ELGA ombudsmen and **ELGA healthcare providers**, i.e. medical doctors and supporting medical staff, if and as far as these persons do not act on behalf of national, regional or local governments in their sovereign capacity (Hoheitsgewalt);
2. usage of health data is strictly limited to purposes of medical treatment or exercise of the ELGA participants' rights;
3. patients may opt-out of their participation in ELGA at any time;
4. patients may declare to participate just in particular ELGA applications, as for example the e-medication services;
5. patients may declare that their data is not to be included within ELGA ("right to object") at any time and
6. patients keep clear control over their data via the Access Control Centre.

It is important to note that not all healthcare providers according to Sect. 2.2 HTA [2], will be addressees of the ELGA provisions. Only a little subset of them, the so called ELGA healthcare providers, will be subject to ELGA regulations. By doing so healthcare providers, that are no ELGA healthcare providers are excluded by law from using ELGA. Conversely all ELGA healthcare providers are "normal" healthcare providers, which means that they have to adhere to the data security requirements of Part 2 HTA [2].

2.1.3 The Net-Based Concept of ELGA: Protecting Data and Investments

Hospital information systems are de facto standard in Austria. Additionally, some hospital co-operations use shared data pools, as for example the Viennese Hospital Association. To put it another way: major investments in shared IT-infrastructure have already been made and these expenditures should not be frustrated by new laws. The expected costs have been the main reason for the lengthy discussion on the data security provisions of the HTA, which finally resulted in the transitional provision of Sect. 19 HTA [2]. One outcome of this discussion was the decision that faxing should be a legally accepted way of communicating personal health data, as explained above in chapter 1.3.5.

To not give rise to such discussions again, it was considered to set up ELGA upon existing infrastructure and introduce a flexible system, that is based upon decentralised document registries and document repositories. This approach facilitates the re-use of existing registers. Another benefit of this solution is, that a longstanding calling of data privacy activists for decentralised storage of personal health data, is satisfied [13].

2.1.4 Participation in ELGA: Opt-In, Opt-Out or Mandatory Participation

One of the main legal issues in the Austrian discussion on national EHR systems has been the question whether participation in ELGA should be mandatory or not. As already mentioned above in chapter 1.1, the fundamental right to privacy is constitutional law and may according to Sect. 1.2 DPA 2000 [1] only be restricted, in case of:

1. vital interests or
2. consent given by the data subject or
3. overriding legitimate interests of others.

At least one of these three requirements has to be met by a future EHR law, because otherwise its provisions could easily be suspended[29] by the Austrian Constitutional Court due to non-conformity to the fundamental right to privacy. Due to the higher rank of constitutional law an ordinary statutory law based upon "overriding legitimate interests of others" cannot rule out "vital interests" or "data subject's consent" [53] as legal base for the usage of personal data. That means, that the consent of the data subject may also legitimate usage of data, which is not regulated by the future "normal ranked" EHR law.

Participation can either be stipulated in form of an opt-in, opt-out or mandatory participation. The first two approaches would take the will of the data subject, i.e. the patient, into account, whereas a mandatory approach would oblige all patients to be ELGA participants, regardless of their intention to participate or not[30].

According to the Data Protection Directive a national ELGA law could basically be based upon:

- explicit consent[31],
- necessity for healthcare purposes (Art. 8.3 DPD [11]) or
- substantial public interests (Art. 8.4 DPD [11]).

The potential legal bases for a national ELGA law are illustrated in figure 2, both on EU and Austrian constitutional law level. To be compliant with EU law each legal base for processing data according to Art. 8 DPD [11], must be covered by a correspondent legal base of the Austrian fundamental right to privacy. Otherwise the fundamental right to privacy would breach Art. 8 DPD [11]. Figure 2 shows how the legal bases for data processing correlate on European and national level and that for example the usage of data for healthcare purposes allowed at European level by Art. 8.3 DPD [11], must be a legitimate overriding interest at national level according to Sect. 1.2 3rd case DPA 2000 [1].

The Art. 29 Data Protection Working Party believes that "opt-out solutions will not meet the requirement of being 'explicit'" [17], so only the necessity for healthcare purposes (Art. 8.3 DPD [11]) or substantial public interests (Art. 8.4 DPD [11]) could justify opt-out solutions. Concerning the usage of data for healthcare purposes, the Art. 29 Data Protection Working Party is not convinced that Art. 8.3 DPD [11] can serve as sole legal basis for a national EHR law [17]. This seems a bit too strict and unfounded, as especially the e-medication tools of EHRs can increase drug security remarkably [55] and thus save

[29] Judicial review (Normenkontrolle) is one of the most important tasks of the Austrian Constitutional Court. That means, that the court may repeal any law or ordinance, that contradicts or interferes with higher ranking law.

[30] Mayer [18] criticises that an opt-out approach cannot replace the requirement for the data subjects' consent, because data is already processed before the data subjects, i.e. the patients, have the possibility to decide, whether they opt out or not. This is definitely not true for the current draft of the ELGA law, as the transitional provisions require that ELGA participants are entitled to opt out from summer 2013 onwards, whereas ELGA is intended to start in January 2015. So ELGA participants have one and half year of time to declare, that they are not willing to participate in ELGA, without having any personal health data about them processed in ELGA during this time. Even after the 1st of January 2015 patients can effectively avoid to have their personal health data included in ELGA, by opting out before their first healthcare encounter or even later by exercising their right to object during the healthcare encounter and opting out afterwards. Also Frohner [54] acknowledges the opt-out approach, as suggested by the EHR law draft, as an appropriate safeguard according to Art. 8.4 DPD [11].

