This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No. 875299

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 D10.5:

GDPR in the Pharmacy Setting

Version:	1.0
Status:	Final
Dissemination Level[1]:	PU
Due date of deliverable:	31.05.2021
Actual submission date:	30.11.2021
Work Package:	WP10: Socio-economic impact, legal and governance aspects
Lead partner for this deliverable:	IHD
Partner(s) contributing:	EMP, DWIZ
Deliverable type[2]:	R
Delivery date:	

Main author(s):

Petra Wilson IHD

Other author(s):

Dipak Kalra IHD
Farah Diehl-Fahim EMP

Resource consumption estimate:	Person months
IHD – Petra Wilson	0.6
IHD – Dipak Kalra	
EMP	0.1

[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 fillings, videos, etc.; OTHER; ETHICS: Ethics requirement; ORDP: Open Research Data Pilot

Revision history

Version	Date	Changes made	Author(s)
0.1	20.05.21	Outline concept developed	Petra Wilson, Dipak Kalra, Farah Diehl-Fahim
0.2	25.05.21	Concept developed based on input from WP8 on pilots and app development	Petra Wilson, Lucia Comnes
0.3	30.6.21	First complete draft	Petra Wilson
0.4		Commentary and feedback from I-HD team	Dipak Kalra
0.5		Review	Farah Diehl-Fahim
1.0	11.11.21	Final edit	Petra Wilson

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This deliverable contains original unpublished work except where clearly indicated otherwise.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 healthcare settings and the IDMP enabled solutions developed within the UNICOM project.

The objective of Deliverable 10.5 is to further develop the overview of the GDPR as set out in Deliverable 10.4, with **direct guidance on its application in pharmacy practice (both community and hospital) and its application to the UNICOM pilots.** The present deliverable does this on a step by step basis, and includes also a separate section on the **use of data for research purposes**.

With respect to the UNICOM pilots the guidance provided in the present deliverable should be read in conjunction with the wider ethical guidance developed in WP13.

The present report constitutes Part 1 of Deliverable 10.5 and addresses compliance with the GDPR and other related legislation such as the NIS Directive. In Part 2, which will be delivered in month 40 of the project, we will address issues arising under the **MDR** with respect to solutions and apps developed to support use of IDMP. It will also consider the **draft Data Governance Act,** and the **draft AI Act,** as well as any legislation which has by that time been proposed or adopted in the context of the establishment of the European Health Data Space.

Keywords: Data Protection, General Data Protection Regulation, GDPR, 2016/679, data subjects rights, research, data re-use

TABLE OF CONTENTS

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
LIA	Legitimate Interests Assessment

Executive summary

The UNICOM project is concerned with the use of International Organization for Standardization (ISO) suite of IDMP (IDentification of Medicinal Products) standards to support the drive for improved patient safety and better healthcare for all. The purpose of the UNICOM project is to support 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 legal strand of Work Package 10 comprises two tasks:

- to provide general guidance on compliance with legal and regulatory requirements of the General Data Protection Regulation (GDPR), Medical Devices Regulation (MDR) and other applicable legislation in the context of healthcare provision where applications and solutions using IDMP standards may be used; these are predominately in healthcare settings where medicines are prescribed and dispensed. This work is theoretical, rather than applied, as the UNICOM project itself is not developing solutions and bringing them to market, but is undertaking the groundwork to support the deployment of the IDMP standards which may in due course be used in applications and solutions.

- to provide specific guidance on the application of the GDPR, MDR and other relevant legislation in the UNICOM pilots. The four pilots are described in detail in Deliverable 13.2

Deliverable 10.4 provided a general overview of GDPR; this work is developed further in the present deliverable to explore its application in the pharmacy setting and in the context of the UNICOM pilots. This is outlined in the form of a five-step plan addressing:

Step 1 - develop a data processing plan and policy

Step 2 - address the core data processing compliance issues

Step 3 - inform data subjects of processing and their rights

Step 4 - ensure data security and staff training

Step 5 - be prepared for risks and data breaches

The present deliverable also sets out the legal aspects of the re-use of health-related data for healthcare research, planning policy making purposes, including data generated using an IDMP based solution. Such reuse of data for research and planning will become increasingly important as IDMP identifiers are used in the prescribing and dispensation of medicines and the data generated can be used to identify risks and trends, in particular using artificial intelligence. The potential impact of new legislation on artificial intelligence and data use will be further explored in part 2 of the present deliverable, which will also consider the extent to which the MDR impacts IDMP enabled solutions. Part 2 will be delivered in Month 40.

1 Introduction

1.1 Objective of the report

The legal strand of Work Package 10 comprises two tasks: the first is to provide general guidance on compliance with legal and regulatory requirements of the General Data Protection Regulation (GDPR), Medical Devices Regulation (MDR) and other applicable legislation including the Network Information Security Directive (NIS) and emerging legislation including the draft Data Governance Act , the draft AI Act as well as legislation still to be developed to support the role out of the European Health Data Space (EHDS). The second is to provide specific guidance on compliance with EU level legislation in the context of UNICOM pilots.

The four pilots are described in detail in the work packages within which they are conducted, and also in Deliverable 13.2 which is the Data Management Plan of the project. For ease of reference the four planned pilots are also summarized in annex 1 of this report. It should be noted however that the pilot plans are still in development and may be amended before execution. The guidance outlined in this deliverable may therefore also have to be updated. This will be done in the context of workpackage 13; where appropriate this will be done in collaboration with the Ethics Advisory Board.

