Analysis of ethics, privacy, and confidentiality constraints

Deliverable 3.9

Lead Author: KUL

Contributors: Elisabetta Biasin, Daniela Brešić, Erik Kamenjašević, Pierre Notermans

Deliverable classification: (PU)

Co-funded by the Horizon 2020 Framework Programme of the European Union

Version Control Sheet

Title	*Analysis of ethics, privacy, and confidentiality constraints*
Prepared By	*Elisabetta Biasin, Daniela Brešić, Erik Kamenjašević, Pierre Notermans, Anton Vedder*
Approved By	*Philippe Tourron, Ludivine Blanchet, Louis Jallet, Elodie Reuge*
Version Number	*1*
Contact	

Revision History:

Version	Date	Summary of Changes	Initials	Changes Marked
0.1	23/10/2018	Initial draft table of content	P.N.	
0.2	November 2018 – January 2019	Initial draft of deliverable	P.N., E.B., D.B.	
0.3	January 2019	Internal Review of KUL	E.K.	
0.4	January/February	Internal Review of KUL	P.N., E.B., D.B.	
0.5	26/02/2019	Review of KUL, EOS and AP-HM	A.V., DB, E.B., E.K., E.R, P.T., L.B.	
0.6	27/02/2018	Review of EOS	ER	
1	28/02/2018	Final version of the Deliverable		

Table of acronyms and abbreviations

AgID	Agenzia per l'Italia Digitale
Big legislation	Wet op de beroepen in de individuele gezondheidszorg
CDM	Codice di deontologia medica
CERT-FR	Computer Emergency Response Team - France
CERT-PA	Computer Emergency Response Team – Pubblica Amministrazione
CI	Critical Infrastructure
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
CIP	Critical Infrastructure Protection
CIWIN	Critical Infrastructure Warning Network
CJEU	Court of Justice of the European Union
CoE	Council of Europe
CSIRT	Computer Security Incident Response Teams
DIS	Department of Safety Information
ECHR	European Convention of Human Rights
ECI Directive	Directive on European Critical Infrastructures
ECI	European Critical Infrastructure
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
ENISA	European Union Agency for Network and Information Security
EPCIP	European Programme for Critical Infrastructure Protection
EU	European Union
FNOMCeO	Federazione Nazionale degli Ordini dei Medici Chirurghi e degli Odontoiatri
GDPR	General Data Protection Regulation
Ibid.	Ibidem
ICT	Information and Communication Technology
NIS Directive	Network and Information Systems Directive
no	Number
OSP	Operator Security Plan
p.	Page number

para	Paragraph
The 108 Convention	Data Protection Convention
The Charter	Charter of Fundamental Rights of the European Union
WGBO	Wet op de geneeskundige behandelingsovereenkomst
WP29	The Article 29 Working Party

The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under Grant Agreement no 787002.

Contents

List of Tables

The SAFECARE Project

In the last couple of years, the European Union has faced numerous threats that affected the society by changing the lives, the habits and the fears of hundreds of millions of citizens. The sources of these threats have been heterogeneous but they also could be used as weapons to impact the population. Due to the enormous risks and the potential impact these threats may have on society, Europe is required to increase awareness among the population against these attacks that can strike the places we rely upon the most and destabilize our institutions remotely. Nowadays, the lines between physical and cyber worlds cannot be viewed separately as they are increasingly blurred. This is because nearly everything is connected to the Internet and if not, physical intrusion might interfere and rub out the barriers. Threats cannot be analysed solely as physical or cyber, and therefore it is crucial to develop an integrated approach that addresses issues occurring in both worlds in order to fight against such combination of threats. Health services are crucial for maintaining the population's health, however, at the same time they are among the most critical infrastructures and the most vulnerable ones. They are widely relying on information systems to optimise organisation and costs, whereas, by contrast, ethics and privacy constraints severely restrict security controls and thus increase vulnerability. The aim of this project is to provide solutions that will improve physical and cyber security in a seamless and cost-effective way. It will focus on the development of new technologies and novel approaches to enhance threat prevention, threat detection, incident response and mitigation of impacts. The project will also aims at increasing the compliance between security tools and European regulations about ethics and privacy for health services. Finally, project pilots will take place in the hospitals of Marseille, Turin and Amsterdam, involving security and health practitioners, in order to simulate attack scenarios in near-real conditions. These pilot sites will serve as reference examples to disseminate the results and find customers across Europe.[1]

[1] More information about the SAFECARE project available at <https://cordis.europa.eu/project/rcn/214348/en>.

Executive Summary

One of the main aims of the SAFECARE project is to foster the creation of solutions for the improvement of cyber and physical security in the healthcare context, with specific regard to healthcare infrastructures. This deliverable adopts a legal and ethical approach in order to provide legal and ethical guidance to the SAFECARE Consortium Partners in the development and testing of technologies as well in the implementation of the research project.

To this end, three dimensions have been taken into account:

1) The first one relates to the **protection of medical information**. To this regard, privacy and data protection are concepts of main importance. Privacy is recognised by Article 8 of the European Convention of Human Rights[2] recognises privacy as the right to respect one individual's 'private and family life, his home and correspondence'.
   The right to privacy also entails the need for confidentiality between the patient and the healthcare professional. Medical confidentiality is essential, but it is not absolute. The patient needs to reveal certain secrets to the healthcare professional, in confidence, for the purpose of care. In certain circumstances, e.g. in order to share information with other care professionals if needed for the treatment or care of the patient, the healthcare professional will also have to breach the principle of confidentiality.
   Data protection is crucial in times where information technologies are becoming increasingly important. Data protection aims at protecting the health information once it is collected. A series of principles were enshrined in legal binding texts with the objective of protecting the individual's data.
   The concepts of i) **privacy**, ii) **medical confidentiality**, iii) **data protection** are examined in their application within the SAFECARE context, while considering both national and European measures, as relevant.

2) The second dimension relates to the **protection of critical infrastructures (CI) and critical information infrastructures (CIIP)** within the healthcare sector. Because of the 'criticality' of such infrastructures, and because of their interdependency, it is essential that these are protected. The analysis of the legal framework of CIP and CIIP in this deliverable proposes an overview of the European relevant acts and regulations (including European Critical Infrastructure Directive and the NIS Directive) as well as a glance to national legislations, namely France, the Netherlands and Italy.

3) The third dimension relates to the **ethical use of technologies in the healthcare sector**. Next to legal requirements, ethical considerations can support the protection of individuals and the public health as they provide guidelines and can impose constraints on the development and application of technologies. Ethical concepts can build a basis for the law but they can also provide guidance in addition to what the law seems to require. This is sometimes necessary as the current legislation faces its difficulties to cope with upcoming legal issues due to the rapid evolution of information technologies. One concrete example is the collection of large data sets, or so-called big data, which seems to conflict with fundamental data protection principles, i.e. data minimisation. Reflecting on

[2] Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols No. 11 and 14 and supplemented by Protocols No. 1, 4, 6, 7, 12, 13 and 16, 4 November 1950* <https://www.echr.coe.int/Documents/Convention_ENG.pdf>.

ethics allows to think beyond the law, and re-consider the implications for the healthcare sector, especially for the patient, the healthcare professional, and society.

1. Introduction

The objective of the SAFECARE project is to protect health infrastructures, and eventually the safety of the patient. The information collected by the to be developed technologies is supposed to include non-personal data, such as in form of technical data related to attempted physical attacks, but also personal data such as in form of video monitoring that may reveal personal attributes. The envisaged data processing operations may also contain special categories of data, i.e. data concerning health, which are particularly vulnerable to attacks. Taking these matters into account, the deliverable will focus on the analysis of ethical, privacy and confidentiality constraints, which aims at protecting personal data, in particular health data, as safeguarded under data protection legislation. The deliverable will be structured as follows:

This deliverable will firstly examine privacy guarantees, mainly in the framework of the European Convention on Human Rights (Chapter 2 on Privacy). There, it will be pointed out that medical data fall under the scope of the right to privacy, and it will be further expanded on privacy interferences and justifications invoked by Member States. Moreover, the concept of medical confidentiality, in both European and national frameworks, will be examined. The three countries examined are those where SAFECARE pilot hospitals are located; France, the Netherlands, and Italy.

Then, it will be followed by the examination of data protection measures (Chapter 3 on Data Protection). It will start with portraying a global picture of instruments aiming at protecting medical data. The focus lies on the new General Data Protection Regulation[3] (GDPR). There, the principles governing data protection, and the scope of the legislation will be analysed first. The research will then be narrowed down to the specific category of health data, where the conditions are stricter than for an average data set. The last point will cover data security mechanisms as a means to ensure confidentiality. There, national laws nuancing the GDPR on certain aspects concerning health, and notions enshrined in the GDPR such as anonymization, encryption, and data protection by design will be examined.

Next, the critical infrastructures and cybersecurity questions will be addressed (Chapter 4 on Critical infrastructures Protection and Chapter 5 on Protection of Networks and Information Systems). After having paid attention on defining the concepts, the different relevant legal sources will be outlined. It will then focus on critical infrastructures in the healthcare sector. There, the major European measure in the field and the Network and Information Systems Directive (the NIS Directive) will be outlined. National implementation measures of this Directive will also be examined, where the SAFECARE field trials will take place.

Finally, ethical aspects in the health and data protection environment will be pointed out (Chapter 6 on Ethics). After having highlighted the important moral principles in medical ethics, fundamental moral principles from the secondary principles will be distinguished. As technology developments are posing new challenges for the protection of personal data (e.g. created through the processing of big data or surveillance technologies), this chapter will not only examine the challenges appearing or covered by the current legal framework, but also reflect beyond the law.

1.1. Deliverable 3.9

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4 May 2016. It will be referred to as the General Data Protection Regulation, or the GDPR.

Dealing with constraints in the healthcare environment, the aim of Task 3.6 'Ethics, data privacy, data confidentiality, European and national regulations' is to provide an overview of the legal and ethical framework for the protection of personal health data. The four objectives are being addressed in four distinct titles: privacy, data protection, sector specific law (e.g. regulations specifically related to healthcare) and security, and ethical principles.

2. Privacy

Main findings of Chapter 2

- Article 8 ECHR:
  - The notion of "private life" as per Article 8(1) ECHR has to be interpreted broadly; the protection of health data falls under the scope of this article;
  - The right to respect for private life entails positive and negative obligations;
  - In terms of negative obligations, the interference as per Article 8(2) ECHR requires three main prerequisites, namely i) in accordance with the law, ii) legitimate aim, iii) necessary in a democratic society.
- Medical confidentiality:
  - Medical secrecy is not absolute, hence, exemptions may justify the disclosure of information through healthcare professionals;
  - The notion of confidentiality is primarily developed in national systems.

This section will address privacy questions involving health data, mainly in the case law of the European Court of Human Rights. The links with medical confidentiality will be highlighted and discussed further on while drawing developments on the national legislation of the three countries where the SAFECARE field trials will take place (France, the Netherlands, Italy).

2.1. European Convention on Human Rights – Article 8

Article 8 of the European Convention on Human Rights protects the right to respect for private and family life. The objective of this legal provision is to ensure individuals an area of development without arbitrary interference from the public authorities.[4] In order to reach these goals, the European Court of Human Rights (ECtHR) interprets the concept of 'private life' in a broad way.[5] Even when information is not private anymore, i.e. when 'public information is systematically collected and stored in official files, Article 8 may be engaged'.[6] It is also important to note that the concept of data protection is *broader* than the concept of privacy. Even though the term 'privacy' in the European Convention on Human Rights has to be interpreted broadly, it does not necessarily protect all information on identified or identifiable persons whereas data protection specifically aims at protecting this information through concrete data protection

[4] WA Schabas, *The European Convention on Human Rights – A commentary* (Oxford University Press 2015) 366-370.
[5] C Grabenwarter, *European Convention on Human Rights: Commentary* (Bloomsbury Academic 2013) 187.
[6] WA Schabas (n 4) 383; see also *S. and Marper v The United Kingdom* App Nos 30562/04 & 30566/04 (ECtHR, 04 December 2008) para 67.

regulation (e.g. Data Protection Convention[7]).[8] The guaranteed principles are evolutive[9] and context dependent.[10] This means that the Court could interpret the right to respect of privacy in a different way depending on the specific situation at stake.[11]

The European Convention on Human Rights is presented to be an instrument that an individual can invoke towards the State only. This refers to one aspect of human rights obligations, known as the 'negative obligations'. These require that the state actions are not interfering with the enjoyment and exercise of individual's fundamental rights (unless specific exceptions provided by the Convention).[12] Here, human rights are conceived as a protection towards 'the individual against arbitrary action by the public authorities'.[13] By contrast, there is a second type of obligations, the 'positive obligations'.[14] The positive obligations goes one step further. It means that the State will be held responsible for the interference with the rights due to an omission, a lack of action, damageable for the individual. This would be the case for instance if the State did not succeed in adopting procedures that would guarantee privacy rights. Positive obligations may extend from the public sphere (the relations with public authorities) to the private sphere. This means that the relations between individuals themselves could also be impacted by positive obligations, e.g. if a State is obliged to incorporate access to legal procedures in certain matters[15].[16] In the SAFECARE context, we can highlight that State authorities have to ensure that privacy guarantees are complied with healthcare services, also the ones delivered in the private sector.[17] This means that positive obligations *securing* the right to respect for private and family

[7] Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, ETS No. 108, 28.01.1981 <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108>.
[8] J Kokott, C Sobotta, 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR' (2013) 3 (4) International Data Privacy Law 225.
[9] R Ergec, J Velu, *La Convention Européenne des droits de l'homme* (Bruylant 2014) 48-49.
[10] A Vedder, 'Privacy and confidentiality. Medical Data, New information technologies, and the need for normative principles other than privacy rules', in M Freeman, A Lewis (eds.), *Law and Medicine: Current Legal Issues Volume 3* (Oxford University Press 2000) 451.
[11] For instance, in the context of terrorism, the Court adopted a flexible approach and recognized more latitude to state authorities, by contrast with its former case law. See in this regard P Notermans, 'La sécurité nationale comme « nécessité dans une société démocratique » au regard des articles 8 et 10 de la Convention européenne des droits de l'homme - Vers de nouveaux équilibres entre intérêts individuels et collectifs ?' (2018) 3 Revue de la Faculté de Droit de l'Université de Liège 412-413.
[12] *X and Y v The Netherlands* App No 8978/80 (ECtHR, 26 March 1985) para 23; *Refah Partisi (The Welfare Party) and Others v Turkey* App Nos 41340-44/98 (ECtHR, 13 February 2003) para 103; *von Hannover v Germany* App No 59320/00 (ECtHR, 24 September 2004) para 57; *Barbulescu v Romania* App No 61496/08, (ECtHR, 05 September 2017) para 108-112. See also AIL Campbell, 'Positive Obligations under the ECHR: Deprivation of Liberty by Private Actors' (2006) 10 (3) Edinburgh Law Review 399-400.
[13] *Jeunesse v The Netherlands* App No 12738/10 (ECtHR, 03 October 2014) para 106.
[14] WA Schabas (n 4) 371; *Airey v Ireland*, App No 6289/73 (ECtHR, 9 October 1979) para 32; *Z. and Others v. the United Kingdom* App No 29392/95 (ECtHR 10 May 2001) para 74.
[15] *Airey v Ireland*, App No 6289/73 (ECtHR, 9 October 1979) para 31.
[16] WA Schabas (n 4) 371; *Airey v Ireland*, App No 6289/73 (ECtHR, 9 October 1979) para 32; *Z. and Others v. the United Kingdom* App No 29392/95 (ECtHR 10 May 2001) para 74.
[17] L Gonin, O Bigler, *La Convention européenne des droits de l'homme (CEDH) : commentaire des articles 1 à 18 CEDH* (Stämpfli & LexisNexis 2018) 482-483, and the cited case *Storck v Germany* App No 61603/00 (ECtHR, 16 June 2005) para 143.

life exist.[18] Individuals also enjoy a right of effective access to information concerning their health and reproductive status,[19] which means an access to the individual data files.[20]

2.1.1. Interferences with privacy

Health data are recognized by the Court to fall under the concept of private life. The Court refers to a different terminology than in the GDPR. In the privacy debate, an emphasis is made on medical data,[21] whereas in the data protection debate, it is the concept of health data that is guaranteed. We could, however, consider it covers the same concept, as 'medical data' was defined in the Recommendation No R (97) 5 as 'all personal data concerning the health of an individual'.[22]

The Court takes the increasing amount of digital information and its impact for the right to respect of private life into account.[23] In the context of SAFECARE, this would for instance concern the development of Electronic Health Records. On a broader level, the Court ruled in several cases that:

> '[…] the protection of personal data, not least medical data, is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention (art. 8). Respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the Convention. It is crucial not only to respect the sense of privacy of a patient but also to preserve his or her confidence in the medical profession and in the health services in general.
>
> Without such protection, those in need of medical assistance may be deterred from revealing such information of a personal and intimate nature as may be necessary in order to receive appropriate treatment and, even, from seeking such assistance, thereby endangering their own health and, in the case of transmissible diseases, that of the community […]
>
> The domestic law must therefore afford appropriate safeguards to prevent any such communication or disclosure of personal health data as may be inconsistent with the guarantees in Article 8 of the Convention (art. 8) […]'.[24]

The Court highlights here the importance of medical confidentiality, not only for the patient, but also for the healthcare practitioners, in an indirect way. If practitioners do not respect this principle, this would distrust future patients to talk in confidence with professionals of the field.

