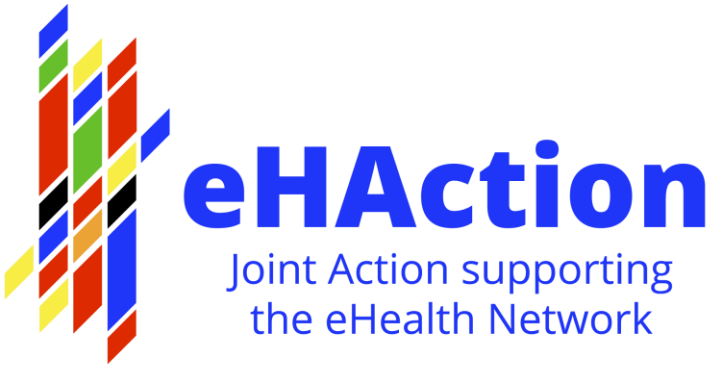

D7.2 Report on best practices and approaches on data protection at national level

WP7 Overcoming implementation challenges

26-10-2018

Revision 0.3

Grant Agreement nº 801558

Co-funded by
the Health Programme
of the European Union

Abstract:

Workpackage 7 is intended to provide the eHealth Network with valuable practical recommendations, guidelines and priorities on three of the most critical issues concerning the eHealth european ecosystem: interoperability, data protection and data and systems security. Also, WP7 will employ stakeholders in order to collect information though questionnaires and organize – under the supervision of WP2 - workshops disseminating its results.

CONTROL PAGE OF DOCUMENT	
Document name	D7.2 Report on best practices and approaches on data protection at national level
Work Package	WP 7– Coordination
Status	Draft for discussion at 14th eHealth Network meeting of 13th Nov 2018
Revision	0.3
Date	26-10-2018
Author(s)	Jiri Borej, Milan Cabrnoch, Jakub Tomas, Tomas Bezouska
Beneficiary(ies)	Ministry of Health of the Czech Republic

REVISION HISTORY				
Revision	**Date**	**Author**	**Organization**	**Description**
0.1	21-09-2018	Tomas Bezouska	MZCR	Outline of the document
0.2	23-09-2018	Milan Cabrnoch	MZCR	Revision of the first draft of the document
0.3	24-09-2018	Tomas Bezouska	MZCR	Revision of the first draft of the document

Ref. n.	**Document**
	eHAction Grant Agreement n. 801558
	Annex I – eHealth Action Proposal
	eHAction Consortium Agreement
	MWP 2018-2021

Table of Content

Acronyms

Acronym	Description
WP	Work Package
GDPR	General Data Protection Regulation
NIS directive	Network and Information Security directive
ICT	Information and Communication Technology
EIF	European Interoperability Framework
MS	Member State
ReEIF	Refined eHealth European Interoperability Framework
MWP	Multi-Annual Work Plan

1. Executive Summary

Work Package 7 is about providing the eHealth Network, national and European health authorities, eHealth professionals and IT staff in large healthcare organizations with guidelines and recommendations for implementing interoperable and secure eHealth services at national and cross-border level. Even though too many initiatives have already been raised, there are issues that need to be addressed; this work package aims at tackling challenges on three of the most critical issues concerning the eHealth European ecosystem: interoperability, data protection (GDPR) and data and systems security (NIS directive).

This document aims at introducing the vision, the objectives/outputs, the operational plan, the work methodology, the findings, the broad context and the possible legal issues related to GDPR in Health Care environment.

Member States are currently facing implementation challenges of new critical European frameworks/regulations on health data and services on the national and cross-border services levels (GDPR, NIS, Patient Summary); this work package aims at aligning all the above to facilitate implementation and fix any relevant issues with the specific focus on the General Data Protection Regulation (GDPR).

WP7.2 will also serve as a link to all current European Commission policies, project calls and other initiatives on eHealth, such as “The Rolling Plan on ICT Standardization” (European Commission, 2018), the European electronic health record format and the new EIF.

Task 7.2’s findings can be disseminated to national health policy makers and other interested bodies and stakeholders to aid in tackling challenges on implementing data protection principles.

Regarding possible risks, this work package can suffer from a lack of participation in the work done by enough experts from all MS and affiliated entities. Another challenging factor is the dissemination of the outcomes of this WP7.2.

The next steps are:

- Sharing the outcomes (deliverables) of this work package to all interested parties.
- Evaluation of the implementation of the knowledge gained in this WP.