The two tasks are addressed over three deliverables. The present report is Deliverable 10.5 Part 1, it builds on the introductory overview of the GDPR set out in deliverable 10.4. In section 1 it explores the application of the GDPR in the pharmacy setting and in the UNICOM pilots through five steps. In addressing the security requirements of the GDPR, reference is also made to the application of the present and draft NIS Directives in the pharmacy setting. In addition to the five-step plan, the present report also addresses, in Section2, the legal compliance issues that arise from the re-use of data generated in the context of the issuing and dispensing of a prescription for medication for the purposes of scientific research.

Deliverable 10.5 Part 2, which is due to be delivered in month 40, will provide specific guidance of the application of the MDR to solutions which use the IDMP identifiers such as the patient facing apps and decision support software which are to be trialled in Pilot C. It will also look at the potential impact of the Data Governance Act and the AI Act, which are still currently in the process of adoption. The final deliverable of work package, deliverable 10.6, will provide a final review of all applicable EU level legislation to the use of IDMP, as well as a review of any experiences on the application of EU level or national level law derived from the execution of the UNICOM pilots and trials.

Section 1: GDPR in the Pharmacy setting and in the UNICOM pilots

Recognizing that the GDPR presented a number of challenges for the community pharmacist, the UK Community Pharmacy GDPR Working Party developed a mnemonic – DATAPROTECTED . – to act as a reminder of the key issues to be addressed.

- **D**ecide who is responsible
- **A**ction plan
- **T**hink about and record the personal data you process
- **A**ssure a lawful basis for processing

- **P**rocess according to data protection principles
- **R**eview and check with processors
- **O**btain consent if needed
- **T**ell people about data processing: the Privacy Notice
- **E**nsure data security
- **C**onsider personal data breaches
- **T**hink about data subject rights
- **E**nsure privacy by design and default
- **D**ata Protection Impact Assessment

In the following pages we develop a five-step guide on how the principles set out in the mnemonic above can be addressed in a pharmacy setting in the context of dispensing a medicine, reporting on adverse events or medication errors, and using data for stock management and other planning purposes. We have re-grouped the key issues outlined above into five steps as follows:

- **Step 1 - develop a data processing plan and policy**
- **Step 2 - address the core data processing compliance issues**
- **Step 3 - inform data subjects of the processing and their rights**
- **Step 4 - ensure data security and staff training**
- **Step 5 - be prepared for risks and data breaches**

In addition to looking at the practical implications of the GDPR in a pharmacy setting, this section also reflects on how each step impacts the UNICOM pilots and the issues that need to be addressed in setting up the pilots. This guidance is further supported by the template documents for a Privacy Information Notice and a Consent Form which will be adjusted for the needs of each pilot site or trial. The templates are provided as part of the Data Management Plan in Deliverable 13.2 and its periodic updates (Deliverables 13.3 – 13.5)

The particular challenges of using personal and sensitive personal data in research are set out in section two. It is important to address this issue separately, as a key objective of the UNICOM project is to support the use of IDMP identifiers in the safer and more sustainable delivery of healthcare services and medicines. This issue will be developed further in part 2 of the present deliverable, looking at the legal implications of artificial intelligence using IDMP enabled data to identify trends and risks.

Step 1 - Develop a data processing plan and policy

1.1 Appoint a person with data protection responsibility and develop a data processing plan and policy

A pharmacy, or indeed any other healthcare professional group, should appoint one person to have core responsibility for compliance with the GDPR. In some cases that person will be titled as the Data Protection Officer (DPO) and will have specific duties. The GDPR (Article 37) calls for the appointment of a DPO if data are being processed by a public authority or body, or the core activities of the organisation require large scale, regular and systematic monitoring of individuals; or the core activities consist of large-scale processing of special categories of data - health related data are classified as special categories of data in the GDPR. Given the parameters set out in Article 37, it is likely that almost all hospital pharmacies and most community pharmacies will need to appoint a DPO. The role may however be shared with other organisations in the same group, so the hospital group DPO could be the DPO for the pharmacy and a pharmacy chain could appoint a DPO to look after several premises. If the DPO is not part of the core team, another person should be appointed who works with the DPO to support day-to-day GDPR compliance. In most EU Member States national level legislation will define if a pharmacy of a particular size is an organization which must appoint a DPO.

1.2 Develop a data protection plan

Working with the DPO or staff member the organisation should develop a data protection plan. This is usually done by undertaking a data protection impact assessment (DPIA) which starts with an audit of all the data categories handled and itemises how they are obtained, why they are collected and processed, as well as how and for how long they will be kept. This will also include identifying data for which the organisation is data controller and where it might be acting as a data processor for another organisation or appointing a data processor to act on its behalf. The data controller is the person (or organisation) with the control over decisions about which data are collected and how they are used, the data processor works on their behalf. In the pharmacy setting the pharmacy as a legal entity or pharmacist as a natural person is likely to be the controller of all information generated in the context of dispensing a prescription; it is likely that in a large pharmacy a data processor may be appointed to support duties on reporting of prescriptions filled and reimbursement claims made. Where this happens the data controller will have to ensure that a contract clearly establishes which data are to be processed and for which purposes.

The data protection plan should include a privacy policy which is communicated to all data subjects (patients or clients) who use the pharmacy. This could be done through an information leaflet, through displayed information, as well as on any website run by the pharmacy.

An objective of UNICOM is to increase the use of IDMP identifiers in prescriptions. While the identifier of a drug its components would not qualify as data subject to the GDPR, when an identifier is used in a prescription it may be adding additional information to person identifiable information and may therefore generate new data about that individual. When a UNICOM based solution is developed or introduced into pharmacy practice, it should include specific guidance for the data controller on any implications it may have for data protection. Where a

data processor is appointed, any tasks making use of IDMP data which is linked to an identifiable person should be clearly described.

