



Project full title: Up-scaling the global univocal identification of medicines
in the context of Digital Single Market strategy
Call identifier: H2020-SC1-DTH-2019

Deliverable D10.4: Review report of the GDPR and other legal requirements

Version: 1.0
Status: Final
Dissemination Level¹: PU
Due date of deliverable: 30.09.2020
Actual submission date: 08.10.2020
Work Package: WP10: Socio-economic impact, legal and governance aspects
Lead partner for this deliverable: IHD
Partner(s) contributing: EMP, DWIZ
Deliverable type²: R
Delivery date: 08.10.2020

Main author(s):

Petra Wilson IHD

Other author(s):

Dipak Kalra IHD
Farah Diehl-Fahim EMP

Resource consumption estimate:	Person months
IHD – Petra Wilson	2,2
IHD – Dipak Kalra	0,3
EMP	0,5

¹ Dissemination level: PU: Public; CO: Confidential, only for members of the consortium (including the Commission Services); EU-RES: Classified Information: RESTREINT UE (Commission Decision 2005/444/EC); EU-CON: Classified Information: CONFIDENTIEL UE (Commission Decision 2005/444/EC); EU-SEC Classified Information: SECRET UE (Commission Decision 2005/444/EC)

² Type of the deliverable: R: Document, report; DEM: Demonstrator, pilot, prototype; DEC: Websites, patent filings, videos, etc.; OTHER; ETHICS: Ethics requirement; ORDP: Open Research Data Pilot

Revision history

Version	Date	Changes made	Author(s)
0.1	30.07.20	Outline concept developed, based on data use inventory within project	Petra Wilson, Dipak Kalra, Farah Diehl-Fahim
0.2	06.08.20	Concept developed based on input from WP8 on pilots and app development	Petra Wilson, Lucia Comnes
0.3	01.09.20	Core elements of GDPR articles developed, including Annex 1	Petra Wilson
0.4	16.09.20	First draft of sections of chapters 3 and 4	Petra Wilson
0.5	21.09.20	First draft chapters 1 and 2	Petra Wilson
0.6	26.09.20	Review of structure	Petra Wilson, Farah Diehl-Fahim
0.6	28.09.20	First full draft	Petra Wilson
0.7	30.09.20	Commentary and feedback from I-HD team	Dipak Kalra
0.8	07.10.20	Full re-draft based on comments from Dipak Kalra	Petra Wilson
0.9	07.10.20	Adjustments based on further comments	Petra Wilson
1.0	08.10.20	Final edit	Farah Diehl-Fahim

Statement of originality

This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation, or both.

Deliverable abstract

Tasks 10.5 and 10.6 of the UNICOM project focus on the legal issues relevant to the use of IDMP within health systems and the solutions developed within the UNICOM project. The objective of Task 10.5 is to provide an overview of the GDPR (set out in Deliverable 10.4) while Task 10.6 (and Deliverable 10.5) will provide practical support tools, including templates for key documents, to support compliance with the legislation both for UNICOM trials, and also for the development of any potential UNICOM solutions, such as the patient facing app foreseen in Work Package 8.

The present deliverable is drafted in response to Task 10.5 and provides an overview of the General Data Protection Regulation (GDPR) as it may apply to the use of health system management tools which incorporate IDMP, and the tools and approaches developed in the UNICOM project.

It provides UNICOM with an overview of the core principles of the GDPR and the ways in which the processing of sensitive data for both the primary purpose of healthcare provision and secondary purposes of pharmacovigilance and research may be legitimated. It also outlines the rights that the GDPR affords the data subject (patient) and how realisation of such rights will impact the organisations using UNICOM solutions.

Keywords: Data Protection, General Data Protection Regulation, GDPR, 2016/679, Patients

This document contains material, which is the copyright of the members of the UNICOM consortium listed above, and may not be reproduced or copied without their permission.

The commercial use of any information contained in this document may require a license from the owner of that information.

This document reflects only the views of the authors, and the European Commission is not liable for any use that may be made of its contents. The information in this document is provided “as is”, without warranty of any kind, and accept no liability for loss or damage suffered by any person using this information.

© 2019-2023. The participants of the UNICOM project.

TABLE OF CONTENTS

Deliverable abstract.....	3
List of abbreviations.....	5
Executive summary	6
1 Introduction.....	7
1.1 Scope of the report.....	7
1.2 What is the GDPR?	8
2 Introduction to the GDPR	9
2.1 Key terms in the GDPR	9
2.1.1 Personal data	9
2.1.2 Processing - by automated means or using a filing system.....	9
2.1.3 Data Controller and Data Processor	10
2.1.4 Consent	10
2.1.5 European Data Protection Board and European Data Protection Supervisor	10
2.2 Material and territorial scope of the GDPR.....	11
2.3 The principles relating to the processing of personal data.....	12
2.3.1 Understanding the core principle in a healthcare setting.....	12
3 The legitimization of processing health-related data	14
3.1 Processing data for care provision - primary purpose.....	15
3.2 Processing data for secondary purposes	17
3.2.1 Secondary processing for health system management.....	17
3.2.2 Secondary processing for scientific research	17
3.3 Processing data in a cross-border care setting.....	18
3.4 Data processing in a patient facing app	19
4 Data Subjects' Rights and the duties of data controllers	20
4.1 Data subject rights in a healthcare setting	21
4.1.1 Transparency and information	21
4.1.2 Access, rectification, restriction and erasure.....	21
4.1.3 Portability.....	22
4.1.4 Automated decision making	22
4.2 Duties of Data Controllers	23
4.2.1 Data Protection Officer (DPO).....	23
4.2.2 Data Protection Impact Assessment (DPIA)	24
Annex 1: Derogation, exemption, variation, restriction of the GDPR though national level legislation.	25

List of abbreviations

Abbreviation	Complete form
GDPR	General Data Protection Regulation
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
DPA	Data Protection Authority
DPO	Data Protection Officer
DPIA	Data Privacy Impact Assessment
eHDSI	eHealth Digital Services Infrastructure

Executive summary

The UNICOM project has been funded to support the implementation of the ISO IDMP (Identification of Medicinal Products) standards in EU Member States' drug databases, to increase the use of IDMP identifiers in patient care plans, and in the prescription and dispensation of medicines across the EU. The UNICOM project is not developing final products to be taken to market, but rather supporting the uptake of the IDMP standards within healthcare system workflow solutions through gap analysis, benefit demonstration and knowledge development to support data migration towards systems that use IDMP. The objective of this Report is therefore to ensure that the project partners have a working knowledge of the General Data Protection Regulation (GDPR) and understand the issues that must become addressed in assessing the use of IDMP and when developing tools to assist in the use of IDMP; and to provide an information resource for project partners leading trials within the project.

The introductory chapter of this Report provides further background to the project and the objectives of the Report. It is followed by three substantive chapters that set out:

- The key terms, scope, and core principles of the GDPR (chapter 2)
- The legitimisation for data processing in care provision and research in the GDPR (chapter 3)
- Data subjects' rights and the duties of data controllers and processors in the GDPR (chapter 4).