[31] Art. 8.2.a DPD [11] reads as follows: "Paragraph 1 [ann: which generally prohibits the use of 'sensitive data'] shall not apply where: (a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent".

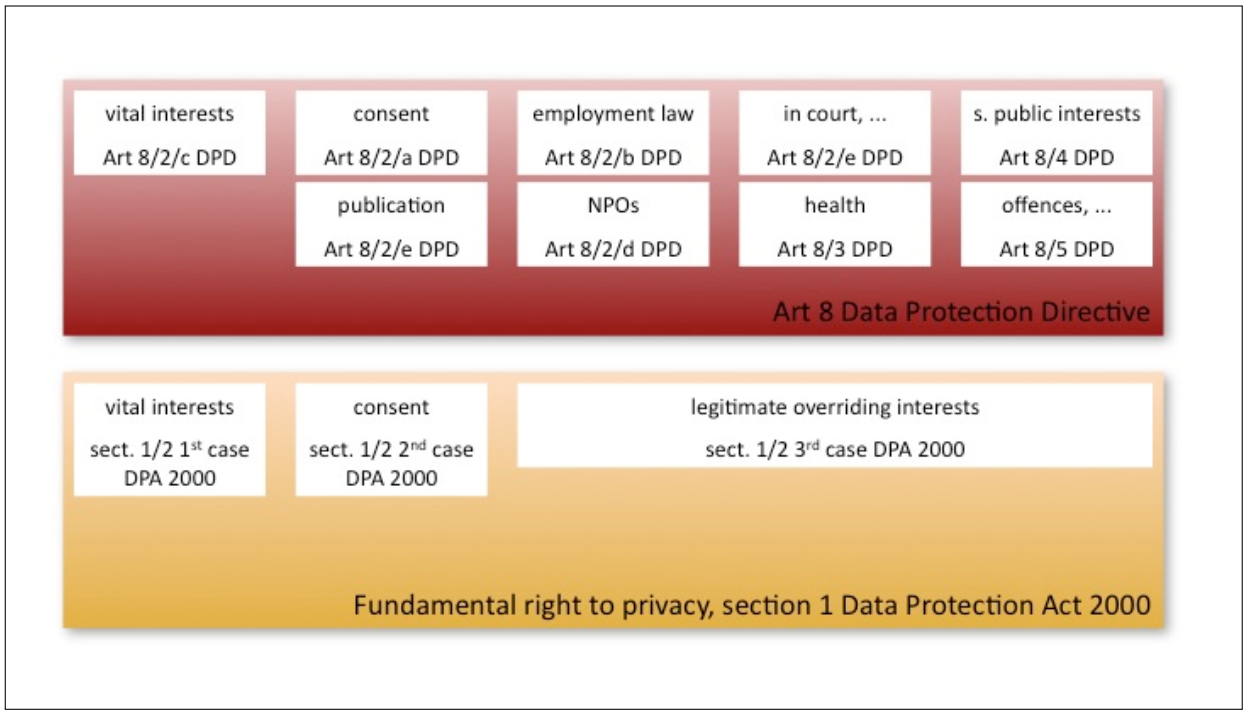

Figure 2: Legal bases for data processing at European and national level.

human lives[32]. These facts indicate medical necessity in the meaning of Art. 8.3 DPD [11], and substantial public interests in the meaning of Art. 8.4 DPD [11], even more when referring to the rulings of the Austrian Constitutional Court, that acknowledged the interest to guarantee financial viability of public health as a substantial public interest [60].

2.1.5 Securing the Patients' Freedom of Choice: the Access Control Centre

Patients' freedom of choice, whether to join an EHR or not, is one of the strongest arguments [13, 61] against ELGA in Austria. Having that in mind a system has been developed that allows full control of the patients over their health data. Compared to the currently used paper documents, an electronic system eases traceability of single steps of data usage and improves transparency for the patients.

At present state the Access Control Centre is designed to store and manage two levels of access rights:

- the abstract access rights, explicitly laid down in the ELGA law and
- the individual access rights, defined individually by each ELGA participant.

The **abstract access rights** make up a binding framework of general entitlements, that must not be extended by the individual access rights. Healthcare providers that are not entitled to use data according the abstract access rights, can also not be authorised by means of individual access rights. Task of the abstract access rights is only to provide standard settings for an optimal balance between data protection, usability and quality of healthcare. Medical doctors and medical staff of hospitals for example are basically entitled to access all personal health data, whereas pharmacists are limited to the medication relevant subset of health data. The abstract access rights can only be limited by the individual access rights, but not extended.

At the level of the **individual access rights** the ELGA participants may further restrict the abstract access rights of their ELGA healthcare providers. Additionally ELGA participants can define for how long their authentication, which can for example be done via e-card, will remain valid. During this period, which is by default 28 days, ELGA healthcare providers do not need to re-authenticate their "ELGA patients" for accessing their ELGA data.