---

[18] *Biriuk v Lithuania* App No 23373/03 (ECtHR, 25 November 2008) para 40; see also *I v Finland* App No 20511/03 (ECtHR, 17/07/2008) para 37.
[19] *K.H. and others v Slovakia* App No 32881/04 (ECtHR, 28 April 2009) para 44.
[20] ibid para 47.
[21] *K.H. and others v Slovakia* App No 32881/04 (ECtHR, 28 April 2009) para 55; See also JF Renucci, *Droit européen des droits de l'homme* (2e edn LGDJ 2012) 282-283.
[22]Council of Europe, 'Recommendation No R (97) 5 of the Committee of Ministers to Member States on the Protection of Medical Data' (Recommendation No R (97), 13 February 1997) Pt 1, <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804f0ed0>.
[23] C Grabenwarter (n 5) 189.
[24] *Z v Finland* App No 22009/93 (ECtHR, 25 February 1997) para 95; *M.S. v Sweden* App No 20837/92 (ECtHR, 27 Augustus 1997) para 41; *L.L. v France* App No 7508/02 (ECtHR, 10 October 2006) para 44; *I v Finland* App No 20511/03 (ECtHR, 17 July 2008) para 38; *Biriuk v Lithuania* App No 23373/03 (ECtHR, 25 November 2008) para 39 & 43; *Armoniene v Lithuania* App No 36919/02 (ECtHR, 25 November 2008) para 40; *Szuluk v The United Kingdom* App No 36936/05 (ECtHR, 02 June 2009) para 47; *L.H. v Latvia* App No 52019/07 (ECtHR, 29 April 2014) para 56.

It has also to be noticed that the Court relies on national concepts of confidentiality, which will be discussed more detailed later in the chapter.[25]

2.1.2. Justifications

The second paragraph of Article 8 outlines the conditions that have to be met in order to justify an interference with the right to respect for private and family life. Following a three step test,[26] an interference with the right to respect for privacy has :: (i) to be in accordance with the law, (ii) to pursue one or more of the exhaustively cited legitimate aims and, finally, (iii) to be necessary in a democratic society. When these three exceptions are met, there is no violation of Article 8. The aim of the first condition is that an interference has to be foreseeable by the individual, as it has to be able to know whether such interference exists. The notion of legitimate aims refers to national security, public safety or the economic well-being of the country, the prevention of disorder or crime, the protection of health or morals, the protection of the rights and freedoms of others. Assessing whether an interference is necessary in a democratic society is similar with a proportionality test, aiming at balancing rights, reaching a fair balance.[27]

2.2. Charter of fundamental rights

Within the framework of the European Union, the right to respect for privacy is guaranteed in the Charter of Fundamental Rights of the European Union in an identical way as in Article 8(1) ECHR.[28] The exceptions are provided by Article 52(1) of the Charter. The Charter specifically guarantees the right to data protection, something that is not laid down expressly in the European Convention on Human Rights.[29] However, the ECtHR has recognised a right to data protection in its case law as 'the right to respect for private life', laid down under Article 8(1) ECHR, has to be interpreted broadly.[30] Besides, fundamental rights as those presented are protected on multiple levels (e.g. through national constitutions, ECHR, or for EU Member States as well through the EU Charter) and accordingly complex is the "'multi-level' protection model", which is relying on the jurisdiction of each court and its interpretation.[31]

2.3. Confidentiality

[25] See this document, Chapter 2.3.1.
[26] See B Rainey, E Wicks, C Ovey, *The European Convention on Human Rights* – (7th edn OUP 2017) 343-360.
[27] J Gerards, *EVRM – Algemene Beginselen* (SDU 2011) 140-141.
[28] For the links between CJEU and ECHR concerning the right to privacy, see H Kranenborg, 'Protection of Personal Data', in S Peers, T Hervey, J Kenner and A Ward (eds.), *The EU Charter of Fundamental Rights: A Commentary* (Hart 2014) 235.
[29] H Kranenborg, ibid 229; F Federico, 'The EU Charter of Fundamental Rights and the Rights to Data Privacy: The EU Court of Justice as a Human Rights Court' in S de Vries, U Bernitz and S Weatherill, *The EU Charter of Fundamental Rights as a Binding Instrument: Five Years Old and Growing* (Hart 2015) 266-267.
[30] See K Vasiliki, *Fundamental Rights in EU Internal Market Legislation* (Hart 2015) 91-92, which is referring to the case *Amann v Switzerland* App No 27798/95 (ECtHR, 16 February 2000). The ECtHR held in *Amann v Switzerland* that the storing of data that is related to one's private life falls under the scope of Article 8(1) ECHR.
[31] See S O'Leary, 'A tale of Two cities: Fundamental Rights Protection in Strasbourg and Luxembourg' (2018) 20 Cambridge Yearbook of European Legal Studies 3-31.

The concept of confidentiality in medical practice is well established and is mentioned in the Oath of Hippocrates[32]. Confidentiality is sometimes interpreted as 'a corollary to the right of privacy'.[33] As it was already stated, the European Court of Human Rights is guaranteeing medical confidentiality. Medical confidentiality is a legal notion primarily developed in national legal systems. In the first part, we will address the concept of medical confidentiality in the three states where the SAFECARE hospitals are located (Chapter 2.3.1). In the second part, further developments will be addressed concerning the concept of confidentiality in the case law of the European Court of Human Rights (Chapter 2.3.2).

2.3.1. National legislations

France

In France, medical confidentiality is guaranteed by Article L. 1110-4 of the Public Health Code (*Code de la Santé Publique*).[34] Every individual treated by a healthcare professional, an institution or a service, a professional or a body ensuring prevention or care in the framework settled by the Public Health Code is entitled to benefit from this principle. Medical confidentiality also applies in the army's health services, as well as in social health services.[35]

The Public Health Code points out further obligations, particularly stating that the medical confidentiality covers all that has come to the knowledge of the healthcare practitioner when exercising the profession[36]: what he or she has been told by the patient, what he or she has seen, heard, or understood.[37] It is therefore what he or she discovered through the means of its profession that has to be protected, not only what has been entrusted to the doctor.[38]

There are exceptions to the principle of medical confidentiality. These are three types: (i) a legal exception, (ii) the concept of shared secret, (iii) and communication to close patient's relatives.[39]

(i) A legal exception means that the legislator expressly decided that, in specific matters, the healthcare professional has to disclose information of a medical nature. For instance, it is required to make disclosures where a doctor has to notify about serious diseases listed in the Public Health Code[40], declare a child's birth[41], or someone's death[42].[43]

---

[32] The Hippocratic Oath is an oath to be obeyed by physicians. In medical ethics, the maxim 'Above all [or first] do no harm' obliges health professionals to treat the sick to the best of their ability and judgement. See TL Beauchamp, JF Childress, *Principles of Biomedical Ethics* (7th edn, Oxford University Press, 2013) 150.

[33] ME Sokalska, 'Medical Confidentiality – Quo Vadis ?' (2004) 11 European Journal of Health Law 35; see also R Gibar, 'Medical Confidentiality and Communication with the Patient's Family: Legal and Practical Perspectives' (2012) 24 (2) Child and Family Law Quarterly 203.

[34] See also A Laude, B Mathieu, D Tabuteau, *Droit de la santé* (3rd edn PUF 2012) 47.

[35] See Code de la Santé publique, art L 1110-4.

[36] See Public Health Code, art R4127-4.

[37] See art R4127-4. Code de déontologie médicale, art 4,

[38] S Welsch, *Responsabilité du médecin – Risques et réalités judiciaires* (Litec 2000) 120.

[39] A Laude, B Mathieu, D Tabuteau (n 34) 328-332.

[40] Code de santé publique, art 3113-1. See for a list of serious diseases requiring disclosure of information, <http://invs.santepubliquefrance.fr/Dossiers-thematiques/Maladies-infectieuses/Maladies-a-declaration-obligatoire/Liste-des-maladies-a-declaration-obligatoire>.

[41] Civil Code, art 56.

[42] Code général des collectivités territoriales, art 2313-17.

[43] See S Welsch (n 38) 125-127.

(ii) The concept of shared secret is when two or more healthcare professionals would exchange the patient's information with the aim of providing the best health services possible.[44] The patient would normally have to agree on this. Concerning a common healthcare staff (e.g. the service of pneumatology), the provided information is considered to be shared with the whole staff.[45]

(iii) In some specific cases, the doctors (not all healthcare staff – this condition is here more restrictive) may share information with the direct family if the medical situation is of a serious nature. The patient may refuse that its personal information is shared. Article 1110-4, subparagraph 9, states that the doctor is authorised to share the information, unless the patient refuses.[46]

In summary, it can be said that French legislation in general interprets the term 'medical confidentiality' broadly, but by contrast, also states well-founded exemptions justifying the disclosure of the patient's information.

The Netherlands

In the Netherlands, medical confidentiality is guaranteed in Article 7:457 of the Civil Code, and in Article 88 of the 'BIG' legislation.[47] It is also further specified in the Dutch Code of Conduct for doctors.[48] Both registered as well as non-registered health practitioners have to comply with this duty.[49] As in the French legal system, the infringement of medical confidentiality could lead to criminal proceedings.[50] The foundations of the concept are similar to the interpretation realised by the European Court of Human Rights: protecting both the individual interest (the patient's privacy) and the collective interest (ensuring that individuals trust the healthcare practitioners).[51]

There are mainly two obligations relying on the healthcare practitioner. The first one is that he or she is not allowed to communicate patient's information to other parties. The second one is that he is allowed to keep the information secret, even if he has to testify before a Court.[52] It is important to specify that the patient's health information has to remain private, even for other medical professionals. For instance, information about psychiatric treatment is not supposed to be accessible by doctors from another department.[53] Nevertheless, this could depend on the context. The European Court of Human Rights ruled, in a case involving an HIV patient, that 'transmission of information on the patient's condition may, under certain circumstances, be relevant and necessary for the purposes of not only guaranteeing appropriate medical treatment for the patient but also ensuring the protection of the rights and interests of the healthcare

[44] A Laude, B Mathieu, D Tabuteau (n 38) 329.
[45] ibid 329-330.
[46] Code de la Santé publique, art L 1110-4 al. 9; see also A Laude, B Mathieu, D Tabuteau (n 38) 331.
[47] See Wet op de geneeskundige behandelingsovereenkomst (WGBO), art 7:457, and Wet op de beroepen in de individuele gezondheidszorg (BIG), art 88.
[48] See KNMG, 'Gedragsregelsvar artsen', Rule II. 15 and III.1<https://www.knmg.nl/advies-richtlijnen/dossiers/gedragsregels-van-artsen.htm>.
[49] Van Hellemondt, Tekst en Commentaar Gezondheidsrecht, commentaar op art. 88 Wet BIG (1 maart 2018) <https://www.navigator.nl>.
[50] Criminal Code, art 272.
[51] See J Nouwt, *Zorg voor privacy – Informatietechnologie en informationele privacy in de gezondheidszorg* (SDU 1997) 95.
[52] WLJM Duijst, MEB Morsink, 'Het medische beroepsgeheim: Heilige huisjes en juridische fictie' (2017) 2 Tijdschrift voor Bijzonder Strafrecht & Handhaving 88.
[53] See HJJ Leenen, e.a., *Handboek gezondheidsrecht* (6th edn Boom 2014)143-145.

providers involved in his treatment and of other patients, by enabling the requisite precautionary measures to be adopted'.[54] The Court further ruled that 'the need to facilitate the efficient provision of treatment and monitoring of a patient may justify the transmission of information among the different medical professionals involved in providing the various types of healthcare'.[55]

Medical confidentiality is not absolute, and there are exceptions allowing to disclose information: in particular, information can be communicated by healthcare practitioners (without being prosecuted) when the patient **consents** to do so, if there is a **legal ground**, or when **conflicting obligations** arise.[56]

(i) Consent may be provided verbally and written. It has to be freely given, and the patient has to be conscious of the consequences of his acts.[57]

(ii) Examples of legal grounds are:[58]
- A consultation following someone's death – no natural death,[59] or following an euthanasia.[60]
- A consultation noticing infectious diseases.[61]
- When minors' death occurs.[62]
- For health insurance purposes[63]

(iii) A concrete example of a conflicting obligation would be when a doctor informs the police authorities of a direct threat for the patient or other people.[64] The interpretation of the concept of 'direct threat' depends on the context: for instance, giving notice of a murder that was already committed would not fall under this exception.[65] Six criterion have been developed by Leenen[66], systematizing the concept. If these are fulfilled, a breach of confidentiality would be allowed. These are:[67]
- All possible actions were undertaken in order to get the consent to communicate the information
- If there would be no breach, this would entail serious consequences for a third party
- The bearer of the secret has to face a moral dilemma
- There is no other way than breaching the secret in order to solve the problem

---

[54] *Y v Turkey* App No 648/10 (ECtHR, 17 February 2015) para 74.
[55] ibid para 76.
[56] J Nouwt, (n 51) 98-99; Van der Meij, T&C Strafrecht, commentaar op art. 272 Sr (1 July 2018). Accessible on <https://www.navigator.nl>.
[57] HJJ Leenen, e.a. (n 53) 148-149.
[58] Van der Meij, T&C Strafrecht, commentaar op art. 272 Sr (1 July 2018). Accessible on <https://www.navigator.nl> .
[59] Wet op de lijkbezorging, art 7(3).
[60] Wet op de lijkbezorging, art 7(2).
[61]Wet publieke gezondheid, art 21. For a list of the diseases and the notice deadline, see <https://www.rivm.nl/sites/default/files/2018-11/20170606%20versie%202.1%20Meldingsnormenx_0.pdf>. The most dangerous diseases that are listed are: The MERS – Coronavirus, the SARS, Poliomyelitis, Smallpox, viral haemorrhagic fever.
[62] Wet op de lijkbezorging, art 10(a).
[63] Wet marktordening gezondheidszorg, art 68 (a).
[64]Van der Meij, T&C Strafrecht, commentaar op art. 272 Sr (1 July 2018). Accessible on <https://www.navigator.nl>.
[65] WLJM Duijst, MEB Morsink (n 52) 91.
[66] See HJJ Leenen, e.a. (n 53) 150.
[67] ibid.

- It has to be quite sure that the breach of that secret would limit or prevent damage to the third party
- The secret has to be breached as little as possible.

In summary, the concept of 'medical confidentiality' under Dutch legislation is not absolute as it considers exceptions justifying the disclosure of information through healthcare practitioners. Besides, the justification in cases of 'conflicting obligations', i.e. direct threat', requires a careful weighting of certain circumstances.