In chapter two the definition of personal data, data processing and consent are described, as well as the functions of the data controller and processor and the organisations of the European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS). Chapter two also sets out the territorial scope of the legislation.

Chapter three assesses the legal bases that legitimate the processing of health related data for care provision, for health system administration, and for research, setting out the way in which the legal bases provided in Article 6(1) and 9(2) are applicable. It also sets out the way in which GDPR applies when data are shared in the context of cross border care, and when data are collected and processed through the use of a patient-controlled app.

In the final chapter the rights of data subjects are addressed, looking at transparency in data processing, the rights of access, rectification, erasure, restriction and objection, and how these are supported by the data controller. It also considers the patient's right to a portable machine-readable copy of information in certain circumstances and the challenges of realising this right. The right not to be subject to automated decision-making is described, noting that it has limited application in a healthcare setting. The chapter also considers the duties of the data controller, notably to appoint a data protection officer (DPO) and conduct a data protection impact assessment (DPIA), which will arise in most cases where health related data are processed.

Chapters two, three and four include a series of highlighted points at the start of each section which set out how the issues described could impact the UNICOM project, and the way in which users of IDMP enhanced health system workflow solutions will need to respond to the requirements of the GDPR.

This Report will be complemented at a later date by a further deliverable that will provide practical support tools, including templates for key documents, to support compliance with the legislation both for UNICOM trials, and also for the development of any potential UNICOM solutions, such as the patient facing app foreseen in Work Package 8. That Report will take account of the applicable national level legislation which the GDPR foresees. A summary of the Articles of the GDPR where potential national variations are possible, or in some cases required, is set out in Annex 1 of this report.

1 Introduction

1.1 Scope of the report

The UNICOM project has been funded to support the implementation of the ISO IDMP (Identification of Medicinal Products) standards in EU Member States' drug databases and to increase the use of IDMP identifiers in patient care plans and in the prescription and dispensation of medicines across the EU. It is hoped that more widespread use of the IDMP identifiers will lead to safer use of cross-border ePrescription/eDispensation, improved pharmacovigilance, improved clinical decision support, better patient empowerment, and will also help support public health and clinical research.

The UNICOM project work plan includes a range of tasks to support the use of IDMP in healthcare workflow systems and apps in both domestic and cross-border care settings. Such systems will necessarily handle the sensitive personal data held in medical records, prescriptions, patient summaries and other patient related documentation, and as such must comply with EU and national law on data protection. At EU level this is embodied within the General Data Protection Regulation (2016/ 679), referred to as GDPR.

The ultimate responsibility of complying with the GDPR falls on the data protection officers within the pharmacies, hospitals and other healthcare settings in which the healthcare workflow systems and apps that incorporate IDMP identifiers are used. However, it is useful for project partners to have a good level of understanding of the requirements of the law. Such knowledge will serve two purposes:

- ensure that the project partners have a working knowledge of the GDPR and understand the issues that must be addressed in assessing the use of IDMP and when developing tools to assist in the use of IDMP;
- provide an information resource for project partners leading trials within the project, to ensure they fully understand the requirements that are detailed in the Ethics Report and Data Management Report developed within Work Package 13.

The UNICOM project is not developing final products to be taken to market, but rather supporting the uptake of the IDMP standards within healthcare system workflow solutions through gap analysis, benefit demonstration and knowledge development to support data migration towards systems that use IDMP. This will include a great deal of baseline work which has no direct connection with personal information and therefore is not directly implicated by the GDPR. The main focus will therefore not be the project *per se*, but rather the use of IDMP identifiers within healthcare system workflow in the course of the UNICOM project and beyond. The following chapters will outline the key elements of GDPR that apply when such systems process patient information, and highlight the implications that must be borne in mind by the people with data protection responsibilities in the settings where IDMP enriched patient information may be used.

The project will undertake small scale trials of applications and services, as well as one larger scale evaluation which will be undertaken on behalf of UNICOM by the European eHealth DSI programme. This pilot will be developed initially using 'dummy' patient data, and will in later stages use the IDMP identified within real ePrescriptions handled by participating Member States through the eHealth DSI programme, which will also assume responsibility for its GDPR compliance. Where the UNICOM pilots and trials use real patient data the project partners executing the pilots will have to comply with GDPR in the conduct of the pilots. The practical compliance issues of such pilots and trials are addressed in the ethical and legal compliance work of Work Package 13, and will be complemented by specific guidance set out in Deliverable 10.5. The work reported in deliverable 10.5 will include guidance on the application of the GDPR in the countries where the trials are conducted, as well as the role of data protection officers in pharmacies and medical practices where the solutions are trialled. It will examine the current practices in the test sites to identify good practices and potential gaps in good practice.

1.2 What is the GDPR?

The GDPR is a European Union Regulation, that is, it is a binding legislative act which must be applied in its entirety across the EU. A “Regulation” is adopted when the EU wants to ensure that rules are applied in a standardised way across the Union, and is used less commonly than a “Directive”, which is a legislative act that sets out goals that all EU countries must achieve, but leaves it up to the individual countries to devise their own laws to reach those goals.

The GDPR applies to any processing of personal data relating to an identified or identifiable natural person. The GDPR begins by setting out material and territorial scope of the law defining the terms used in the law, and the core principles of data protection (Articles 1-4). It then defines the circumstance which legitimates the processing of personal data (Articles 5-11), and sets out the rights of a data subject (Articles 12-23). The duties of a data controller and data processor are also set out in detail in the legislation (Articles 24-43), as well as the rules for transfer of data to countries outside the European Union (Articles 44-50). The remainder of the GDPR (Articles 51-99) address the functions of supervisory authorities at national and EU level and co-operation between them; the liabilities arising under the law and the penalties that may be imposed if breaches of duties arise.

In order to meet the objective of developing a basic understanding of the GDPR, this report provides an easily understandable overview of the issues described above, and outlines the particular impact they have on the use of patient identifiable information within healthcare system workflows. The body of the report is organised in three chapters:

- The key terms, scope and core principles of the GDPR (chapter 2)
- The legitimisation for data processing in care provision and research in the GDPR (chapter 3)
- Data subjects’ rights and the duties of data controllers and processors in the GDPR (chapter 4)

Despite being a Regulation, the GDPR includes several provisions for national level legislation to address certain aspects of the way which the GDPR is implemented. These are discussed in the chapters of this report and also set out in Annex 1.

2 Introduction to the GDPR

Chapter 1 of the GDPR sets out the material and territorial scope for its application and defines the terms used in the Regulation. Here we will begin by explaining the key terms relevant in a healthcare setting and then briefly outline the material and territorial scope of the legislation. For a full description of all terms used in the GDPR, reference should be made to the text of the GDPR which can be accessed in every EU language at <https://eur-lex.europa.eu/legal-content/EN/TXT>.