This shall ease usability of ELGA, because the validity period can be extended beyond the 28 days of the standard rule, which benefits ELGA participants, that are hospi-

[32] A meta analysis of 39 US studies on hospitalised patients revealed, that fatal adverse drug reactions (ADRs) account for 0.32 percent of deaths among hospitalised patients [56]. According to a Swedish study of 2001 based upon 1574 study subjects, fatal ADRs cause approximately 3 percent of all fatalities [57]. Even though the percentage of fatal ADRs differs significantly, fatal ADRs gain increasing importance as the Adverse Events Reporting System (AERS) of the U.S. Food and Drug Administration persuasively demonstrates. According to the AERS the number of fatal ADRs increased by a factor 4 between 2000 and 2010 [58]. 9 percent of the ADR deaths are assumed to be preventable in any case, with only 28 percent assessed to be unavoidable [59].

talised for a longer period of time. Aim of the individual access rights is to strengthen the ELGA participants' autonomy and serve as an appropriate safeguard according to Art. 8.4 DPD [11].

2.1.6 Telemedicine

For the purpose of this article, "telemedicine" should be understood as the provision of healthcare services by means of information and communication technologies (ICT) without simultaneous presence of the persons involved. Apart from Sect. 49.2 DC 1998 [4] there are no explicit rules in Austrian legislation on telemedicine.

The above cited Sect. 49.2 DC 1998 [4] reads as follows:

"Treatment of patients and care for healthy people

(1) [...]

(2) The medical doctor has to exercise his/her profession directly and in person and, if necessary, in co-operation with other medical doctors. He may draw upon auxiliary staff, provided that these persons act upon his exact instructions and under his constant supervision."

On the one hand the requirement to "exercise his profession directly and in person" could be interpreted to rule out telemedicine. On the other hand the authorisation to co-operate with other medical doctors, relaxes this apparent restriction substantially. Actually this is the crucial statement: the co-operation of medical doctors is legally allowed, thus also allowing for online consultation or other forms of ICT based co-operation of medical doctors, provided that at least one physician providers his services in person.

The transmission of data necessary for telemedical treatment is also subject to the HTA [2] as any other transmission of personal health data as for example the communication of x-ray images.

2.2 Expected European Innovations: epSOS

The European large scale pilot epSOS[33] "attempts to offer seamless healthcare to European citizens. Key goals are to improve the quality and safety of healthcare for citizens when travelling to another European country. Moreover, it concentrates on developing a practical eHealth framework and ICT infrastructure that enables secure access to patient health information among different European healthcare systems" [62]. Legal key strategy of epSOS is the so called "circle of trust" or "web of trust" constituted by the National Contact Points (NCPs), which act as gateways and confirm identity, qualification and authorisation of healthcare providers involved as well as compliance with national and international standards on data protection and data security.

2.2.1 The "Opt-In Problem" of epSOS

Since the project was started in July 2008 intense discussions on the **legal bases of data processing** have been held. Currently two approaches are conceivable: either the patients' consent ("opt-in" according to Art. 8.2.a DPD [11]) or processing of personal data for healthcare purposes (Art. 8.3 DPD [11]). As "never touch existing legislation"[34] has always been one of epSOS' guiding principles, the opt-in approach was chosen. Though this is basically comprehensible from the legal point of view, the practical downsides are a logical consequence: likelihood of real use cases is dramatically reduced, as three different "opt-ins" are required: the participation of each epSOS healthcare provider in the patient's home country (country A) and in the country of treatment (country B) as well as the general participation and concrete consent of the epSOS patient himself. This reduces the chance for real-life use cases, which in fact epSOS would essentially need, dramatically. Given an unrealistic high acceptance of 10 percent among patients and doctors such a policy would lead to an overall chance of one per mill (0.1 x 0.1 x 0.1 = 0.001) of all cross border incidents. Considering the little number of cross border encounters another solution should have been chosen to have at least a few use cases for the epSOS pilot.

2.2.2 epSOS and the Art. 29 Data Protection Working Party

The argument of the Art. 29 Data Protection Working Party against EHR systems, that "the mere 'usefulness' of having such personal data contained in an EHR would not be sufficient" [17] to meet the requirements of **Art. 8.3 DPD** [11] is not an EHR-specific argument, but also an argument against "traditional" paper-based medical histories. Art. 3.1 DPD [11] sets the scope of the DPD [11] to the processing of data by automatic means and "the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system". Accordingly the DPD [11] is basically also to be applied to paper-based medical histories, as for example defined in Sect. 10.2 of the Austrian Hospitals- and Sanatoriums Law (HSL) [63]. The medical history definition of Sect. 10.2 HSL [63] covers inter alia: information about anamnesis, current physical condition (status praesens), course of disease (decursus morbi), applied medication and treatment, donation of tissues and organs or living wills. This personal data is processed without consent of the patients. If the arguments of the

[33] epSOS is an acronym for European Patients Smart Open Services [52].

[34] This refers to national as well as international/European level.