Italy

In Italy, medical confidentiality is primarily regulated by professional ethics provisions. Professional ethics provisions are established by a the Italian National Federation of Orders of Doctors' ('*Federazione Nazionale degli Ordini dei Medici Chirurghi e degli Odontoiatri*', *FNOMCeO*), an entity that assemblies and represents the many 'Orders of Doctors'[68] established in the national territory.

Of most importance are the rules set by the 2014 ('*Codice di deontologia medica*', *CDM*), issued by the Italian National Federation of the Orders of Doctors. The code provides ethical and professional rules that have to be respected by doctors in the exercise of their profession.

Article 10 of the CDM is dedicated to the protection of professional secrecy**.** It requires that 'The doctor must keep the secret of everything he knows about his own professional activity'[69].

Article 10 of the CDM also provides further guarantees for doctors, stating that 'the doctor must not report to the competent authority in matters of justice and security any testimonies on facts and circumstances concerned by professional secrecy'.[70]

Also in the Italian case, medical confidentiality does not mean an absolute duty of secrecy. The revelation of the secret may be allowed if motivated by a legitimate cause foreseen by law. Legitimate causes are in doctrine distinguished between 'imperative causes' or 'permissive causes'.[71] Imperative causes occur when medical confidentiality is subject to a specific legal provision imposing the communication of the secret. Included in this matter are mandatory health claims, mandatory certificates, and all cases in which the medical activity responds to specific obligations required by law (appraisals, technical advices, arbitration, etc.). Permissive causes concern, on the other hand, all cases where the secret communication occurs with individual's consent, i.e. in the context of facultative certificates requested by individuals.

The CDM also dedicates a specific article to individual's privacy and protection of personal data (Article 11). According to this, 'the doctor becomes controller for the processing of personal data after having obtained the informed consent of the patient or its legal representative and it is

[68] The Italian 'Order of doctors' are 'noneconomic public bodies' whose tasks and activities are established by law. See D.Lgs.C.P.S. 13/09/1946, n. 233 Ricostituzione degli Ordini delle professioni sanitarie e per la disciplina dell'esercizio delle professioni stesse. GU 23 ottobre 1946, n. 241 art 1(3).
[69] CDM, art 10.
[70] This provision applies without prejudice to art 200 of the Italian Criminal Procedure Code, which states: 'The following categories of subjects cannot be obliged to testify to what they have known by reason of their ministry, office or profession, except in cases where they have the obligation to report to the judicial authorities: a) ministers of religious confessions [...]; b) lawyers [...], technical consultants and notaries; c) doctors and surgeons, pharmacists, midwives and any other practicing a health profession [...]'.
[71] S Del Vecchio, S Gualandri, G Pelosi and A L Santunione, *Lineamenti di medicina legale per il medico di medicina generale* (Edizioni Medico-Scientifiche 2007) 55.

subject to the respect of privacy of the patient, with particular regard to data concerning health and sex life of the individual'. 'The doctor shall ensure the 'non-identifiability of the involved subject in the context of scientific publication of medical studies or clinical trials'.[72]

The doctor has to ensure the non-identifiability of the subjects involved in the publications or scientific disclosures of data and clinical studies. Furthermore, the doctor shall not collaborate in the establishment, management or use of databases of assisted persons in the absence of guarantees on the preliminary acquisition of their informed consent and on the protection of the confidentiality and security of the data'.[73]

The respect of professional ethics rules is in first instance subject to the control of every Order of Doctors in the national territory, which have the power to start disciplinary procedures and impose disciplinary sanctions.[74] Depending to the gravity of the misconduct, disciplinary sanctions may vary from a warning to the suspension from the exercise of the medical profession (up to six months), to the radiation from the national medical register.[75]

Finally, it has to be noted that the non-respect of obligations concerning medical confidentiality may entail other legal consequences, such as under criminal law. Worth to be reported is Article 622 of the Italian Criminal Code, titled 'Revelation of professional secret' (Rivelazione di segreto professionale). The provision establishes that 'anyone who is informed of a secret, by reason of his or her state, office, profession or art, and reveals it without any legitimate cause or uses it to his/her own profit, will be punished with imprisonment up to a year or with a fine up to 516 euros'.

2.3.2. European Convention on Human Rights

When dealing with the interferences of national measures on privacy, The importance of confidentiality in healthcare relations has already been pointed out. If there are interferences with the right to respect of privacy, the Court stated that 'any unavoidable interference in this connection should be limited as far as possible to that which is rendered strictly necessary by the specific features of the proceedings and by the facts of the case'.[76] From this excerpt, it can be concluded that the Court is adopting a strict approach, being protective for the confidentiality. In the same vein, and when there is a breach of medical secrecy, the Court will also have a look at subsidiary means. In other words, it will consider whether the outcome of the procedure could have been reached without mentioning the medical data and by using other information without harming the individual's privacy interests.[77] The collection of medical data by a third party (an Inspectorate of 'Quality Control for Medical Care and Fitness for Work') several years (in the case *L.H. v Latvia* it has been seven years[78]) after the medical intervention on a patient was also considered to be problematic with regard to confidentiality hHere, the Court ruled that 'such a

[72] CDM, art 11.
[73] ibid.
[74] See D.P.R. 5-4-1950 n. 221 - Approvazione del regolamento per la esecuzione del decreto legislativo 13 settembre 1946, n. 233, sulla ricostituzione degli Ordini delle professioni sanitarie e per la disciplina dell'esercizio delle professioni stesse. GU 16 maggio 1950, n. 112, S.O, Capo IV.
[75] ibid., art 40.
[76] *L.L. v France* App No 7508/02 (ECtHR, 10 October 2006) para 45.
[77] ibid para 46.
[78] *L.H. v Latvia* App No 52019/07 (ECtHR, 29 April 2014) para 50.

broad interpretation of an exception to the general rule militating against the disclosure of personal data might not offer sufficient guarantees against the risk of abuse and arbitrariness'.[79]

All interferences do, nevertheless, not automatically mean the conviction of the Member State. As recognized by the Court itself, medical secrecy is not absolute.[80] This means that, when there are competing interests at stake, the Court may choose to favour one instead of another. For instance, the Court emphasized that 'the interests of a patient and the community as a whole in protecting the confidentiality of medical data may be outweighed by the interest in investigation and prosecution of crime and in the publicity of court proceedings'.[81] The Court ruled in this case in favour of the State, recognizing 'very weighty public interests militated in favour of the investigation and prosecution of X for attempted manslaughter'.[82] The specific situation justified a breach of medical confidentiality. The Court further exposed that 'the various orders requiring the applicant's medical advisers to give evidence were supported by relevant and sufficient reasons which corresponded to an overriding requirement in the interest of the legitimate aims pursued'.[83] In another case, a patient was complaining that a communication of his medical data by one public institution to another was violating the recognized guarantees by law. As the communication was intra-services and achieved upon request by the applicant in order to obtain a benefit,[84] the Court did not conclude there was a breach of the principle of confidentiality. Important is to note the existence of limitations and 'effective and adequate safeguards against abuse'.[85] The possibility to claim compensation 'for damages caused by an alleged unlawful disclosure of personal data was not sufficient to protect her private life. What is required in this connection is practical and effective protection to exclude any possibility of unauthorized access occurring in the first place'.[86]

[79] ibid.
[80] *Eternit v France* App No 20041/10 (ECtHR, 27 March 2012) para 37.
[81] *Z v Finland* App No 22009/93 (ECtHR, 25 February 1997) para 97.
[82] ibid para 102.
[83] ibid para 105.
[84] *M.S. v Sweden* App No 20837/92 (ECtHR, 27 August 1997) para 42.
[85] ibid.
[86] *I v Finland* App No 20511/03 (ECtHR, 17 April 2008) para 47.

3. Data protection

Main findings of Chapter 3

- The right to privacy and the right to data protection:
  - Both concepts are closely related but have to be viewed separately;
  - The right to privacy has to be interpreted broadly, however, it does not cover all types of data processing.
- The protection of personal data under the GDPR:
  - The GDPR protects personal data, which is defined in Article 4(1) as 'information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'; therefore, non-personal data, which is not related to an identified or identifiable natural person, does not fall under the scope of the GDPR;
  - The GDPR sets out principles for the protection of personal data and pays particular attention to the principle of accountability;
- The protection of special categories of data, i.e. data concerning health, under the GDPR:
  - The processing of special categories of personal data is generally prohibited, unless one of the conditions set out in Article 9(2) GDPR applies;
  - Member States are able to introduce further national requirements for the protection of data concerning health.
- Data security mechanisms (e.g. anonymisation, data protection by design etc.) may be considered as means to ensure confidentiality.

This section will address data protection questions. It will first refer to instruments adopted before the new GDPR, and specifically related to the SAFECARE context. A particular attention will then be paid to the GDPR[87], the notion of special category of personal data and the protection mechanisms enshrined in the Regulation such as encryption and anonymization.

Privacy and data protection are two concepts that have to be distinguished. Even if closely put into relation, the 'right to privacy' and the 'right to data protection' are distinct rights. The two protect similar values – the human dignity and autonomy of individuals – but nonetheless, they are different. The 'right to privacy' includes different aspects of private and family life (as enshrined in Article 8 of ECHR). It aims at protecting the private sphere of an individual. The 'right to the protection of personal data' comes into relevance whenever occurs the processing of

[87] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4 May 2016. It will be referred to as the General Data Protection Regulation, or the GDPR.

personal data. 'Personal data' is defined by EU data protection law as 'any information relating to an identified or identifiable natural person'. Therefore, the right to data protection aims at creating guarantees for individuals with regard to data that may be ascribed to an individual, even if not pertaining to the private/family sphere of him or her.[88]

The concepts of privacy and data protection have to be further distinguished from the concept of 'medical confidentiality' as outlined more in detail under Chapter 2.3. For the purposes of Chapter 2.3., the concept of 'medical confidentiality' has to be associated to the duty of 'professional secrecy' of the healthcare professional, aimed at guaranteeing one of the most important moral values in patient care, i.e. 'confidentiality' as 'the promise or duty to protect informational privacy'.[89]

Data protection measures are however not only examined within the GDPR framework but also by the Council of Europe. Therefore, the following sections will begin with the examination of the measures adopted by the Council of Europe , and continue with the analysis of measures provided by the GDPR.

3.1. Council of Europe instruments

The 108 Convention[90] was adopted in 1981, as an objective to ensure a higher protection level for personal data than the framework provided by the European Court of Human Rights at that time.[91] It is described as the first international legal instrument to be legally binding for CoE Members.[92] All members from the Council of Europe joined, but it is also open to other states.[93] Health data were already categorized as a special category of data.[94]

In 1997, the European Convention for the Protection of Human Rights and Dignity for the Human Being with Regard to the Application of Biology and Medicine was adopted.[95] With the main goal to protect against genetic discrimination, the Oviedo Convention also recognized to the patient information rights.[96] It entered into force in 29 of the 47 Member States of the Council of Europe.[97]

---

[88] Recital 26 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4 May 2016. It will be referred to as the General Data Protection Regulation, or the GDPR.

[89] See G Neitzke, Confidentiality, Secrecy, and Privacy in Ethics Consultation HEC Forum (2007) 19 (4): 293-302.

[90] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 108, 28.01.1981.

[91] LA Bygrave, *Data privacy law– An international perspective* (Oxford University Press 2014) 34.

[92] EJ Kindt, *Privacy and data protection issues of biometric applications – a comparative legal analysis* (Springer 2013) 91.

[93] As from the 1st of October 2018, CoE 108 entered into force in Cabo Verde, Mauritius, and Mexico. The remaining non CoE member countries are Uruguay, Senegal, and Tunisia. See <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=zf4VaBr5 >.

[94] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CoE 108), art 6.

[95] Convention for the protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine.

[96] See IV Motoc, 'The international Law of Genetic Discrimination: The Power of 'Never Again', in T Murphy (ed.) *New technologies and Human Rights* (Oxford University Press 2009) 227.

[97] See <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/164/signatures?p_auth=OtnFXPfS>.

This legal instrument is described as an important text aiming at protecting 'human rights in the bioethical and biomedical field on a regional scale',[98] and could be used as a tool in order to interpret the European Convention on Human Rights.[99] This could be useful when dealing with human genome questions.[100]

Recommendation No R (97) 5 of the Committee of Ministers to Member States on the protection of medical data consists in the further outline of the obligations enshrined in Article 6 of the 108 Convention. Developments around consent, the exceptions allowing the processing of sensitive data, and data security principles were already addressed therein.[101]

3.2. The General Data Protection Regulation

3.2.1. General remarks

The GDPR replaced in May 2018 the former Data Protection Directive of 1995.[102] The aim was to adopt a legal text taking into account the evolution in the digital field while ensuring harmonization in all EU countries. This also explains the choice for a Regulation and not a Directive. In principle, a Regulation is directly applicable in all Member States without an intervention of these national authorities. Nevertheless, the GDPR provided that the Member States are in some cases allowed to adopt their own measures. In the SAFECARE context, this is especially true concerning health data. In other words, this means that Member States could introduce more requirements in order to protect the individual's health data.[103]

The GDPR enshrines the following data protection principles:[104] Lawfulness, fairness and transparency;[105] Purpose limitation;[106] Data minimisation;[107] Accuracy;[108] Storage limitation;[109] Integrity and confidentiality.[110] These principles have to be respected by the data controller, who will also have to be able to show the compliance to these principles.[111] However, this does not mean that the processor is exempted from any obligation: both the processor and the controller remain responsible for the security of the data.[112]

---

[98] F Seatzu, S Fanni, 'The Experience of the European Court of Human Rights with the European Convention on Human Rights and Biomedicine' (2015) 31 Utrecht J. Int'l & Eur. L. 5.
[99] ibid 14.
[100] See GT Laurie 'Genetics and Patients' Rights: Where Are the Limits' (2000) 5 Med. L. Int'l 27.
[101] Recommendation No R (97) 5.
[102] See J Castro-Edwards, *EU General Data Protection Regulation – A guide to the new law* (The Law Society 2017) 2-4.
[103] GDPR, art 9(4).
[104] GDPR, art 5 (1).
[105] GDPR, art 5 (1)(a).
[106] GDPR, art 5 (1)(b).
[107] GDPR, art 5 (1)(c).
[108] GDPR, art 5 (1)(d).
[109] GDPR, art 5 (1)(e).
[110] GDPR, art 5 (1)(f).
[111] L Townsend, 'Data processors', in R Jay e.a. (eds) *Guide to the General Data protection regulation – A companion to Data Protection Law and Practice* (4th edn Sweet & Maxwell 2017) 113.
[112] R Jay, L Townsend, 'Security Obligations and Breach Notification' in R Jay, e.a. (eds) *Guide to the General Data protection regulation – A companion to Data Protection Law and Practice* (4th edn Sweet & Maxwell 2017) 132; see also see L Feiler, N Forgó, M Weigl, *The EU General Data protection Regulation (GDPR) : A commentary* (German Law Publishers 2018) 14.

A *processor* is defined as 'a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller';[113] a *controller* is defined as 'natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law'.[114]

Lawfulness, fairness and transparency

The notion of lawfulness implies that processing personal data is allowed when it meets one of the six sub-paragraphs of Article 6 GDPR. These are consent (i), performance of a contract (ii), compliance with a legal obligation (iii), protection of vital interests of the data subject or someone else (iv), public interest (v), the legitimate interests of the data controller or a third party (vi). These grounds have to be selected and pointed out before the processing of data.[115]

The concept of fairness is not yet well established in the literature.[116] Processing could in any case be considered as unfair 'if the data subject is likely to feel that it is "sneaky, creepy, or dishonest"'.[117] It therefore implies that the data have to be processed with a peculiar focus on 'the interests and reasonable expectations of data subjects'. [118] Processing operations should not be carried out secretly and data subjects should be aware of potential risks of the processing.[119]

With transparency, the European legislator sends the message that data subjects should be 'enabled to understand what is happening to their personal data'.[120] The notion of transparency was, in the former Data protection Directive examined under the principle of fairness.[121] It is now enshrined at article 12 GDPR.[122]

Purpose limitation

The principle of purpose limitation specifies that the data is '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 […]'.[123] Explaining to the data subject for which purposes its data have to be processed is very much linked with the concept of transparency.[124] This means that processing data for purposes that were not communicated to the data subject is in principle unlawful. However, a new purpose might be 'compatible' with the former one if:

---

[113] GDPR, Art 4 (8).
[114] GDPR, Art 4 (7).
[115] R Jay, 'The principles and grounds for processing', in R Jay, e.a. (eds) *Guide to the General Data protection regulation – A companion to Data Protection Law and Practice* (4th edn Sweet & Maxwell 2017) 85.
[116] LA Bygrave (n 90) 146.
[117] J Castro Edwards (n 101) 17.
[118] LA Bygrave (n 90) 146.
[119] See S Wachter 'The GDPR and the Internet of Things: a three-step transparency model' (2018) 10(2) Law, Innovation and Technology 272.
[120] P Voigt, A von dem Bussche, *The EU General Data protection regulation (GDPR) – A practical Guide* (Springer 2017) 88.
[121] LA Bygrave (n 90) 147.
[122] See WP29, Guidelines on transparency under Regulation 2016/679, WP260 rev.01, adopted on 29 November 2017 as last revised and adopted on 11 April 2018.
[123] GDPR, art 5(1)(b).
[124] J Castro Edwards (n 101) 22-23.