In the context of UNICOM pilots, it is important that project partners running pilots undertake a DPIA. This will need to itemise the data to be collected and plan for its use, including how long it will be kept. It will demand also that the identity of the DPO, or other responsible person in the organisation or organisations running the pilot are informed about the trial and have agreed to it being conducted. Where the trial involves patients or citizens it is very likely that the approval of the ethics committee of the organization or region in which it is located will have to be obtained. In addition, the Ethics Advisory Board of the UNICOM project will have looked at the pilot plans and will have advise on ethical compliance, note however that the UNICOM Ethics Advisory Board will not be able to give ethical approval for the conduct of the trial.

Any organization handling personal data should have a continuous education and training plan in place to ensure that all staff understand their data protection duties. The plan should also include the process for creating and updating information for pharmacy customers.

Training of pharmacy staff should be updated to address any new issues raised by use of IDMP identifiers within prescriptions, including any new personal data fields that will be created or stored differently; as well as updating any guidance or educational materials used in the pharmacy to accommodate the changes made.

Information notices for pharmacy customers and patients should be updated to include information on the use IDMP identifiers and any privacy implications they may create for an individual.

Specific information notices will need to be created for each pilot or trial, for more detail see step 3 below.

Step 2 - Address the core data processing compliance issues

2.1 Identify the legal bases for data the data processing

The first core requirement is that data are processed lawfully. This means ensuring that data are collected in accordance with one of the legal grounds listed in Article 6(1) of the GDPR. These are:

a) Consent (where explicit consent is given by the data subject)

b) Contract (where processing is necessary to fulfil a contractual obligation or as part of entering a contract)

c) Legal Obligation (where processing is necessary for compliance with a common law or statutory obligation)

d) Vital interests (where processing is necessary to protect someone's life)

e) Public interest (where processing is necessary to perform a specific task in the public interest that is set out in law)

f) Legitimate interests (where processing is necessary for the purpose of legitimate interests, but public authorities cannot rely on this)

The data collected in pharmacies in the context of dispensing a medication are classified as sensitive data by the GDPR. According to Article 9(1) processing of sensitive data is prohibited unless one of the exceptions in Article 9(2) can be applied. While Article 9(2) provides several exceptions, only some are relevant for health-related data. They are:

a) Explicit consent (where the data subject has given explicit consent to the processing of those personal data for one or more specified purposes)

h) Provision of health or social care treatment (where processing is necessary as part of the data controller's role as part of a healthcare organisation, e.g. the provision of health or social care or treatment or the management of health or social care systems and services)

i) Public health (where 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)

j) Public Interest (including scientific research in accordance with Article 89(1))

The relevant exception to be used in a pharmacy setting will be defined in national level legislation, accordingly it is important for the DPO of the pharmacy to be familiar with the national legislation. For the data processed in the context of issuing and dispensing a prescription in most EU Member States it will be Article 6(1) (c) in conjunction with 9(2)(h) or 9(2)(i), although in some countries consent has been indicated as the correct legal base. In those countries where 9(2)(h) - provision of care or treatment - is the legal base, it should be noted that Article 9 (3) requires that a healthcare professional, such as a pharmacist or a pharmacy technician subject to registration and regulatory oversight, or a person with a duty of confidentiality under a legal provision, must be responsible for the processing of personal data for these purposes. More detail on the role of consent is provided in section two below.

Where an IDMP based solution is used in a pharmacy, it is unlikely that any change will arise with respect to the legal basis for data processing. As discussed above it is likely to be based in the provision of health care, with some countries preferring the legal base of consent.

In the context of UNICOM pilots however, the legal basis will be consent, as the data are collected for research purposes rather than healthcare. Where however research is conducted using data collected first for the purpose of care provision and later analysed for research purposes, the legal base is likely to be public interest. This issue is further discussed in section two below.

In addition to having a legal base, the data controller must also ensure that data are processed in a fair and transparent manner. Furthermore, the data must be collected for a specified purpose and not kept in a way that allows the identification of the data subject for longer than necessary to fulfil the specified purpose.

In a pharmacy this means that records must be kept about which data are collected and purpose to which this put. It is likely that much of this will be based in the legal requirements of reimbursement and insurance which will necessitate the processing of personal information.

In the context of UNICOM pilots the key issue is the transparency. If data are being collected and processed solely for the purposes of a pilot, this must be made clear to the participants, and will usually mean that the data are collected on the basis of consent in Article 6(1)(a) and 9(2)(a). However, where the data analysed in the pilot derive from data collected in the process of routine care, the legal basis may be different, as such use would be a secondary use of the data. For more detail see section two on GDPR in research.

2.2 Set up data processing agreements

While the owner of a pharmacy will be the data controller, she or he may be working with several data processors, which will include the providers of ePrescription services and decision support software. In a pharmacy it is also likely to include data capture and reporting systems which help manage stock and reimbursement systems. In the context of IDMP based solutions it is therefore very likely that both the data controller and one or more data processors will be involved in using the solution, and in handling personal data that flows through it.

The relationship between a data controller and a data processor must be set out in a specific contract or agreement. In some cases the relationship between the two parties will be such that both are controllers and both have the duties of a controller, in this case a joint controller agreement will have to be established. The agreement between a data controller and processor or between two data controllers should be detailed, it should not merely restate the provisions of the GDPR, but should provide for specific and concrete information as to how the GDPR requirements will be met. It should also provide details on any sub-processors, their processing activities, locations and implemented safeguards.

In UNICOM the primary focus of the relationship between the pharmacist (data controller) and the service provider (data processor) will be the technical and semantic interoperability of their systems to ensure that full use can be made of all the IDMP tagged data to create safer medication delivery systems. From a data protection perspective, the key issue is one of knowledge and understanding. Where the use of a new solution, or the engagement in a UNICOM pilot, changes the nature of the data handled or the way in which it is handled.