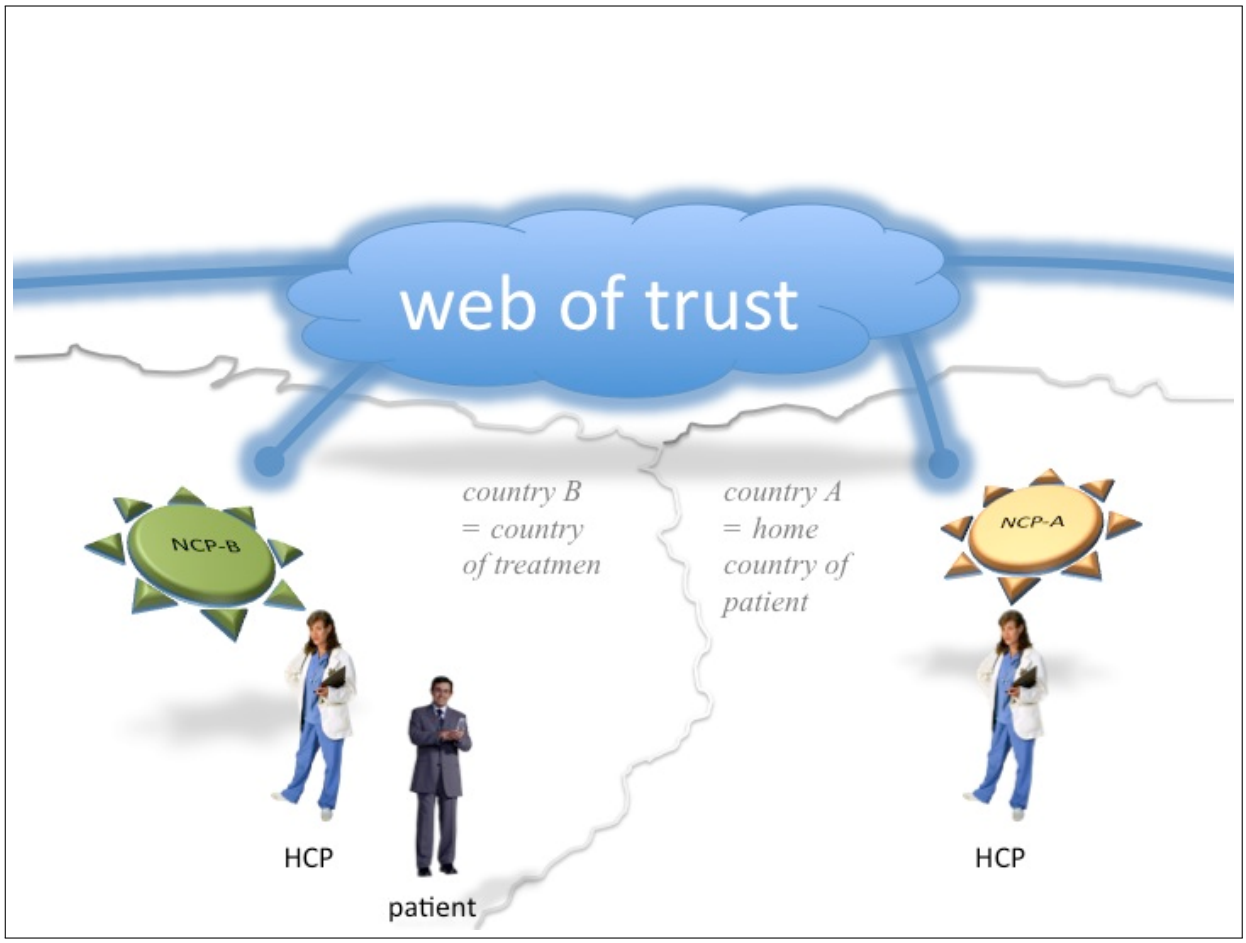

Figure 3: Structure of epSOS.

Art. 29 Data Protection Working Party were true, all medical histories, that are kept without consent of the patients, would be illegal, due to the fact that there is definitely some data collected, without being used once again. Nevertheless *collecting such data, is not just* ***useful****, but* ***necessary*** *in terms of treatment*, as neither the course of diseases nor secondary diseases can be foreseen. Due to the reference to "vital interests" (Art. 8.2.c DPD [11]), that may suspend data protection under distinct circumstances and Art. 8.3 DPD [11] itself, the obvious precedence of health over privacy interests are clearly expressed in the DPD [11].

Another deficiency of the documents [16, 17] of the Art. 29 Data Protection Working Party is, that the fundamental question regarding the application of the DPD [11] have not even been asked. However, *applicability of the DPD [11] cannot doubtlessly be assumed*, as Art. 3.2 DPD [11] excludes the processing of personal data "in the course of an activity which falls outside the scope of Community law" from the scope of the DPD [11]. According to Art. 168.7 of the Treaty on the Functioning of the European Union (TFEU) [64] the "Union action shall respect the responsibilities of the Member States [...] for the organisation and delivery of health services and medical care". For the first time, the European Court of Justice ruled upon the applicability of the DPD [11] in the case "Rechnungshof vs ORF" [65] and concluded, that the DPD [11] applies to the publication of remunerations of the public broadcasting's employees, even though this kind of publication might be "an activity which falls outside the scope of Community law" according to Art. 3.2 DPD [11]. The decisive argument has been, that Art. 100a of the Treaty establishing the European Community (TEC) [66] on the approximation of laws and legal base of the DPD [11] "does not presuppose the existence of an actual link with free movement [...] in every situation referred to by the" DPD [11]. The European Court of Justice ruled similarly in the case "Lindqvist" [67], when it had to decide whether the publication of personal health data on a website for private purposes is subject to the DPD [11] or not. The court affirmed the application of the DPD [11], because a "contrary interpretation [of Art. 3.2 DPD] could make the limits of the field of application of the directive particularly unsure and uncertain, which would be contrary to its essential objective of approximating the laws" [67].

