

# SMART 2007/0059

—

Study on Legal Framework of  
Interoperable eHealth in Europe

## NATIONAL PROFILE POLAND

—

European Commission  
Directorate General Information Society

Brussels

—

---

## Table of Contents

|   |           |
|---|-----------|
| <b>SMART 2007/0059</b>  | <b>1</b>  |
| <b>EUROPEAN COMMISSION</b>                                      | <b>1</b>  |
| <b>1 DOCUMENTS</b>  | <b>4</b>  |
| 1.1 APPLICABLE DOCUMENTS  | 4         |
| 1.2 REFERENCE DOCUMENTS   | 4         |
| <b>2 GLOSSARY</b>   | <b>6</b>  |
| 2.1 DEFINITIONS   | 6         |
| 2.2 ACRONYMS  | 7         |
| <b>3 INTRODUCTION</b>   | <b>9</b>  |
| 3.1 GENERAL OVERVIEW OF THE POLISH HEALTHCARE SYSTEM            | 9         |
| 3.2 USE OF ICT IN THE POLISH HEALTHCARE SECTOR                  | 11        |
| 3.3 NATIONAL EHEALTH STRATEGY                                   | 11        |
| 3.4 REGULATORY FRAMEWORK FOR PATIENTS' SUMMARIES                | 13        |
| 3.5 REGULATORY FRAMEWORK FOR TELEMEDICINE                       | 14        |
| 3.6 REGULATORY FRAMEWORK FOR ELECTRONIC PRESCRIPTIONS           | 14        |
| 3.7 OVERVIEW OF RELEVANT LEGISLATION                            | 14        |
| <b>4 REGULATORY FRAMEWORK FOR THE HEALTHCARE PROFESSION</b>     | <b>16</b> |
| 4.1 LEGAL CONDITIONS FOR THE PRACTICE OF HEALTHCARE             | 16        |
| 4.2 CONTROL OVER THE PRACTICE OF MEDICINE                       | 17        |
| 4.3 PROFESSIONAL LIABILITY                                      | 17        |
| 4.4 PROFESSIONAL SECRECY  | 18        |
| <b>5 PROCESSING OF PERSONAL HEALTH DATA</b>                     | <b>19</b> |
| 5.1 SHORT OVERVIEW OF PERSONAL DATA PROTECTION LEGAL FRAMEWORK  | 19        |
| 5.2 TRANSPOSITION OF ARTICLE 8 OF DIRECTIVE 95/46/EC            | 20        |
| 5.3 INFORMATION AND ACCESS RIGHTS OF DATA SUBJECTS              | 21        |
| 5.4 OTHER RELEVANT RULES REGARDING PERSONAL DATA PROTECTION     | 21        |
| <b>6 RIGHTS AND DUTIES OF HEALTHCARE PROVIDERS AND PATIENTS</b> | <b>26</b> |

**Study on Legal Framework of Interoperable eHealth in Europe**

---

|  |  |           |
|--|--|-----------|
| <b>6.1</b>   | <b>SCOPE OF THE LAW</b>  | <b>26</b> |
| <b>6.2</b>   | <b>DUTY OF THE PATIENT TO CO-OPERATE</b>                       | <b>26</b> |
| <b>6.3</b>   | <b>RIGHT TO QUALITY CARE</b>                                   | <b>27</b> |
| <b>6.4</b>   | <b>RIGHT TO FREE CHOICE</b>                                    | <b>27</b> |
| <b>6.5</b>   | <b>RIGHTS RELATED TO INFORMATION ABOUT THE STATE OF HEALTH</b> | <b>27</b> |
| <b>6.6</b>   | <b>RIGHT TO GIVE CONSENT</b>                                   | <b>28</b> |
| <b>6.7</b>   | <b>RIGHTS RELATED TO THE PATIENT'S MEDICAL RECORD</b>          | <b>29</b> |
| <b>6.8</b>   | <b>RIGHT TO PROTECTION OF PRIVACY AND INTIMACY</b>             | <b>29</b> |
| <b>6.9</b>   | <b>RIGHT TO REPRESENTATION IN CASE OF INCOMPETENCE</b>         | <b>29</b> |
| <b>7</b>   | <b>IDENTITY MANAGEMENT IN THE HEALTH SECTOR</b>                | <b>30</b> |
| <b>7.1</b>   | <b>OVERVIEW</b>  | <b>30</b> |
| <b>7.2</b>   | <b>THE SIS CARD</b>  | <b>31</b> |
| <b>7.3</b>   | <b>CROSSROADS BANK FOR SOCIAL SECURITY</b>                     | <b>32</b> |
| <b>7.4</b>   | <b>PATIENT IDENTIFIER</b>                                      | <b>32</b> |
| <b>7.5</b>   | <b>AUTHENTICATION OF HEALTHCARE PROFESSIONALS</b>              | <b>32</b> |
| <b>7.6</b>   | <b>EXCHANGE OF HEALTH-RELATED DATA</b>                         | <b>34</b> |
| <b>8</b>   | <b>ELECTRONIC PRESCRIPTION</b>                                 | <b>35</b> |
| <b>9</b>   | <b>GENERAL ASSESSMENT</b>                                      | <b>36</b> |
| <b>ANNEX: CONTACT DETAILS OF NATIONAL CORRESPONDENTS</b> |  | <b>37</b> |
| <b>9.1</b>   | <b>PRIMARY CONTACT</b>   | <b>37</b> |
| <b>9.2</b>   | <b>ALTERNATIVE CONTACT</b>                                     | <b>37</b> |

**Study on Legal Framework of Interoperable eHealth in Europe**

## 1 Documents

### 1.1 Applicable Documents

|       |                                       |
|-------|---------------------------------------|
| [AD1] | Services Contract 30-CE-0162056/00-04 |
|       |                                       |

### 1.2 Reference Documents

|       |  |
|-------|--|
| [RD1] | Communication from the Commission, e-Health - making healthcare better for European citizens: An action plan for a European e-Health Area, 2004<br><a href="http://ec.europa.eu/information_society/doc/qualif/health/COM_2004_0356_F_EN_ACTE.pdf">http://ec.europa.eu/information_society/doc/qualif/health/COM_2004_0356_F_EN_ACTE.pdf</a> |
| [RD2] | eHealth Action Plan, Progress Report<br><a href="http://ec.europa.eu/information_society/activities/health/docs/policy/ehealth-ap-prog-report2005.pdf">http://ec.europa.eu/information_society/activities/health/docs/policy/ehealth-ap-prog-report2005.pdf</a>  |
| [RD3] | Recommendation of the Commission on eHealth interoperability,<br><a href="http://ec.europa.eu/information_society/activities/health/docs/policy/200807_02-interop_recom.pdf">http://ec.europa.eu/information_society/activities/health/docs/policy/200807_02-interop_recom.pdf</a>   |
| [RD4] | Database of European eHealth priorities and strategies (Empirica),<br><a href="http://www.ehealth-era.org/database/database.html">http://www.ehealth-era.org/database/database.html</a> (country profiles)   |
| [RD5] | European Observatory on Health Systems and Policies, Health Systems in Transition (HiT) country profiles,<br><a href="http://www.euro.who.int/observatory/Hits/TopPage">http://www.euro.who.int/observatory/Hits/TopPage</a>   |
| [RD6] | European Observatory on Health Systems and Policies, Patient Mobility in the European Union. Learning from experience,<br><a href="http://www.euro.who.int/observatory/Publications/20060522_4">http://www.euro.who.int/observatory/Publications/20060522_4</a>  |
| [RD7] | Report on Priority Topic Cluster One and Recommendations: Patient Summaries, <a href="http://www.ehealth-era.org/documents/eH-ERA_D2.3_Patient_Summaries_final_15-02-2007_revised.pdf">http://www.ehealth-era.org/documents/eH-ERA_D2.3_Patient_Summaries_final_15-02-2007_revised.pdf</a>   |
| [RD8] | Pilot on eHealth indicators: 'Benchmarking ICT use among General Practitioners in Europe (Empirica), final report:<br><a href="http://ec.europa.eu/information_society/europe/i2010/docs/benchmarking/">http://ec.europa.eu/information_society/europe/i2010/docs/benchmarking/</a>  |

Study on Legal Framework of Interoperable eHealth in Europe

|        |   |
|--------|---|
|        | <p><a href="#">gp_survey_final_report.pdf</a>,<br/>Country profiles:<br/><a href="http://ec.europa.eu/information_society/eeurope/i2010/benchmarking/index_en.htm">http://ec.europa.eu/information_society/eeurope/i2010/benchmarking/index_en.htm</a></p>  |
| [RD9]  | <p>Communication from the European Commission, “A Community framework on the application of patients' rights in cross-border healthcare”, 2 July, 2008, <a href="http://ec.europa.eu/health-eu/doc/com2008415_en.pdf">http://ec.europa.eu/health-eu/doc/com2008415_en.pdf</a></p>   |
| [RD10] | <p>Proposal for a Directive of the European Parliament and of the Council on the application of patients' rights in cross-border healthcare, <a href="http://ec.europa.eu/health-eu/doc/com2008414_en.pdf">http://ec.europa.eu/health-eu/doc/com2008414_en.pdf</a></p>  |
| [RD11] | <p>European Commission, IDABC, eID interoperability for public government services (with country profiles):<br/><a href="http://ec.europa.eu/idabc/en/document/6484/5938">http://ec.europa.eu/idabc/en/document/6484/5938</a></p>   |
| [RD12] | <p>European Commission, IDABC, eSig-Web (Electronic signatures applications in public government services – country overviews):<br/><a href="http://ec.europa.eu/idabc/en/chapter/6000">http://ec.europa.eu/idabc/en/chapter/6000</a></p>   |
| [RD13] | <p>Legally eHealth, Study on Legal and Regulatory Aspects of eHealth, <a href="http://www.ehma.org/projects/default.asp?NCID=140">http://www.ehma.org/projects/default.asp?NCID=140</a></p>   |
| [RD14] | <p>Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, <a href="http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML">http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML</a></p> |
| [RD15] | <p>Article 29 Data Protection Working Party, Working Document on the processing of personal data relating to health in electronic health records (EHR), WP 131,<br/><a href="http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp131_en.pdf">http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp131_en.pdf</a></p>   |
| [RD16] | <p>International Encyclopedia of Medical Law (editor: Herman Nys), <a href="http://www.ielaws.com/medical.htm">http://www.ielaws.com/medical.htm</a>, (with country monographs)</p>   |

## 2 Glossary

### 2.1 Definitions

In the course of this Study, a number of key notions are frequently referred to. To avoid any ambiguity, the following definitions apply to these notions and should also be used by the correspondents.