2.1 Key terms in the GDPR

2.1.1 Personal data - identified, identifiable, pseudonymised, anonymised

Personal data is information relating to natural persons through which they may be identified directly or indirectly. Information must 'relate to' the identifiable individual to be personal data, this means that it does more than simply identifying them – it must concern the individual in some way. Personal data may be pseudonymised, that is given an alternative label rather than a name, address or other easily identifiable label. Pseudonymising data is good practice to help reduce privacy risks by making it more difficult to identify individuals, but pseudonymised data remain personal data in the terms of the GDPR.

If data can be fully anonymised, then the GDPR no longer applies. However, as the guidance provided by the French DPA (CNIL) emphasises, account must be taken of all the means available to the data controller to determine whether a person is identifiable from the data. Only if it is impossible to re-identify data can it be truly called anonymous data. In the healthcare setting this is especially significant in cases of combined medical information. In the context of the UNICOM project and the use of IDMP identifiers, it is unlikely that data could ever be anonymised and still serve the purposes for which it was collected, such as identifying of unique clinical patterns which are dependent on the use of many items of identifiable information, including the temporal sequence of health issues and care interventions.

The GDPR applies only to natural persons, that means it does not apply to information about companies (legal persons), nor to information about a deceased person. Note however that data about a deceased person may also include personal information about an identifiable living individual. For example, a deceased person's medical records may contain information about other individuals, such as carers and relatives, accordingly the medical records of a deceased person could nevertheless be classified as personal data in the context of the GDPR.

The GDPR distinguishes between personal data and sensitive personal data. Sensitive data are those which reveal racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic or biometric data (where used for identification purposes); data concerning health; a person's sex life; or a person's sexual orientation. The GDPR prohibits the processing of sensitive personal data unless special requirements in Article 9(2) can be met.

2.1.2 Processing - by automated means or using a filing system

Data processing includes collecting, recording, storing, using, analysing, combining, disclosing or deleting data using some form of 'filing system'. A filing system is defined as any structured set of personal data that are accessible according to specific criteria whether centralised, decentralised or dispersed on a functional or geographical basis. The GDPR applies to the processing of personal data by both automated and manual means provided that the personal data are contained, or are intended to be, contained in a filing system. The GDPR does not cover information, which is not, or is not intended to be, part of a filing system. Note however that in some countries certain data held in paper records and not organised into any form of filing system may be covered by additional national level data protection legislation. In the UK, for example, unstructured manual information processed by public

authorities constitutes personal data under the Data Protection Act 2018 (which is the UK implementation of the GDPR).

2.1.3 Data Controller and Data Processor

A data controller is the person or organisation that decides how and why to collect and use data. This will usually be an organisation, but can be an individual (e.g. a sole trader). The controller must ensure that the processing of data complies with data protection law, including the GDPR.

A processor is a separate person or organisation (not an employee) who processes data on behalf of the controller and in accordance with their instructions. Processors have some direct legal obligations, but these are more limited than the controller's obligations.

Controllers shoulder the highest level of compliance responsibility, they must demonstrate compliance with all the data protection principles as well as the other GDPR requirements, and they are responsible for the compliance of their processor(s). In some cases, two organisations may jointly determine the purposes and means of the processing for the same personal data, in such a case they are joint controllers. However, they are not joint controllers if they are processing the same data for different purposes. This may often be the case in a healthcare setting where the same data are processed both for care and for wider public health or research purposes by two legal entities that work closely together.

2.1.4 Consent

Consent is defined with GDPR in a strict way. Consent must be freely given and fully informed, this means the purpose of processing data and all types of processing planned must be made clear to the data subject in a concise, user-friendly and easily understandable way at the time at which data are collected. The process by which consent may be withdrawn must also be clearly explained to the data subject.

Consent requests must be unbundled from other terms and conditions for services or goods which the data subject might be receiving from the data controller. Consent must be given by way of active opt-in, not using any pre-ticked boxes or other passive consent mechanisms. The controller must be identified by name and a way of contacting the controller must be provided.

The GDPR further requires that when the consent is for the processing of sensitive data, such as health data, consent must be explicit. The GDPR does not clearly set out the difference between consent and explicit consent, but practice in the Member States suggests that explicit consent is confirmed in a clear statement (whether oral or written) and is separate from any other consents being sought. In healthcare this means the consent to treatment is separate from consent to processing data. The data controller should keep records that show who consented, when, how, and what information was provided prior to consent being given.

2.1.5 European Data Protection Board and European Data Protection Supervisor

The European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS) are important bodies in developing the understanding of the GDPR and its application. The EDPB is defined on its website³ as an independent European body which contributes to the consistent application of data protection rules throughout the European Union, and promotes cooperation between the EU's data protection authorities. The EDPB is composed of representatives of the national data protection authorities, and the European Data Protection Supervisor (EDPS). The European Data Protection Supervisor (EDPS)⁴ is the EU's independent data protection authority. It monitors and ensures

³ See https://edpb.europa.eu/about-edpb/about-edpb_en

⁴ See https://edps.europa.eu/about-edps_en

compliance with the GDPR when the EU institutions and bodies process the personal information of individual and advises EU institutions and bodies on all matters relating to the processing of personal data. It is also consulted by the European Commission on proposals for legislation and international agreements which might impact on data protection and privacy.

2.2 Material and territorial scope of the GDPR




The opening chapter of the GDPR also defines the material and territorial scope of the GDPR in Articles 2 and 3. With respect to material scope it states that the GDPR applies to the processing of personal data wholly or partly by automated means and to the processing of personal data which form part of a filing system or are intended to form part of a filing system, whether by automated or other means.

In terms of territorial scope the law applies to the processing by a controller or processor carried out in the context of the activities of an establishment of that controller or processor in the Union, regardless of the actual place of the processing. In order to clarify this scope the EDPB provides a Guideline⁵, which includes several examples, one of which described a pharmaceutical company with headquarters in Stockholm which has located all its processing activities with regards to its clinical trial data in its branch based in Singapore. Even though the data processing activities take place in Singapore, the processing is carried out in the context of the activities of the pharmaceutical company in Stockholm i.e. of a data controller established in the Union, and accordingly the GDPR applies to the processing that takes place in Singapore.

Where the data controller has no EU presence, the GDPR will still apply whenever an EU resident's personal data is processed in connection with goods or services offered to him or her; or, when the behaviour of individuals within the EU is "monitored". This will be relevant to many apps which track location, as well as localised advice services.

It applies also to any processing of data of an individual in the EU, regardless of their citizenship. The wording of Article 3(2) refers to "personal data of data subjects who are in the Union". This provision of the GDPR reflects EU primary law which also lays down a broad scope for the protection of personal data, not limited to EU citizens, with Article 8 of the Charter of Fundamental Rights providing that the right to the protection of personal data is not limited but is for everyone⁶.

What does Chapter 1 of the GDPR mean for UNICOM?