As a part of WP7, Task 7.2 is focused on GDPR implementation and its implications for (not only) cross-border healthcare. The aim of this task is to share best practices and approaches on data protection at national level and to monitor the situation regarding data protection and the new requirements GDPR brings to eHealth.

The task is motivated by both urgent needs for correct GDPR adoption in the health care sector and the utilization of GDPR potential for comprehensive respect for human rights in health care provision practice in long-term run.

In Section 2 the general objectives, vision, scope and objectives of WP7 and its deliverables are presented stressing out the purpose of WP7, its importance and its contribution to the project, as well as the operational plans of each work package task.

Section 3 describes the work methodology, giving emphasis to the cooperation procedures that will be followed between partners. Also, this section will outline the work package

outcome evaluation approaches as well as the work package results exploitation, impact and outreach.

Section 4 presents the references to the topic of data protection in health care. Also, this section briefly presents the relationships between WP7.2 and the internal and external eHAction environment. Section 4 will focus on the relationship of each WP7.2 task with other eHAction tasks and with the external eHAction environment, namely external stakeholders, giving special attention to the potential impact of WP7.2 results on them.

Finally, section 5 outlines legal issues that might arise which may produce risks on WP7.2 activities, while section 7 summarizes the document conclusions, listing the next steps of WP7.2.

2. Introduction

As defined in the project documents, Task 7.2 is focused on GDPR implementation and its implications for cross-border healthcare. This document represents the main deliverable of the task. The aim of this document is to share best practices and approaches on data protection at national level, the situation regarding data protection, and the new requirements that GDPR brings to eHealth.

The topic is implemented in 5 steps:

1. Review of the GDPR topic in general and review of its impact on healthcare stakeholders.
2. Characteristics of main points and requirements of GDPR adoption in the healthcare sector
3. Proposal of the set of relevant recommendations/policies for successful completion of GDPR adoption in the healthcare sector
4. Sketches of collaborative instruments for related information and education at present and in future dealing with the GDPR topic in healthcare settings.
5. Foresight – vision and mission - of the future fulfilment and development of the GDPR

The task is motivated by both urgent needs for correct GDPR adoption in the healthcare sector and the utilization of GDPR potential for comprehensive respect for human rights for healthcare provision practice in the long term.

2.1. Cooperation with Public Interest Groups

In topics No. 2, 3 and 5 the cooperation with public interest groups (patient and healthcare professionals' organizations) will be actively sought and utilized. The following groups are planned to be contacted:

To be completed in next version of the document.

3. Methods and Means

3.1. Short overview of Personal Data Protection

The area of personal data protection was regulated on the EU level since October 1995 by the Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data. This Directive drew up some basic rules on personal data protection but most of the regulation was delegated to the national level and left to be solved by national legislation. That resulted in varying approaches towards the personal data protection and problems have arisen especially in cross-border data sharing and processing of data in multiple countries.

With growing exchange and transfer of personal data related to the expansion of digital economy, and increased mobility of both people and services, it become necessary to synchronise the approach to personal data protection among member states and to define a new level of personal data protection in reaction of growing risks of personal data being misused or mishandled.

As a reaction, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) was created and came into effect on 25 May, 2018.

This new regulation defines among other things:

- key principles of personal data protection,
- rights of the data subject,
- controller and processor of personal data and their obligations,
- transfers of personal data to third countries or international organisations,
- independent supervisory authorities.

A two-year period was set for adaptation of national legislation for the new regulation as well as for its implementation in personal data processing methods and tools of every subject acting as an controller or processor.

Since the healthcare industry is one of the most personal-data-heavy industries and personal data processing lies at the core of most tasks handled by all the subjects operating in this field, the implementation of the general regulation's principles and requirements in specific regulations, standards and procedures of the industry was paramount to the successful adoption of the new regulation.

On national level there are huge differences in approach to providing a universal healthcare services, both in terms of the financial and organizational levels and in terms of extent and methods of regulation of the industry, which has a tremendous impact on the implementation of the General Data Protection Regulation both in national legislation and in the general practice of personal data processing.

3.2. Guiding Principles and Methods Used

To be completed in next version of the document.

3.3. Survey – Best Practice data collection

3.3.1. Areas of interest

There are several areas of interest covered by the survey, each area tackled by a series of questions. All areas were defined to cover some key aspects of the General Data Protection Regulation, its implementation at the national level both in the general legislation and with special focus on Health Care services and its providers.