- 'any link between the purposes for which the data were collected and the intended further processing;
- The context of the collection, in particular the relationship between the controller and the data subject;
- The nature of personal data and whether data in the special categories or personal data relating to criminal convictions or offences as defined in Article 10 are processed;
- The possible consequences of the intended processing for the data subjects; and
- The existence of safeguards, for example encryption or anonymization.'[125]

This list is not considered to be exhaustive and may vary depending on the circumstances.[126]

Data minimisation

The data minimisation principle requires to limit the processing of data to what is necessary in order to achieve a legitimate purpose. Synonyms used are '"data avoidance" and "data frugality"'.[127] Zarsky[128] contributes to the ongoing debate in the scientific literature whether purpose limitation and data minimisation are compatible with Big Data analytics.[129] Even if the envisaged data processing initially may not relate to the patient, the use of big data analytics may bear the risk to disclose correlations revealing personal data. This is especially true in SAFECARE context, where 'large scale data collection [could] allow virtually infinite possibilities and combinations of data analysis methods that can be used to search for medically relevant correlations in datasets'.[130] This does not only pose some concerns in lights of the current GDPR framework. It also appeals further reflexions on the impact of big data on a societal aspect, that will be dealt with in the ethics part. SAFECARE partners should be careful to process personal data in a limited way, i.e. relevant for the specified purposes. Alternative measures should be taken into account such as anonymization or pseudonymization, reducing the amount of data and the direct linking with individuals.

Accuracy

The accuracy principle entails that the personal data must be accurate and up to date. This is of importance for the data subject, as the collected data is supposed to allow 'reconstructing a situation or the characteristics of an individual'[131] and therefore produce legal consequences.[132] The consequences could also be dramatic for patients if their health record is not reflecting the reality.[133] Therefore, in order to achieve accurate datasets, SAFECARE partners should verify the quality of the data. When processing, 'every reasonable step' should be achieved in order to ensure accuracy. This is another flexible notion that will depend on the purposes of processing.

[125] R Jay, 'The principles and grounds for processing' (n 139) 87.
[126] ibid.
[127] LA Bygrave (n 90) 151.
[128] TZ Zarsky, 'Incompatible: The GDPR in the Age of Big Data' (2017) 47 Seton Hall L. Rev. 1005-1011.
[129] ibid.
[130] E Vayena, A Blasimme, 'Health Research with Big Data: Time for systemic oversight' (2018) 46 The Journal of Law, Medicine & Ethics 124.
[131] P Voigt, A vom den Bussche (n 119) 91.
[132] ibid.
[133] J Castro Edwards (n 101) 24.

Storage limitation

The storage limitation principle implies that personal data must not be kept for longer than is necessary for the purposes for which they are processed. The duration of storage is hard to anticipate in advance and might be examined depending on the concrete circumstances; an unlimited retention should be avoided.[134] It would be advised to document the data storage in internal policies.

Integrity and confidentiality

The integrity and confidentiality principle is related to the security of the data. Further developments are enshrined in Articles 32-34 GDPR. The principle entails that data is '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'.[135] The notion of appropriateness with respect to 'technical and organisational measures' was inserted by the European legislator on purpose, instead of introducing a concept that would be quickly outdated. Appropriate therefore imply an idea of flexibility. It requires a proactive evaluation by the controller – on the basis of the prior assessment of risk that may be implied by the processing – for the adoption of technical and organisational measures as 'adequate' to ensure security of data with specific regard to the environment in question. It should nevertheless be noted that when dealing with sensitive data (such as health data), stronger protection safeguards should be implemented.[136]

Accountability

The notion of accountability is enshrined by Article 5(2) GDPR. The underlying idea is to make sure that 'data controllers are able to demonstrate compliance with the principles' of the GDPR.[137] The accountability principle is a principle guiding the whole Regulation.[138] The controller will therefore have to think twice before assessing whether ongoing practices are compliant with the data protection regulation, risking to be held liable for non-compliance with it.[139] Nevertheless, for other authors in the academic literature, such as Jay[140], 'accountability appears to be a general exhortation rather than an enforceable obligation'.[141] In any case, considering the sensitivity of the processed data, it might be advised to the processor to follow carefully the accountability principle.[142]

As a consequence of the accountability principle, the controller must adopt a 'risk based approach'. Hence, Article 24 GDPR requires that the controller, '[t]aking into account the nature,

---

[134] ibid 25.
[135] Art 5(1)(f) GDPR
[136] J Castro Edwards (n 101) 25.
[137] ibid 26.
[138] A Vedder, L Naudts, 'Accountability for the use of algorithms in a big data environment' (2017) 31 (2) International Review of Law, Computers & Technology 211.
[139] A Tamò-Larrieux, *Designing for Privacy and its Legal Framework – Data protection by design and default for the internet of things* (Springer 2018) 96.
[140] R Jay e.a. (eds) *Guide to the General Data protection regulation – A companion to Data Protection Law and Practice* (4th edn Sweet & Maxwell 2017).
[141] R Jay, 'Accountability', in R Jay e.a. (eds) *Guide to the General Data protection regulation – A companion to Data Protection Law and Practice* (4th edn Sweet & Maxwell 2017) 173.
[142] See ME Gonçalves, 'The risk based approach under the new EU data protection regulation: a critical perspective' (2109) Journal of Risk Research 5, and the cited references.

scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of data subjects […] shall implement appropriate technical and organisational measures'. The risk level associated with data processing operations also explains the need for a Data Protection Impact Assessment (DPIA).[143] Moreover, the controller is required to 'implement data protection by design and default in order to identify and ameliorate defined risks to data subjects'.[144] The processor has also to comply with further obligations, such as 'record-keeping'.[145]

3.2.2. Scope

As previously examined, the GDPR applies to controllers and processors.[146] Even if it is the controller that, by contrast with the processor, holds the main compliance responsibilities with regard to the GDPR,[147] both remain responsible for ensuring data security.[148] In the case of sub-contracting the processing activities to a sub-processor, this has to be realized:[149]

- On behalf of the controller
- In accordance with its written authorization
- With the same data protection obligations that are set out in the contract or other legal act between the controller and the processor (Article 28(4) GDPR)

Material and personal scope

The GDPR defines personal data as follow: 'any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly […]'.[150] It further applies a distinction between processing of personal data by automated means; and processing other kinds of data 'which form part of a filing system or are intended to form part of a filing system'.[151] Following the recent case law of the Court of Justice of the European Union, dealing with the former Data protection Directive, 'a filing system is defined as 'any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis'.[152] This means that once information can be linked to an individual, it has to be interpreted as personal data.

The main criterion is that the information has to relate to an identified or identifiable natural person. One other aspect of this personal scope is to analyse the activity of processing information. Here, the GDPR defines it as follows: '"processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or

[143] R Jay, 'Accountability' (n 139) 171.
[144] ibid.
[145] ibid.
[146] See L Feiler, N Forgó, M Weigl (n 111) 14.
[147] L Townsend, 'Data Processors' (n 110) 109.
[148] See R Jay, L Townsend, 'Security Obligations and Breach Notification' in in R Jay e.a. (eds) *Guide to the General Data protection regulation – A companion to Data Protection Law and Practice* (4th edn Sweet & Maxwell 2017) 132; see also see L Feiler, N Forgó, M Weigl (n 139) 14.
[149] See L Townsend (n 110) 119.
[150] GDPR, art 4(1).
[151] GDPR, art 2.
[152] Case C-25/17 *Jehovan todistajat* [2018] ECLI:EU:C:2018:551 para 55, see also in the same way Recital 15 of the GDPR.

alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction'.[153]

For such identification to take place, all means likely reasonably to be used shall be taken into account throughout the lifetime of the data processed.[154] It should be pointed out that non-personal data, that is data not relating to an identified or identifiable natural person, fall outside the scope of the data protection regime.[155]

The data subject has a series of rights that can be exercised through the means of a request that in principle should be addressed to the data controller.

- **Right to information**: the data subject is entitled to be informed if there is collection and processing of its personal data;
- **Right to access:** the data subject is entitled to obtain, after having introduced a request, information about the processing of personal data relating to them or obtain a copy of the data;
- **Right to rectification:** the data subject has the right that the collected data remains up to date;
- **Right to erasure:** when the individual is entailed to exercise this right, he has the right to have personal data erased (equates the 'right to be forgotten');
- **Right to restriction of processing:** in specific cases, data subjects have the right to temporarily restrict a controller from processing their personal data;
- **Right to data portability:** in specific cases, data subjects have the possibility to ask the transfer of their data from a controller to another, if technically possible;
- **Right to object**: in specific cases, data subjects have the right to refuse their personal data is processed.

The scope of these rights might be restricted through legislative measure of Member States.[156] If such restriction occurs, and in conformity with Article 23(1) GDPR, such restriction has to respect the essence of the fundamental rights and freedoms, and has to be necessary and proportionate for the achievement of a provided legitimate goal. Considering the stakeholders involved and the objective of the project, the following three restrictions are of relevance in SAFECARE context.

- Monitoring or regulatory function connected to the exercise of official authority in certain cases;
- Protecting the data subject or the rights and freedoms of others;
- Objectives of general public interest, such as public health.

Territorial Scope

The GDPR applies when 'processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not',[157] and when 'processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to offering of goods and services to data subjects in EU; monitoring of

[153] GDPR, art 4(2).
[154] GDPR, Recital 26.
[155] ibid; see also J Castro-Edwards (n 101) 10.
[156] GDPR, art 23(1).
[157] GDPR, art 3(1).

behaviour of data subjects in the EU'.[158] Concerning the question of the activities, the Court of Justice of the European Union (CJEU) ruled that: 'that provision requires the processing of personal data in question to be carried out not "by" the establishment concerned itself but only "in the context of the activities" of the establishment'.[159] This means that the criterion is a large one. Even if the processing of the data is not realized by a healthcare provider and is carried out outside the European Union, the GDPR may apply.[160]

3.2.3. Special categories of personal data: health data

The processing of special categories of personal data, or sensitive data as they are commonly referred to, is **in principle prohibited, unless** one of the conditions exhaustively enumerated in the GDPR applies.[161] Special categories of personal data distinguished by the GDPR are:

- data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership;
- 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.

In the context of the SAFECARE project, we will draw a specific attention to the category of health data, considered to be – with the aforementioned points – as sensitive data. These data sets consists, for instance, of the information stored in the electronic health record system.[162] It could also include any information that may be collected in the course of the registration for, or the provision of, health care services; any number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; any information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject – independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.[163] The Article 29 Working Party[164] further defined the concept of personal data in healthcare, covering situations such as the fact that someone wears contact lenses, smokes or drinks, information related to the intellectual or emotional capacity of a person.[165] The Court of Justice of the European Union also ruled that the category of health data has to be interpreted broadly, 'so as to include information concerning all aspects, both physical and mental, of the health of an individual'.[166]

---

[158] GDPR, art 3(2).
[159] Case C-191/15 *Verein für Konsumenteninformation v Amazon EU Sàrl* [2016] ECLI:EU:C:2016:612 para 78.
[160] In the same sense, see L Feiler, N Forgó, M Weigl (n 111**Erreur ! Signet non défini.**) 16.
[161] GDPR, art 9.
[162] WN II Price, 'Risk and Resilience in Health Data Infrastructure' (2017) 16 Colo. Tech. L.J. 67.
[163] See GDPR, Recital 35.
[164] The independent European Article 20 Working Party dealt with privacy and data protection issues until 25 May 2018, and has been replaced by the European Data Protection Boad (EDPB) since then. See <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=629492>.
[165] WP29, Annex to Letter from the WP29 to the European Commission, DG CONNECT on mHealth, 5 February 2015, p. 2.
[166] Case C-101/01 *Lindqvist* [2003] ECLI:EU:C:2003:596 para 50.

As was pointed out by *Voigt* and *von dem Bussche*, 'these categories of personal data merit specific protection as they allow conclusions about an individual that are linked to his fundamental rights and freedoms, and their processing might entail high risks for the latter […]'.[167] Following this line, Article 9 GDPR states that the processing of such personal information is prohibited unless an exception applies. Herein below are outlined the main exceptions foreseen:

- Concerning the **consent**: it has to be explicit (Article 9(2)(a) GDPR). On the other hand, consent is not required if it is impossible to retrieve it from a data subject who is physically or legally incapable of giving consent and when there is a need to protect vital interests of the data subject (Article 9(2)(c) GDPR). Furthermore, explicit consent is not required if the data is made public by the data subject (Article 9(2)(e) GDPR).
- Particular field of **employment / social security / social protection law**: 'Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject […] in so far as it is authorised by Union or Member State law or a collective agreement' (Article 9(2)(b) GDPR).
- 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 European Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3 (h); with a need to be 'subject to the obligation of professional secrecy',[168] as defined within the relevant national legislations.
- Processing is necessary for **reasons of public interest in the area of public health** (Article 9(2)(i) GDPR).