In the context of UNICOM pilots the instruction for changes in processing tasks must come from the data controller to the data processor. In some cases this will mean reviewing the terms and conditions of the data processing contract and ensuring that the new tasks are properly provided for, and that the needs of the pilot can be accommodated.

Step 3 - Inform data subjects of processing and their rights

3.1 Information on data use, access and portability

The data controller must make clear what rights the data subject has (access, rectification etc - see below) and how those rights can be exercised. If the processing is based on consent, the way in which consent can be revoked must be made clear, as well as the right to make a complaint to a supervisory authority. The data subject must also be informed about the

existence of automated decision-making, including profiling, referred to in Articles 22(1) and (4) of the Regulation (namely where the profiling produces legal effects or otherwise significantly affects a data subject or involves special categories of personal data). When the controller is engaged in profiling, it also should supply meaningful information about the logic involved, and the significance and envisaged consequences of the processing for the data subject.

As noted in step 2 and further explained in Deliverable 10.4, consent is rarely the legal basis for processing personal data in a healthcare setting. However, where the data are processed in a healthcare setting, but not for a healthcare purpose, consent will be the most likely legal base. However, regardless of the legal base used, the GDPR requires that data subjects are informed about the data collected and the purposes to which it is put.

Data portability was a new concept introduced by the GDPR, giving data subjects the right to receive their personal data, which they have provided to a controller, in a structured, commonly used and machine-readable format and to transmit the data to another controller without hindrance from the controller. Technically, the controller must either hand the data over to the data subject in a usable fashion, or—at their request (Article 20(2))—transfer the data directly to the recipient of the data subject's choice, where technically feasible. However, the right only arises where data have been collected on the basis of consent or on the basis of a contract, which as we have seen above will only rarely pertain to data processing in a pharmacy.

Pharmacies must create a Privacy Information Notice which is either given to pharmacy users in the context of care provided, or displayed in a manner that is accessible to all people using the pharmacy services. Thus, where a physical site is used the notice must be displayed on a wall, while if a web or app-based service is provided the information notice must be displayed at the start of the interaction. In this situation it is usual also to require some form of confirmation of having read the notice.

In the context of UNICOM information notices are needed for all pilots. More detail on the nature of such notices can be found in section two below. These will have to be localised to each pilot site, but can be based on the template Privacy Information Notice provided in the Data Management Plan set out in deliverable 13.2 (and updated in its later iterations).

3.2 Right to be forgotten

Article 17(1) establishes that data subjects obtain the right to have their personal data erased in certain circumstances. However, the data controller does not have to comply with a request for erasure if the data are necessary for the performance of a task carried out in the public interest, such as public health, archiving and scientific, historical research or statistical purposes, insofar as the right to erasure is likely to render impossible or seriously impair the achievement of the objective of research. It is therefore unlikely to apply in a pharmacy setting where there is a public interest in pharmacies maintaining records, and indeed this is a requirement of national legislation in some form in all Member States. This means that the right to be forgotten is in conflict with national law which require pharmacies to keep records of prescriptions filled, reimbursement, audit and professional liability reasons.

Step 4 - Ensure data security and staff training

Data security is the key to GDPR compliance, and was a legal requirement long before GDPR came into force. Data security must be addressed in terms of physical security of buildings and data held on paper, film or any other medium, and electronic security and also the data security of human interaction. In the pharmacy context these three elements of security include physical security of buildings and physical data storage places; cyber security of data both in terms of its usage and transfer; and human usage security, which addresses how workforces are trained and supported in maintaining data security.

4.1 Physical security

Good data security requires the prevention of unauthorised access to the pharmacy premises by ensuring that it is locked as required, and that all data that are kept on a physical medium, such as paper or film, are secured. This means locked filing cabinets and a system for tracing who can access the keys to the filing cabinet and when they have been used. It also means screens on which electronic data are displayed are safe from unauthorized viewing. This demands that the screen is positioned in such a way that it cannot be viewed by unauthorized individuals, and also demands that screen have automatic shutdown timers set and that access is based in secure log-in mechanisms.

4.2 Cyber security

Many data items used in a healthcare setting will however never be stored physically, but will be stored in the cloud. This demands that adequate cyber security protocols are developed and implemented. In many Member States national standards, including using an approved cloud storage provider and approved secure email servers.

The Network and Information Security Directive (Directive 2016/1148) provides a baseline of standards in meeting cyber security. This EU level legislation which must be transposed into national level legislation to be enforceable, provides legal measures to boost the overall level of cybersecurity in the EU, focusing on Member States' preparedness, by requiring them to set up a competent national NIS authority and a Computer Security Incident Response Team (CSIRT). It also seeks to drive cooperation among all the Member States, by setting up a Cooperation Group to support and facilitate strategic cooperation and the exchange of information among Member States. Its primary focus is on the so-called operators of essential services sectors that are vital for society and rely heavily on ICTs, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure. Businesses identified by the Member States as in the above sectors will have to take appropriate security measures and to notify relevant national authorities of serious incidents. Key digital service providers, such as search engines, cloud computing services and online marketplaces, will have to comply with the security and notification requirements under the NIS Directive. To support Member States the Commission has created the NIS toolkit, which provides practical information to Member States on the Directive, including best practices on implementing the Directive from other Member States, with explanation and interpretation of specific provisions to clarify how the NIS Directive should work in practice.

Following the review of the NIS Directive in 2020, a new draft NIS2 Directive was proposed by the European Commission in March 2021. It has a broader range and now includes services

linked to healthcare. It has been argued by Biasin and Kamenjašević (2021), that the new focus on cyber security in NIS2 has been driven by, on the one hand serious incidents such as the cyber attack on the European Medicines Agency in December 2020.