Legal situation is however different regarding health services and medical care (Art. 168.7 TFEU [64]). The competence to approximate laws is only applicable insofar as not otherwise provided in the treaties (Art. 114.1

TFEU [64]). The regulation, that the competences regarding health services and medical care remain with the member states in Art. 168.7 TFEU [64] is explicitly enough, to assume that:

- legal foundations for activities in such areas cannot be harmonised according to Art. 114 TFEU [64] and
- such activities fall outside the scope of EU law according to Art. 3.2 DPD [11].

Being sure about the applicability of the DPD [11] is a pre-requisite to derive legal consequences from it. An objective answer, that meets academic requirements, should be given by the Art. 29 Data Protection Working Party. Knowledge about the scope of the DPD [11] with regard to health affairs is *extremely important for national legislation*, in particular when specialised provisions on new developments shall be enacted, as for example *regarding EHR systems or bio banks*.

2.2.3 Implementation of the epSOS Framework Agreement

epSOS' legal centrepiece is the so called Framework Agreement (FWA) [68]. This is a blueprint for national contracts to establish on the one hand the epSOS NCPs and on the other hand to shape the framework for the legal relationships between NCPs and epSOS healthcare providers. Some countries, among them Austria[35], established their NCPs by assigning the NCP role not by contract but ministerial decision, ordinance or directive. In these countries the only contracts needed for the implementation of epSOS are the contracts between the NCP and the epSOS healthcare providers. The patients' rights and the duties of the NCP and epSOS healthcare providers are governed by these NCP-HCP contracts as laid down in the FWA [68]. Healthcare providers, especially physicians, that are interested in participating in epSOS, can register online [69].

epSOS is a pilot project and therefore it is very likely that due to new experiences gained, the FWA [68] requires amendments in near future. Therefore Art. 9 of the FWA [68] implements a **general amendment procedure**. According to this procedure the decisions taken by the epSOS Project Steering Board[36] (PSB) shall be published nationally within four weeks, after the PSB's decision. Within sixteen weeks following the PSB decision the national contracting partners (pilot sites) have the right to rescind the national contracts, therewith guaranteeing that the pilot sites are not subject to provisions, they could not accept (Art. 9.2 FWA [68]).

2.2.4 Liability and Enforcement Issues

epSOS duration and number of participants were extended in 2011. Among the new participating nations there are also two third countries, Switzerland and Turkey. This raises new legal questions in the field of data protection and liability for e.g. regarding medical malpractice. Whereas the European data protection framework offers clear answers – Switzerland has been confirmed by decision of the EU Commission [70] to share the same level of data protection as the EU member states do or standard contractual clauses could be used for the exchange of personal health data with Turkey – things are not that clear with regard to international private law issues, especially enforcement. The main three questions regarding international private law are:

1. Where is the place of jurisdiction? (jurisdiction)
2. Which law is to be applied? (choice of law)
3. How and where can judgements be enforced? (foreign judgements)

In the context of jurisdiction and foreign judgements the so called Brussels regime[37] is to be applied among the EU member states and Switzerland. Austria and Turkey concluded an agreement on recognition and enforcement of judgements in civil and commercial matters [74]. Among the EU member states the choice of law is governed by the EU regulations Rome I [75] and Rome II [76].

From the Austrian point of view the international private law issues seem to be solved for the moment. Nonetheless in case that other third countries join, these issues may become important again.

2.3 Proposal for a General Data Protection Regulation

By the end of January 2012 a proposal for a general data protection regulation [77] has been published by the EU Commission. The most evident innovations to the current European data protection law in the field of e-health would be:

1. the explicit statement that consent is not the only legal foundation for processing personal health data, thus *allowing explicitly opt-out approaches*; [38]

[35] The NCP-AT, i.e. the NCP for Austria, is the Austrian Federal Ministry of Health (Bundesministerium für Gesundheit).

[36] The epSOS Project Steering Board is the highest decision-making committee of epSOS.

[37] The Brussels regime consists of the Brussels Convention [71], the Lugano Convention [72] and the Brussels I regulation [73]. The differences between these three documents are marginal – the Brussels Convention [71] was the first to be agreed in 1968, the Lugano Convention [72] twenty years later to allow for the integration of the European Free Trade Association (EFTA) member states and last but most important the Brussels I regulation [73], supplanting more or less the Brussels Convention [71]. Due to its EFTA relevance and in contrast to the Brussels Convention [71], the Lugano Convention [72] is still relevant in cases relating to EFTA states.

[38] Recital 123 of the proposal [77] states that "the processing of personal data concerning health may be necessary for reasons of public interest in the areas of public health, without consent of the data subject [, ...] meaning all elements related to [...] resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing".