-  *The UNICOM project seeks to support the use of IDMP in information systems used in providing healthcare services. Such services will be subject to the GDPR when they include the use of identifiable patient information.*
-  *The Unicom project will undertake trials which will process identifiable patient information, such trials must be conducted in accordance with the GDPR.*
-  *When a service using IDMP is used, such as ePrescription/dispensation service, if the data subject is in the EU, the service provider will be subject to the GDPR, regardless of where the service provider is geographically located.*

⁵ Guidelines 3/2018 on the territorial scope of the GDPR https://edpb.europa.eu/our-work-tools/our-documents/riktlinjer/guidelines-32018-territorial-scope-gdpr-article-3-version_en

⁶ Charter of Fundamental Right of the European Union, Article 8(1) "Everyone has the right to the protection of personal data concerning him or her".

2.3 The principles relating to the processing of personal data

The core principles of data processing are set out in Chapter 2 (Article 5) of the GDPR. Article 5 lists seven key principles which lie at the heart of the general data protection regime. They are set out in full in Box 1:

BOX 1: Article 5 of the GDPR

- 1) Personal data shall be:
 - a) processed **lawfully, fairly and in a transparent** manner in relation to the data subject ('lawfulness, fairness and transparency');
 - b) collected for **specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
 - c) **adequate, relevant and limited** to what is necessary in relation to the purposes for which they are processed ('data minimisation');
 - d) **accurate** and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
 - e) kept in a form which permits identification of data subjects for no **longer than is necessary** for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
 - f) processed in a manner that ensures **appropriate security** of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').
- 2) The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

2.3.1 Understanding the core principle in a healthcare setting

Healthcare providers, whether public or private, in a consumer setting (such as a pharmacy) or a specialist setting (such as a hospital) are bound by the requirements of the GDPR and must respect the data rights of any person to whom they provide services. Third parties who do not have a direct relationship with a patient, such as a public authority with administrative responsibility for healthcare services, or a research organisation with access to a patient's data, will also be bound by the GDPR if the data they are processing identify or permit identification of a natural person. This means that healthcare service providers, and all those who process identifiable patient information on their behalf, must be fair and transparent in their data processing. Healthcare provision is often intimately tied up with data collection - in fact almost every encounter between a healthcare professional and patient





begins with the anamnesis, the taking of the medical history during which a great deal of sensitive personal information will be revealed.

In order to be fair and transparent the purpose of processing data must also be clear, noting that in a healthcare setting there may be several purposes – to provide care, to support the administrative aspects of care provision such as reporting and billing, as well as wider health system management purposes and research purposes. All these purposes will not be readily apparent to a patient and should be explained in patient information notices.

Article 5 also requires that the data must be adequate to meet the needs of the stated purpose and that only data that are relevant for the purpose are collected; the data must be kept only as long as they are needed to meet that purpose. These requirements are not as difficult to satisfy in the healthcare setting, as adequacy of data in healthcare may be widely interpreted, as a clinician will often need as much information as possible to treat a patient in a holistic manner. Many Member States have sectoral laws which define how long data must be kept, which will often be for a period of years after last treatment or after the patient's death.

The data must also be accurate, kept up to date and stored in a secure manner. The requirement for accuracy poses few problems in healthcare, as the act of providing care itself demands that the information is accurate and up to date. In fact, the emphasis on these qualities mean that data are often collected repeatedly by different healthcare providers because each provider want to be sure they have accurate and up to date information to hand. The need to keep data in a secure manner is also well established in healthcare settings, but as data breaches have shown, often simple human mistakes compromise data security, rather than artful cyber-attacks.

What do the core principles mean for UNICOM?

-  *Meeting the GDPR requirements means that all the purposes to which data may be put should be made clear to the patient. This means providing information to patients that outlines not only the primary purpose of collecting data to provide care, but also the secondary purposes of health system management and potential further research if it is appropriate to do so.*
-  *Care must be taken to collect an adequate amount of information to meet the needs of the stated purpose and data must be kept only as long as necessary for the stated purpose. These requirements must be understood in the context of health sector legislation which may require certain data to be collected and stored for a defined period of time.*
-  *It requires that the IT system(s) used, and programmes and applications used in it, must be designed and built with data protection principles in mind and with the capacity to meet not only the security requirements of the GDPR, but also of related EU legislation such as the Network Information Security Directive 2016/1148/EU.*
-  *Security includes physical security of premises, demanding that computer screens are not visible to unauthorised persons, that conversations cannot be overheard, and that rooms and premises can be secured against the theft of devices that store data. It also means that staff must be educated about their data protection duties and supported in executing them.*

3 The legitimization of processing health-related data

The GDPR requires that data collection and processing must be legitimated by reference to one of the legal bases for processing personal data set out in Article 6(1) GDPR. Where the data are sensitive data, which includes all data relating to health, one of the legal bases set out in Article 9(2) GDPR must *also* be satisfied.

All data controllers must be able to point the legal base(s) being used for any data processing. Box 2 sets out the six legal bases of Article 6(1) and the seven legal bases for processing sensitive data relevant to health-related data. Article 9(2) includes ten legal bases in total, however 9(2)(d) applies to processing details of membership of a political, philosophical, religious or trade union bodies and will therefore not include healthcare information; while 9(2)(e) and (f) concern data that have been made public by the data subject or data are to be used for establishing a legal claim or by a court acting in a judicial capacity, while these actions may include health related information, these legal bases are not addressed to data controllers in a healthcare setting.

Box 2: Article 6(1) of the GDPR

- (1) Processing shall be lawful only if and to the extent that at least one of the following applies:
- a) The data subject has given **consent** to the processing of his or her personal data for one or more specific purposes;
 - b) Processing is necessary for the **performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
 - c) Processing is necessary for **compliance with a legal obligation** to which the controller is subject;
 - d) Processing is necessary in order to protect the **vital interests** of the data subject or of another natural person;
 - e) Processing is necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the controller;
 - f) Processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. When relying on this legal basis, an assessment of the necessity and the purpose of the processing operation as well as a balancing test between the interest of the data subject against those of the controller and third parties are required.

Box 3: Article 9 of the GDPR

- (1) Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.
- (2) Paragraph 1 shall not apply if one of the following applies:
- a) The data subject has given **explicit consent** to processing those personal data for one or more specified purposes, except when Union or Member State law provides that the data subject cannot give consent.

- (b) Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and **social security and social protection law** in so far as it is authorised by Union or **Member State law** or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.
- (c) Processing is necessary to protect the **vital interests of the data subject or of another natural person** where the data subject is physically or legally incapable of giving consent
- (g) Processing is necessary for reasons of **substantial public interest**, on the basis of Union or **Member State law** which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject
- (h) Processing is necessary for the purposes of **preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services** on the basis of Union or **Member State law** or pursuant to contract with a health professional and subject to the conditions and safeguards.
- (i) Processing is necessary for reasons of **public interest in the area of public health**, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or **Member State law** which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.
- (j) Processing is necessary for **archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1)** based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject.

As noted in the definitions, the GDPR distinguishes between ordinary personal data and sensitive personal data, which is defined in Article 4 as any data related to the physical or mental health of an individual, including data generated in the context of providing health services which reveal information about his or her health status. In a healthcare setting of any type, the data controller will therefore have to find a legal base in both Article 6(1) and Article 9(2).