There were defined following areas of interest:

- Legislation
  - National Legislation on Personal Data Protection
  - Legislation implementing GDPR on national level
  - Other relevant Regulations
  - Enforcing GDPR
  - National Legislation on Health Records
- Key impacts of GDPR implementation on Health Care
  - Lawfulness of Personal Data processing in Health Care
  - Patient Data, Health Care Documentation, Electronic Health Records in practical use
  - Access to Patient Data
  - Execution of Rights of the Data Subject
  - Practical impacts of GDPR on Health Records
- Known challenges for implementing GDPR in Health Sector

3.3.2. The Questionnaire

Not all questions are relevant for all respondent groups. The complete list of questions comprises a body that is to be modified for each type of respondent accordingly. Below there are listed all the questions and comments explaining their purpose or related agenda.

Survey Question	Comment
Identification and contact details	**Basic identification of the survey respondent for the possibility of further clarification of provided responses or follow-up questions if necessary.**
E-mail address	Contact information
Full Name	Contact information
Institution / Organisation	Contact information
Work Phone	Contact information

Survey Question	Comment
National Legislation on Personal Data Protection	**This section focuses on information regarding National Legislation on Personal Data Protection**
Was there (in your country) any Legislation regarding Personal Data Protection in place prior to GDPR? If so, please provide a short description (up to 1000 characters) and an English translation where possible.	According to Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data each EU member state was required to have personal data protection law in place, the legislation was of varying nature and extent, the question aims to gather information on the state of personal data protection regulation before GDPR was introduced.
Is there any Legislation implementing GDPR in place as of today? If so, when was it passed? Please provide a short description (up to 1000 characters) and an English translation where possible.	GDPR expects national states to implement state-specific legislation addressing particular areas defined within GDPR as well as any other areas national legislation would consider relevant. The question aims to gather information on such legislation.
If not, is it planned to pass such Legislation and in what time frame? What is the key reason for the delay?	National legislation is expected to be passed by GDPR itself to adjust particular areas according to needs of individual states. The question aims to find out what is the time frame for such legislation to be passed and what are main reasons it was not passed during the implementation period of GDPR.
What does / will the Legislation regulate within the framework for national regulations defined by GDPR?	This question aims to find out the specific areas regulated by the national legislation.
Is there any relevant Legislation other than GDPR and its implementing legislation or any generally implemented standards relevant for Personal Data Protection in Health Care sector in place? If so, please provide a short description (up to 1000 characters) and an English translation where possible.	This question aims to find out the specific areas regulated by other local regulatory frameworks.

Survey Question	Comment
Enforcing GDPR	**National Supervisory Authority according to Article 51 of GDPR.**
Who is the Supervisory Authority responsible for monitoring the application of Personal Data Protection legislation on the national level?	This question aims at identifying the National Supervisory Authority as described in Article 51 and the following articles of the GDPR.
Are there so far any experiences or other outcomes of problems / issues / incidents / infringements / penalties regarding the Personal Data Protection legislation and its implementation? If so, please provide a short description (up to 1000 characters) and an English translation where possible.	This question aims to find out whether there are so far any results of the regulatory oversight by the National Supervisory Authority in terms of identified breaches of personal data protection and what were the consequences of the identified misconduct.
National Legislation on Health Records	**This section is focused on legislative regulation of Health Care records and Patient Data**
Is there any specific legislation regarding Patient Data, Health Care Documentation, Electronic Health Records, etc.? If so, please provide a short description (up to 1000 characters) and an English translation where possible.	This question aims to find out what legislation applies to handling of Patient Data.
What are the key provisions of such legislation in terms of data formats and standards of Patient Data, Health Care Documentation, Electronic Health Records, etc.? Please provide a short description (up to 1000 characters)	This question aims to find out specific impacts of legislation related to handling of Patient Data on formats and standard applicable to this data.
What are the key provisions of such legislation in terms of handling and use of Patient Data, Health Care Documentation, Electronic Health Records, etc.? Please provide a short description (up to 1000 characters)	This question aims to find out specific impacts of legislation related to handling of Patient Data.
What are the key provisions of such legislation in terms of exchange and sharing of Patient Data, Health Care Documentation, Electronic Health Records, etc.? Please provide a short description (up to 1000 characters)	This question aims to find out specific impacts of legislation related to sharing and exchange of Patient Data.