If approved as it is now, the NIS2 may bring new requirements for actors operating in the healthcare sector, notably in the field of medical devices and pharmaceuticals. New types of entities were added to already existing healthcare providers ones. Medical device and in vitro diagnostic medical devices manufacturers could in future be considered important entities. Essential entities may include EU reference laboratories, entities carrying out R&D activities of medicinal products, entities manufacturing basic pharmaceutical products and preparations manufacturers of medical devices considered as critical during a public health emergency.

NIS2 is also intended to address the security of supply chains through the requirement for individual companies to address cyber security risks in supply chains and supplier relationships. The proposed changes also aim to strengthen supply chain cyber security for key information and communication technologies at European level. Finally, the new Directive is intended to enhance the role of the current NIS Cooperation Group in shaping policy on emerging technologies and new trends. It aims to increase information sharing and cooperation between member state authorities and enhance operational cooperation through the establishment of the European Cyber Crises Liaison Organisation Network (EU-CyCLONe). This will support coordinated management of large-scale cybersecurity incidents and crises at EU level. At the time of writing (April 2021) the draft is in negotiation, once it is agreed and adopted, member states will have 18 months to transpose it.

UNICOM is not developing products to bring to market; however it is aiming to support the deployment if IDMP standards within software applications used in pharmacies and other healthcare settings. Some of those applications may be classified as within the scope of the NIS2 Directive, accordingly it is important for the developers of such applications to ensure they support a high level of information security. Conversely, it should be noted that the use of IDMP standards can itself support the critical services security which the NIS and NIS2 seek to support.

4.3 Security measures and training

Physical and electronic security must be complemented with training and support measures to ensure that the people handling data understand how to implement physical and electronic data security systems. This demands regularly updated training and, where data are processed on the basis of Article 6(1)(h) that staff have confidentiality requirements in their contracts or professional registration schemes.

Security measures are practical tools, procedures and processes that support good security management, this includes measures such as user authentication and access controls and audit trails which record all data touching events. The requirements and standards to be met for such security measures are often included in national level legislation, much of which will be sector specific.

In the context of the UNICOM pilots, the security requirements are addressed in ensuring that all personal data collected in the context of a pilot are stored safely in accordance with normal security requirements. This includes physical as well as electronic security as described above.

It may also include using suitable techniques for data pseudonymization, as described in section 2 below.

A further aspect of data security is the inclusion of data security by design and by default. According to the GDPR this means that appropriate technical and organisational measures have been implemented to support the integration the principles of data protection into all data processing activities.

Step 5 - Be prepared for risks and data breaches

5.1 Data breaches

Despite high levels of security, data breaches will occur. These may be the result of malicious attacks, or of negligence on the part of the data holder. The GDPR includes a draconian fines scheme, which allows data protection authorities in the Member States to impose fines of up to €20 million or 4% of annual global turnover (whichever is higher). A well known example of a malicious attach was the WannaCry cyber attack on the national health system in the UK in 2017, which has been identified as leading to significant impact including death, missed appointments, and significant financial costs.

The GDPR demands that an organization must report a breach to the data protection authority, within 72 hours of becoming aware of it, if it is likely that the breach will pose a risk to the rights and freedoms of individuals. Where the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the controller must also inform those individuals without undue delay.

Pharmacies using new solutions must be hypervigilant of any potential 'backdoors' created by new software, hardware or applications which could provide a potential for a data breach. The use of any new software or other tool based on the inclusion of IDMP identifiers must be carefully examined to address such potential.

In the context of UNICOM pilots, all pilot partners must be vigilant about potential data breaches. The management and reporting of any breach will however be conducted at the level of the partner affected. However, as the pilots foresee only very limited use of sensitive personal data, it is unlikely that a data breach in an institution running a UNICOM pilot will have a very significant impact on individual data subjects.

The five steps outlined provide an overview of the general issues that must be addressed in a healthcare setting and in UNICOM pilots to ensure that the requirements of the GDPR are met. However, the actual compliance actions must be undertaken with regard to any national level legislation which further specifies the GDPR, or which impacts on data processing through national law on health care provision.

Section 2 - GDPR and research

As noted in section one, processing data must be lawful, that means one of legal bases in Article 6 must apply, and where the data are sensitive data, such as health-related data, one of the exceptions in Article 9(2) must apply.

The use of data for research purposes is an especially complex issue, and varies significantly from Member State to Member State. A detailed analysis conducted in a study for the European Commission in 2020 established that although in theory the GDPR provides for the collection of data for research purposes (where the research is the primary purpose for which the data were collected) and when data are used for research that were collected originally for another purpose, where the research is a secondary purpose, the interpretation of the law is very varied across the Member States.

Article 6(4) GDPR 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 (known as the purpose limitation principle). When it comes to research this should be read in conjunction with Article 5(1)(b) which carves out a privileged position for research, stating that further processing for scientific research purposes in accordance with Article 89(1) is not considered incompatible with the principle purpose. However, it should be borne in mind that the European Data Protection Supervisor (EDPS) makes a distinction between 'genuine research' and other research in this respect (EDPS 2020). This means that the research organisations should have a formal record stating which legal base they are using, which should usually also be reflected also in the privacy information notice and in the data asset register an organisation creates.

This will demand that the legislator defines which type of researchers may make use of the public interest criterion. It will also demand that the legislator has weighted the risks to the individual against public benefits. One such balance test applied in the context of research has been called the 'duty of easy rescue' test, described by Porsdam Mann et al as arising when it is possible to benefit others at no or minimal cost to oneself. They argue that where the duty of easy rescue does not apply because there are significant risks involved in data sharing and where these risks cannot be minimized by security management, research can only ethically proceed without informed consent when obtaining consent would be impossible or impracticable, the public benefit of the research very significantly outweighs the risks, the public is adequately informed, and any resulting harms are compensated.