2. the *definition of health data at European level*: Art. 4.12 of the proposal [77] defines "'data concerning health' [as] any information which relates to the physical or mental health of an individual, or to the provision of health services to the individual";

3. the legal empowerment of the EU Commission to *harmonise the implementation of data security* requirements according to Art. 30.4 of the proposal [77]. This is of great importance for the international exchange of personal health data, as differing national data security requirements are one of the biggest show-stoppers for international projects like epSOS; and last but not least

4. a special provision on the processing of personal data concerning health, laid down in *Art. 81 of the proposal* [77]; Art. 81.1.a of the proposal [77] for example, is very similar to the existing Art. 8.3 DPD [11], that focuses on the usage of health data for treatment purposes by healthcare providers, subject to a special secrecy obligation; genuine innovations are

   (a) the reference to "ensuring high standards of quality and safety" which is acknowledged as public interest, possibly legitimating e-medication (Art. 81.1.b of the proposal [77]) and

   (b) Art. 81.2 of the proposal [77], that even allows the usage of personal data concerning health for scientific research purposes.

The impact of the Proposal for a General Data Protection Regulation [77] as of January 25th 2012 would be enormous on international as well as national level. At national level most of the data protection legislation would need to be repealed and at international level a new level of harmonisation, even regarding technical details as for example the data security measures, could be achieved.

3 Conclusion

Austrian legislation has *already resolved* crucial questions arising from the field of e health, above all by its Health Telematics Act [2] (chapter 1.3), that defines on the one hand the minimum data security requirements for exchange of electronic personal health data and introduces on the other hand an information governance framework (chapter 1.3.7). Administrative fines ensure that the requirements of the HTA [2] are obeyed.

An important cornerstone regarding e-health in Austria is the E-Government Act [3] (chapter 1.4), that provides basic rules for a national identity management system. This allows an unambiguous and data protection compliant identification, not only of Austrian citizens, but also foreign citizens and entities.

The *next steps to be taken* at Austrian level are first and above all the enactment of the ELGA law (chapter 2.1). This would inaugurate a new e-health era in Austria. Trust would be provided by fundamental rules regarding data protection and investment protection. Further challenges come from the European level in the context of international exchange of patient data in the course of the EU funded large scale pilot epSOS (chapter 2.2). Special attention is drawn to the opt-in issue on national level regarding ELGA (chapter 2.1.3) as well as on European level regarding epSOS (chapter 2.2.1). Another important approach to assure the patients' freedom of choice is the Access Control Centre of ELGA (chapter 2.1.5), that will give patients full control over their data.

Acknowledgements

I would like to express my thanks to Mascha Glomb and Valerie Kainz for their assistance in structuring and preparing the German translation.

References

[1] Data Protection Act 2000 (DPA 2000 – Datenschutzgesetz 2000) Federal Law Gazette, Part I No. 165/1999 as amended by Federal Law Gazette, Part I No. 135/2009. In German.

[2] Health Telematics Act (HTA – Gesundheitstelematikgesetz) Federal Law Gazette, Part I No. 179/2004 as amended by Federal Law Gazette part I no. 103/2010. In German.

[3] E-Government Act (EGovA – E-Government-Gesetz) Federal Law Gazette, Part I No. 10/2004 as amended by Federal Law Gazette part I no. 111/2010. In German.

[4] Doctors Code 1998 (DC 1998 – Ärztegesetz 1998) Federal Law Gazette, Part I No. 169/1998 as amended by Federal Law Gazette, Part I No. 61/2010. In German.

[5] General Social Insurance Law (GSIL – Allgemeines Sozialversicherungsgesetz) Federal Law Gazette, No. 189/1955 as amended by Federal Law Gazette, Part I No. 24/2011. In German.

[6] Insurance Agreement Act 1958 (IAA – Vertragsversicherungsgesetz 1958) Federal Law Gazette, No. 2/1959 as amended by Federal Law Gazette, Part I No. 58/2010. In German.

[7] Genetic Engineering Act (GEA – Gentechnikgesetz) Federal Law Gazette, No. 510/1994 as amended by Federal Law Gazette, Part I No. 13/2006. In German.

[8] European Convention on Human Rights (ECHR), Federal Law Gazette, No. 210/1958 as amended by Federal Law Gazette, Part III No. 47/2010. In German.

[9] Basic Law on the General Rights of Nationals (BLGRN – Staatsgrundgesetz) Imperial Law Gazette, No. 142/1867 as amended by Federal Law Gazette, No. 684/1988. In German.

[10] Federal Constitutional Law (Bundes-Verfassungsgesetz) Federal Law Gazette, No. 1/1930 as amended by Federal Law Gazette, Part I No. 127/2009. In German.

[11] 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 (Data Protection Directive – DPD). OJ L 281, 23.11.1995, p. 31-50.

[12] Directive 2011/24/EU on the application of patients' rights in cross-border healthcare (Patients' Rights Directive – PRD). OJ L 88, 4.4.2011, p. 45-65.

[13] String-Commission. Electronic lifelong Health Record (EHR) – A privacy impact assessment – Version 1.0. Vienna: String-Commission; 2003. In German.

[14] Berner ES, Detmer DE, Simborg D. Will the Wave Finally Break? A Brief View of the Adoption of Electronic Medical Records in the United States. Journal of the American Medical Informatics Association 2005 Jan-Feb; 12(1): 3-7.

[15] http://ec.europa.eu/justice/policies/privacy/workinggroup /wpdocs/index_search_en.htm [cited 2012 Feb 20].