- **Authorization:** refers to:
  - the permission of an authenticated entity (e.g. a person) to perform a defined action or to access a defined resource/service
  - or: the process of determining, by evaluation of applicable permissions, whether an authenticated entity is allowed to perform a defined action or has access to a defined resource.
- **Data authentication:** information provided for verification, with more or lesser degrees of certainty, of the origin and the integrity of data.
- **eHealth:** a very broad term that encompasses many different activities related to the use of the information and communication technology (ICT) for healthcare. Many of these activities focus on administrative functions such as claims processing or records storage. However, there is an increasing use of e-health related to patient and clinical care.
- **Electronic health record:** a comprehensive medical record or similar documentation of the past and present physical and mental state of health of an individual in electronic form, and providing for ready availability of these data for medical treatment and other closely related purposes;
- **Electronic signature:** data in electronic form which are attached or logically associated with other electronic data and which serve as a method of data authentication.
- **ePrescription:** a medicinal prescription, as defined by Article 1(19) of Directive 2001/83/EC47, issued and transmitted electronically
- **Healthcare:** the prevention, treatment, and management of illness and the preservation of mental and physical well being through the services offered by the medical, nursing, and allied health professions. Health care embraces all the goods and services designed for people's health, including preventive, curative and palliative interventions, whether directed to individuals or to populations.
- **Health professional:** a doctor of medicine or a nurse responsible for general care or a dental practitioner or a midwife or a pharmacist within the meaning of Directive 2005/36/EC of the European Parliament and of the Council of 7 September 2005 on

**Study on Legal Framework of Interoperable eHealth in Europe**

the recognition of professional qualifications or another professional exercising activities in the healthcare sector which are restricted to a regulated profession as defined in Article 3(1)(a) of Directive 2005/36/EC.

- **Identification:** using claimed or observed attributes of an entity (e.g. a person) to distinguish the entity in a given context from other entities it interacts with (= entity authentication).
- **Identifier:** attribute or set of attributes of an entity (e.g. a person) which uniquely identifies the entity in a given context.
- **Identity management:** Identity management (ID management) is a broad administrative area that deals with identifying entities in a system (such as a country, a network, or an enterprise) and controlling their access to resources within that system by associating user rights and restrictions with the established identity.
- **Patient:** any natural person who receives or wishes to receive health care in a Member State;
- **Patient summary:** subsets of electronic health records that contain information for a particular application and particular purpose of use, such as an unscheduled care event or ePrescription;
- **Registration:** process in which a partial identity is assigned to an entity and the entity is granted a means by which it can be authenticated in the future.
- **Telemedicine:** exchange of medical information from one site to another via electronic communications with the purpose to improve patients' health status.

**2.2 Acronyms**

|                      |  |
|----------------------|--|
| <b>eIDM</b><br>..... | Electronic Identity Management   |
| <b>DRG</b><br>.....  | Diagnosis Related Groups   |
| <b>EKUZ</b><br>..... | Electronic Card for Health Insurance<br>( <i>Elektroniczna Karta Ubezpieczenia Zdrowotnego</i> ) |
| <b>HCI</b> .....     | Healthcare Institution   |
| ...                  |  |
| <b>HiT</b> .....     | Health in Transition   |
| ....                 |  |

**Study on Legal Framework of Interoperable eHealth in Europe**

---

|                   |  |
|-------------------|--|
| <b>NHF</b> .....  | National Health Fund   |
| .....             |  |
| <b>PKI</b> .....  | Public Key Infrastructure                                      |
| ....              |  |
| <b>RUM</b> .....  | Register of Health Services ( <i>Rejest Usług Medycznych</i> ) |
| ..                |  |
| <b>SIS</b> .....  | Social (security) Information System                           |
| ..                |  |
| <b>SSIN</b> ..... | Social Security Identification Number                          |
| ..                |  |

### 3 Introduction

#### 3.1 General overview of the Polish healthcare system

The evolution of the Polish healthcare system has been extensively analyzed in the Polish HiT country report published by the European Observatory on Health Systems and Policies (written by Krzysztof Kuszewski, Christian Gericke), referenced under [RD 5]:

“The Law on Universal Health Insurance, dated 6 February 1997, with later amendments, came into force on 1 January 1999 and radically changed the system of public health care, in terms of the structure and sources of finance. The establishment of mandatory health insurance broke with the centralized system of a national health service financed from the state budget. The former system was based on the right of every citizen to health services, which was administered by state authorities (Ministry of Health and voivodas). Health services were provided by public Healthcare Institutions with the status of budgetary entities. Sixteen regional sickness funds and one sickness fund for the uniformed forces were set up under the new system. They became holders of public health care funds that were raised primarily through health insurance contributions. The right to health services was linked to registration with a mandatory health insurance and payment of contributions. Public Healthcare Institutions changed their status to independent Healthcare Institutions obliged to cover their expenditures with their revenues from health services delivery. In April 2003, the sickness funds were replaced by a single National Health Fund, partly because of rising discontent with the new system among the insured population and partly for political reasons. The 1997 reform together with its numerous modifications introduced two major public sources of health care financing: universal health insurance contributions and budgetary expenditures from the state budget and budgets of voivodship, county and commune authorities. Owing to its dual nature, the system is defined as an insurance-budgetary system.” (p. 20-21).

“The NHF has the responsibility for planning and purchasing public financed health services. Health insurance contributions for certain groups of individuals not covered by the standard scheme and specific public health activities (such as the national health programmes which mainly focus on health prevention and promotion objectives) are funded directly by the state through general taxation. Complementary sources of financing include both formal and informal out-of-pocket payments, and to a lesser extent pre-payment schemes. Private health expenditure accounted for 27.5% of total health care expenditure in 2002. Around 60% of all out-of-pocket spending was on drugs and medical devices.” (p. XV)

Financial issues of healthcare services financed from public funds are comprehensively covered by the Act of 27 August on Health Care Services Financed from Public Sources<sup>1</sup>. Art.

---

<sup>1</sup> *Ustawa z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych*, Journal of Laws, No. 210, item 2135, with further amendments.

**Study on Legal Framework of Interoperable eHealth in Europe**

---

79(1) thereof establishes mandatory health insurance contributions at rate of 9.0% of its base, the latter generally corresponding to taxable income.

Organizationally, publicly financed healthcare services are predominantly provided by Independent Healthcare Institutions (HCIs) governed by the Act of 30 August 1991 on Healthcare Institutions.<sup>2</sup> For a brief outline of the system in this respect it is worth quoting the Polish HiT country report again:

“At present, territorial self-governments are founders of 90% of HCIs. Other forms – budgetary entity or budgetary enterprise – are permissible only if the founder agrees to maintain HCIs in one of those forms. The main characteristic of independent HCIs is their dependence on health insurance contributions. HCIs are distinguished by their legal status, which is acquired through registration by a relevant court. However, registration by a court must be preceded by registration in the register of Healthcare Institutions. This register is opened and kept by the Minister of Health or the voivoda, depending on the organizational structure and type of legal status granted by the Minister of Health or the voivoda.

HCIs (state or self-government) are completely separate from a founder, which is a specific legal form of public ownership. They are the successors of the former ZOZ and still get their revenues in the form of budgets. The founder does not bear responsibility for the obligations of the HCIs, which thereby gain substantial autonomy but also risk. Each HCI operates on a self-financing basis and covers all the costs of its operations and obligations. If an HCI is unable to cover its loss, then the founder of the HCI is obliged to do so. HCIs do not pay income tax. The independence of each HCI with respect to its founder is also limited by the founders’ supervising authority. In Poland, public and non-public Healthcare Institutions are put on an equal footing.” (p. 17)

It should be added that the public healthcare system in Poland has fallen into a decline, despite the health insurance contributions’ rate has risen from 8,25% in 2004 to 9% in 2007. Financial flows into the system have been magnified also by the unemployment rate falling down and the GNP growing dynamically in the years following the Polish accession to the EU. The decline has been manifested by high degree of hardly controllable debts which HCIs have taken out in previous years, patients’ dissatisfaction with long waiting lists and quality of public healthcare services, on the one hand, and recurring protests of medical professionals against their working conditions, on the other.