Step 1 - choose a general legal basis

Research is not designated as a lawful purpose in its own right. Where research is conducted on general personal data (i.e. not health data) any one of the legal bases in Article 6 may be applicable. Note however that the basis of legitimate interests is available only to private entities, not public entities.

- For universities or publicly funded research institutes, the most appropriate legal reason to hold and use general personal data is likely to be Article 6(1) (e) - public interest. In order to justify the use of this legal basis, the organisation must have reference to a research purpose in the statutes, charter or other legal document documenting the creation of the organisation.

- For care providers, such as hospitals or medical clinics, where the entity is a publicly healthcare provider and providing care to the data subject, it would be possible also to cite Article 6 (1)(c) - legal obligation, since as a public entity they may have a legal duty to carry out research.
- For commercial entities, or research organisations funded from non-public monies such as charity research institutes that are not public authorities, the most appropriate lawful basis is likely to be Article 6(1)(f) - legitimate interests.
- It is also possible for a research entity, whether publicly funded or not to use the legal base of consent in Article 6 (1)(a). However, this legal basis is not recommended as the most appropriate legal base for using data for research by bodies such as the Ethics Advisory Group established by the European Data Protection Supervisor Ethics and the UK Medical research Council.

Step 2 – conduct a Legitimate Interests Assessment if necessary

Where Article 6(1)(e) or (f) are used, it is important to note that the data controller is advised to carry out a legitimate interests assessment (LIA). LIA is a type of light-touch risk assessment based on the specific context and circumstances of the processing. While there is no specific requirement in the GDPR to undertake a LIA, in practice data controllers and processors are required to be able to show an audit trail of the decisions and justification for processing on the basis of legitimate interests. Conducing a LIA helps to ensure that processing is lawful and that having a record of an LIA also helps to demonstrate compliance with the principles and appropriate organisational measures in line with the accountability obligations under Article 5(2) and Article 24. The LIA consist of completing a document which addresses three sets of questions asking:

- Do I have a legitimate interest in processing the data (the purpose test)
- Do I need the data to fulfil that legitimate interest (the necessity test)
- Does the data subject have interests in data privacy that outweigh my legitimate interest (the balancing test)

Step 3 - choose a legal basis for using sensitive data

Article 9(2) sets out the exceptions to the general provision of Article 9(1) that sensitive data may not be processed can be exempted. This means that after choosing an Article 6 basis for allowing an organisation to process personal data, a further legal basis for processing sensitive, including health-related data, must be chosen. For health related data these are:

- Using health related data for medical care purposes - Article 9(2)(h) provides that sensitive data may be used where processing is necessary for medical diagnosis or health care provision. Note however the 9(3) provides that this reason may only be used where the data are processed by a professional who is subject to a professional obligation of secrecy. It is rather unlikely that this will be used as a legal basis for

conducting research on data collected for first for another purpose, but it could be the basis where data are collected specifically for research for a particular medical purpose.

- Using health related data for reasons of public interest in public health - Article 9(2)(I) provides that sensitive data may be used if this is for public health reasons such as protecting against serious cross-border threats or ensuring high standards if medical products or devices. Note that this should be provided for in national or EU law which includes specific safeguards such as professional secrecy.
- Using data for legitimate research purposes - Article 9(2)(j) provides that data may be processed for scientific research if such processing is necessary for the research, and the processing is done in accordance with the requirements of Article 89(1) based on EU or Member State laws. This is the most commonly used legal basis for reusing data for research purposes. This requires that the processing is "proportionate to the aim pursued, respects the essence of the right to data protection and provides for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject". When using this provision, the research entity must therefore be able to satisfy three tests:

  - Processing the data is necessary to support research
  - Processing the data will only be undertaken to support legitimate research activities that are considered to be in the public interest, and
  - The interests of the data subject in data protection are safeguarded/protected.

Article 89(1) clarifies that "those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner".

3.1 The role of consent when using health-related data in research

Informed, voluntary and fair consent is the cornerstone of ethical research involving people. It is a mechanism, to ensure the rights of individual participants can be respected. It is through the consent process that research participants can understand what taking part in a specific study will mean for them, so they can make an informed choice and feel able to express their wishes.

Consent is therefore key to the involvement of people in research. They must be informed about what is likely to happen to them and be able to provide their consent freely. These legal duties lie within the law of medical care, practice and research and are separate and additional to the consent to processing their data in the context of the research required under the GDPR. This is noted specifically in Recital 54, which complements Article 9, and states: "The processing of special categories of personal data may be necessary for reasons of public interest in the areas of public health without consent of the data subject. Such processing should be subject to suitable and specific measures so as to protect the rights and freedoms of natural persons". Accordingly, the GDPR itself specifically foresees using health related

data without consent for public health purposes. In this context it is important that Recital 54 notes that 'public health' should be interpreted as defined as including "all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status". The Recital goes on to note that such processing of data concerning health for reasons of public interest should not result in personal data being processed for other purposes by third parties such as employers or insurance and banking companies.

The reason that consent is not always regarded as appropriate in the research setting is that if consent is used for health research the consent must be explicitly given for a specific research purpose. Recital 33 notes that this could pose a challenge because "it is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of collection". Accordingly, guidance of data protection authorities and research funders suggest that other legal bases may be more appropriate.

Consent in a research context should therefore focus on the consent of the research subject to be involved in a study, not on the data collection. Note that the British Medical Association, in its briefing to GPs states: "When processing data for medical research the Article 6 lawful basis is 6(1)(e) '… for the performance of a task in the public interest…' The special category condition is Article 9(2)(j) '… research purposes…'. Reliance on this Article 6 lawful basis and Article 9 condition means that explicit consent is not required for GDPR purposes".