Consent

Consent is defined by the GDPR as 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'. [169] It is a clear ground relying on an 'opt-in' approach, i.e. following the decision of a data subject to agree on the processing of its data.[170]

Consent requirements under data protection law[171]	
'Freely given'	Data subjects must be able to make a real choice and exercise a control over their data. If the data subject has no real choice, feels forced to consent or will

[167] P Voigt, A von dem Bussche (n 119) 110.
[168] GDPR, art 9(3).
[169] GDPR, art 4(11).
[170] O Lynskey, *The foundations of EU Data Protection Law* (Oxford University Press 2015)186; In April 2018, WP29 issued the 'Guidelines on consent under Regulation 2016/679' and provided further guidance for the interpretation thereof; see WP29 Guidelines on Consent under Regulation 2016/679, WP259 rev.01, adopted on 28 November 2017, as last revised and adopted on 10 April 2018, p. 7 (hereinafter: WP29 Guidelines on Consent).
[171] This table is part of a previous deliverable, see E Biasin, E Kamenjasevic, 'Deliverable 6.1 – Legal and ethical inventory and in-depth analysis in the Made4You project, EU H2020 grant agreement No. 780298.

	face negative consequences in case he or she does not consent, then consent will not be considered as valid. *Example*: A consent bundled as a non-negotiable part of terms and conditions for of a contract or a registration form in a website may not be considered as 'freely given'.
'Specific'	Consent must be given in relation to one or more specific purposes, in order to provide the data subject with the possibility to choose for each of these. To comply with this element, the controller must: (i) adequately specify each of the purposes for which it will carry out the processing; (ii) apply granularity in consent requests, and (iii) separate the information related to the acquisition of consent for data processing activities from information concerning other matters. *Example*: A unique consent acquired by the controller for different processing purposes may not be considered as specific.
'Informed'	It is fundamental to provide information to the data subject prior to obtaining his or her consent, as that enables him or her to make informed decisions. The GDPR foresees specific information to provide to data subjects prior to obtaining consent. *In practice:* The following information should be provided for obtaining valid consent: 1. Controller's identity 2. Purpose of each processing operation 3. Type of data to be collected and use 4. Existence of the righto to withdraw consent 5. Information about the use of the data for automated decision-making, where relevant 6. Possible risk of data transfers due to absence of appropriate safeguards.
'Unambiguous'	Consent must be given by a statement or a clear affirmative action, e.g. through a written or a recorded oral statement, including by electronic means. It must be obvious that the data subject has consented to the particular processing. *Example*: Pre-ticked boxes or opt-out constructions that require an intervention from the data subject to prevent agreement (e.g. 'opt-out boxes') may not entail the acquisition of an unambiguous consent.
'Explicit'	For the processing of special categories of data (including data concerning health) consent must be provided explicitly. The term 'explicit' means that the person concerned must provide an 'express statement of consent'[172] in form

[172] WP29, 'Guidelines on consent under Regulation 2016/679', Adopted on 28 November 2017 as last revised and adopted on 10 April 2018, p. 18.

	of oral or written statements. However, oral statements may be difficult to prove. *Example:* Consent in form of a written statement; in the digital context: filling in electronic forms, sending an email, uploading a scanned document including the data subject's signature.[173]

Table 1 – Consent requirements under data protection law

It should be recalled that asking for consent is one thing, keeping record of it is another. The data controller has therefore to prove the data subject, in line with the principle of accountability, consented to the data processing.[174] More specifically, it is necessary that the controller not only acquires consent but also keeps track of it. Even if there are no formal requirements, it would nevertheless be advised to ask explicit consent in writing.[175] It is also important to note that consent can be withdrawn by the data subject, and it should be possible to do so as smooth as to give consent.[176]

Employment / social security / social protection

This could refer to social reimbursements of patient visits to the healthcare practitioner. Other examples could include pension regulations, collective work agreements, or taking care of sick or disabled employees.[177]

Preventive or occupational medicine & Provision of healthcare

The GDPR refers here to the patients' rights Directive when defining the concept of personal data concerning health, and more specifically the provision of healthcare services. There, '"healthcare" means health services provided by health professionals to patients to assess, maintain or restore their state of health, including the prescription, dispensation and provision of medicinal products and medical devices'.[178] It basically refers to the access by healthcare professionals to individual's health data for the purpose of their medical treatment.

Reasons of public interest (public health)

In Recital 54 of the GDPR, reference is made to Regulation 1338/2008 for the definition of the concept of public health. There, the definition reads as follows: 'all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, healthcare needs, resources allocated to health care, the provision of, and universal access to, healthcare as well as healthcare expenditure and financing, and the causes of mortality'.[179]

---

[173] ibid.
[174] See GDPR, art 7(1) and WP29, 'Guidelines on consent under Regulation 2016/679', Adopted on 28 November 2017 as last revised and adopted on 10 April 2018, p. 20.
[175] R Jay, 'The principles and grounds for processing' (n 139) 101.
[176] GDPR, art 7(3).
[177] See HR Kranenborg, LFM Verhey, *De Algemene Verordening Gegevensbescherming in Europees en Nederlands* perspectief (Wolters Kluwer 2018) 182.
[178] Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare [2011] OJ L201 (Directive 2011/24), art 3(a).
[179] Council Regulation (EC) 1338/2008 of 16 December 2008 on Community statistics on public health and health and safety at work [2008] OJ L354/70, art 3(c).

Taylor distinguishes between three different aspects in terms of public health protection[180]:

(i) Health protection: This aspect was further dealt with in the section addressing national developments. The topical example would be the communication of a patient's critical status following one dangerous disease.

(ii) Health improvement: This means that using the health related elements could have a positive impact on the patients' health status.

(iii) Public health: This relates to 'the quality, safety, efficacy, effectiveness, value for money, and accessibility of healthcare services'.[181] It should be pointed out that this exception should not be used by insurance companies.[182]

3.2.4. Breach of personal data

A final remark has to be illustrated concerning the GDPR provision with respect to the breach of personal data. In the eventuality of a data breach, the data controller has to notify the breach to the national supervisory authority, within 72 hours. In the case notification would occur later on, reasons would have to mentioned.[183] A data breach is defined by the GDPR as 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'.[184] The data breach has to be notified to the data subject if it 'is likely to result in a high risk to the rights and freedoms of natural persons'.[185] This tight timing is important as risks for personal data would increase as the time passes by. For instance, it induces 'the individual's loss of control over his or her personal data, limitation of the individual's rights, discrimination, identity theft, fraud, financial loss, unauthorized reversal of pseudonymised data, damage to reputation and loss of confidentiality of personal data protected by professional secrecy'.[186] In line with the controller's compliance obligations, he should keep record of the processing activities.

[180] MJ Taylor, 'Legal bases for disclosing confidential patient information for public health: distinguishing between health protection and health improvement' (2015) 23 (3) Medical Law Review 362.
[181] ibid.
[182] R Jay, 'The principles and grounds for processing' (n 139) 104.
[183] GDPR, art 33 and 55.
[184] GDPR, art 4(12).
[185] GDPR, art 34.
[186] J Castro Edwards (n 101) 47.

3.3. Data security mechanisms as a means to ensure confidentiality

The principle of confidentiality is referred to in the GDPR by using two different terms; namely confidentiality and professional secrecy. The notion of confidentiality itself points out to the concepts of data security.[187] As it was already exposed before, confidentiality is one of the principles relating to processing of personal data enshrined in Article 5 of the GDPR. It states that 'personal data shall be: 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')'.[188] Using confidentiality in the data protection debate is one way to address some threats towards the classical concept of confidentiality, with regard to the larger amounts of persons involved in the healthcare process, and the use of data sets for research purposes.[189]

Professional secrecy comes as a tool to guarantee confidentiality. It is referred to as an important tool enshrined in Member State laws in order to safeguard the rights and freedoms of the data subject (e.g., when processing health data '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'). [190] [191] Therefore, we can see that in both privacy matters (ECHR) and data protection (GDPR) national legislations are of importance.

We will first examine the national measures implementing the GDPR with regard to the specific category of sensitive data. Taking into account the digital environment, we will then move to three main mechanisms that could be referred to when talking about data security.

3.3.1. National implementation measures – sensitive data

France

In France, the national requirements for sensitive data are laid down in the framework of the Law of 1978.[192] The French legislator provided the possibility to exceptionally process data concerning health if the data are, within a short period of time, to be subject to an anonymisation procedure. The paragraph requires that the French data protection authority CNIL has earlier approved the anonymisation procedure.[193]

The Netherlands

In the Netherlands, the implementation measures are laid down in the *'Uitvoeringswet Algemene veordening gegevensbescherming'*. Article 30 of the Dutch legislative measure is more detailed

[187] GDPR, art 5(1)(f) and Recitals 49, 75, 83, 85, 162.
[188] GDPR, art 5(1)(f).
[189] See J Nouwt (n 51) 105-106. For the current debate around Big Data, see S Salas-Vega, A Haimann, E Mossialos, 'Big Data and Health Care: Challenges and Opportunities for Coordinated Policy Development in the EU' (2015) 1 (4) Health Systems & Reform 289.
[190] ibid.
[191] GDPR, art 9(2)i.
[192] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[193] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. 'N'entrent pas dans le champ de l'interdiction prévue au I les données à caractère personnel mentionnées au même I qui sont appelées à faire l'objet, à bref délai, d'un procédé d'anonymisation préalablement reconnu conforme aux dispositions de la présente loi par la Commission nationale de l'informatique et des libertés', art 8, III.

that the GDPR. The most pertinent in the SAFECARE context are the measures related to Article 9(2)(h) of the GDPR. As already stated, this article concerns data processing 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'.[194] There, Article 30 of the Dutch measure provides that the healthcare professionals (hulpverleners), and hospitals (instellingen of voorzieningen voor gezondheidszorg) may process health data. The processing must be necessary in order to provide good care to the patient, or to ensure the good administration of the said health institution (het beheer van de betreffende instelling of beroepspraktijk).[195]

It is important to notice that, following Kranenborg and Verhey[196], Article 30 has to be read together with medical confidentiality. This means that, when Article 30 does not apply, the rules of medical confidentiality still have to be taken into account. The authors mention that it has first to be checked whether the information may be disclosed under a medical confidentiality point of view. The next step would then be to examine if the conditions provided by Article 30 are fulfilled. The third step would then be to search for a base in Article 6 GDPR.[197]

Italy

Legislative Decree No 101/2018 (LD 101/2018) is the legal act containing provisions for the adaptation of the GDPR into Italian national legislation.[198] LD 101/2018, has been published on the Italian Official Journal on 4 September 2018 and became effective on 19 September 2018. The Decree implied substantial modifications to the former law concerning data protection in Italy, the so-called Privacy Code.[199]

For what concerns the processing of data concerning health, LD 101/2018 has provided significant changes, notably to Part II ('Principles') and Title VI ('Processing of personal data in the health context') of the Privacy Code. Herein below are reported the main innovative points:

- **Implementation of Article 9(1)(i) GDPR** (Public interest as legal basis for processing personal data in the area of public health): LD 101/2018 introduced a new article in the Privacy Code (art 2-sexies) listing the matters under which data processing put in place by public bodies in the area of public health may be considered of 'public interest' in the meaning of Article 9(1)(i) GDPR. Matters listed therein include, inter alia:

[194] GDPR, art 9 (2)(h).
[195] Uitvoeringswet Algemene Verordening Gegevensbescherming, art 30 (3) (a).
[196] HR Kranenborg, LFM Verhey, De Algemene Verordening Gegevensbescherming in Europees en Nederlands perspectief (Wolters Kluwer 2018) 181.
[197] ibid.
[198] Decreto legislativo 10 agosto 2018, n. 101 Disposizioni per l'adeguamento della normative nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (18G00129) G.U. n. 205 del 4/9/2018 (LD 101/2018).
[199] Decreto legislativo 30 giugno 2003, n. 196 Codice in materia di protezione dei dati personali (recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE)). (GU n.174 del 29-7-2003 - Suppl. Ordinario n. 123).

  - Tasks of the national health service and of the subjects operating in the health sector, as well as duties of hygiene and safety in the workplace and safety and health of the population, civil protection, protection of life and physical safety;
  - Administrative and certification activities related to those of diagnosis, assistance or health or social therapy;
  - Planning, management, control and evaluation of health care, including the establishment, management, planning and control of relations between the administration and the subjects accredited or affiliated with the national health service;
  - Processing operations put in place for purposes of scientific research.
- **Implementation of Article 9(4) GDPR** (Guarantees for the processing of genetic data, biometric data and data concerning health): as implementation of Article 9(4) GDPR, Article 2-septies of the amended Privacy Code clarifies that the processing of genetic, biometric data and data concerning health is allowed if in line with the 'measures of guarantee' set by the applicable **Italian DPA decisions**. It also states that the Italian DPA shall seek the opinion of the Ministry of Health for the adoption of decisions concerning 'measures of guarantee' concerning genetic data and data concerning health for the purposes of prevention, diagnosis and cure of diseases (Article 2-septies(6)).
- Title V of the Privacy code concerning the '**Processing of personal data in the health context'** has been subject to various modifications.
  Worth to report is the amended Article 75 of the Privacy Code. In its actual formulation, the article requires that the processing of personal data for the purpose of data subject's health protection must be made in accordance with Article 9(2)(h) and (i), and Article 9(3) GDPR, article 2-septies of the Privacy Code, as well as in compliance with the specific provisions of the sector. Other amended articles concern the modalities to inform data subject for the processing of personal data (Articles 77-79) and other specific hypothesis entailing the processing of data concerning health within the healthcare context.

3.3.2. Data security mechanisms

Following recital 78 of the GDPR, data protection by design mechanisms imply obligations not only for controllers. It should also be taken into account by 'developers, designers, and service providers'.[200]Article 32 of the GDPR provides that 'processors have a direct obligation to implement appropriate technical and organizational security measures'.[201] This has to be read in combination with Article 5(1)(f) imposing a data security burden on the controller. Both controllers and processors should then ensure the security of the data, taking into account that if there is a severe risk, the safeguards and security measures should be stronger.[202]

The GDPR provides specific suggestion for what type of security measure might be considered by controllers as 'appropriate to the risk', including[203]:

a) the pseudonymisation and encryption of personal data;

[200] L Townsend (n 110) 114.
[201] ibid.
[202] R Jay, L Townsend, 'Security Obligations and Breach Notification' (n 139) 132-133.
[203] GDPR, art 32.

b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

We will focus the analysis on three mechanisms aiming at protecting the data. These are pseudonymisation and its differences with anonymisation; encryption; and data protection by design.

Anonymisation vs pseudonymisation

The concept of anonymisation is heavily debated in the literature. It is also sometimes mixed up with the concept of pseudonymisation. In general, pseudonymisation consists in the replacement of one attribute (normally a unique identifier) in a record by another. This process does not ensure full anonymity and allows to identify the data subject indirectly. This is why pseudonymised data is personal data. By contrast, when data sets are anonymised, i.e. when 'the data subject is not or no longer identifiable',[204] the GDPR does not apply anymore.[205]

Anonymised data represent the following paradox: the concept of anonymisation theoretically ensures the non-applicability of the GDPR, while in practice, anonymization techniques are not effective. This means that there are re-identification possibilities.[206] In this regard, the Article 29 WP issued guidance and advised to examine *in concreto* which technique would be the best to assure anonymity.[207] In practice, difficulties arise as the combination of data sets, perfectly anonymous taken on a separate way, would not be anonymous anymore after this combining process. Also, the GDPR requires that 'all objective factors, such as the costs and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments'.[208]

This is why some authors argue that – following the WP29 recommendations – anonymisation could have 'a significant deterrent effect on the carrying out of beneficial longitudinal research studies that rely upon the reuse of personal data once it has undergone anonymization methods such as in the health or education sectors'.[209] This combination of data sets is likely to increase in the future taking into account the development of the Internet of Health Things and Big Data. Considering the inter connection of data sets, data falling at first glance outside the category of health data could, at a further stage, become health data.[210]

[204] GDPR, Recital 26.
[205] ibid.
[206] P Ohm, 'Broken Promises Of Privacy: Responding To The Surprising Failure Of Anonymization'(2010) 57 (6) UCLA Law Review 1716 and sq.
[207] WP29, Opinion 5/2014 on 'Anonymisation Techniques', WP216, 10 April 2014.
[208] GDPR, Recital 26.
[209] S Stalla-Bourdillon, A Knight, 'Anonymous Data v. Personal Data - False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data' (2016) 34 Wis. Int'l L.J. 299.
[210] See EDPS, Opinion 1/2015, 'Mobile Health, Reconciling technological innovation with data protection', 21 May 2015.

Encryption

Encryption is recognized as one of the mechanisms aiming at guaranteeing the confidentiality of the data. It is described as being able to protect individual's privacy while guaranteeing innovation, or the use of the data.[211] The process of encryption supposes that an information in plain text is converted in a ciphertext, i.e. the information in an encrypted form.[212]

Encryption can be realized at different moments. We will therefore distinguish encryption of data in transit; or encryption of data at rest.[213] One major principle in encryption is that an encryption algorithm 'should be secure if everything is known about it except the key'.[214] This is why we already wish to point out to the SAFECARE partners the need to be cautious when storing the deciphering key, particularly if the storage is taking place in cloud facilities. As it was mentioned at the beginning of this section, the GDPR is referring to the concept of state of the art. This means that the SAFECARE partners should have a look at techniques commonly used and recognized in the field. Nevertheless, these security obligations do not impose an excessive burden on the controllers, as 'the costs of implementation' of these encryption technologies will be taken into account. In any case, partners should be more cautious in the current context as health data is at stake, a specific nature of personal data, requiring a higher level of protection.[215]

Data protection by design

The aim of data protection by design is 'to ensure that, by default, only personal data that is necessary for the specific purpose for which it was collected is processed.'[216] There is therefore a link between the data protection principles guaranteed in Article 5 GDPR, and the technical tools that should be used in order to enhance the protection of the individual's rights.