In order to understand which combination of legal bases in Articles 6(1) and 9(2) are appropriate for a specific act of health-related data processing, it is important to distinguish between primary and secondary purposes of data processing. The primary purposes are those to which data are put soon after collection and will, in a healthcare setting, usually be directly related to care provision. The same data may later be used for secondary purposes such as billing, health system management and planning, or research related such as pharmacovigilance or scientific research. The two uses of data are discussed in further detail below.

3.1 Processing data for care provision - primary purpose

When data are collected, or generated, in a healthcare setting such as a doctor's office or a care facility, or in an on-line care setting (such as a remote consultation) they are often used first for the purpose directly presented to the data subject at the time of data collection. Although the data collected at the point of care will usually be used in that setting, it may also need to be shared with other care providers for the continuity of care, with administrative services and in some cases also across EU borders when patients receive care in a Member State other than their usual Member State of residence.

Depending on any sector specific law that may exist in a Member State, the legal basis given for processing data in a healthcare setting for the purposes of care provision will vary between Member States and may also vary between different types of service providers - pharmacists, hospitals, private doctors may be governed by different requirements.




The GDPR does not prescribe which combination of legal bases in Article 6(1) and 9(2) should be used when a healthcare professional processes health related data, and research has shown that a wide range of combinations is used across the EU, which has led many to argue that the GDPR is fragmented and the high level of harmonisation of legislation usually expected to result from the adoption of a Regulation has not been achieved for the GDPR in the context of health-related data.⁷

Articles 6(1)(a) and 9(2)(a) provide consent as one of the legal bases for data processing. Despite the fact that this is the first legal base named and also because consent is widely used to legitimate data processing outside the healthcare setting (note for example to consent boxes that appear whenever a web site is accessed), consent is rarely used as the legal basis for the processing of health related information by a healthcare professional. This is primarily because it is difficult to meet the requirement that the consent to data processing in a healthcare setting is freely given. It is difficult to provide care to a patient without information about the patient's history, accordingly, sharing such history may not be a free choice if the patient wants to be cared for. Furthermore, the GDPR notes that consent may not be appropriate where there is imbalance between the data subject and the controller, in particular where the controller is a public authority.

In the healthcare setting it is far more common that the legitimation for processing health data is found in national level legislation adopted in accordance Article 6(1) (c) or (e) and 9(2)(b), (g), (h), or (i). A study on the use of the GDPR in the healthcare setting across all Member States published in 2020⁸ found that the most frequently used legal bases for legitimating the processing of health-related data for care provision were Article 6(1)(c) used in conjunction with Article 9(2)(h). This combination was reported in 20 Member States, with four giving this as the only legal base used to legitimate data processing.

It is worth noting that the legal base of vital interest (Article 6(1)(d) and 9(2)(c)) will be used rarely, as it is reserved for cases of significant need. Recital 46 clarifies that the vital interests legal base applies when processing data is necessary to protect an interest which is essential for the life of the data subject or that of another natural person and where the processing cannot be based on another legal basis.

Which legal bases are most likely to be used where IDMP identifiers and UNICOM based solutions are used in care provision?

-  *A legal base in Article 6(1) and Article 9(2) must be referenced by the data controller to legitimate the processing of health-related data for care purposes. In some cases this will be consent (Article 6(1)(a) and 9(2)(a)), but in most cases national legislation governing healthcare services will exist, meaning that Article 6(1)(c) used in conjunction with Article 9(2)(h) will often be the legal base.*
-  *The data controller in a healthcare setting using a workflow system that includes IDMP identifiers must take due note of national legislation as well as GDPR.*
-  *In the context of providing a prescription for a medicine, or dispensing such a medicine, it is very likely that the healthcare professional will need to comply with administrative rules on prescribing and dispensing of medicinal products, which require the creation of a written prescription which is stored and communicated to payer organisations as well as oversight bodies.*

⁷ Not yet published, reference will be supplied on publication

⁸ Not yet published, reference will be supplied on publication

3.2 Processing data for secondary purposes





3.2.1 Secondary processing for health system management

It is widely acknowledged that safe, efficient and sustainable healthcare systems are highly dependent on data⁹. As well as being used for the primary purpose of providing care, health-related data are also used for healthcare system planning, supervision and improvement.

The UNICOM project seeks to ensure that the use of IDMP can support such use of data, notably for wider public health purposes including planning, management, administration and improvement of health and care systems; prevention or control of communicable diseases; protection against serious threats to health and ensuring high standards of quality and safety of healthcare and of medical products and medical devices. Such purposes entail the re-use of health data that were collected initially in the context of providing care, but which can later be re-used for secondary use exercised by public entities such as national health systems, statutory payers, public health bodies and by regulators such as medicines agencies.

In many cases such secondary use will be set out in national level sector specific legislation, in some cases adopted in accordance with EU level legislation. This would be the case, for example, where prescription data are re-used in the context of pharmacovigilance. Although pharmacovigilance is based on an EU directive (2010/84/EU), the directive does not state that personal data may be processed for this purpose, accordingly in most Member States legislation has been put in place to allow such secondary use.

Which legal bases are most likely to be used where IDMP identifiers and UNICOM based solutions are in the context of secondary processing for health system management?

-  *The data controller in a healthcare setting using a workflow system that includes IDMP identifiers must take due note of national legislation as well as GDPR.*
-  *Where data are further processed to report to public authorities the data controller will need to cite reliance on Article 6(1)(c) or (e) and 9(2)(h) or (i) identifying the relevant national legislation that has been enacted to address such further processing.*
-  *Where data are further processed by private sector actors, such as insurers, the legal bases may be Article 6(1)(f) - legitimate interest and 9(2)(h) – healthcare.*
-  *If no such legislation exists, patient consent would need to be obtained for sharing nominative data with public authorities, or the data would need to be fully anonymised.*

3.2.2 Secondary processing for scientific research

Health-related data are often also further processed for scientific research purposes rather than for a health system management task. Article 6(4) states that data can only be further processed for a purpose other than the purpose stated at the time of collection if it is compatible with that purpose. When it comes to research, this should be read in conjunction with Article 5(1)(b) which carves out a privileged position for scientific research, stating that further processing for scientific research purposes in accordance with Article 89(1) is not considered incompatible with the principle purpose.

In some Member States legislation has been adopted which allows for secondary use of data for research by reasons of public interest in research. Where such legislation exists Article 6(1)(e) and

⁹ Delvaux et al 2019, OECD 2019

9(2)(i) may be cited as the legal bases in GDPR. In many countries such legislation is however applicable only to public bodies.

The GDPR creates in Article 9(2)(j) and Article 89(1) a wide margin for national legislators to specify safeguards and derogations in the context of research. Where therefore a data controller wants to use the data generated in the context of healthcare provision for scientific research that cannot rely on the public interest provision of Article 9(2)(i), the national level laws on access to data for research purposes will provide the only legal basis for such further processing of data for research purposes. These can only be circumvented if patient consent to use the data for research is granted, or the data are fully anonymised. However, wide variation exists between Member States in the national level legislation they have implemented, and as a result data exchange between Member States for research purposes is often difficult.