Accordingly, where data were originally collected in the context of general care provision, or for another ethically accepted research study, use of that data for research is best based on Article 6(1)(e) coupled with Article 9(2)(j) if the research entity is publicly funded or Article 6(1)(f) coupled with Article 9(2)(j) if a privately funded entity is undertaking.

Step 4 - Ensure data subject rights can be met

Regardless of whether the legal basis being used is explicit consent or research purposes, other legal duties set out in the GDPR are relevant to the way in which data are processed in research. These include:

4.1 Information to data subjects

While the traditional Informed Consent Notice is not needed for using health-related data for research, Article 12(1) requires controllers to "take appropriate measures" to inform data subjects of the nature of the processing activities and the rights available to them, "in a concise, transparent, intelligible and easily accessible form, using clear and plain language".

This means that a Privacy Information Notice, informing the data subject about a study and more generally about how data will be used is needed. This is because the GDPR requires organisations to be fair and transparent in how they hold and use personal data. In other words, organisations must be open and honest with research participants about how they intend to use personal data, and the types of data they will be using, etc.

This information should be concise, transparent and intelligible; consider the audience; use clear, plain language; and be easily accessible. In addition, organisations should provide corporate level and possibly departmental level / research group level information about the

work they do and how the handle data. All of these sources should align, and complement each other. This information should be provided at the time when the data is first collected and it must include:

- the controller's identity and contact information
- the intended purposes of the processing activities
- the data subject's rights notice of the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period
- where applicable, that the data will be transferred to another entity or to a third country

An updated notice should be provided where a controller intends to further process data for a different purpose, including for research.

4.2 Right to objection and erasure

Recognising that research may be negatively impacted if a data subject exercises their right to object to data processing or to exercise her right data erasure, Article 89(2) allows Member States or the EU to adopt legislation which limits data subject rights to access, rectification, restriction, and the right to object where processing is for research purposes subject to the appropriate safeguards. However, this is not be a blanket authority to derogate from these rights. The derogations must be "necessary for the fulfilment of [the research] purposes" and they are only permissible if allowing data subjects to exercise their rights likely would "render impossible or seriously impair the achievement of the specific purposes."

Step 5 - Data Minimisation and Pseudonymisation

A general principle of the GDPR is that only as much data as is needed for the specified processing purpose should be collected. This is known as data minimisation and applies also to data collected for research and data collated from existing data pools for re-use in research. Data must be adequate, that is sufficient to properly fulfil your stated purpose; relevant, it must have a rational link to that purpose; and minimized to what is needed for that purpose.

Pseudonymisation is a technique that replaces or removes information in a data set that identifies an individual, and can be used as part of the data minimization process.

Article 4(3)(b) describes pseudonymization as "…the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person."

Unlike anonymisation, pseudonymisation techniques will not exempt controllers from the ambit of GDPR altogether. It does however help researchers meet their data protection obligations, particularly the principles of 'data minimisation' and 'storage limitation' (Articles 5(1c) and 5(1)e), and processing for research purposes for which 'appropriate safeguards' are required.

Pseudonymisation may involve replacing names or other identifiers which are easily attributed to individuals with, for example, a reference number. Whilst it is possible to link that reference number back to the individual, that is dependent on access to the relevant information, which

must in turn be protected by technical and organisational measures to ensure that this additional information is held separately. In practice this means the key data to unlock coded data must be stored separately and with suitable physical and technical barriers. It should also include mechanisms that can identify if the key codes have been accessed or used.

Where pseudonymised data used a residual risk of re-identification identification by an unauthorised party remains. In some settings it may be useful to apply the 'motivated intruder test' to assess the likelihood of this. Once assessed, a decision can be made on whether further steps to de-identify the data are necessary. By applying this test and documenting the decisions, the study will have evidence that the risk of disclosure has been properly considered.

Step 6 - Transferring personal data to third countries for research purposes

The GDPR prohibits the transfer of personal data to countries outside of the EU unless they offer an "adequate level of protection" as determined by the European Commission (Article 45(1)). A controller also may transfer personal data to a third country if it has implemented specific safeguards, including Binding Corporate Rules and standard contractual clauses, or if the data subject has provided explicit consent after being informed of the risks related to the transfer (Article 46(2); Article 49(1)(a)).

In the absence of any of the above measures, the GDPR introduces a new basis for transferring data which is particularly relevant for researchers and did not exist under the Directive. Under Article 49(1), a controller may transfer data to a third country when "necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject." Recital 113 makes clear that "the legitimate expectations of society for an increase of knowledge" should be taken into account when determining whether a "compelling legitimate interest" exists.

To make use of this transfer mechanism, however, researchers must meet stringent requirements. The transfer may be based on this ground only if it is not repetitive, it concerns a limited number of data subjects, and "the controller has assessed all the circumstances surrounding the data transfer and has on the basis on that assessment provided suitable safeguards" (Article 49(1)). Moreover, the controller must inform the data subject as well as the data protection authority of the relevant member state of the international transfer.

6.1 Transfer to third countries

The GDPR sets out three potential bases for transfer of personal data to a third country t in Articles 44 to 49, which create what Kuner has called a three-tier hierarchy, ranging from adequacy decisions to agreements and specific situations.

Adequacy decisions are addressed under Article 45 GDPR, and require a decision from the European Commission that protection for personal data in a third country is 'essentially equivalent' to that in the EU. Such as decision has recently been issued with respect to the United Kingdom whose data protection law is fully in line with GDPR since it was drafted at a

time when the UK was still required to directly transpose EU regulations. If an adequacy decision in place, transfers can proceed freely, subject to conditions in the decision.