Recital 78 of the GDPR provides that it entails to 'minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations'.[217]

The concept of data protection by design is enshrined in Article 25 GDPR. The principle's scope is wider than the classical privacy enhancing technologies. It applies 'to business strategies and other organizational practices as well'.[218] Even if data protection by design is linked with accountability, it should nevertheless be recalled that, as in the anonymization debate, privacy

---

[211] G Spindler, P Schmechel, 'Personal Data and Encryption in the European General Data Protection Regulation', (2016) 7 J. Intell. Prop. Info. Tech. & Elec. Com. L. 163-164.
[212] A Tamò-Larrieux (n 130) 109.
[213] A different terminology is sometimes used, referring to encryption of data in transmission, or in storage. See CA Tschider, *International Cybersecurity and Privacy Law in practice* (Wolters Kluwer 2018) 232.
[214] OS Kerr, B Schneier, 'Encryption Workarounds' (2018) 106 Geo. L.J. 993.
[215] See GDPR, Recital 83.
[216] J Castro Edwards (n 101) 41.
[217] GDPR, Recital 78 (own emphasis).
[218] LA Bygrave, 'Data Protection By Design and by Default: Deciphering the EU's legislative requirements' (2017) 4 Oslo Law Review 107.

enhancing technologies can also lead to re-identification.[219] As it seems there is no 'magic' tool aiming at protecting personal data without any remaining risk, an author pointed out the need to 'communicat[e] realistic expectations'[220] of personal's data protection, rather than give the impression of a fully secured environment. There is also uncertainty about the application of the principle. Article 25 GDPR concerns the data controller, whereas Recital 78 addresses the developers of applications. The wording of both provisions are, nevertheless, different. Whereas the controller has to implement 'technical and organizational measures',[221] the IT developer 'should be encouraged'[222] to do so. As already highlighted in the literature by Bygrave, the measures enshrined in Article 25 'might not equate with when a particular data processing device is actually designed and manufactured'.[223]

The European Data Protection Board (EDPB) recently issued guidance on data protection by design.[224] According to EDPB, the obligation of data protection by design has various dimensions. Therefore, four main points should be taken into consideration. Data protection by design should be an aim followed throughout the development of a project. This is tempered by the fact that, considering the risk management approach, the state of the art at the implementation costs will be taken into account. The measures have to be appropriate and effective, i.e. being compliant with the GDPR and protecting individual rights. The safeguards should also be part of the processing activities.

[219] S Wachter (n 118) 285.
[220] ibid.
[221] GDPR, art 25(2).
[222] GDPR, Recital 78.
[223] LA Bygrave, 'Hardwiring Privacy', in R Brownsword, E Scotford, K Yeung (eds), *The Oxford Handbook of Law, Regulation and Technology* (Oxford University Press 2017) 770.
[224] See EDPS, Opinion 5/2018, Preliminary Opinion on privacy by design, 31 May 2018 (hereinafter: 'EDPS Opinion on privacy by design').

4. Protection of critical infrastructures

Main findings of Chapter 4

- The concept of 'Critical Infrastructure Protection' (CIP) and 'Critical Information Infrastructure Protection' (CIIP):
  - CI is being defined as, 'an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions' as per Article 2(1)(a) ECI Directive;
  - CIIP is a subset of a comprehensive protection effort to the CIP and it focuses only on the critical information infrastructure.
- The protection of CI on EU level:
  - The protection of CI is implemented by initiatives and by means of law, namely i) the European Programme for CIP, ii) the CI Warning Network, iii) Directive 2008/11/EC on European CI.
- European Critical Infrastructure (ECI):
  - National CI are a matter of national regulation, whereas only ECI can be embraced under the ECI/EPCIP framework;
  - ECI 'means critical infrastructure located in Member States where the disruption or destruction of which would have a significant impact on at least two Member States. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure' as defined in Article 2(b) Directive 2008/114/EC.

4.1. General remarks

The present section is aimed at providing an overview of the applicable framework for SAFECARE concerning the protection of critical infrastructures and critical information infrastructures (including cybersecurity) with a focus on the healthcare sector.

A first part of this section introduces the concept of critical infrastructure (Chapter 4.2.1) and outlines the difference between the two concepts of 'Critical Infrastructure Protection' (CIP) and 'Critical Information Infrastructure Protection' (CIIP) (Chapter 4.2.1). Further to these introductory sections, it is provided an overview of the CIP European legal framework, so that the main initiatives and pieces of legislation concerning the protection of critical infrastructures at European level are illustrated (Chapter 4.4). Chapter 7.5 questions the application of such framework within the healthcare sector.

Section 8 will be instead devoted to the illustration of the European framework concerning the protection of network and information systems (NIS Directive). The illustration of such framework will further comprehend a brief explanation of national legislations having

implemented the NIS Directive in their respective legal systems (Chapter 5.2). Specific focus is again put on France, the Netherlands and Italy, where the SAFECARE project field trials are going to take place.

4.2. Critical Infrastructure protection and Security: preliminary considerations for SAFECARE

> '*Over the last decade the European Union has faced numerous threats that quickly increased in their magnitude, changing the lives, the habits and the fears of hundreds of millions of citizens. The sources of these threats have been heterogeneous, as well as weapons to impact the population. Threats have demonstrated to be not only physical but also cyber and therefore the lines between physical and cyber worlds are increasingly blurred. Nearly everything is connected to the Internet and if not, physical intrusion might rub out the barriers. Threats cannot be analysed solely as physical or cyber, and therefore it is critical to develop an integrated approach in order to fight against such combination of threats*'. [225]

The passage reported above is retrieved from the SAFECARE project outline. These lines depict how threats to infrastructures – especially those which may be considered as 'critical' – need to be protected by attacks (which may be physical or cyber ones). To this extent, the purpose of the SAFECARE project is to serve the objective **of protection of critical infrastructures from physical and cyber-attacks**, with a focus on healthcare environments and in particular on hospitals. SAFECARE aims at providing solutions for the improvement of physical and cyber security in a seamless and cost-effective way. [226]

Having such premised, it is of importance for the purposes of the SAFACARE project to provide an outline concerning the legal framework on critical infrastructure protection and provide some observations with regard to the sector of healthcare.

4.2.1. Definition of the concept of Critical infrastructure

Critical Infrastructures are essential services for the security and well-being of citizens. Without an adequate level of CI protection, serious consequences would be entailed for society, as society itself is dependent on their continuous functioning. Indeed, modern society is characterised by a strong interdependency between processes, resources and the correct functioning of infrastructural systems, whose interruption, damage or unavailability may cause economic damages for the society, and may imply dominos effects also in the provision of services and social development.[227] Critical infrastructures are vulnerable: it is important to ensure an adequate level of protection and to limit as far as possible any detrimental effects of disruptions.

Infrastructures are considered 'critical' when their disruption could have an impact on the functioning of the society (in terms of economy, security and people's wellbeing). According to EU law, a critical infrastructure is 'an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or

[225] See CORDIS website, SAFECARE project outline on <https://cordis.europa.eu/project/rcn/214348/en>.
[226] ibid.
[227] See SM Rinaldi, JP Peerenboom, and TK Kelly, '*Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies*' [2001] IEEE Control Systems Magazine 11.

social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions'.[228]

4.2.2. Critical Infrastructure v Critical Information Infrastructure

Before outlining the relevant legal framework concerning the protection of critical infrastructure and the related cyber security aspects, it is also important to draw a distinction between two concepts – that may be seen as interchangeable but that still have a slightly different meaning – often in use in the matter of critical infrastructure protection: **Critical Infrastructure (CI) and Critical Information Infrastructure (CII)**.

In order to set a clear distinction between the two terms, it is worth to highlight what follows. Critical Infrastructure Protection (CIP) is meant to comprise all critical sectors of a nation's infrastructures, whereas Critical Information Infrastructure Protection (CIIP) has to be seen as only a subset of a comprehensive protection effort and it is focused only on the critical information infrastructure.[229] CIIP has to be seen as a part of the overall CI protection. Critical infrastructures are a combination of two elements: i) the physical element, which is easily conceptualised as the physical structure itself (or part thereof), and ii) the intangible element, which refers the information or data stored on or in the physical element.

As illustrated above, a sole focus only on one of these categories of protection might not be enough for ensuring the protection and security of critical infrastructures. The legal framework needs to be assessed in a holistic manner in order to adequately assess the applicability of the relevant legislative instruments. This deliverable refers to CIP as including CIIP. Any variation will be expressly noted.

4.3. Critical Infrastructure Protection and the European legal framework

The protection of critical infrastructures is a topic that has been under debate since the early 2000s, after major terrorist events took place in the U.S. and in Europe. The occurrence of these circumstances underlined the asymmetry between risks and vulnerabilities of industrial society.

In the wake of these events, EU governments started to question how to enhance the protection of national and European critical assets, in order to mitigate the potential knock on effects or any disruption they could cause to the society. In 2004, the protection of critical infrastructures became a topic on the political agenda of the European Union as the European Council asked for the preparation of an overall strategy to protect critical infrastructures. On 20 October 2004, the Commission adopted the Communication on critical infrastructures protection in the fight against terrorism.[230] The Communication proposed the creation of an **European Programme for Critical Infrastructure Protection** and the establishment of a network – the **Critical Infrastructure Warning Network** (CIWIN) – 'to assist Member States, EU Institutions, owners and operators of critical infrastructure to exchange information on shared threats, vulnerabilities and appropriate measures and strategies to mitigate risk in support of critical infrastructure

[228] The definition provided herein is set by art 2(1)(a) of the ECI Directive (see Chapter 4.3.3 for a more detailed overview).
[229] M Dunn, 'Understanding Critical Information Infrastructures' in M Dunn and V Mauer (eds) *International CIIP Handbook 2006 vol II* (Center for Security Studies at ETH Zurich, 2006).
[230] Communication from the Commission of 20 October 2004 on Critical Infrastructure Protection in the Fight against Terrorism COM(2004) 702 final [2004].

protection'[231]. With Communication n 786 of 2006[232], the Commission established the EPCIP and outlined the principles and necessary tools to take into account for the implementation of the European Programme for the Protection of Critical Infrastructures.[233]

On 8 December 2008, the Council of the European Union adopted the **Directive 2008/11/EC** on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.[234]

The following sections are devoted to the further illustration of the key initiatives and pieces of legislation of the European legal framework on critical infrastructure protection, and namely:

1) The European Programme for Critical Infrastructure Protection (Chapter 4.3.1)
2) The Critical Infrastructure Warning Network (Chapter 4.3.2)
3) Directive 2008/11/EC on European Critical Infrastructures (Chapter 4.3.3)

4.3.1. European Programme for Critical Infrastructure Protection (EPCIP)

The European Programme for Infrastructure Protection has been launched in 2006 with the objective of improving the protection of critical infrastructures in the EU.
Communication n 786 of 2006 – which originated the EPCIP – established the following guiding principles for the Programme:

- **Subsidiarity**. While the EU principle of subsidiarity safeguards critical infrastructures as a national matter, it establishes that the EU should 'focus on infrastructure that is critical from a European, rather than a national or regional perspective'.[235]
- **Complementarity**. Within the EPCIP, the duplicating of existing efforts – whether at EU, national or regional level – should be avoided where these have proven to be effective in protecting critical infrastructure. EPCIP has to complement and build on sectoral measures and it should take into account best practices also developed at country-level.
- **Confidentiality**. This principle requires that information related to critical infrastructure protection must be classified and restricted in access both at EU and Member State levels. Information sharing regarding CI must take place in an environment of trust and security.
- **Stakeholder cooperation**. All relevant stakeholders should be involved in the development and implementation of EPCIP, including the owners/operators of critical infrastructures designated as ECI as well as public authorities and other relevant bodies.
- **Proportionality**. EU measures and regulations must only emerge where security gaps are identified. In light of the proportionality principle, these measures will at all times be balanced against the seriousness and nature of the associated threat.

[231] ibid.
[232] Communication from the Commission on a European Programme for Critical Infrastructure Protection COM (2006) 786 final [2006].
[233] Communication from the Commission of 20 October 2004 on Critical Infrastructure Protection in the Fight against Terrorism COM(2004) 702 final [2004].
[234] Council Directive 2008/11/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection [2008] OJ L345/75 (ECI Directive).
[235] COM 2006 (786) 3.

- **Sector-by-sector approach**. With this principle, the European Commission established the need for tailored and customised CIP, on a sector-by-sector basis.

4.3.2. Critical Infrastructure Warning Information Network

The CIWIN is an initiative which aims at improving the protection of critical infrastructures in the Union and in all relevant sectors of economic activity. The CIWIN provides a public information and communication system. It offers to its members the opportunity to exchange CIP-related information, serving also as internet portal to exchange ideas, studies and good practices in the field and as a repository for CIP information. As illustrated in the Impact Assessment of a Council Decision on the creation of CIWIN[236], its scope is to enable co-ordination and co-operation on information on the protection of critical infrastructure at EU level, ensuring secured and structured exchange of information and allowing its users to learn about best practices in other EU Member States in a fast and efficient way.

4.3.3. Directive 2008/11/EC

Directive 2008/114/EC is the most important piece of the European legislation concerning the physical protection of critical infrastructures. The primary objective of the Directive is the establishment of 'a procedure for the **identification and designation of European Critical Infrastructures (ECI)** and a common approach to the assessment of the need to improve the protection'[237] thereof. The ECI Directive focuses on protection of *European* Critical Infrastructures, meaning the identification and protection of national Critical Infrastructures that only affects one Member State remain outside the scope of the Directive.

The Directive follows a **sectorial scope** and proposes a focus ('priority') only to the energy and transport sectors. Further observations concerning the notion of critical infrastructures, the ECI Directive and national legislations with respect to the health sector are provided below (Chapter 4.4.1).

The focus on the ECI Directive is nevertheless of importance as it constitutes a first common piece of legislation for Member States concerning critical infrastructures. Indeed, as outlined above, the Directive represented a first step for an European definition of 'Critical Infrastructure', i.e. according to Article 2(a) thereof, an 'asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions'.

The ECI Directive provides minimum common standards for EU Member States as the matter is regulated at national level. Hence, the ECI Directive has been transposed into every Member States' legal systems via national legislations.

The key points foreseen by the ECI Directive are as follows:

[236] Commission Staff Working Document Accompanying document to the Proposal for a COUNCIL DECISION on creating a Critical Infrastructure Warning Information Network (CIWIN) {COM(2008) 676 final} {SEC(2008) 2702} IMPACT ASSESSMENT.
[237] ECI Directive, art 1.

- Member States have to identify and designate each European Critical Infrastructure on their territory, having regard to the harmonised 'cross-cutting' and 'sectorial' criteria listed thereby.[238]
- Member States must appoint a 'European critical infrastructure protection contact point' (or **ECIP contact point**) in charge of coordinating, within the Member State, the protection of critical infrastructure and to exchange on those matters with other Member States and the European Commission.[239]
- Without prejudice to rules adopted by the Member State to protect critical infrastructures, the ECI Directive requires the setting up in each designated ECIs of a '**Operator Security Plan'** (OSP).[240] The OSP consists of internal rules for the protection of the critical infrastructure and it must be based on risk analysis. The OSP identifies the critical infrastructure assets and the security solutions in place or to be implemented.[241]
- Also, each ECI shall have designated a '**Security Liaison Officer**', whose function is to communicate, when appropriate, with the competent public authority.

The ECI Directive represents an important outcome for the protection of critical infrastructures in Europe. However, it has to be noted that:

- The subsidiarity principle requires that every Member States autonomously regulates on National CIPs; and that
- the 'primary and ultimate responsibility for protecting ECI falls on the Member States and owners/operators of such infrastructures'.[242]

Hence, the ECI Directive does not contain specific and substantive measures to be taken into account by Member States in order to protect critical infrastructures, as these fall within the competences of Member States and in a second stance, within the authority of the operator of the European critical infrastructure as part of its OSP.