It has turned out, therefore, that the healthcare system suffers from high and structural inefficiencies, which can not be remedied merely by capital investments. During a “White Summit,” which collated the government and so called social partners, main themes of the future agenda were preliminary drawn. The themes, put together in “Recommendations of the White Summit Conference”, were endorsed on 19 March 2008 and published by the Ministry of Health on its web-site ([www.mz.gov.pl](http://www.mz.gov.pl)).

The Recommendations regard the most serious issues of the current situation: the question of reforming the HCIs system, rationalizing their management, restructuring their debts,

---

<sup>2</sup> *Ustawa z dnia 30 sierpnia 1991 r. o zakładach opieki zdrowotnej*, Journal of Laws Year 2007, No. 14, item 89, with further amendments.

## Study on Legal Framework of Interoperable eHealth in Europe

---

elaborating on private co-financing, determining a list of services guaranteed in return for the health insurance contributions,<sup>3</sup> introducing private health insurances, or improving working conditions for medical professionals.

Two points relating to the e-Health have been enclosed in the Recommendations, also. First, establishing a transparent IT system for registration of healthcare events and services, in compliance with rules on the medical data protection, was agreed. Second, the need for digital access of patients to information on services and their providers in the system was highlighted.

### 3.2 Use of ICT in the Polish healthcare sector

A latest report on status of the use of ICT by *general practitioners* in Poland has been drafted in the framework of the European Pilot Study on eHealth indicators: 'Benchmarking ICT use among General Practitioners in Europe' (Empirica), referenced under [RD 8].

From the Polish country brief, the following key findings can be taken over:

"In terms of infrastructure, 72% of the Polish GP practices use a computer. 62% of practices dispose of an Internet connection. In Poland, broadband connections have not yet arrived in force; they are used in only 32% of the GP practices. For all types of infrastructural prerequisites for a successful uptake of eHealth solutions, Poland scores below the EU27 averages.

When it comes to the use of eHealth solutions, Poland also shows results that are below the EU27 averages. Poland displays its best eHealth performance in the area of patient data storage. Yet even here usage rates lie far below the EU27 average. Administrative Patient data is recorded in around 50% of Polish GP practises while at least some type of medical electronic patient data is registered in around 40% of the GP practices.

In Poland, computers are used in consultation with the patients only to a very limited extent (11% of the GP practices). This percentage lags far behind the EU27 average of 66%. The use of Decision Support Systems is also rather the exception than the rule. 19% of Polish GPs use Decision Support Systems either for diagnosis or prescribing purposes, which corresponds to one of the lowest usage rates with regard to this indicator in the EU27.

The electronic transfer of individual patient data has as yet not very much arrived on the agenda of Polish GPs. An exception is the exchange of administrative patient data with reimbursers via networks, which is used by 23% of Polish GP practices. The exchange of medical data via networked connections is much less common: only 2% of the GP practices participating in the survey reported having exchanged medical data with other care providers while 10% received results from laboratories this way."

### 3.3 National eHealth strategy

---

<sup>3</sup> So far only a "negative" list of services excluded from the scope of services provided pursuant to Act on Health Care Services Financed from Public Sources has been defined, as an appendix to the Act.

## Study on Legal Framework of Interoperable eHealth in Europe

---

There have been three eHealth strategies in Poland so far:

1. “Poland – eHealth Strategy for 2004-2006” (*Strategia e-Zdrowie Polska na lata 2004-2006*, internal document of the Ministry of Health, September 2004);
2. “Strategy of information infrastructure development in healthcare and introduction of the European Health Insurance Card and Health Insurance Card” (*Strategia rozwoju systemu informacyjnego ochrony zdrowia oraz Koncepcja wdrażania Europejskiej Karty Ubezpieczenia Zdrowotnego i Karty Ubezpieczenia Zdrowotnego*, endorsed by the Council of Ministers in May 2005);
3. “Strategy of using information sources by the NHF and directions of developing the informatics system in the years 2007-2010” (*Strategia wykorzystania zasobów informacyjnych przez NFZ oraz kierunki rozwoju systemu informatycznego NFZ na lata 2007-2010*, internal document of the National Health Fund, updated version of October 2007), hereinafter: NHF Strategy.

None of the strategies has been implemented, though, which might be deemed one of the main reasons for the backwardness of the e-Health in Poland. To understand the reasons it is enough to pay attention to the fact that their implementation requires strong political support in a longer time-horizon. Yet the strategies have been devised shortly before parliamentary elections leading to entirely new government coalitions, and new concepts for e-Health again in need for time to ripen.

The last among the abovementioned strategies is the best example. The Strategy, endorsed by the management Council of NHF in July 2007, is based on the following conceptual assumptions: decentralization of processing, population mode of data gathering, avoiding monopolies, open standards, interoperability with public registers and making the information available to entitled bodies.

Based on these premises, the strategy outlines several aims: organizing data structure (medical event - product reimbursed), improving reliability of data (transaction authorization, data verification and cleaning systems), on-line processing of data on service providers and recipients, automation of data transfers, development of on-line modules, extension of information gathering on Electronic Health Record elements, optimization of processing (iterative review of historic solutions, elastic data archiving, adaptation of new tools), processing security (back-up hardware, hacking prevention, usage of the PKI).

To achieve these aims, the Strategy devises four main IT projects. These are:

1. Register of Health Services II (Rejest Usług Medycznych II) – RUM II;
2. digital prescription;
3. data warehouse of the second generation;
4. fraud detection system;

The RUM II - by far the biggest among the projects - presupposed developing a record system collecting detailed data about authorized healthcare events (services or transactions of relevance to the financial system of the healthcare). Within RUM II the data would encompass information about the nature of medical services, their providers, prescribed medicines, laboratory and consultation orders, referrals to hospital, etc. It would therefore aim at registering a set of basic data describing each contact of a patient with the service provider

**Study on Legal Framework of Interoperable eHealth in Europe**

---

of a certain specialization, in order to allow for objective assessment of healthcare processes on multiyear basis. The cost of e-cards and the IT infrastructure within the NFZ was assessed at about 400 mln PLN (circa 130 mln €). Production and personalization of the e-cards totaled 80% of the sum. The plans set a 2 year horizon for completing the project. Expected savings (elimination of mismanagement, fraud and waste) were calculated at 10 % of the health system budget, i.e. 4 billion PLN a year.

The idea and the functional details were taken over from RUM I, a pilot project which have been undertaken in the heaviest populated Polish region of the Upper Silesia (5 mln inhabitants) since 2001.<sup>4</sup> Using RUM I as a point of reference allowed for developing RUM II on the basis of an already working system. Yet it also opened the discussion about competition, because it favored the consortium of companies involved in RUM I. The concerns were only to a limited degree alleviated by declarations of the NHF management, according to which, as abovementioned, avoiding provider dependence ranked among the main assumptions of the implementation.

The second project – the digital prescription - was to provide stricter control over the trade in pharmaceuticals refunded by the Polish state. The budget of this project, devised for 2008-2009, amounted to 3 mln PLN.

The data warehouse was to replace the current basic system of monitoring healthcare events, allowing for aggregating and profiling these events, the data on which are collated by the regional branches of the NHF. This project, which aimed at clearing (verifying) the data processed regionally and presupposed enhanced on-line cooperation, was to be implemented in a year, starting from the second part of 2008, and had a budget allocation of 10-30 mln PLN.

Finally, a fraud detection system, the cost of which was estimated at 30-40 mln PLN, was to trace irregularities in financial flows, in order to discover fraud.

In the fall 2007 launching the implementation of all the four projects was announced, which was accompanied by declarations of appropriate financial coverage.

At the same time, however, parliamentary elections led to a new government. Head of the NHF, a person who had headed the regional branch of the Fund which implemented the RUM I and who essentially devised the Strategy, was removed from the office soon after the elections. Moreover, and of far more significance for the e-Health systems, the whole 2007 Strategy was denounced by the new Minister of Health as premature and preliminary, with the consequence of setting back its implementation. No substituting policy has been proposed so far.

**3.4 Regulatory framework for patients' summaries**

There is no regulatory framework for this field in Poland. No extracted version of patients' records is used in practice.

---

<sup>4</sup> See also sec. 7.2 of this report.

**Study on Legal Framework of Interoperable eHealth in Europe**

---

**3.5 Regulatory framework for telemedicine**

Art. 42 Act of 5 December 1996 on Professions of Physician and Dentist<sup>5</sup> provides explicitly that the doctor announces the state of health of a given person after examining him/her personally, unless separate legislation provides otherwise. No such a provision regarding telemedicine exists, which excludes setting diagnosis remotely, implicitly assuming that proper assessment requires physical contact with the patient, in order to receive the information which otherwise might be missing. Except for this only aspect of setting the (final) diagnosis, there is no other regulatory framework allowing or precluding telemedicine. It is assumed, without an explicit legal provisions in this matter, that the profession of a physician is to be exercised with due diligence, using appropriate means, current medical knowledge and professional ethics (compare sec. 6.3 of this report). If, therefore, a given telemedicine practice complies with the standards, it fits into both the obligations of medical professionals and rights of patients. On the other hand, as long as more old-fashioned treatment is still the only one available to the doctor, and complies with the medical knowledge requirement at the same time, the physician can not be blamed for not using telemedicine.

**3.6 Regulatory framework for electronic prescriptions**

Electronic prescriptions do not fit into the Polish law. Ordinance of the Minister of Health of 17 May 2007 on medical prescriptions,<sup>6</sup> issued pursuant to Art. 45(3) Act of 5 December 1996 on Professions of Physician and Dentist, makes it clear that prescriptions may assume only the paper form. For a more extensive discussion on this point compare sec. 8 of this report.