Where an adequacy decision has not been taken by the European Commission, data may also be transferred to a third country for health research purposes if it can be based on bi- or multilateral arrangements with recipients which assure the standard of protection elaborated by EU law. Article 46 outlines several relevant approaches: 'a legally binding and enforceable instrument between public authorities'; 'binding corporate rules'—agreements valid within a company or group of companies; 'data protection clauses'—contractual clauses on data transfer; 'codes of conduct'; 'certification mechanisms'; and 'provision inserted into administrative arrangements between public authorities'.

Finally, EU researchers might also be able to transfer personal data to a third country based on 'specific situation' justifications outlined in Article 49. Several such justifications are relevant for health research, including: if a subject 'has explicitly consented to the proposed transfer'; 'the transfer is necessary for important reasons of public interest'; 'the transfer is necessary…to protect…vital interests'; and the transfer 'is necessary for the purposes of compelling legitimate interests pursued by the controller…not overridden by the interests or rights and freedoms of the data subject'.

The three-tier approach of the GDPR is, however, subject to judicial interpretation, as exemplified in the decision was taken by the CJEU in the Schrems II case on 16 July 2020. The case concerned Facebook's transfers of personal data from the EU to the US and the validity of the tier two 'Privacy Shield' adequacy decision that had been made previously and which allowed for personal data to be transferred from the EU to the USA, was not valid. However, it did not invalidate the use of specific contract clauses, but it did specify that such clauses can only be used to legitimate transfers if: (i) a third country already provides 'essentially equivalent' protection; or (ii) supplementary measures assuring 'essentially equivalent' protection—contractual, technical, organisational, or other—can be put in place.

Recognising that the Schrems II decision created a great deal of confusion and also a burden on business and researchers, the European Commission on 4th June 2021 adopted two new sets of Standard Contract Clauses, which are an important step forward, but do not remove all the obstacles for researchers. The new standard contractual clauses provide for a mandatory data transfer impact assessment to be carried out by the contract parties. Both parties have to warrant that they have no doubts that the data importer's country's requirements comply with European standards. The impact assessment must be documented and submitted to the supervisory authorities upon request. The new standard contractual clauses follow a modular approach: Instead of different sets of standard contractual clauses, there will be only one set of standard contractual clauses in the future, which can be adapted by using certain modules and omitting others, depending on the specific details of the respective data transfer. Although this increases flexibility, it remains to be seen whether this will make use of the clauses more difficult. In addition to EU level measures, it should noted that some Member States will follow-up with national level assessments, notably the Berlin Data Protection Authority announced in June 2021 that it will conduct a nationwide audits of international data transfers by German undertakings, which could also address personal data transfers for research purposes.

Conclusion

The materials set out in this deliverable provide a further set of guidance for the project partners on compliance with the GDPR and other applicable legislation. The guidance will be further developed in deliverable 10.5 part 2, which will look at the impact of the Medical Devices Regulation, as well as emerging issues around the Data Governance Act and future legislation supporting the European Health Data Space.

In addition, the preparation of the work of the Ethics Advisory Board and the Data Management Plan will address the deeper legal and ethical issues that must be addressed if IDMP based tools are used to inform decisions on prescribing and healthcare. These issues cannot however be further advanced until the work of task 8.5 has established if it is indeed possible to develop decision support system to select patients, based on their medication list. This will include an examination of the manual process of medication review, (i.e. the optimization of therapy by removing unnecessary drugs, and substituting those that are dangerous with safer drugs) at the Federico II University Hospital. This will be used as a case study to assess the potential impact of IDMP on this process, presently undertaken in the absence of precision software tools but relying on publicly available online databases. Whether IDMP can help the process of medicine reconciliation (i.e. the correct transfer of information about drug therapy at the time when a patient moves from one hospital to another or from the hospital to the community or vice versa) will be evaluated as well. Good practices will be developed for how to prepare for IDMP coded datasets in the future, merging existing software solutions and developing new solutions.

Based on the conclusions of this assessment deliverable 10.6 will include discussion of the cross-border data transfer challenges, including to third countries, as well as the liability issues. It should be noted however that the objective of workpackage 10 is primarily to support the project partners in the execution of the project, rather than addressing the full complexity of post project software applications that could be used as part of pharmacovigilance or decision support systems.

References

- Community Pharmacy GDPR Guidance https://psnc.org.uk/wp-content/uploads/2018/03/Guidance-for-Community-Pharmacy-Part-1-Version-1.pdf

- Biasin & Kamenjašević, Medical device cybersecurity. Regulatory challenges in the EU. In I. Glenn Cohen and others, The Future of Medical Device Regulation: Innovation and Protection (forthcoming, Cambridge University Press 2021)

- Ghafur, S., Kristensen, S., Honeyford, K. et al. A retrospective impact analysis of the WannaCry cyberattack on the NHS. npj Digit. Med. 2, 98 (2019). https://doi.org/10.1038/s41746-019-0161-6

- Kuner CB. Transborder data flows and data privacy law. Oxford, UK: Oxford University Press. 2013.

- Bovenberg J, Peloquin D, Bierer B, Barnes M, Knoppers BM. How to fix the GDPR's frustration of global biomedical research: Sharing of data for research beyond the Standard Contract Clauses hEU must improve. Science 2020;370:40–42

- Peloquin D, DiMaio M, Bierer B, Barnes M. Disruptive and avoidable: GDPR challenges to secondary research uses of data. Eur J Hum Genet. 2020;28:697–705

- S. Ghafur, S. Kristensen, K. Honeyford, G. Martin, A. Darzi & P. Aylin A retrospective impact analysis of the WannaCry cyberattack on the NHS NPJ Digital Medicine volume 2, Article number: 98 (201