[16] Article 29 Data Protection Working Party. Working Document on the processing of personal data relating to health in electronic health records (EHR) [internet]. Brussels: Article 29 Data Protection Working Party; 2007; WP 131 [cited 2012 Mar 20]. Available from: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs /2007/wp131_en.pdf.

[17] Article 29 Data Protection Working Party. Working Document 01/2012 on epSOS [internet]. Brussels: Article 29 Data Protection Working Party; 2012; WP 189 [cited 2012 Mar 20]. Available from: http://ec.europa.eu/justice/data-protection /article-29/documentation/opinion-recommendation /files/2012/wp189_en.pdf.

[18] Mayer H. Legal opinion on the draft of an "Electronic-Health-Records-Framework Act – EHR-A" [internet]. Vienna: Medical Association of Vienna; 2012. p. 5 [cited 2012 Feb 12]. Available from: http://www.aekwien.at/media/ELGA-Gutachten.pdf. In German.

[19] Austrian Constitutional Court. Ruling 16.342/2001 of 2001 Nov 26. In German.

[20] Austrian Constitutional Court. Ruling 11.760/1988 of 1988 Jun 24. In German.

[21] http://www.wienkav.at/kav/ikt/ZeigeText.asp?ID=28413 [cited 2012 Feb 7]. In German.

[22] Industrial Code (IC – Gewerbeordnung) Federal Law Gazette, No. 194/1994 as amended by Federal Law Gazette, Part I No. 111/2010. In German.

[23] Austrian Data Protection Council. Opinion on the draft of an Health Telematics Act. 6/SN-341/ME of the 21st Austrian legislative term. [cited 2012 Feb 20]. p. 1 et sqq. Available from http://www.parlament.gv.at/PAKT/VHG/XXI/ME /ME_00341_06/imfname_000000.pdf. In German.

[24] Arge Daten. Opinion on the draft of an Health Telematics Act. 27/SN-341/ME of the 21st Austrian legislative term. [cited 2012 Feb 20]. p. 2 et sqq. Available from http://www.parlament.gv.at/PAKT/VHG/XXI/ME /ME_00341_27/imfname_000000.pdf. In German.

[25] Federal Chancellery. Opinion on the draft of an Health Telematics Act. 29/SN-341/ME of the 21st Austrian legislative term. [cited 2012 Feb 20]. p. 1 et sqq. Available from http://www.parlament.gv.at/PAKT/VHG/XXI/ME /ME_00341_29/imfname_000000.pdf. In German.

[26] Huber M. EHR law: Unconstitutional! Journal of the Austrian Medical Association 2012 Apr; 7a: 10. In German.

[27] Austrian Constitutional Court. Ruling 18.405/2008 of 2001 Mar 6. In German.

[28] Austrian Constitutional Court. Ruling 15.447/1999 of 1999 Mar 4. In German.

[29] Austrian Constitutional Court. Ruling 14.573/1996 of 1996 Sep 24. In German.

[30] Austrian Constitutional Court. Ruling 10.313/1984 of 1984 Dec 12. In German.

[31] Austrian Constitutional Court. Ruling 14.936/1997 of 1997 Oct 1. In German.

[32] Health Telematics Ordinance (HTO – Gesundheit-stelematikverordnung) Federal Law Gazette, Part II No. 451/2008 as amended by Federal Law Gazette, Part II No. 464/2010. In German.

[33] Electronic Signature Act (Signaturgesetz) Federal Law Gazette, Part. I No. 190/1999 as amended by Federal Law Gazette, Part I No. 75/2010. In German.

[34] Electronic Signature Ordinance 2008 (Signaturverordnung 2008) Federal Law Gazette, Part II No. 3/2008 as amended by Federal Law Gazette, Part II No. 401/2010. In German.

[35] Federal Law Gazette, Part I Nos. 23/2008, 36/2009 and 103/2010.

[36] Federal Law Gazette, Part I No. 103/2010.

[37] https://www.gesundheit.gv.at/Portal.Node/ghp/public/files /Ueberblick_Qualitaetskriterien.pdf [cited 2012 Feb 5]. In German.

[38] https://www.gesundheit.gv.at [cited 2012 Feb 7]. In German.

[39] http://www.who.int/classifications/icd/en [cited 2012 Mar 30].

[40] http://en.wikipedia.org/wiki/Triple_DES [cited 2012 Mar 30].

[41] SourcePin Register Authority. Creation of sourcePINs for natural persons [internet]. Vienna: Austrian Data Protection Commission [cited 2012 Mar 30]. Available from: http://www.stammzahlenregister.gv.at/site/6001 /default.aspx#sz. In German.

[42] http://en.wikipedia.org/wiki/Cipher_block_chaining - Cipher-block_chaining_.28CBC.29 [cited 2012 Mar 30].

[43] http://www.stammzahlenregister.gv.at/site/5109/default.aspx [cited 2012 Feb 2]. In German.

[44] http://www.stammzahlenregister.gv.at/site/6085/default.aspx [cited 2012 Feb 2]. In German.

[45] http://www.stammzahlenregister.gv.at/site/5983/default.aspx [cited 2012 Feb 2]. In German.

[46] Dentists Code (Zahnärztegesetz) Federal Law Gazette, Part I No. 126/2005 as amended by Federal Law Gazette, Part I No. 57/2008. In German.