Which legal bases are most likely to be used where IDMP identifiers and UNICOM based solutions are in the context of secondary processing for scientific research?

- ➔ *Where data are further processed for scientific research purposes that are in the public interest, the data controller will be able cite to rely on Article 6(1) (e) and 9(2)(c) identifying the relevant national legislation that has been enacted to address such further processing.*
- ➔ *Where data are further processed for scientific research purposes that are based on a wider public interest, the data controller will need to cite reliance on Article 6(1) (f) and 9(2)(j) identifying the relevant national legislation that has been enacted to address such further processing, in addition technical and organisational safeguards must be adopted, including data minimisation, as set out in Article 89(1).*
- ➔ *If no such legislation exists, patient consent would need to be obtained for sharing nominative data with public authorities, or the data would need to be fully anonymised.*

3.3 Processing data in a cross-border care setting

When care is provided in a cross border setting the GDPR will apply alongside any special rules adopted for the particular cross-border setting. The Cross Border Care Directive (2011/24/EU) is the legal basis for cross-border healthcare provision within the EU. It creates the eHealth Network¹⁰, which is in charge of diverse eHealth objectives, including the cross-border sharing of patient data for ePrescription/Dispensation. For the purposes of the UNICOM project the key legal guidance will come from the eHealth Member States Experts Group, whose legal advisors have prepared various reports, of which the most relevant to date is the eHealth Digital Service Infrastructure Legal Report drafted as part of the eHealth Joint Action¹¹.

In a cross-border eHealth setting, the services used will almost certainly have to use electronic identification of patients and healthcare professionals. This demands that the requirements of Regulation EU/910/2014 on electronic identification and trust services for electronic transactions in the internal market (referred to as the eIDAS Regulation) are taken into account. This means that Member States are obliged to recognise notified eID Schemes for online service provision. It stipulates that in cross border cases, authentication assurance levels of eIDs electronic signatures shall be harmonised. As noted by the report of the eHDSI Working Group, once fully implemented, the eIDAS Regulation will create enabling conditions for secure transfer of health data across borders in the EU, e.g. by overcoming the specific challenge that the involved human and organisational actors are usually only

¹⁰ Details on the functioning and tasks of the eHealth Network can be found in the Commission Implementing Decision 2011/890/EU

¹¹ Available at https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20190611_co222_en.pdf

recognised within one of the participating countries while being active participants in flows in other countries. The eIDAS Regulation can foster the establishment of regulation-backed cross-border trust relationships between Member States and provide both the identification and authentication of health professionals and patients as well as assure the integrity and confidentiality of the sensitive health data shared cross-border for eHDSI.

Which legal bases are most likely to be used where IDMP identifiers and UNICOM based solutions are used in a cross-border context?



Where data are used for care provision purposes at present the most likely legal bases will be consent as provided for in Articles 6(1)(a) and 9(2)(a), because to date no Member States have adopted specific legislation for such data sharing. However, the interpretation of consent, in particular if this differs between the Member States involved in the care, will depend on the guidance offered by eHealth Member States Experts Group and in due course the implementing legislation for the eHDSI.

3.4 Data processing in a patient facing app

The UNICOM project is developing apps that may be used by patients or citizens to help them better understand the medicines they are taking, notably by integrating IDMP into such apps.

As anyone who has downloaded a healthcare app for use on a personal device will know, the processing of personal data in a healthcare app is (or should be) based on consent. In order to be valid, consent must be freely given, specific, informed and unambiguous as defined in Article 4 (11) GDPR.

In some situations, an app will be directly linked to care provided to a patient, such as an app to help diabetes patients manage insulin dosing, or an app to measure output from an implanted device. In such cases the app may be directly linked to the provision of care, and the legal basis for legitimising such data processing will be the same as for the processing of data for care provision, as described in section 3.1 above.

Which legal bases are most likely to be used where IDMP identifiers and UNICOM based solutions are used in a cross-border context?



Where an app is made available to patients, valid consent for the processing of data within the app will usually be required. In order to be valid consent, the patient must be fully informed about what data are collected, who has access to them, for what purpose they will be used and for how long they will be stored.



When the use of the app is directly linked to a specific medicine, therapy or device, the processing of data may be the same as for processing data for care provision purposes, such as Article 6(1)(c) or (e) and 9(2)(h) or (i).

4 Data Subjects' Rights and the duties of data controllers

The GDPR sets out a number of rights of the data subject, including the right to access data, rectify mistakes and in some cases have data erased - the so called 'right to be forgotten'. The data subject will in certain cases also have a right of data portability, allowing the data subject to take the data in a machine-readable format from one data controller to another. The GDPR also sets out the duties of data controllers and data processors, defines the circumstances in which data may be transferred outside the EU and also establishes the remedies, liabilities and penalties if data breaches occur.

The rights of data subjects which may be summarised into four broad categories as set out in box 4 below:

Box 4: Data Subjects' Rights

- **Information and transparency** (Articles 12,13,14): The data subject has the right to be clearly informed why the data is needed, how it will be used and to whom it will be accessible. This includes giving contact details of a person who must be able to respond to a data subject's questions in a timely manner. Where the legitimation for using data is based in the data controller's legitimate interest (Article 6(1)(f)), such legitimate interests must be clearly explained. The data subject must also know for how long data will be stored and must also be informed about the way in which their rights data are processed on the basis of consent, the information provided must be sufficient to make such consent valid.
- **Access** (Article 15) **Rectification** (Article 16) **Erasure** (Article 17) or **Restriction** (Article 18) and **Objection** (Article 21): Article 15 provides that the data controller must provide access in the form of copies of the personal data being processed, and where data are processed electronically such copies should be electronic. The data subject also has several rights to limit the way in which data are processed. The right of rectification means the data controller must correct any inaccuracy the data subject identifies as soon as possible, and to restrict processing while correction takes place. Erasure, also known as 'the right to be forgotten' is available only if the data are no longer necessary for the purposes for which they were collected or when the data subject withdraws consent. However, Article 17(3)(c) states the right shall not apply when data are processed for healthcare provision (Article 9(2)(h)) or public health purposes (Article 9(2)(i)), while 17(3)(d) extends the exemption to data processed for scientific research purposes in accordance with Article 89(1). Article 19 requires the data controller to notify any parties who have received data about any correction, restriction or erasure of data. Article 21 provides the right to object to processing, particularly in relation to direct marketing, but limits such right in the context of scientific research.
- **Data Portability** (Article 20): The data subject has the right to receive a portable copy of any data concerning him or her that the data controller holds. This should be provided in a common machine-readable format and must allow the data subject to transfer the data to another data controller. This right is however restricted to data which has been processed on the basis of consent and which is processed by automated means.
- **Automated decision making and profiling** (Article 22): Where data are processed on the basis of public interest or legitimate interest (Articles 6(1)(e) and (f)), the data subject may object to any automated processing where such processing produces legal effects or similarly affects him or her. This right may be limited by national legislation.