Survey Question	Comment
What are the key provisions of such legislation in terms of storage and disposal of Patient Data, Health Care Documentation, Electronic Health Records, etc.? Please provide a short description (up to 1000 characters)	This question aims to find out specific impacts of legislation related to storage and disposal of Patient Data.
Key impacts of GDPR implementation on Health Care **Please provide a short description (up to 1000 characters) of impacts on rights, obligation and/or other aspects of GDPR implementation on particular groups listed in questions below regarding their work with Patient Data, Health Care Documentation, Electronic Health Records, etc. in connection with providing Health Care services.**	**This section is focused on key impacts GDPR has on particular group of professionals or organizations in Health Care.**
What are the key impacts of GDPR implementation on Health Care Professionals (doctors, medical personnel, etc.)?	This question relates to Health Care Professionals
What are the key impacts of GDPR implementation on Emergency Health Care Providers?	This question relates to Emergency Health Care Providers
What are the key impacts of GDPR implementation on Health Care Providers (hospitals, clinics, medical practice owners, pharmacies, etc.)?	This question relates to Health Care Providers
What are the key impacts of GDPR implementation on Health Care Insurance Providers?	This question relates to Health Care Insurance Professionals
What are the key impacts of GDPR implementation on National Authorities and Organisations collecting Patient Data, Health Care Documentation, Electronic Health Records, etc.?	This question relates to National Authorities
Lawfulness of Personal Data processing in Health Care. Please provide a short comment (up to 1000 characters)	What is the main legal basis for Personal Data processing in Healthcare according to GDPR in case of particular types of providers?

Survey Question	Comment
• Consent • Performance of a Contract • Compliance with a Legal Obligation • Protection of a Vital Interest • Public Interest or Exercise of an Official Authority • Legitimate Interest	• Health Care Professionals • Emergency Health Care Providers • National Authorities and Organisations
Patient Data, Health Care Documentation, Electronic Health Records in practical use	**This section is focused on the use of Patient Data in each phase of its lifecycle.**
What is the prevailing form for Patient Data, Health Care Documentation, Health Records? (paper/digital) • in major hospitals • in specialised practices and clinics • in primary care	This question aims to find out the extent of Patient Data digitization.
What regulatory obligations are in place related to the use / handling / exchange / sharing / storage of Patient Data, Health Care Documentation, Health Records (e.g. compulsory exchange, storage or use in certain situations)?	This question aims to identify key legislation and other regulations applicable to Patient Data.
How are the above-mentioned obligations related to the use / handling / exchange / sharing / storage of Patient Data, Health Care Documentation, Health Records fulfilled in practice?	This question aims to identify how key legislation and other regulations are applied to Patient Data.
If there is no particular regulation besides GDPR in place, how are obligations related to the use / handling / exchange / sharing / storage of Patient Data, Health Care Documentation, Health Records fulfilled in practice?	This question aims to identify what key principles are applied to Patient Data in situations where there is no applicable legislation.
How has the GDPR and related legislation affected the use / handling / exchange / sharing / storage of Health Records?	This question aims to identify what was the key impact of GDPR on above described legislation and its implementation.

Survey Question	Comment
Are there any challenges in implementation of GDPR and relevant national legislation in terms of Patient Data, Health Care Documentation, Health Records and its use / handling / exchange / sharing / storage?	This question aims to identify what problems are met during the implementation of GDPR and related national legislation.
Access to Patient Data	**This section is related to the access of Patient Data in various circumstances**
What are the implications of GDPR and related legislation on patients' access to their own Patient Data, Health Care Documentation, Electronic Health Records?	This question aims to find out how patients' access to their own data is granted.
How is the access to Patient Data, Health Care Documentation, Health Records without the consent of the patient implemented in the legislation?	There are certain situations when it is not possible to obtain a patient's consent to access his medical history and other personal data. This question aims to find out what tools, procedures or other measures are implemented to circumvent the patient's consent in such situations and what protective measures are in place to prevent misuse of such tools and procedures.
On what level is a unique Patient ID implemented? • Patient ID unique on a national level • Patient ID unique on a regional level • Patient ID unique on a level of a Health Care Provider • Patient ID unique for every case of a Health Care service • Other	This question aims to find out whether there is some form of unique Patient ID implemented and on what level is it unified / shared.
Execution of Rights of the Data Subject	**This section is related to personal data other than data on the course and outcomes of provided health care services.**
What defines rules for execution of a right to rectification (please describe how the right is implemented by Health Care providers)?	Question related to the right to rectification according to Article 16 of the GDPR.