Finally, it has also to be noted that the ECI Directive does not provide detailed provisions on **confidentiality for security-related information**, as it is under the competence of Member States to regulate on these. Nevertheless, it requires that 'Member States, the Commission and relevant supervisory bodies shall ensure that sensitive European critical infrastructure protection-related information […] is not used for any purpose other than the protection of critical infrastructures'.[243]

4.4. Further considerations in terms of Critical Infrastructure Protection on national and EU level

4.4.1. Critical Infrastructures and European Critical Infrastructures

As substantiation of the principles of EU sovereignty and subsidiarity, it has to be underlined **that only systems classified as European CI (ECI) can be embraced under the ECI/EPCIP**

[238] ECI Directive, art 3.
[239] ECI Directive, art 10.
[240] ECI Directive, art 5.
[241] ibid.
[242] ECI Directive, Recital 6.
[243] ECI Directive, art 9.

framework. The protection of National Critical Infrastructures – inasmuch not falling within the definition of ECI – are subject to **national regulation**.

In order to provide further clarity, it is reported thereunder the definition of ECI, as enshrined in Article 2 (b) of Directive 2008/114/EC: '"European critical infrastructure" or "ECI" means critical infrastructure located in Member States where the disruption or destruction *of which would have a significant impact on at least two Member States*. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure.'

Aside from the ECI identification issue, the definition and identification of critical infrastructure at Member State level is not harmonised. The current trends followed by Member States include definition of critical infrastructure based on defence strategies, national emergency management and long term national traditions. The section that follows aims at illustrating critical infrastructure protection with specific regard to the sector of healthcare.

4.4.2. Critical Infrastructures and the healthcare sector

Before illustrating the national strategies for the protection of critical infrastructures with respect to the healthcare sector, some preliminary distinctions need to be made. Firstly, it is of importance to further stress a distinction for the protection of critical infrastructures between the European level and the national level.

European level

At European level, as illustrated above, it is necessary to take into account the ECI Directive as well as the EPCIP further guidance on this matter.[244]

Concerning the ECI Directive, it foresaw transport and energy as the priority sectors under which there should have been harmonisation within MS concerning ECI. Any other specific sector was not taken into consideration for these purposes. However, the ECI Directive provided that the same 'should be reviewed with a view to assessing its impact and the need to include other sectors within its scope, inter alia, the information and communication technology ('ICT') sector.[245]

Some experts pointed out[246] that the result of the ECI Directive should have been regarded as a temporary result, a compromise that has been reached at EU level in order to reach as fast as possible a common strategy among Member States for the protection of critical infrastructures.

Concerning on the one hand the EPCIP and the guidance documents issued by the same, it has to be noted that it outlined the necessity to protect also other sectors concerning the critical infrastructures.

---

[244] Commission Staff Working Document on the ex post evaluation of the 'Prevention, Preparedness and Consequence Management of Terrorism and other Security related risks" 2007-2013 Programme (CIPS) Accompanying the document Report from the European Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions ex post evaluation for the period 2007 to 2013 of actions financed by the 'Prevention and fight against crime' programme (ISEC) and the 'Prevention, Preparedness and Consequence Management of Terrorism and other Security related risks' programme (CIPS) SWD(2018) 331 final Annex 8.

[245] ECI Directive, Recital 5.

[246] Luisa Franchina, 'Le infrastrutture critiche nazionali ed Europee' [2012] Quaderno n. 3 I quaderni del Network AIAS 1, 15.

The table reported hereinafter illustrates how the substantial difference in the identification of sectors relevant for the protection of critical infrastructure from the ECI and the EPCIP. The sectors highlighted in blue are the sectors taken into consideration both by the ECI Directive and by the EPCIP. The other sectors are on the contrary contemplated only by the EPCIP.

Critical Infrastructures Sectors in EU
Energy
Transport
Nuclear industry
Information communication technologies (ICT)
Water
Food
Health
Financial
Chemical industry
Space and research facilities
Other sectors (incl. government)

Table 2 - Critical Infrastructure Sectors in EU. Elaboration from ECI Directive and EPCIP SWD(2018) 331 final

Member States

As outlined above, in the light of the subsidiarity principle **Member States are primarily responsible for the definition and identification of national critical infrastructures and their respective sectors**. In the light of previous researches in the field[247], it appears that the status of harmonisation concerning the physical protection of critical infrastructure across the EU is disparate, including the specific sector of the healthcare. With specific regard to National strategies for CIP protection and their inclusion/contemplation of the healthcare sector, for France, the Netherlands, and Italy it may be observed as follows:

- France: according to the French Defence Code ('*Code de la Défense*')[248] are considered as critical all infrastructures that are vital for the maintenance of the social and economic progress. The French government identified 12 sectors for critical infrastructures within 3 macro-areas.[249] Health care is included in these.
- The Netherlands: Before 2015, the healthcare sector was expressly listed in the 12 critical sectors as identified by the Ministry of the Interior and Kingdom Relations of the Netherlands.[250] In 2014 the critical infrastructure framework of the Netherlands was

[247] See THREATS, 'An Analysis of Critical Infrastructure Protection Measures Implemented within the European Union: Identifying which European Member States includes the Health Sector as part of Critical National Infrastructure and which facets of Health Infrastructure are considered Critical' [2014] Report No: DR/1/001 <http://www.threatsproject.eu/WP1%20D1%20final.pdf >.
[248] Ordonnance n° 2004‐1374 du 20 décembre 2004 Code de la Défense.
[249] Arrêté du 2 juin 2006 fixant la liste des SAIV et les ministres coordonnateurs.
[250] See E Luiijf, H Burger, M Klaver, 'Critical Infrastructure Protection in the Netherlands: A quick-scan', in U E Gattiker (ed), *EICAR Best Paper Conference Proceedings,* EICAR 2003.

reviewed.[251] The review has led to a 'shift from critical sectors to critical processes, as not all processes in a sector are critical'.[252] Therefore, the current focus has been moved from 'sectors' to critical 'processes'. The Ministry of Justice and Security of the Netherlands provided a comprehensive list of critical processes of the Netherlands. In such list, sectors associated with critical processes have not been put in direct association to the 'healthcare' sector.

- Italy: Italy has put in place initiatives and legislations for the protection of CI and CII with regard to the healthcare sector.[253] [254] Worth to report in particular the national and regional legislation concerning civil protection with respect to 'sanitary risk activities'.[255]

[251] Ministry of Justice and Security of the Netherlands, 'Review of policy on critical infrastructure' < https://english.nctv.nl/topics_a_z/critical_infrastructure_protection/review_policy_critical_infrastructure.aspx>.
[252] ibid.
[253] ibid 43.
[254] G di Matteo, 'Infrastrutture Critiche: Prospettive Nazionali ed Europee per la Creazione di uno Spazio di Liberta', di Sicurezza e di Giustizia [2008] 43.
[255] For an extensive overview of national and regional acts and regulations, see Protezione Civile, 'Attività rischio sanitario' <http://www.protezionecivile.gov.it/jcms/it/attivita_sanitario.wp>.

5. Protection of Network and Information Systems

Main findings of Chapter 5

- The objective of the NIS Directive:
  - The main objective of this Directive is to provide cyber protection for critical infrastructures;
  - The Directive provides a minimum harmonisation with a margin for Member States to develop further requirements on a national level;
- Operators of essential services:
  - Operators of essential services are public or private entities that have to be identified by every Member States, occurring the criteria identified by Article 4(4) NIS Directive;
  - In France, healthcare practitioners and practitioners involved in urgent care are being considered as operators of essential services;
  - In the Netherlands, the healthcare sector is not being considered as an operator of essential services, however, it is being regulated by norms;
  - In Italy, healthcare providers are being considered as operators of essential services.
- Member States have to develop national strategies on the security of network and information services.

5.1. General remarks

The protection of critical infrastructures passes through a physical as well as a cyber-perspective. As noted also above, the cyber-perspective is becoming more important for the protection of critical infrastructures. Through the protection of network and information systems, the European legislator set up a common framework (primarily to be regarded in the NIS Directive[256]) for the cyber protection of (also) critical infrastructures.[257] To such extent, the EU framework concerning the protection of network and information systems is provided in the following sections and by taking into account the French, Dutch and Italian legislations.

5.1.1. The scope of the NIS Directive

The NIS Directive represents the main piece of legislation ascending from the '2013 EU Cybersecurity Strategy'[258]. The NIS Directive represents the cornerstone of the EU's efforts to find

[256] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L194/1 (NIS Directive).
[257] It is worth to note, hence, that art 1(4) of the NIS Directive states that the directive 'applies without prejudice to Council Directive 2008/114/EC'.
[258] Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace [2013] JOIN(2013) 1 final.

a harmonised framework for cybersecurity among Member States. To such purpose, it introduces rules on the security of networks and information systems within sectors of essential services and digital services.

The aim of the NIS Directive is to[259]:

a) lay down obligations for all Member States to adopt a **national strategy on the security of network and information systems**;
b) to establish **security and notification requirements for operators of essential services** and for digital service providers;
c) create a **Cooperation Group** in order to support and facilitate strategic cooperation and the exchange of information among Member States;
d) to create a computer security incident response teams network (**CSIRT network**) to promote swift and effective operational cooperation between Member States;
e) to lay down obligations for Member States to **designate national competent authorities**, single points of contact and CSIRTs with tasks related to the security of network and information systems.

The Directive aims at a minimum harmonisation, allowing for stricter rules to be adopted at a national level. Member States had to transpose the Directive into their national legislative framework before 9 May 2018.

Some preliminary definitions are listed hereunder in order to provide more clarity to the illustration of the key points of the NIS Directive in the following section.

Network and information system	Network and information system means[260]: a) an electronic communications network within the meaning of point (a) of Directive 2002/21/EC[261] b) any device or group or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data c) digital data stored, processed, retrieved or transmitted by elements under points (a) and (b) for the purposes of their operation, use, protection and maintenance
Security of network and information systems	The security of network and information systems has to be intended as the 'ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the

[259] NIS Directive, art 1.
[260] See NIS Directive, art 4(1).
[261] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications network and services [2002] OJ L108 (Framework Directive), see art 2(a): 'electronic communications network means transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed'.

	related services offered by, or accessible via, these network and information systems'.[262]
Operators of essential services	Operators of essential services are public or private entities[263] that have to be identified by every Member States, occurring the criteria identified by Article 4(4) of the NIS Directive. According to such article, private or public entities may be identified as operators of essential services on the condition that and in so far as they (1) provide a service 'which is essential for the maintenance of critical societal and/or economic activities' which (2) 'depends on network and information systems' where (3) an incident on the later would have a 'significant disruptive effect of the provision of that service'. Annex II of the NIS Directive lists the 'Types of entities' for the purposes of Article 4(4) of the Directive, which are classified per 'Sectors' and 'Subsectors'. The **health sector** is expressly mentioned (point n. 5) and it is declined in one subsector, ie 'Health care settings (including hospitals and private clinics)'. The type of entity considered as essential services operators are 'Healthcare providers as defined in point (g) of Article 3 of Directive 2011/24/EU of the European Parliament and of the Council'.[264]

5.1.2. An overview of the NIS Directive

National strategy on the security of network information systems

One of the main objectives of the NIS Directive is the requirement for Member States to adopt a '**national strategy** on the security of network and information services defining the strategic objectives and appropriate policy and regulatory measures'[265]. The Directive lists the key points to be tackled within the single national strategies, and Member States have been provided with large room of manoeuvre for their design.

Member States had to transpose the NIS Directive by 9 May 2018. An overview of the implementation acts of the NIS Directive in France, the Netherlands and Italy is provided in Chapter 5.2.

Security and notification requirements for operators of essential services

As outlined above, the NIS Directive provides the minimum body of rules that Member States must impose on operators of essential services. The NIS Directive foresees several requirements which apply to the operators of essential services. Accordingly, the Directive foresees that Member States shall ensure that operators of essential services:

1. **'Take appropriate and proportionate technical and organizational measures to manage the risks posed to the security of network** and information systems which

[262] NIS Directive, art 4(2).
[263] See also NIS Directive, art 4(4).
[264] Directive 2011/24, art 3: [healthcare provider] 'means any natural or legal person or any other entity legally providing healthcare on the territory of a Member State'.
[265] NIS Directive, art 2(2)(a).

they use in their operations' **according to the risk posed** and 'having regard to the state of the art'.[266]

2. 'Take appropriate measures to **prevent and minimise the impact of incidents** affecting the security of the network and information systems used for the provision of such essential services, with a view of continuity of those services'.[267]
3. **Notify, without undue delay**, the competent authority or the CSIRT of any occurred incident having a significant impact on the continuity of the essential services they provide.[268]

These legal provisions require the adoption by operators of essential services of a **risk management approach**. The scope of risk management is defined in the Directive and it may include the identification, prevention, detection and handling of risks as well as mitigation of their impact.[269] Notably, security have to be contemplated with regard to all operations relating to data – storage, transmission and processing – and operators of essential services shall ensure the security of the network and information systems 'which they use in their operations'.[270] The risk management measures shall be taken by the operators of essential services with a view to the continuity of their services.[271]

Concerning the first and second points, it has to be noted that the Directive does not provide a list of security measures to comply with. The regulation of security measures falls within the competences of Member States and – depending on the transposition of the Directive in their national legislations – the operators of essential services themselves.

Concerning the third point, the Directive specifies that the obligation for operators of essential services to notify the competent authority or the CSIRT must concern incidents 'having a significant impact on the continuity of the essential services'[272]. In order to assess whether incidents have a *significant impact* on the continuity of the essential services, the following parameters have to be taken into consideration[273]:

- the number of users affected by the disruption of the essential service;
- the duration of the incident;
- the geographical spread with regard to the area affected by the incident.

Finally, it is worth to underline that the NIS Directive, while it provides for a duty to notify on the part of the operators and further incentivises Member States and relevant operators to exchange information on security incidents, it acknowledges **national regulation on secrecy of cybersecurity information to be held by operators and/or by Member States**.

Strategic cooperation and the exchange of information among Member States

The strategic cooperation between national and European authorities enshrined by the NIS Directive establishes **ENISA** at its core. ENISA is the European Union Agency for Network and

[266] NIS Directive, art 14(1).
[267] NIS Directive, art 14(2).
[268] NIS Directive, art 14(3).
[269] NIS Directive, Recital 46.
[270] NIS Directive, Recital 52.
[271] NIS Directive, art 14(2).
[272] NIS Directive, art 14(3).
[273] NIS Directive, art 14(4).

Information Security. It provides guidance and advice to the European Commission, Member States and private actors with regard to technical security standards and it coordinates and supports cooperation among the national authorities at European level.

Also, the NIS Directive aims at establishing a network of 'computer security incident response teams' (CSIRT) composed of representatives of the Member States CSIRT and CERT-EU 'in order to contribute to the development of trust and confidence between Member States and to promote swift and effective cooperation'[274].[275] Every Member State is required to 'designate one or more CSIRTs, as foreseen and further detailed in Article 9 and Article 12 of the NIS Directive.

Finally, the Directive thereby establishes a **Coordination** Group, 'in order to support and facilitate strategic cooperation and the exchange of information among Member States […] and with a view to achieving a high common level of security of network and information systems in the Union'[276].

Identification of the competent authority

The implementation and enforcement of the NIS Directive is delegated to the monitoring by the **'competent authorities'** as identified by every Member State.[277] Member States are required to designate 'one or more national competent authorities on the security and information systems' which have the role to monitor the application of the Directive at national level.[278]

Member States have to provide to the competent authority the powers and means to require essential operators to provide:

- the necessary information to assess the security, including documented security policies; and
- the 'evidence of the effective implementation of security policies' within the operator of essential services (e.g., the results of a security audit carried out by the competent authority or a qualified auditor).

Competent authorities may work in cooperation with data protection authorities when addressing incidents resulting in personal data breaches.

Also, Member States have to identify a '**single point of contact'** on the security of network and information systems. These figures will have a 'liaison function' to ensure cross-border cooperation of Member State authorities and with the relevant authorities in other Member States as well as with the Cooperation Group and the CSIRT network (see point iii. above).

5.2. National implementations

The NIS Directive foresees that 'Member States shall adopt and publish by 9 May 2018, the laws, regulations and administrative provisions necessary to comply with'[279] the Directive and should apply such measures as from 10 May 2018.[280]

[274] NIS Directive, art 1(2)(c).
[275] NIS Directive, art 1(2)(c), art 12 (2).
[276] NIS Directive, art 11.
[277] NIS Directive, art 15.
[278] NIS Directive, art 8(2).
[279] NIS Directive, art 25(1).
[280] NIS Directive, art 25(2).