4.1 Data subject rights in a healthcare setting

The rights as described above are general rights that apply to all data subjects and all types of data. When applied to health-related data and in the healthcare setting they must be interpreted in the context of healthcare, where a number of other legal requirements with respect to data will exist at national level. Most importantly this will include regulations that require health-related data to be collected and processed in a particular way, often including minimum retention periods. In most countries there will also be legal provision to facilitate accessing or processing data in an emergency situation where usual rules of providing information to the data subject cannot be adhered to, as well as situations where normal rules of access to data by the patient may be overruled in the interests of protecting the patient or others. Such exceptions are much less common than they once were. Overriding of patients' rights now almost always requires careful justification and documentation, but nevertheless, in the healthcare setting the rights as set out above cannot always be exercised as a matter of absolute right. The GDPR itself foresees this, providing in Article 23 (1) that Union or Member State law may be adopted that limits the rights in Articles 12-22 in certain circumstances, including the interests of public health (Article 23(1)(e)). However, such restrictions must respect the fundamental rights and freedoms of individuals and must be necessary and proportionate to the public or individual interests that are being safeguarded. Special reference is made in the GDPR to possible derogations from certain data subject rights when data are processed for scientific research purposes. Article 89(2) provides that Member States may adopt national level legislation that limit the rights of data subjects to access data concerning them, as well as limiting the rights to rectify data, or in some way restrict or object to its use.

4.1.1 Transparency and information

The rights related to transparency and information are not usually directly exercised by patients, but are the result of certain duties that a data controller must inform data subjects about how data are to be processed. In practice these duties are usually discharged when a data controller provides information notices about data collection and processing.

As well as being informed about what the data controller intends to do with the data, the data subject must also be informed about their rights and how to exercise them. Where consent is used as the legal basis for processing the right to withdraw consent must be made clear, and if the data controller loans to use 'legitimate interest' in processing data (Article 6(1)(f)), this must also clearly explained. The data subject must be informed about the means by which to make a complaint about the way in which their data are being handled, this information must be provided in a clear, accessible and intelligible manner, meaning that issues of intellectual capacity to understand as well as physical aspects of accessibility, such as font size in written information, must be taken into account.

Recognising that it is not always possible to provide all this information, some exceptions are allowed. Article 14 provides particular exceptions in the case of further processing of data for research purposes where providing all the information to the data subject would involve a disproportionate effort or impair the objectives of the research (Article 14(5)(b)). However, if use is made of this exception, then the safeguards referred to in Article 89(1) must be observed.

4.1.2 Access, rectification, restriction and erasure

The rights associated with access, rectification or erasure of records (Articles 15, 16 and 17, respectively), are particularly complex in the case of health-related data and must be understood in the context of healthcare provision and research. Although the GDPR confers these rights as a matter of general principle, in the healthcare setting they have to be understood within a wider framework because a healthcare record is not only a record of data concerning a patient, it is also a record of the professional interventions as well as a reflection of the opinions of the healthcare professionals who interact with the patient. The right of access to information concerning the data subject in a health record is, in most

countries, enshrined also in patients' rights laws and can usually only be denied when to grant access would be medically detrimental to the patient.

The right to erasure is however more limited. It arises only where the data are no longer necessary for the purpose for which they were originally collected, or when consent was the original legal base of data collection and such consent is withdrawn. Both these cases are unlikely to arise in a healthcare setting, since the purpose of recording patient information is generally patient care and that purpose usually persists at minimum for the lifetime of the patient, and may be relevant well beyond the patient's life time as the health records of antecedents can be important diagnostic aides for living patients.

4.1.3 Portability



With respect to healthcare, the right to portability is perhaps the most important right from a patient perspective, since it supports the patient in seeking care from a new healthcare professional in his or her own country as well as in other countries. The GDPR creates a general right of portability of data in two situations: when the data have been collected on the basis of consent or for the performance of a contract; and where the data are processed electronically, the latter because the Article 20 specifically notes that portable data must be provided in a machine readable format. The right does not apply to all the data that might exist about a patient in a healthcare setting, as it applies only to the data provided by the data subject and not to additional data that the data controller has created based on the data an individual has provided. In a healthcare setting that could be interpreted to mean that a radiological image must be provided in a portable format, but not necessarily the medical annotation of the image. Note however that access must be provided to that information if patient asks for it, but such access would not have to entail the transfer of the data in a machine-readable format.

In practical terms it is often not easy for a healthcare provider to comply with a request for data portability, not for legal reasons, but because limited use standards in healthcare information technology makes the transfer of data from one healthcare provider to another complex. Furthermore, lack of understanding about the right of portability among healthcare professionals and health system administrators often makes realisation of the right very challenging for patients.

4.1.4 Automated decision making

Article 22 creates the right not to be subject to a decision based solely on automated processing, if such processing is based on public interest (Article 6(1)(e)) or legitimate interest (Article 6(1)(f)), and if such processing produces legal effects for the data subject. This right has limited application in the healthcare setting because the rule applies to decisions made solely on the basis of automated decision making, which is rare in a healthcare setting where automation tools are usually decision support for healthcare professional, rather than decision replacement. In addition, such tools will often be used on the basis of patient consent, although here the validity of the consent should be addressed carefully as patients will need to understand the way their data are used within the system. Note also, consent to be treated based on an automated decision cannot be bundled with the use of data that it necessarily demands, this must be provided separately.

How could the rights granted to patients under the GDPR impact the use of IDMP and related solutions?

-  *The solutions and apps developed in the context of the UNICOM project, and other solutions which incorporate the IDMP identifiers will often include the processing of patients' information, and as such will create a situation in which a patient can exercise the rights set out in the GDPR.*
-  *The right to transparent information about all processing, including potential secondary or further processing, should be set out in patient facing information that is understandable and accessible. This means language, intellectual and physical capacities of patients need to be taken into account.*

- ➔ *Where secondary use of data is made, suitable additional safeguards must be implemented as set out in Article 89(1), and some of the rights to access, rectification, restriction and objection may be limited insofar as national level legislation allows for this.*
- ➔ *Where the service is offered on the basis of consent or in the context of the performance of a contract the patient can ask for a portable copy of the data provided to the data controller. This unlikely to be frequently useable in the UNICOM context, but should be borne in mind when apps or services are provided on the basis of consent.*
- ➔ *In the event that any tools developed in UNICOM, or other tools utilising IDMP, use automated decision-making data controller should review the possible impact of the right not to be subject to such decision making*

4.2 Duties of Data Controllers

Most of the duties of data controllers have been discussed in the context of data subjects' rights and in relation to the core principles of the GDPR. The data controller is accountable to the data protection authority for the compliance of the organisation with the GDPR and must be able to demonstrate such compliance. This means that he or she must be able to:

- Show that personal data are processed fairly and transparently by demonstrating that adequate information was given to data subjects about the data processing and to be able to identify the legal base for data processing.
- Show that personal data are processed lawfully by identifying the appropriate legal base for data processing and compliance with its specific requirements.
- Show that personal data used in the organisation are accurate, are limited to what is needed for the stated purpose and are not stored for longer than needed for that purpose.
- Show that the integrity and security of data can be respected by demonstrating cyber and physical security in the way data are processed and stored.