**3.7 Overview of relevant legislation**

No specific regulatory framework for telemedicine seems the most optimal solution. It allows for perceiving it from the right perspective, of the medical treatment which should be compliant with the current medical profession standards. By providing an environment which is flexible about means and clear about general medical treatment purposes, the regulatory framework is also appropriately accommodative for the new applications of the ICTs. The requirement that medical prescriptions is to be in paper form only may be regarded as outdated and running against the idea of e-Health. Nevertheless, what should be taken into account is that providing for the possibility of introducing e-prescriptions would not warrant their introduction in practice, as using them requires appropriate and complex interoperable medical infrastructure. This point highlights importance of an appropriate eHealth strategy, which in Poland seems by far more problematic and difficult than establishing its legal environment. If this prime drawback is overcome, then adjusting the executive act regulating

---

<sup>5</sup> *Ustawa z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty*, Journal of Laws Year 2005, No. 226, item 1943, with further amendments.

<sup>6</sup> *Rozporządzenie Ministra Zdrowia z dnia 17 maja 2007 r. w sprawie recept lekarskich*, Journal of Laws, Year 2007, No. 97, item 646, with further amendments.

**Study on Legal Framework of Interoperable eHealth in Europe**

---

medical prescriptions to the interoperable e-Health environment should be a task relatively easy to accomplish.

## 4 Regulatory framework for the healthcare profession

### 4.1 Legal conditions for the practice of healthcare

Art. 5(1) Act on Professions of Physician and Dentist authorizes regional medical councils (bodies of regional medical chambers) to grant the right of exercising the profession of a physician or dentist if the applicant:

- 1) is a citizen of Poland or another EU member state;
- 2) he/she holds:
  - a) a medical doctor (physician or dentist) diploma issued by a Polish higher education institution or
  - b) a document (associated with an appropriate certificate) formally confirming qualifications of the physician or dentist, issued by another EU member state in compliance with minimum educational requirements set by EU law, if the state is enrolled on a list promulgated by the Minister of Health;
  - c) a medical doctor diploma issued by states outside the EU if the diploma has been recognized as equal in Poland and complies with minimum educational requirements set by EU law,
- 3) is of full legal actions capacity;
- 4) his/her health allows for exercising the profession;
- 5) is of impeccable ethical conduct;

Additionally, regional medical councils grant citizens of other EU countries complying with the abovementioned conditions the right to exercise the medical profession if the applicant can use spoken and written Polish to the extent specified by an executive act and necessary to exercise the profession (art. 5(2)). This requirement does not apply to those who have studied medicine in Polish (*Id.*).

Polish or third countries' doctors should, additionally, accomplish medical placement and pass a state exam (art. 5(3)). These requirements do not regard medical doctors from other EU countries if they possess the abovementioned appropriate certificate (*Id.*).

Doctors from other EEA member states and Switzerland, who do not comply with the abovementioned requirement of documents formally certifying qualifications may be granted the right to exercise the profession if (art. 5a):

- 1) he/she possesses, first, a document certifying required medical qualifications, confirming that the education started before dates specified in the act regarding each member state and, second, a certificate issued by relevant authorities of a given member state confirming that the doctor has actually and legally exercised the profession for at least three consecutive years during five years directly preceding issuing the certificate, or
- 2) he/she possesses, first, a document confirming formal medical qualifications issued by another EU member state, other than documents from the list produced by the Minister of Health and a certificate issued by the relevant authorities of the member state certifying that the studies completed by its bearer comply with minimum requirements set by the relevant EU legislation and that the document is recognized as equal with documents from the abovementioned list.

Similar requirements are provided for dentists (Art. 5b).

Further mechanisms of mutual recognition are laid down for situations of inability to provide the abovementioned certificate confirming required periods of exercising the profession (Art. 5c).

## Study on Legal Framework of Interoperable eHealth in Europe

---

The right should be granted not later than 3 months after delivering all the required documents to the regional medical council (Art. 6a(1)).

Doctors granted with the right are entered into a register held by the relevant regional medical council (art. 8.1). For a more extensive discussion on this point compare sec. 7.5 of this report.

### 4.2 Control over the practice of medicine

Pursuant to Act on Professions of Physician and Dentist medical practices (individual, special individual and group) are supervised by the relevant body holding the register of medical practices (Art. 54(1)), i.e. the regional medical council relevant for the place of exercising the profession (Art. 50(1)). The supervising body is entitled to undertake necessary inspections and to issue recommendations aiming at removing shortages and imperfections (Art. 54(2)). The Chief Medical Council has the same authority over the whole country (Art. 54(3)). Controlling bodies may share inspection information with relevant authorities, on their request (Art. 54(4)).

HCIIs are controlled by their establishers (Art. 67(1) Act on Healthcare Institutions). The control encompasses not only medical aspects, but also relevant management and financial issues (Art. 67(3)).

### 4.3 Professional liability

The Act on Medical Chambers<sup>7</sup> and an executive ordinance to it<sup>8</sup> provide for a specific disciplinary liability framework. Disciplinary proceedings before the courts of the medical vocational corporation may be triggered by an offence to the medical ethics, professional deontology and by an infringement of the provisions on exercising the profession of the medical doctor (art. 41 Act on Medical Chambers). The medical court may adopt the following penalties (art. 42.1):

- 1) admonition;
- 2) reprimand;
- 3) suspension of the right to exercise the profession, for the period of 6 months to 3 years;
- 4) deprivation of the right to exercise the profession.

Appeals are directed to relevant labor and social insurance state courts (art. 42.2).

Civil liability and criminal liability of physicians for damage or injury caused by improper performance of the medical duties is governed by the general rules of civil and criminal law.

---

<sup>7</sup> *Ustawa z dnia 17 maja 1989 r. o izbach lekarskich*, Journal of Laws, Year 1989, No. 30, item 158, with further amendments.

<sup>8</sup> Ordinance of the Minister of Health and Social Welfare of 26 September 1990 on procedure regarding professional liability of physicians (*Rozporządzenie Ministra Zdrowia i Opieki Społecznej z dnia 26 września 1990 r. w sprawie postępowania w przedmiocie odpowiedzialności zawodowej lekarzy*), Journal of Laws, Year 1990, No. 69, item 406, with further amendments.

**Study on Legal Framework of Interoperable eHealth in Europe**

---

Civil liability of a physician originates from tort or contract. Different liability patterns may occur in practice. Contractual liability occurs when a physician or a healthcare institution signs a service provision contract directly with the patient. When, however, the service is remunerated from the health insurance scheme, and no separate contract is signed with the patient, the liability is based on tort. The same holds for liability of a physician employed by a healthcare institution, if he/she does not sign a separate contract with the patient. Liabilities of the healthcare institution (contractual or based on tort) and of the physician (based on tort) concur in such a situation. Physicians are liable for damages caused by their personnel on general terms.

Underinvestment and comparatively poor organization of the healthcare system in Poland, and difficult working conditions of physicians (multiplying employment due to limited salaries) in public HCIs have been the main cause of damages or injuries leading to civil liability trials.

**4.4 Professional secrecy**

Professional medical secrecy is broad in Poland, encompassing “information related to the patient and received by reason of exercising the profession” (art. 40(1) Act on Professions of Physician and Dentist). The information can not be revealed even after demise of the patient (art. 40(3)).

Infringement of the obligation leads to an offence of revealing professional secrecy and ensues penal sanctions pursuant to Art. 266 § 1 Penal Code.

The Penal Code provides, however, that the sanction is triggered only when revealing takes place against a statutory provision or the obligation assumed voluntarily. Act on Professions of Physician and Dentist is relevant in this matter, also, as it provides certain exceptions to the general obligation of professional secrecy. The obligation is exempted when (art. 40(2)):

- 1) it is provided so in separate legislation;
- 2) medical test or examination has been undertaken at the request of the person authorized by bodies and institutions pursuant to separate legislation; in this situation the physician is obliged to inform only the bodies and institutions about the health status of the patient;
- 3) secrecy may cause danger to life or health of the patient or other persons;
- 4) the patient or his/her representative consents to reveal the information, after being informed about disadvantages of revealing the information;
- 5) it is necessary to reveal the information to another physician or persons participating in providing healthcare service;
- 6) it is necessary for practical professional education of medicine;
- 7) it is necessary for scientific purposes;
- 8) it is necessary to reveal the information to a court physician.

---

## 5 Processing of personal health data

### 5.1 Short overview of personal data protection legal framework

The Directive 95/46/EC was transposed into the Polish law by the Act of 29 August 1997 on Protection of Personal Data.<sup>9</sup>

Its provisions follow the directive closely with regard to:

- definitions of essential concepts: personal data, processing, controller, third party and consent (art. 2 of the Directive); the Polish law does not, however, recognize a separate category of processors, treating them as a certain kind of third parties and aligning their obligations with those of “processors” as defined in the directive; the only category which is defined differently (narrower) than the counterpart term in the directive is the “recipient”. While the directive excludes from the term only “authorities which may receive data in the framework of a particular inquiry” (art. 2g), the Polish act (art. 7(6)) does not treat as recipients also:
  - a) data subjects;
  - b) those authorised to process the data;
  - c) representatives of entities processing personal data which have their seat or place of residence in a third country;
  - d) parties acting as “processors” pursuant to the directive;
- rules regarding data quality (art. 6 Directive), which are set by the Polish law in the context of obligations put on the data controller (art. 26 Act on Protection of Personal Data); the directive provision according to which “further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards” (art. 6(1)(b)) is transposed by allowing processing for these purposes only when it does not infringe rights and freedoms of data subjects and, additionally, another legitimate ground for processing exists (art. 26(2) Act on Protection of Personal Data). By requiring another ground for processing, the separate exception referring to historical, statistical or scientific purposes becomes a dead letter;
- the criteria for making personal data processing legitimate (art. 7 of the Directive); the Act on Protection of Personal Data provides, however, that deletion of data does not require a data subject’s consent (art. 23(1)(1)).
- information to be given by the controller to the data subject (art. 10-11 of the Directive); the Act on Protection of Personal Data requires that, when the data have

---

<sup>9</sup> *Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych*, Journal of Laws, Year 2002, No. 101, item 926, with further amendments.