Survey Question	Comment
What defines rules for execution of a right to erasure (please describe how the right is implemented by Health Care providers)?	Question related to the right to erasure according to Article 17 of the GDPR.
What defines rules for execution of a right of access (please describe how the right is implemented by Health Care providers)?	Question related to the right of access by the data subject according to Article 15 of the GDPR.
Practical impacts of GDPR on Health Records	**This section is related to implications and impacts of implementing GDPR in Health Care environment**
What are implications that prevent any group of stakeholders in Health Care from fully implementing GDPR?	This question aims to find out whether there are any problems preventing the full implementation of GDPR.
Are there any excessive costs or other types of excessive induced resource consumption due to implementing GDPR?	This question aims to find out if the full implementation of GDPR is prevented by lack of available resources.
What is the estimated cost of GDPR implementation?	This question aims to quantify the overall cost of GDPR implementation (analysis, change of processes, information systems, etc.) and the increase of operational expenditure related to GDPR adoption.
Are there any other obstacles to GDPR implementation (e.g. personnel capacity, cybersecurity issues, etc.)?	This question aims to find out if there are any obstacles preventing full GDPR implementation and compliance other than direct financial costs.
What are the expected benefits to be derived from the general adoption of GDPR and related national legislation?	This question aims to find out what benefits may arise from GDPR implementation.
Known challenges for implementing GDPR in the Health Care Sector	**This section aims to identify key problems related to implementing GDPR (obstacles, challenges and problems addressed during the implementation) and key problems related to GDPR being implemented (complications and problems in day to day operations resulting from GDPR implementation).**
What are the key issues and challenges related to implementing GDPR in the Health Care sector?	This question aims to identify main challenges in the Health Care sector.

Survey Question	Comment
How are these issues addressed at the Health Care providers level?	This question focuses on issues at the level of particular organizations and their perception of GDPR.
How are these issues addressed on national level / legislation?	This question focuses on issues at the national level in terms of policy and legislation and the challenges faced.

3.3.3. Survey Respondents

To obtain representative results covering all key aspects of the Health Care industry and the impact of the General Data Protection Regulation, the following key respondent groups to be surveyed were defined in every member state:

1. eHAction Member / National Partner
2. National Ministry of Health
3. National Authority for eHealth (where applicable)
4. National Supervisory Authority according to GDPR Article 51
5. Hospitals / Clinics / Primary Health Care providers (5)
6. Emergency Health Care provider (1)
7. Health Care Insurance Provider (1)

3.3.4. Analysis of Survey Data

To be completed in next version of the document.

4. Best practices and approaches on data protection

To be completed in next version of the document.

5. References

Multi-Annual Work Plan of the eHealth Network 2018-2021 adopted by the eHN in November 2018
https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20171128_co01_en.pdf

JAseHN T5.1 Trusted eHealth National Contact Points

- D5.1.2_Country_Guide_for_NCPeH_Implementation.pdf

JAseHN T5.2 Electronic Identification for eHealth

- D5.2.1 eID specific Framework for eHealth
- D5.2.2 Guidelines on the interoperability of electronic professional registries
- D5.2.3 Report on notification of national eID under the scope of the eIDAS Regulation

JAseHN T5.3 Update & revision of EU eHealth Guidelines

- D5.3.0 General Guideline
- D5.3.1 Update Guideline on PS
- D5.3.2 Update Guideline on eP
- D5.3.3 Report on elements to be taken into consideration for updating the PARENT Joint Action guidelines for Patient Registries

JAseHN T5.4 Alignment of standardization activities in eHealth

- D5.4.1 Proposal for a platform consisting of the relevant standards developing organizations
- D5.4.2 Policy paper proposing actions to promote the use of common standards or technical specifications in eHealth within the EU
- D5.4.3x Report on standardisation developments in eHealth incl. recommendations for the rolling plan
- D5.4.4 Refined eHealth European Interoperability Framework (ReEIF)

JAseHN T5.5 Semantic Interoperability

- D5.5 Report on European semantic interoperability in eHealth

JAseHN T6.1 Implementation of eHealth guidelines

- D6.1.1 Report on the implementation of PS Guideline
- D6.1.2 Report on the implementation of eP Guideline
- D6.1.3 Report on the implementation of PR Guideline

JAseHN T7.5 Patient access to Electronic Health Records and health data portability

- D7.5.1 Report on EU state of play on patient access on eHealth data
- D7.5.2 Recommendations for patient access to electronic health records

To be completed in next version of the document.

6. Conclusions

Section 7 summarises the document conclusions listing the next steps of WP7.2.
To be completed in next version of the document.

7. Bibliography

European Commission. (2018). *Rolling plan on ICT standardisation*. Ανάκτηση 08 02, 2018, από eHealth, Healthy Living and Aging, Policy: https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/ehealth-healthy-living-and-aging

To be completed in next version of the document.

8. Appendix I

Use the appendix for detailed data points and supporting evidence