The issues related to security are referred to in the GDPR as 'data protection by design and by default'. This issue is dealt with in more detail in deliverable 10.5.

In situations where sensitive data or large volumes of personal data are processed by the organisation, it may be necessary to appoint a Data Protection Officer and conduct a Data Protection Impact Assessment.

4.2.1 Data Protection Officer (DPO)

The GDPR states in Article 37 that certain organisations must appoint a Data Protection Officer (DPO), although other organisations may choose to do so even if they are not legally required to do so.

A DPO must be appointed if:

- the data processing is carried out by a public authority or body (except for courts acting in their judicial capacity);
- the core activities of the organisation require large scale, regular and systematic monitoring of individuals (for example, online behaviour tracking); or
- the core activities of the organisation consist of large-scale processing of special categories of data or data relating to criminal convictions and offences.

The tasks of the DPO are set out in Article 39 as follows:

- to inform and advise the organisation about its obligations to comply with the GDPR and other data protection laws;

- to monitor compliance with the GDPR and other data protection laws, and with the internal data protection policies of the organisation, including managing internal data protection activities; raising awareness of data protection issues, training staff and conducting internal audits;
- to advise on, and to monitor, data protection impact assessments;
- to cooperate with the supervisory authority; and
- to be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

The organisation must involve the DPO in a timely manner; the DPO must not receive any instructions from the controller or processor for the exercise of their tasks and must report directly to the highest level of management of the organisation.

➔ The UNICOM project is working towards IDMP standards being used routinely in a healthcare setting, given the nature of the data involved and the volume of data that the organisations using IDMP identifiers in their workflow are likely to have, it is highly likely that the organisations using the solutions explored in the project will have a DPO. The DPO will have to be familiar with the privacy implications of using the solutions and ensure that the privacy policy of the organisation is adequate for such data processing and that all employees are informed about their duties and able to comply with them. Where two or more UNICOM partners are working together on a pilot a close collaboration between DPOs will be needed, which may also include addressing differences in requirements that arise as a result of national legislation applicable to different pilot sites.

4.2.2 Data Protection Impact Assessment (DPIA)

A Data Protection Impact Assessment (DPIA) is defined in Article 35 GDPR as a process to help the data controller to identify and minimise the data protection risks of a particular data processing activity the organisation plans to undertake. The GDPR states that a DPIA must be undertaken if the processing that is likely to result in a high risk to individuals, and notes that this may arise in particular where new data processing technologies are used. A DPIA is always required where sensitive data covered by Article 9(1) are to be processed.

The DPIA must be conducted before the proposed data processing starts and must be designed to assess the potential risk it poses the privacy of data subjects. The Data Protection Authority of a country or region may set out special requirements for the scope and content of a DPIA, meaning that a data controller intending to process sensitive data should be in contact with their relevant Data Protection Authority. The DPIA must:

- describe the nature, scope, context and purposes of the processing;
- assess necessity, proportionality and compliance measures;
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.

To assess the level of risk, the data controller must consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm. If a high risk is identified that cannot be mitigated, the data controller must contact their national or regional Data Protection Authority before starting the processing.

➔ The UNICOM project is working towards IDMP standards being used routinely in a healthcare setting, given that the data by the organisations using IDMP identifiers in their workflow, it is very likely that a DPIA will have been undertaken by such organisations. If the inclusion of IDMP identifiers changes the way in which data are processed a new DPIA may be appropriate.

Annex 1: Derogation, exemption, variation, restriction of the GDPR through national level legislation

One of the primary goals of the General Data Protection Regulation (GDPR) is to harmonize data protection laws across the European Union (EU). However, under the GDPR, EU Member States are allowed some flexibility to add or modify certain provisions of the GDPR to fit their local needs and laws. The table below identifies the key Articles which provide for some form of derogation, exemption, variation, restriction of the way in which the GDPR is implemented at national level.

Article	Derogation, exemption, variation, restriction	Potential impact for UNICOM
6 (3)	Member States shall maintain or introduce more specific provisions to adapt the application of the rules of the GDPR with regard to processing data in compliance with a legal obligation to which the data controller is subject, or where processing is in the public interest. This address the legal bases for data processing set out in Article 6(1) (c) and (e).	UNICOM partners and service providers using IDMP based solutions should take note of national legislation.
8(1), (2)	Child consent - Member States may adopt legislation that specifies the age at which a child may give consent to data processing in the context of the provision of an information society service. This age may range between 13 and 16 years.	UNICOM partners and service providers using IDMP based solutions involve children in any way, they should take note of national legislation.
9(2)	<p>Certain provisions for the processing of sensitive information, including all health-related information, require that national level legislation is adopted to define the circumstances in which such provisions apply. They are:</p> <p>9(2)(b) - legal obligations of a data controller</p> <p>9(2)(g) – processing in the public interest</p> <p>9(2)(h) – processing for healthcare purposes</p> <p>9(2)(i) - processing in the interest of public health</p> <p>9(2)(j) – processing for scientific research purposes</p>	UNICOM partners and service providers using IDMP based solutions should take note of national legislation.
9(4)	Member States shall maintain or introduce legislation the addresses the use of genetic, biometric or data concerning health	UNICOM partners and service providers using IDMP based solutions should take note of national legislation.
	<p>Member States may adopt national level law that restricts the obligations of data controllers or the rights of data subjects provided for in Articles 12-22 ie:</p> <ul style="list-style-type: none"> • Transparency of information about processing • Access to personal data that has been processed • Correction (rectification) of personal data • Right to erasure – ‘right to be forgotten’ • Right to restriction of processing by the data subject • Right of data portability • Right to object to automated processing and profiling of personal data • Limits to the obligations to communicate a data breach 	UNICOM partners and service providers using IDMP based solutions should take note of national legislation.

36	Member States may require prior consultation of DPA in certain circumstances	UNICOM partners and service providers using IDMP based solutions should be in consultation with DPA where appropriate
37	Member States may require appointment of DPO	UNICOM partners and service providers using IDMP based solutions should be in consultation with DPA where appropriate
85	Member States may adopt legislation which reconciles the rights under GDPR with to freedom of expression and processing for journalistic, academic, artistic or literary purposes. All such provisions to the European Commission.	Not likely to be relevant to UNICOM
86	Member States may adopt legislation which reconciles the right to access data held by a public body, or processed for a public body by a private entity, with the rights under GDPR	Not likely to be relevant to UNICOM
87	Member States may determine the specific conditions for processing national identification number, subject to appropriate safeguards.	Could be relevant to UNICOM or IDMP users in some countries
88	Member States may determine the specific conditions for processing in the employment context	Not likely to be relevant to UNICOM
89	Member States may determine the specific conditions for processing for archiving, scientific, historical research or statistical purposes	UNICOM partners and service providers using IDMP based solutions should take note of national legislation.
91	Member States may determine the specific conditions for processing in the context of churches and religious associations	Not likely to be relevant to UNICOM