## Study on Legal Framework of Interoperable eHealth in Europe

---

not been obtained from the data subject, the latter should be informed about the source of the data as well (art. 25(1)(3)).

- the data subject's rights (art. 12, 14 and 15 of the Directive), which are clipped together in the Act on Protection of Personal Data by a general right to control data processing by the data subject (art. 32(1));
- provisions with regard to confidentiality and security of processing (art. 16-17 of the Directive);
- notification of processing to the data protection supervisory authority (art. 18-19 of the Directive);
- status and competences of the data protection supervisory authority (art. 20, 21, 22 and 28 of the Directive): more details about the Polish Inspector General for the Protection of Personal Data can be found at <http://www.giodo.gov.pl>.
- liability for damages as a result of illegal processing (art. 23 of the Directive);
- transfer of personal data to third countries, outside the EU (art. 25-26 of the Directive).

### 5.2 Transposition of article 8 of Directive 95/46/EC

Data on health status and genetic code are regarded by the Act on Protection of Personal Data as sensitive personal data (art. 27(1) Act on Protection of Personal Data).

The list of exceptions to the general prohibition of processing sensitive data is, in compliance with art. 8(4) Directive, longer than the five item list of its art. 8(2) Directive. The relevant provision (art. 27(2) Act on Personal Data Protection) regards 10 situations.

For the purposes of this study the following exceptions should be cited:

1. the data subject has consented in writing, unless processing is restricted to deletion of data (art. 27(2)(1)), or
2. specific purpose of separate legislation allows for processing the data without consent of the data subject and provides complete data protection guarantees (art. 27(2)(2)), or
3. processing is necessary to protect vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his/his consent, until a legal representative is established (art. 27(2)(3)), or
4. data is processed for provision of care or treatment or provision of health-care services by those professionally providing treatment, other medical services or health-care management, and if complete data protection guarantees are provided (art. 27(2)(7));
5. processing is necessary for scientific research; research results can not be published in a way identifying data subjects (art. 27(2)(9)).

## Study on Legal Framework of Interoperable eHealth in Europe

---

The following comments can be made with regard to art. 27 Act on Protection of Personal Data:

- Data on health status is a very broad category, covering all possible health situations, in any time-span.
- The consent should be “in writing”; the term does not cover in Poland electronic means, unless the consent is signed with a secure (equivalent of advanced) electronic signature verified with a qualified certificate; electronic documents are equal with written ones only if they are associated with this form of an electronic signature.
- Processing of sensitive data (including those regarding health-status) or certain processing legality conditions (e.g. a consent of the data subject) do not ensue additional information obligations for the data controller; it may be attributable to the broad range of the basic informational obligations, covering also issues like reasons for processing and a list of the categories of persons who might have access to the data.
- “Complete data protection guarantees” should be understood as corresponding to the protection standard of the Act on Protection of Personal Data.
- Authorization to process the data by those professionally providing treatment, or other medical services, or healthcare management is a broad one, including the whole span of medical services and the whole healthcare management.

### 5.3 Information and access rights of data subjects

Personal data regarding health is contained in patients’ records. Provisions on the records and rules for accessing them are discussed in the next sec. of this report.

### 5.4 Other relevant rules regarding personal data protection

Legislation on medical records defines the breadth of the “healthcare exception” (art. 27(2)(7) Act on Protection of Personal Data) and establishes independent protection regimes, despite based on similar assumptions as the general data protection system.

There are two regulatory frameworks for medical records in Poland. The first derives from Art. 41 Act on Professions of Physician and Dentist, which requires that medical doctors keep individual medical records (sec. 1). The Ordinance of the Minister of Health of 30 July 2001 on types of individual medical patients’ records, modes of holding them and detailed conditions for making them available<sup>10</sup> elaborates on the issue.

---

<sup>10</sup> *Rozporządzenie Ministra Zdrowia z dnia 30 lipca 2001 r. w sprawie rodzajów indywidualnej dokumentacji medycznej, sposobu jej prowadzenia oraz szczegółowych warunków jej udostępniania*, Journal of Laws Year 2001, No. 83, item 903.

## Study on Legal Framework of Interoperable eHealth in Europe

---

When the medical profession is exercised within a health care institution, art. 18 Act on Healthcare Institutions provides for the framework of processing the health care data. As a general principle, HCIs are obliged to protect data enclosed in patients' records (art. 18(2)). The records are made available to (art. 18(3)):

1. the patient or his/her legal representative or a person authorized by the patient;
2. HCIs, organizational entities of the institutions and persons exercising the medical profession outside the HCIs, if the documentation is necessary for providing continuity of healthcare;
3. state authorities responsible for health and bodies of the vocational corporation, to the extent necessary for performing control and supervision;
4. minister responsible for health, courts, public prosecutors, court doctors, disciplinary courts and prosecutors - in relation to given proceedings;
5. bodies and institutions authorized pursuant to separate legislation, if the examination is given on their request;
6. pension authorities - in relation to given proceedings;
7. registers of medical services – to the extent necessary for holding them;
8. insurance companies – on terms established by separate legislation.

Medical records may be made available also for educational or research purposes, in form precluding identifying the data subject (art. 18(4)).

Medical records are made available (art. 18(4a)):

- 1) for inspection in the health care institution;
- 2) through making copies;
- 3) through handing over the original document after receiving a receipt and on the condition of return, if the body authorized demands original documents.

The issues of what information patients' records in HCIs should comprise in detail and how the records are to be processed are left to executive ordinances: one on HCIs in general, and three for more specific kinds of HCIs: those established by the Minister of Interior and Administration, the Minister of Justice and the Minister of Defence. The general Ordinance of the Minister of Health of 21 December 2006 on types and scope of medical records in Healthcare Institutions and modes of processing them<sup>11</sup> will be further discussed in detail, while the other two will be mentioned only briefly, in the context of digital patient's records.<sup>12</sup> The Ordinance based on the Act on Professions of Physician and Dentist: on types of individual medical patients' records, modes of holding them and detailed conditions for making them available refers to healthcare services provided outside HCIs (§ 1). It defines the "medical record" as each physically separated information carrier which allows, at least, for

---

<sup>11</sup> *Rozporządzenie Ministra Zdrowia z dnia 21 grudnia 2006 r. w sprawie rodzajów i zakresu dokumentacji medycznej w zakładach opieki zdrowotnej oraz sposobu jej przetwarzania*, Journal of Laws Year 2006, No. 247, item 1819, with further amendments.

<sup>12</sup> The third Ordinance specific HCIs, of the Minister of Defence, has not been issued so far. (spr.)

**Study on Legal Framework of Interoperable eHealth in Europe**

---

determining the patient, the physician, data regarding health status of the patient or health services provided and date of creating the record (§ 2.2).

The records are held in the written form (§ 3). Yet additionally they can also be recorded on a digital carrier if the following conditions are fulfilled (§ 5):

- 1) selective access to the information filing system is retained;
- 2) the information filing system is protected from unauthorized access;
- 3) the information filing system is protected from destruction;
- 4) the information filing system allows for holding the record in a written form;
- 5) printouts signed by the physician are produced and stored;

Heeding the requirements, EHRs outside HCIs may be regarded only as back-up copies of their paper counterparts.

Information from medical records may be shared with other doctors when necessary for examinations, tests, or consultations (§ 10). Moreover, the doctor submits the medical records for inspection or allows for making copies paid by the requesting person (§ 18(1)). Submitting medical records for inspection may be requested by: the patient, his/her legal representative, a person authorised by the patient or by separate legislation, and, in case of demise, those authorised by the patient to receive the record (§ 18(2)).

The Ordinance based on Act on Healthcare Institutions (on types and scope of medical records in Healthcare Institutions and modes of processing them) devotes a separate, extensive chapter to EHRs. This is justified by the fact that HCIs provide most of medical services and in fact all the more complex ones. Thus they require more flexible legislative approach towards digital storage and processing of the documents, allowing for more efficient processing and retrieval.

HCIs may hold EHRs if the following conditions are fulfilled (§ 54(1)):

- 1) selective access to the information filing system is retained;
- 2) the information filing system is protected from unauthorized access;
- 3) the information filing system is protected from destruction, damage, or loss;
- 4) record of inserts and their originators is kept;

The abovementioned requirement of protecting the information filing system is complied with if the following conditions regarding the system are fulfilled on a permanent basis (§ 60(1)):

- 1) it is available only for those authorized;
- 2) it is protected from random or unauthorised destruction;
- 3) protective means and methods used are of universally recognized effectiveness.

Moreover, protection of digital records requires in particular (§ 60(2)):

- 1) systematic risk analysis;
- 2) establishing and using protection procedures, including those regarding access and storage;
- 3) using adequate protection means;
- 4) instant control of all organizational and technical protection means, and periodic assessment of their effectiveness.