[47] Leitner H. §54. In: Emberger H, Wallner F, editors. Commentary on the Austrian Doctor's Code. 2nd ed. Vienna: Verlagshaus der Ärzte; 2008. p. 259-68. In German.

[48] Federal Law Gazette, Part I No. 172/1999. In German.

[49] Milisits C. Wesentliche Neuerungen im Gesundheitsbereich. In: Karl B, Marko-Herzeg, Herausgeber. Jahrbuch Sozialversicherungsrecht 2010. Wien: Neuer Wissenschaftlicher Verlag; 2010. S. 83-104. German.

[50] Federal Law Gazette, Part I No. 1/2002. In German.

[51] Registration Act 1991 (Meldegesetz 1991) Federal Law Gazette, No. 9/1992 as amended by Federal Law Gazette, Part I No. 135/2009. In German.

[52] http://www.epsos.eu [cited Feb 3].

[53] Reimer S. The consent according to the data protection law. St. Gallen: Intelligent Law and Internet Applications; 2011. p. 65 et sq. [cited 2012 Feb 20]. Available from http://www.ilia.ch/downloads/20110205_ilia_ch_version.pdf. In German.

[54] Frohner J. Privacy and E-Health. In: Bauer L, Reimer S, editors. Manual on Austrian Data Protection Law. Vienna: Facultas; 2009. p. 253-71. In German.

[55] Reeve JF, Tenni PC, Peterson GM. An electronic prompt in dispensing software to promote clinical interventions by community pharmacists: a randomized controlled trial. British Journal of Clinical Pharmacology 2008; 65(3): 377-85.

[56] Lazarou J, Pomeranz BH, Corey PN. Incidence of Adverse Drug Reactions in Hospitalized Patients, JAMA 1998; 279(15): 1200-5.

[57] Wester K, Jönsson AK, Spigset O, Druid H, Hägg S. Incidence of fatal adverse drug reactions: a population based study. British Journal of Clinical Pharmacology 2008; 65(4): 573-9.

[58] US Department of Health and Human Services, US Food and Drug Administration. AERS Patient Outcomes by Year. Silver Spring: US Department f Heath and Human Services; 2010. [cited: 2012 Feb 16]. Available from http://www.fda.gov/Drugs /GuidanceComplianceRegulatoryInformation/Surveillance /AdverseDrugEffects/ucm070461.htm.

[59] Lee A. Adverse Drug Reactions. 2nd ed. London: Pharmaceutical Press; 2006.

[60] Austrian Constitutional Court. Ruling 17.500/2005 of 2005 Mar 10. In German.

[61] Constitutional Service of the Federal Chancellery. Opinion on the draft of an EHR Framework Act. Vienna: Constitutional Service of the Federal Chancellery; 2011; BKA-601.349/0001-V/5/2011. p. 4 et sqq. [cited 2012 Feb 20]. Available from http://www.parlament.gv.at/PAKT/VHG/XXIV/ME/ME_00260_24/imfname_210643.pdf. In German.

[62] http://www.epsos.eu/home/about-epsos.html [cited 2012 Feb 16].

[63] Hospitals- and Sanatoriums Law (Krankenanstalten- und Kuranstaltengesetz) Federal Law Gazette, No. 1/1957 as amended by Federal Law Gazette, Part I No. 147/2011. In German.

[64] Treaty on the Functioning of the European Union [consolidated version]. OJ C 83, 30.3.2010, p. 47-199.

[65] European Court of Justice. Case "Rechnungshof vs ORF" C-465/00, of 2003 May 20.

[66] Treaty establishing the European Community [consolidated version]. OJ C 325, 24.12.2002, p. 33-184.

[67] European Court of Justice. Case "Lindqvist" C-101/01, of 2003 Nov 6.

[68] epSOS. Framework Agreement on National Contact Points in the context of the Smart Open Services for European Patients Project (epSOS) – (version 2) [internet]. [cited 2012 Feb 20] Available from http://www.epsos.eu/fileadmin/content/pdf/Framework_Agreement_on_National_Contact_Points_V2.pdf.

[69] http://www.epsos.eu/for-health-professionals/how-can-health-professionals-participate.html [cited 2012 Mar 30].

[70] Commission Decision pursuant to Directive 95/46/EC on the adequate protection of personal data provided in Switzerland, 2000/518/EC. OJ L 215, 25.8.2000, p. 1-3.

[71] Brussels Convention on jurisdiction and the enforcement of judgments in civil and commercial matters [consolidated version]. OJ C 27, 26.1.1998, p. 1-27.

[72] Convention on jurisdiction and the enforcement of judgments in civil and commercial matters; done at Lugano on 1988 September 16, 88/592/EEC [consolidated version]. OJ L 319, 25.11.1988. p. 9-28.

[73] Regulation (EC) No. 44/2001 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters. OJ L 12, 16.1.2001, p. 1-23.

[74] Federal Law Gazette, No. 571/1992 as amended by Federal Law Gazette, No. 949/1994. In German.

[75] Regulation (EC) No. 593/2008 on the law applicable to contractual obligations (Rome I). OJ L 177, 4.7.2008, p. 6-16.

[76] Regulation (EC) No. 864/2007 on the law applicable to non-contractual obligations (Rome II). OJ L 199, 31.7.2007, p. 40-9.

[77] Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [internet]. COM(2012)11 final. [cited 2012 Feb 19] Available from: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