Information systems used for holding EHRs should allow for printing the documents (§ 54(2)). Creating and signing EHRs consists of recording a data set on a data carrier and signing it with a digital signature (§ 55(1)). The documents non-existing in the digital form (e.g. X-rays) should be scanned to a usable format and placed in an appropriate digital file,

**Study on Legal Framework of Interoperable eHealth in Europe**

---

together with the electronic signature of the scanning person (§ 55(4)). If it is necessary to attach a physical material to the record, the material should be marked in a way allowing for its association with the digital record (§ 55(5)). The records, to retain their readability and standardisation, should be produced in the XML format (§ 55(2)). Time stamping should be used for ascertaining the date of creating the document, of signing it and in order to retain chronology of inserts in the internal overall records (§ 55(3)). EHRs should be recorded on a digital carrier in a way which allows for verifying its integrity, verifying the digital signature or other identifying data and which allows to read all the information contained therein, up to expiry of the retention period (§ 56).

The Ordinance provides that digital records are made available by (§ 57(1)):

- 1) handing over the digital carrier with a recorded copy of the record;
  - 2) electronic transfer of the record;
  - 3) handing over printouts;
- depending on request of the entitled person.

Making the EHRs available should respect its integrity and data protection rules (§ 57(2)). In order to reinforce the first of the requirements, digital records made available should be signed with a secure (equivalent to advanced) electronic signature verified by a qualified certificate (§ 57(3)). The recipient is to confirm receiving the digital record with a handwritten or a digital signature (§ 57(5)).

Regardless of the form, the record is made available to the patient, his/her legal representative and bodies authorised pursuant to other acts in a way guaranteeing personal data confidentiality and protection (§ 52(2)).

Records should be stored for a statutory period (of 20 years in general) and irretrievably deleted afterwards (§ 50(1)). If durability of the carrier is shorter than the storage period, then the records should be moved to another carrier before the durability period expires (§ 58(3)). The first of the ordinances on more specific HCIs - the Ordinance of the Minister of Interior and Administration of 25 October 2007 on types and scope and modes of processing of medical records in Healthcare Institutions established by the Minister of Interior<sup>13</sup> - follows the provisions of the general ordinance regarding EHRs literally. The other one – the Ordinance of the Minister of Justice of 19 September 2007 on types and scope of medical records in Healthcare Institutions for prisoners and modes of processing them<sup>14</sup> - contains only more general provisions regarding digital patients' records. These are based on the general ordinance either.

---

<sup>13</sup> *Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 25 października 2007 r. w sprawie rodzaju i zakresu oraz sposobu przetwarzania dokumentacji medycznej w zakładach opieki zdrowotnej utworzonych przez ministra właściwego do spraw wewnętrznych*, Journal of Laws Year 2007, No. 217, item 1614.

<sup>14</sup> *Rozporządzenie Ministra Sprawiedliwości z dnia 19 września 2007 r. w sprawie rodzajów i zakresu dokumentacji medycznej w zakładach opieki zdrowotnej dla osób pozbawionych wolności oraz sposobu jej przetwarzania*, Journal of Laws Year 2007, No. 185, item 1319.

**Study on Legal Framework of Interoperable eHealth in Europe**

---

To sum up, the Polish law provides for a comprehensive regulatory framework for EHRs in HCIs, which seems to strike the right balance between security, elasticity and feasibility. To less extent the same can be said about EHRs held by medical professionals, when the profession is exercised outside the institutional framework of HCIs. Digital filing systems are then regarded only as an ancillary method of holding the records, introduced along the paper ones. This feature diminishes attractiveness of the digital form, and it may be argued that, instead of introducing the obligation to print out documents stored in a digital filing system, an obligation to use a system which allows for printing the documents (without a duty actually to do this) should suffice. Such an obligation would facilitate introduction of EHRs in private practices and would align rules in this respect with those binding on HCIs.

## 6 Rights and duties of healthcare providers and patients

There are two statutory acts pertinent to general rights and duties in the healthcare sector: Act on Professions of Physician and Dentist and Act on Healthcare Institutions. First of the two provides for principles of performing the profession (including medical experiments) (Chapter 5). The other one devotes a separate chapter (No. 1a) to patient's rights in HCIs.

### 6.1 Scope of the law

The term "patient" is not defined in either of the two acts, as implicitly clear enough. "Healthcare service" is defined, in art. 3 Act on Healthcare Institutions, as an action aimed at preserving, rescuing, restoring, and improving health, and other medical actions stemming from the medical process or separate provisions on principles of performing them, in particular related to:

- 1) examination and medical consultation;
- 2) treatment;
- 3) examination and psychological therapy;
- 4) medical rehabilitation;
- 5) medical care over pregnancy;
- 6) care over healthy children;
- 7) diagnostic tests, including medical analysis;
- 8) nursing patients;
- 9) nursing disabled;
- 10) palliative and hospice nursing;
- 11) announcing opinions about health status;
- 12) medical prevention;
- 13) technical activities regarding prosthodontics and orthodontics;
- 14) supply of orthopedic articles and auxiliary materials;

Health professionals in the current state of the legislation are: physicians, dentists, midwives, pharmacists, physiotherapists, nurses, dentist assistants, laboratory diagnosticians, dieticians, paramedics, medical physicists, dentist hygienists, speech therapists, massage therapists, medical caregivers, baby-minders, optometrists, ear prosthodontists, medical rescuers, electroradiology technicians, dentist technicians, technicians of medical analysis, orthopaedic technicians, pharmacy technicians, optical technicians, exercise therapists.<sup>15</sup>

### 6.2 Duty of the patient to co-operate

There is no general duty of a patient to cooperate. Such a duty would go counter the consent related rights. In cases when the medical service may be provided irrespective of the refusal to consent, an implicit obligation to cooperate may be deduced. Yet it is highly questionable whether the obligation is enforceable in practice by any other means than appropriate

---

<sup>15</sup> List available at the web-site of the Ministry of Health: <http://www.mz.gov.pl/wwwmz/index>.

## Study on Legal Framework of Interoperable eHealth in Europe

---

professional persuasion, an issue which resides in the sphere of due diligence and medical knowledge rather than law.

### 6.3 Right to quality care

The Act on Professions of Physician and Dentist provides indications for the required standard of quality care. According to its art. 4 “the doctor is obliged to carry out his profession in compliance with recommendations of the current medical knowledge, means and preventive measures available to him, diagnosis and curing in conformity with professional ethics and due diligence”. Similarly, pursuant to art. 19 Act on Healthcare Institutions patients have the right to healthcare services complying with medical knowledge. Disregard for these principles may amount to claims for damages.

### 6.4 Right to free choice

Scope of the right to free choice of publicly financed healthcare services is determined by the Act on Healthcare Services Financed from Public Sources. Free choice is unquestionable, though not legally determined, in privately financed services.

As a general principle, recipients of public medical services have the right to choose the physician, nurse and midwife of the basic healthcare services twice a year, pursuant to art. 28(1) of the Act. Fee for each next change is 80 PLN.

Providers of outpatient specialist medical services and hospitals may be freely chosen from the list of those which have signed a contract with the NHF (art. 29). The same applies to services provided by dentists, if the service has been entered into the list of guaranteed services (art. 31).

In practice the free choice is limited by capabilities of the HCIs to provide services, which is by far under the generally expected level in Poland.

### 6.5 Rights related to information about the state of health

Patients have the right to learn about their state of health pursuant to art. 19(1)(2) Act on Healthcare Institutions. Moreover, according to art. 31(1), (2), (5) and (6) Act on Professions of Physician and Dentist, doctors are obliged to provide the patient (when he/she is at least 16 years old) or his/her legal representative (when the representative has been established) with an accessible information about: his/her health status, the diagnosis, proposed and possible methods of diagnosis and treatment, foreseeable consequences of applying or abandoning them, medical outcome and prognosis. Others may receive the information from the doctor only when the patient consents (art. 31(2)). If the patient is under 16 years old, the doctor provides him/her with information necessary for the treatment and allows him/her to express an opinion (art. 31(7)). A representative or a person having custody of the patient is informed comprehensively in these cases (art. 31(6)).

In exceptional situations, when the prognosis is unfavorable to the patient, the doctor may limit information on health status and prognosis, if, according to his/her assessment, it is in the interest of the patient. Instead, the patient’s representative or another person authorized by

**Study on Legal Framework of Interoperable eHealth in Europe**

---

the patient should be informed. If the patient demands so, the information should be revealed to him/her nevertheless (art. 31(4)).

**6.6 Right to give consent**

The right to consent, or refuse it after receiving appropriate information, is another right pursuant to Act on Healthcare Institutions (art. 19(1)(3)). Moreover, art. 32(1) Act on Professions of Physician and Dentist allows for examination or providing other medical treatment after the patient consents, unless otherwise provided in legislation. If the patient is minor or unable to express the consent consciously, a consent of his/her legal representative is required, and when no legal representative has been established or the representative is unreachable – of a tutelary court (art. 32(2), (8)). The doctor may provide medical treatment without consent when the delay endangers seriously health or life of the patient. In this situation the physician is obliged, if possible, to consult another physician, preferably of the same specialization (art. 32(9)).

The consent may be expressed orally or even by behavior which undoubtedly expresses the will to undergo medical activities proposed by the doctor (art. 32(7)). A person having custody of the patient may also consent examination (art. 32(3)). Generally the obligation to obtain the consent applies if the patient is more than 16 years old (art. 32(5)). Yet when he/she is less than 18 years old, but more than 16 years old, a consent of a tutelary court outweighs refusal, even if the refusal is supported by a legal representative or a person having custody of the patient. The same applies when those declared legally incapacitated, psychiatric patients or mentally handicapped, but of a sufficient insight, refuse medical service (art. 32(6)). Examination or another medical service may be provided without consent also when the patient needs an immediate medical assistance, due to the state of his/her health or his/her age receiving the consent is impossible and it is impossible to communicate with a legal representative or a person having custody of the patient (art. 33(1)). The decision, when possible, should be consulted with another physician (art. 33(2)) and in any case recorded in the patient's medical record (art. 33(3)).

A written consent is required for surgery or applying a medical or diagnostic method of a high risk (art. 34(1)). Before receiving the consent, the doctor is obliged to provide the patient with information described in sec. 6.5 of this report (art. 34(2)). In the case of minors, those declared legally incapacitated or unable to express their consent in writing consciously, a legal representative should consent, and when the representative has not been established – a tutelary court (art. 34(3)). Yet if the patient is more than 16 years old, also his/her written consent is required (art. 34(4)). When the patient is less than 18 years old, but more than 16 years old, a consent of a tutelary court may outweigh refusal, also when a legal representative or a person having custody of the patient supports it. The same applies when those declared legally incapacitated, psychiatric patients or mentally handicapped, but of a sufficient insight, refuse medical service (art. 34(5)).

When a legal representative does not agree on an uncertain medical service necessary for removing serious danger to health or life, the service may be provided with a consent of the tutelary court (art. 34(6)). Uncertain medical services may be provided without consent also

**Study on Legal Framework of Interoperable eHealth in Europe**

---

when the patient needs an immediate medical assistance, due to the state of his/her health or age receiving the consent is impossible and it is impossible to communicate with a legal representative or a person having custody of the patient (art. 34(7)). Circumstances of such a situation should be noted in the medical record, if the consent is obtained otherwise than from the patient, or if the medical service is provided without it (art. 34(8)).

If, during surgery or treatment, a situation occurs which should be taken into account not to expose the patient to a serious danger, and receiving the consent is not feasible, the physician may reschedule the service in order to take the situation into account, even without the consent. He/she should consult another physician, of the same specialization if feasible (art. 35(1)). The situation should be noted in the medical record. The patient, his legal representative, person having custody of the patient or the tutelary court should receive appropriate information (art. 35(2)).

**6.7 Rights related to the patient's medical record**

Legislation on medical records (compare *supra*, sec. 5.4) does not provide rights regarding patient's records other than the right to access. Therefore general data protection legislation applies in this respect.

**6.8 Right to protection of privacy and intimacy**

The right to protection of intimacy and dignity is the patient's right pursuant to art. 19(1)(4) Act on Healthcare Institutions. Moreover, pursuant to art. 36(1) Act on Professions of Physician and Dentist, doctors are obliged to respect intimacy and dignity of the patient when providing medical services. Only necessary medical personnel may witness the service. Others may be present when consented by the patient and the doctor (art. 36(2)). There is one exception to the principle. Students may witness medical services in academic HCIs without consent, if it is necessary for educational purposes. Yet for a demonstration of purely educational provenance patient's consent is required (art. 36(4)).

**6.9 Right to representation in case of incompetence**

As abovementioned, rights of patients should be exercised by a legal representative, a person having custody of the patient and/or a tutelary court when the patient is minor, is legally incapacitated or unable to express the consent or to apprehend the information on his/her health state.

## 7 Identity management in the health sector

### 7.1 Overview

Only a reporting eIDM system, without advanced functionalities, has been implemented in Poland on a nationwide basis and, as mentioned in sec. 3.3 of this report, no strategy of introducing more advanced solutions has been decided on a sustainable basis.

Data on insurance bearers and payers, service providers, offers and contracts for providing publicly funded services, waiting lists for medical services and pharmacy data are collected and stored by the IT system of the NHF pursuant to the Ordinance of the Minister of Health of 27 July 2005 on the scope of necessary information collated in the information system of the National Health Fund and the scope and means of transferring it to the minister responsible for health, province governors and province assemblies.<sup>16</sup> Data on trade in medicaments refunded by the NHF is also transferred electronically to the NHF's IT system, pursuant to the Ordinance of the Minister of Health of 28 September 2004 on the scope of necessary information collected and transferred by pharmacies to the entities responsible for financing healthcare from public sources.<sup>17</sup> Similar reporting obligations regarding healthcare services were laid down in the Ordinance of the Minister of Health of 27 June 2006 on the scope of necessary information collected by service providers, detailed mode of registering these information and transferring them to entities responsible for financing healthcare from public sources.<sup>18</sup> The last ordinance, however, expired on 30 March 2008 and, as for 17 June 2008, it has not been replaced with a new one.

Generally the IT system of the NHF is based on regional subsystems managed by regional branches of the Fund. Half (eight) of them uses solutions of one provider, while the other eight - of another consortium of two companies. Data required by the central system is transferred to it from the regional subsystems with a WAN network. Also, according to the first of the aforementioned Ordinances the Minister of Health, province governors and

---

<sup>16</sup> *Rozporządzenie Ministra Zdrowia z dnia 27 lipca 2005 r. w sprawie zakresu niezbędnych informacji gromadzonych w systemie informatycznym Narodowego Funduszu Zdrowia oraz zakresu i sposobu ich przekazywania ministrowi właściwemu do spraw zdrowia oraz wojewodom i sejmikom województw*, Journal of Laws Year 2005, No. 152, item 1271, with further amendments.

<sup>17</sup> *Rozporządzenie Ministra Zdrowia z dnia 28 września 2004 r. w sprawie zakresu niezbędnych informacji gromadzonych i przekazywanych przez apteki podmiotom zobowiązanym do finansowania świadczeń ze środków publicznych*, Journal of Laws Year 2004, No. 213, item 2167, with further amendments.

<sup>18</sup> *Rozporządzenie Ministra Zdrowia z dnia 27 czerwca 2006 r. w sprawie zakresu niezbędnych informacji gromadzonych przez świadczeniodawców, szczegółowego sposobu rejestrowania tych informacji oraz ich przekazywania podmiotom zobowiązanym do finansowania świadczeń ze środków publicznych*, Journal of Laws Year 2006, No. 114, item 780, with further amendments.

**Study on Legal Framework of Interoperable eHealth in Europe**

---

province assemblies should receive certain reports. Generally an electronic transfer is used in this respect, though quarterly reports from the NHF to the Minister of Health are additionally handed over in the paper form (§ 11(3)). Moreover, partial decentralization described above does not hold true for a register of service recipients (Central Register of Insured – *Centralny Wykaz Ubezpieczonych*), which was established on the basis of art. 97(4) Act on Healthcare Services Financed from Public Sources. The register is stored in a central database.

**7.2 The SIS Card**

No nationwide SIS Card system has been established in Poland. Some of the plans for a digital ID card (pl.ID) cover this functionality. Yet these are rather unclear and remote. Nevertheless, a digital health insurance card (EKUZ) has been successfully trialled within RUM I and was to be introduced into the RUM II according to the NHF Strategy. For reasons discussed in sec. 3.3 of this report the plans have been delayed at least.

The EKUZ, which has been implemented within RUM I, has been lately discussed in the National IDABC-report referenced under [RD9]. From the report the following passages are taken over:

„An Electronic Card for Health Insurance EKUZ (Elektroniczna Karta Ubezpieczenia Zdrowotnego) has been issued since 1999 by the Silesian Voivodeship Department of National Health Fund (Śląski Oddział Wojewódzkiego Narodowego Funduszu Zdrowia (NFZ))<sup>19</sup>.

The cards and 2.500 readers are the part of the START system for health service registration. The system has been rolled out since 1999 by Sygnity Company<sup>20</sup> (previously: Computerland). START is the closed system for the management of documents and information concerning particular medical services. It is used for the current monitoring of activities associated with contracts between NFZ and health service enterprises and pharmacy. The system has been established mainly for the purpose of facilitating the creation of reports concerning services realized by health service units and physicians as well. It is also used for data exchange between physicians and NFZ, and for the delivery of detailed information concerning health services. The START system transmits medical and statistical information between entities financing and performing medical services.

The registration process is based on the data stored inside electronic card memories. Those cards are issued for all insured members of the Silesian voivodeship community. The cards play the role of identifiers and data carriers for basic personal data. The cards are ID-1 format memory cards (integrated circuit SLE 4428<sup>21</sup> inside), but other mechanisms increasing data security have been implemented in the system (including SAMs with strong cryptomechanisms). The smart card is without a photo of the bearer.

The following data are printed on the front and back side of the EKUZ::

---

<sup>19</sup>

[http://www.nfz-katowice.pl/index.php?&k0=3\\_ubezpieczony&k1=6\\_karta\\_ubezpieczenia\\_zdrowotnego](http://www.nfz-katowice.pl/index.php?&k0=3_ubezpieczony&k1=6_karta_ubezpieczenia_zdrowotnego)

<sup>20</sup> [www.sygnity.pl](http://www.sygnity.pl)

<sup>21</sup> The producer of integrated circuits is Infineon, <http://www.infineon.com/>

## Study on Legal Framework of Interoperable eHealth in Europe

- 
- PESEL number
  - name and surname
  - address
  - date and place of birth
  - codes of community, voivodeship and payer
  - RUM<sup>22</sup> local office number
  - a leading physician number
  - a leading unit number
  - other data (e.g. card serial number).

The same data are stored in a card memory.

Entities wishing to use the system are authenticated before any access is granted. System terminals are equipped with active Security Application Modules (SAM). Those modules are smart cards with a cryptoprocessor. About 600 terminals with SAM are introduced in the EKUZ system.”

### 7.3 Crossroads Bank for Social Security

No Crossroads Bank for Social Security has been discussed in Poland. As abovementioned, reporting data for purposes of financing the health security system from public funds is stored in an IT system of the National Health Fund. The system, however, is not interoperable with external systems and often stores redundant data. It may be argued that the system requires rationalization, enhancing its efficiency and improved fraud detection, features which RUM II and its concomitant projects were to provide.

### 7.4 Patient identifier

Regulatory framework for the nationwide Health Service Register provides for patient identifiers incorporated into the health certificates (art. 32e(6) Act on Healthcare Institutions). Neither the register nor the identifier have been introduced so far, however.

The IT system of the National Health Fund requires all the basic identifiers, including the personal identification PESEL number<sup>23</sup>, tax identification NIP number<sup>24</sup> and the number of the patient’s ID (§ 3(1)(5) Ordinance of the Minister of Health on the scope of necessary information collated in the information system of the National Health Fund (...)).

### 7.5 Authentication of healthcare professionals

Physicians granted with the right to exercise the profession are entered into the register held by the regional medical chamber relevant for the location of intended practice (art. 8(1) Act on Professions of Physician and Dentist). Detailed provisions on holding the register have

---

<sup>22</sup> Rejestr Usług Medycznych (Medical Service Register)

<sup>23</sup> Number in the General Electronic System for Citizens Evidence (*Powszechny Elektroniczny System Ewidencji Ludności*).

<sup>24</sup> Number in the Tax Identification Numbers (*Numer Identyfikacji Podatkowej*).

**Study on Legal Framework of Interoperable eHealth in Europe**

---

been enacted by the Supreme Medical Chamber, pursuant to authorization by art. 8(2) Act on Professions of Physician and Dentist.<sup>25</sup>

The register is available on the Internet, as a searchable database (<http://www.nil.org.pl/xml/nil/rejlek/hurtd>). It is aimed at physician data verification by patients and other physicians. The Supreme Medical Chamber allows for its commercial exploitation only on the basis of separate agreements establishing remuneration for access. Registration of physicians is of purely confirmative character. To put it in other words, it is not the registration which establishes the right to exercise the profession. Instead, authentication is rather performed by issuing one of four categories of documents by the relevant regional medical chamber: “Entitlement to perform profession of physician”, “Entitlement to perform profession of dentist”, “Entitlement to perform restricted profession of physician”, “Entitlement to perform restricted profession of dentist” (art. 6(10) Act on Professions of Physician and Dentist). Additionally, the chambers are authorised to issue certificates confirming that at a certain moment the given person was entitled to perform the profession, and that this entitlement is not limited, withdrawn, or influenced by disciplinary proceedings to which the doctor might be subjected (art. 6(11)(3)). These two kinds of documents are much more important in terms of authentication of doctors than the register itself.

Moreover, medical practices should be registered in the register held by regional medical chamber relevant for the location of the intended practice (art. 50(1) Act on Professions of Physician and Dentist). Registration authority should register the practice within 50 days following submission of a complete set of documents (art. 50b(1) Act on Professions of Physician and Dentist). In any case, the applicant may start the practice 60 days after a complete set of documents has been delivered to the registration authority and after prior notice in writing (art. 50b(1a)). The registers are held as IT systems (art. 50b(4)) HCIs may operate only after having been inserted into the register of healthcare institutions (art. 12(1) Act on Healthcare Institutions) held either by a geographically relevant province governors or the Minister of Health, depending on which of the two established the given HCI. Digital format of the register is not settled statutorily, but in practice the register is in the form of a central database maintained by the Centre of Information System of Healthcare<sup>26</sup>. The register is to be open and accessible for third parties (art. 12(2) Act on Healthcare Institutions) and is searchable online, at <http://www.rejestrzoz.gov.pl/RZOZ/>.

---

<sup>25</sup> Resolution No 104/97/II of the Supreme Medical Council on detailed mode of procedure regarding granting entitlements to perform the profession of physician and dentist and holding registers of doctors, with further amendments (*Uchwała Nr 104/97/II Naczelnej Rady Lekarskiej w sprawie szczegółowego trybu postępowania w sprawach przyznawania prawa wykonywania zawodu lekarza i lekarza stomatologa oraz prowadzenia rejestrów lekarzy*), consolidated text announced by the Announcement No 1/01/III of the President of the Supreme Medical Chamber of 3 January 20001.

<sup>26</sup> <http://www.csioz.gov.pl/>.

**Study on Legal Framework of Interoperable eHealth in Europe**

---

**7.6 Exchange of health-related data**

As mentioned in sec. 7.3 of this report, reporting information regarding services financed from public funds is stored and processed in an IT system of the National Health Fund. Exchange of health-related data with external registers is not an issue, however, because the system is not interoperable with other systems. Even within the system the transfer is generally one-way (upstream) with some information exchange features of communication with pharmacies. Attempts to establish an interoperable system architecture (which would make a case for digital health insurance cards for instance) have failed so far, along the NHF Strategy described in sec. 3.3 of this report.

## 8 Electronic prescription

The Ordinance of the Minister of Health of 17 May 2007 on medical prescriptions,<sup>27</sup> issued pursuant to Art. 45 Act on Professions of Physician and Dentist, makes it clear that the Polish law does not allow for digital prescriptions.

First, issuing a prescription requires affixing a handwritten signature (§ 2.1). Second, any alteration must be endorsed with “inserting” a stamp (§ 2.2), which may occur only when the prescription is recorder on a physical carrier. Third, the term “prescription” is used throughout the Ordinance only in the context of a printout (e.g. § 2.4) and an annex to the Ordinance (No. 6) defines both the content and size of each of the prescription pages (§ 9.1). Finally, confirmation that the prescription has been realized requires that the pharmacist puts a handwritten signature on it (§ 14.2.2).

---

<sup>27</sup> *Rozporządzenie Ministra Zdrowia z dnia 17 maja 2007 r. w sprawie recept lekarskich*, Journal of Laws, Year 2007, No. 97, item 646, with further amendments.

## **9 General assessment**

The Polish healthcare system has been in an acute, and increasing, crisis for the last years, because of the organisational and management deficiencies and underfinancing. More importantly, no general healthcare strategy of overcoming the crisis has received lasting political support nor has been accepted by the general public and physicians. As an upshot, the general decline of the system has led to the point in which providing basic healthcare services for patients by healthcare institutions on continuous basis, and appropriate remuneration for physicians have become by far the main issues. It seems that advanced eHealth solutions have been perceived in this situation rather as means to improve the system when it works properly. Moreover, after abandoning the last strategy on e-Health apparently for political reasons, the Ministry of Health has not found capacity to work out another one early enough to implement it before another general elections in 2011.

It may be argued that certain eHealth applications would be particularly desirable in such a situation, especially those making financial flows more transparent and the cost/benefit analysis of particular system components more accurate. Some initiatives in this regard have been pursued lately, e.g. introduction of the DRG methodology of coding healthcare services for the purposes of reporting to the NHF. An overall strategy, however, would require long-time perspective of planning, implementation, assessment and adjustments - conditions which, mainly for political reasons again, are particularly difficult to achieve in Poland. The general trend, therefore, is rather to wait for the outcome of the current discussion on the reform of the healthcare system in general, and to adjust IT systems to final decisions on the management and organisational structure.

In any case, the foregoing considerations clearly overshadow the questions of cross-border eHealth services or interoperability of eHealth systems. This consequence logically stems from the fact that the lower level of domestic eHealth services and system interoperability is yet to be accomplished.

Polish law seems much more prepared for eHealth than technical planning and implementation. In general the legal system has been steadily adjusted to the needs of eHealth applications and systems. Sometimes it even anticipates future IT deployments. However, this may lead to empty norms when deployment plans are cancelled or suspended. By way of example, provisions on the Health Services Register, introduced to insert in the Act on Healthcare Institutions (Chapter 3a), despite plans to deploy the register subsequently have been withdrawn.

Dariusz Adamski  
17 June 2008

## Annex: Contact details of National Correspondents

### 9.1 Primary Contact

|                        |  |
|------------------------|--|
| <b>Country</b>         | Poland                                 |
| <b>Name</b>            | Dariusz Adamski                        |
| <b>Organisation</b>    | University of Wrocław                  |
| <b>Position</b>        | Assistant Professor                    |
| <b>Mailing Address</b> | ul. Uniwersytecka 7/10, 51-136 Wrocław |
| <b>Work Phone</b>      | +48 71 375 21 00                       |
| <b>Mobile Phone</b>    | +48 693 407 224                        |
| <b>Fax</b>             | +48 71 375 21 00                       |
| <b>E-Mail</b>          | dadamski@prawo.uni.wroc.pl             |

### 9.2 Alternative Contact

|                        |      |
|------------------------|------|
| <b>Country</b>         | n.a. |
| <b>Name</b>            | n.a. |
| <b>Organisation</b>    | n.a. |
| <b>Position</b>        | n.a. |
| <b>Mailing Address</b> | n.a. |
| <b>Work Phone</b>      | n.a. |
| <b>Mobile Phone</b>    | n.a. |
| <b>Fax</b>             | n.a. |
| <b>E-Mail</b>          | n.a. |