The present section is devoted to the illustration of the actual status of the NIS Directive transposition in the following Member States: France, the Netherlands, Italy.

5.2.1. France

Security of the information systems are defined by the French legislator as the ability to resist, at a certain confidence level, to actions compromising the availability, authenticity, integrity or confidentiality of the stored data, communicated or processed, and the related services offered by or accessed through these information systems.[281] Fines relating to the non-compliance with these provisions range from 50.000 to 100.000€.[282]

When transposing the NIS Directive, the French legislator choses to define healthcare practitioners (‘*prestataires de soins de santé’*) and practitioners involved in urgent care (prestataires fournissant un service d’aide médicale d’urgence) as operators of essential services. Both public and private hospitals or private medical clinics are concerned. The specific activities are, for the healthcare practitioners: a service in relation with prevention, diagnostic, or care. For the practitioners in a situation of urgency, it concerns the management of phone calls, as the mobile urgency service and resuscitation.[283]

The French legislator adopted a set of 23 Rules aiming at ensuring the protection of these network information systems. These rules will have to be complied with from the moment when the ‘operator of essential services’ – e.g. hospitals – are categorized as such by a Prime Minister’s decree (*‘Arrêté du Premier Ministre*’). This classification will be notified to the concerned parties.[284] The security rules read as follows: 1- Risk analysis; 2- Security policy; 3- Security homologation; 4- Indicators; 5- Security audits; 6- Cartography; 7- Configuration; 8- Partitioning; 9- Remote access; 10- Filtering; 11- Administrator accounts; 12- Administration information’s systems; 13- Identification; 14- Authentication; 15- Access rights; 16- Procedure relative to security conditions; 17- Physical and environmental security; 18- Detection; 19- Logging; 20- Correlation and analysis of the logs; 21- Incident’s response; 22- Treatment of the alerts; 23- Crisis behaviour. The content of these rules is very technical. The aim of the following lines is to precise in a synthetic way the content of each of these.

Part1. Security on the networks and information systems

Rule 1. Risk Analysis

[281] Art. 1. LOI n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité ,art 5; Annex 1 Décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique, PRESTATAIRES DE SOINS DE SANTÉ → Service concourant aux activités de prévention, de diagnostic ou de soins; PRESTATAIRES FOURNISSANT UN SERVICE D'AIDE MÉDICALE D'URGENCE → Réception et régulation des appels Service mobile d'urgence et réanimation.
[282] ibid, art 15.
[283] NIS Directive, art 4(4), Annex 1 Arrêté du 14 septembre 2018 fixant les règles de sécurité et les délais mentionnés à l'article 10 du décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique.
[284] Décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique, art 3.

The operator of essential services has to perform and update a risk analysis of its essential information systems. Important is to show the kind of analysis performed, in order to identify the systems as an essential information system.

Rule 2. Security policy

The operator of essential services has to create, update, and execute a security policy regarding networks and information systems. This policy has to describe the procedures and the organisational and technical means employed by the operator in order to guarantee the security of these essential information systems. Further precisions are developed regarding security governance, protection, defence, or activities' resilience.

Rule 3. Security homologation

The operator of essential services proceeds to the security homologation of each essential information system. He uses the homologation procedure described in its security policy. The decision to homologate is a formal decision adopted by the operator. It shows that the risks impacting the system's security have been identified and that the necessary measures were adopted to protect it. It also shows that the remaining residual risks were identified and accepted by the operator. The homologation procedure has to be read together with Rule 5 related to security audits. Further precisions are developed concerning the decision to homologate, and the related conditions.

Rule 4. Indicators

The operator of essential services evaluates and holds up to date a range of measures ('*indicateurs*'). These are very technical and concerns elements related to the kind of user accessing the information, the characteristics of the infrastructure (is it still supported).

Rule 5. Security audits

A security audit has to be realized for each essential information system. The aim of this audit is to control the effectivity of security measure and the compliance with these rules in each system.

Rule 6. Cartography

The operator of essential services has to collect and keep up to date the following elements for each essential information system, such as the installed applications, IP addresses, network descriptions (access points, interconnection with other networks), IT architecture, a listing of the accounts with extended access rights.

Part2. Protection of networks and information systems. (*Protection*)

Rule 7. Configuration

The operator of essential services has to follow a series of rules when installing services and equipment's on essential information systems. These include disabling additional features; dealing with other devices with caution (the connection of these devices has to be indispensable for the functioning or security of the essential information systems. External storage may only be used for operational, maintenance, administration or security purposes).

Rule 8. Partitioning

When partitioning the different essential information systems, attention is paid at limiting the interconnection of these EIS in order to prevent harm.

Rule 9. Remote access

Remote access systems have to be protected. If the system has to be accessed via public network, encryption tools have to be developed in order to protect the communication. The standards of the national agency on security of information systems[285] should be followed.

Rule 10. Filtering

The operator of essential services has to create mechanisms filtering the data flows in order to prevent unnecessary flows, susceptible to increase the likelihood of hacking.

Rule 11. Administrator accounts

When creating accounts with administrator rights, the operator of essential services has to limit the scope of these rights to an access that has to be strictly necessary. These rights will be adapted depending on the specific tasks the administrator has to deal with. Administration tasks should be performed using these administrator accounts. If a technical error occurs, having as a consequence that administration tasks would be exercised from another kind of account, this should be logged.

Rule 12. Administration of information systems

This rule aims at describing the rules that have to be followed concerning hardware and software solutions. It is again highlighted that when these resources are used for administration purposes, these have to be used only for administration.

Rule 13. Identification

Each user should have a distinct account, allowing for traceability. If this is not possible for technical reasons, additional measures should be taken in order to reduce the risks associated with shared accounts.

Rule 14. Authentication

The authentication process implies the existence of a secret element. Further precisions are outlined concerning the modification and renewal of this secret element, for instance when the machines are equipped with standard security tools. Whether the security mechanism used is a password, these have to comply with the state of the art as recognized by the National agency for the security of information systems.

Rule 15. Access rights

Access rights are granted in the case it is strictly necessary for accomplishing the user's tasks. Access rights have to be periodically reviewed by the operator, at least each year.

Rule 16. Procedure relative to security conditions

[285] Agence nationale de la sécurité des systèmes d'information.

This procedure aims at guaranteeing a security level of the essential information systems, taking into account the threat's evolutions. The operator has to verify the position of the Governmental centre on cyberattacks[286] on the current threats.

Rule 17. Physical and environmental security

These measures are conducted by the operator of essential services taking into account its global security policy for networks and information systems. It relates to situations such as the control of employees, physical access controls, and environmental protection such as natural disasters.

Part3. Protection of networks and information systems. (*Défense*)

Rule 18. Detection

A procedure aiming at detecting security incidents has to be developed, encompassing both organizational as well as technical measures.

Rule 19. Logging

The logging process will concern who authenticates, which access levels the individuals have, which resources, the functioning of the essential service of information, and will log any modification of the security rules. It has to be stored for at least 6 months.

Rule 20. Correlation and analysis of the logs

This correlation system aims at detecting security incidents, by analysing log details. It is ran on a separate computer, only used for these purposes.

Rule 21. Incident's response

A procedure concerning the processing of security incidents has to be elaborated. Specific requirements have to be followed.[287] A specific information system has to be created in order to deal with the incidents.

Rule 22. Treatment of the alerts.

The legal provision foresees that the hospital has to hold a service responsible for the exchange of information with the national agency involved with the security of information systems and take the appropriate measures. The hospital will also have to share information related to this service (name, phone and email contacts).

Rule 23. Crisis behaviour

A procedure has to be elaborated in order to be able to face security incidents impacting widely the essential services. This has to be in concordance with the global security policy for networks and information systems.

5.2.2. The Netherlands

[286] CERT-FR (centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques).
[287] See référentiel en matière de réponse aux incidents de sécurité pris en application de l'article 10 du décret n° 2015-350 du 27 mars 2015.

The Dutch legislator did not classify the healthcare sector as an operator of essential services.[288] The kind of norms governing these matters in the Netherlands is therefore different, as there are normalisation norms issued by the NEN.[289] NEN is a private organization shaping conformity norms.

If these norms have to be complied with (i.e. when the legislator requires doing so) then these are freely available on the NEN Connect platform.[290] The aim of the following lines is not to provide an extensive overview on the NEN norms. The developments would be too far reaching. Pointing out some key concepts in the four main NEN instruments pertinent for the SAFECARE project will allow the partners to have a broad understanding of the regulatory framework. More precise developments could be attained for the next deliverable, providing specific attention to the technology that – at that stage – will be developed.

The first norm is the NEN 7510-1, issued in December 2017. It is about Health informatics - Information security management in healthcare - Part 1: Management system. The second norm is the NEN 7510-2, issued in December 2017. Health informatics - Information security management in healthcare - Part 2: Controls.

The objectives and application of both norms aims at guaranteeing availability, integrity, and confidentiality of health data. Confidentiality is intrinsically linked with integrity. Through measures addressing integrity, it is possible to check whether there was unauthorized access. This unauthorized access could have disastrous consequences for the patient, even fatal ones. Availability is even essential, as medical information have to be available when it is the most needed. This norm applies to both healthcare institutions (*zorginstellingen*) and other administrators (*beheerders*) of personal health data. The relations with data security obligations provided by Article 32 of the GDPR are further outlined. If a healthcare institution complies with the four norms (7510-1;7510-2;7512;7513 NEN), it means that it is compliant with Article 32.

In Annex A, of NEN 7510-1, there are 16 objectives regarding security policies. They are hereunder summarized, and further outlined in the NEN 7510-2 norm.

1. Policy on securing information
2. Organization of the information securitization
    a. Internal organization (Defining the responsibilities and Separation of tasks (avoiding conflicts of interests))
    b. Specific attention on mobile applications

[288] TK Memorie van toelichting Cybersecurity NIB Richtlijn 'Vooralsnog wordt niet voorzien dat Nederland zorgaanbieders aanwijst als AED', p 25. <https://www.rijksoverheid.nl/documenten/kamerstukken/2018/02/15/tk-memorie-van-toelichting-cybersecurity-nib-richtlijn>; <https://www.security.nl/posting/568604/Cybersecuritywet+ziet+ziekenhuizen+niet+als+essenti%C3%ABle+dienst>.

[289] NEN 7510 Medische informatica - Informatiebeveiliging in de zorg, D.1 Management systeem, D.2. Beheersmaatregelen; NEN 7512 Medische informatica - Informatiebeveiliging in de zorg - Vertrouwensbasis voor gegevensuitwisseling; NEN 7513 Medische informatica - Logging - Vastleggen van acties op elektronische patiëntdossiers. Available on https://www.nen.nl

[290] See NEN Connect platform at <https://www.nen.nl/Over-NEN/Vrij-beschikbare-normen.htm>.

3. Control on the employees (screening, permanent education)
4. Administration of organization's goods
    a. Identification of these goods
    b. Classification of the goods and the level of protection needed
    c. Policy on external media (encryption on USB keys, etc.)
5. Access control (access rights, responsibility of users, etc.)
6. Encryption
7. Equipment (protection, maintenance, etc.)
8. Operational procedures
9. Protection against malware (Backup, logging, synchronization)
10. Securing of communication systems
11. Acquisition, development, maintenance of IT systems
12. Relations with suppliers (Access to the facilities, monitoring, etc)
13. Management of issues (reporting, etc)
14. Continuity policy (*Bedrijfcontinuïteitsbeheer*)
15. Redundancy (in the light of availability)
16. Compliance

The third norm is the NEN 7512, issued in January 2015. It concerns Health informatics - information security in healthcare - Requirements for trusted exchange of health information. It is dealing with the exchange of data, guarantees and security requirements. NEN 7512 has to be read together with NEN 7510, as NEN 7512 provides for more precision. It is important to notice that the 7512 standards have to be complied with (*moeten*). This should be distinguished with other situation where other standards should be respected (*behoren te*). A reliable and safe exchange of data requires, following the NEN standards, a reliable source, a reliable receiver, and a reliable communication channel. As for the scope, this norm concerns electronic communication in the healthcare sector. This means that communication between healthcare practitioners and healthcare institutions, and with patients or clients, health insurers and third parties in care activities are covered.

In order to exchange data in a secure way, several steps have to be adopted.

1. The parties involved in the communication process have to follow a risk management approach
    a. Classification of the data exchange in light of the three following principles: availability, integrity, confidentiality. For each principle, a risk classification procedure is defined, taking into account the consequences of a breach of the principle, from low (few consequences) to super high (dramatic consequences). These consequences are further explored taking into account the patients, the concerned organizations, or the society.

   b. Classification of the threats, following two approaches: the likelihood the threat occurs, and the associated consequences.
   c. Identification of the vulnerable aspects
   d. Treatment of the risks
2. Management measures
   a. Procedure for data exchange (Exchange agreements; Specific rules for third parties)
   b. Procedure for the execution of the agreements
3. Management and compliance

The fourth norm is the NEN 7513, issued in May 2018. It concerns Health informatics – Recording actions on electronic patient health records. The aim of this norm is to ensure a log of each action when personal health data is processed, which can be accessed by the clients/patients. As a consequence, healthcare institutions are able to show they process health data in a cautious way. This norm is of importance not only for healthcare institutions but also for the other administrators of personal health data. In addition, supervisory authorities (*toezichthouders*), developers of IT systems, and patients, clients, or anyone whose personal health information is processed, are also concerned by the norm. NEN 7513 has to be read together with NEN 7510. The precisions brought by NEN 7513 are related to the security of logs, preventing further modification. The clarifications also relate to the kind of events, the kind of data, the quality of the logging, and the time period of storage. It is important to highlight that NEN 7513 does not apply to event logging concerning paper files.

The norm prescribes that all systems dealing with data related to a patient file must log:

- The kind of event that happened (e.g. creation of a file, access, copying, printing, searching in files)
- Date and time of the event
- The client concerned
- The user concerned and the access point
- The supervisor of the user

Further precisions exist for the patients, healthcare institutions, and supervisory authorities. It has to be pointed out that enabling or disabling the logging procedure has always to be logged. This is a logic consequence of the requirement that logging should give a true picture on the reality. The norm exposes that the healthcare institution, or any other organization processing personal health data is responsible for the logging. This is why someone within the institution has to be appointed as the logging manager. The logging has to be available,[291] but with restricted access, as the information dealt with are sensitive. As for the archiving of logging (*bewaartermijnen*), NEN 7513 prescribes that log data has to be stored between 2 and 15 years. In the case that legal measures would differ from this, these legal measures would prevail. The mentioned period is therefore indicative and subsidiary. Attention is also drawn on the interoperability.

5.2.3. Italy

[291] The norm refers here to art 12 GDPR.

The NIS Directive has been transposed into national legislation with the Legislative Decree No 61/2018, which has been approved by the Italian Council of Ministers on 9 June 2018.[292] The following paragraphs provide a brief outline of its key points.

Identification of operators of essential services

The criteria for the identification of operators of essential services are set in art 4(2) LD 65/2018, which proposes the same criteria as art 4(4) of the NIS Directive does.

Annex II of LD 65/2018 identifies sectors and sub-sectors for the operators of essential services. Concerning the healthcare sector, '**healthcare providers**' (in the meaning of Art. 3(1)(h) of Legislative Decree 38/2014[293]) are **indeed recognised as operators of essential services and thus subject to the obligations** foreseen by the Legislative Decree.

Furthermore, Article 4(1) of the Legislative Decree foresees that NIS competent authorities have to identify and list all the essential operators residing in the national territory. The essential operators providing healthcare assistance in Italy have to be identified by the national Ministry of Health ('*Ministero della Salute'*).

Identification of a national strategy

In accordance with Article 7 of the NIS Directive, LD 65/2018 provides for the **adoption of a national cyber security strategy** by the President of the Council of Ministers.[294] In particular, the strategy should include inter alia the objectives and priorities in the matter of network and IT security, a governance framework in order to achieve these objectives and priorities, the measures for the preparation, response and recovery of services following IT incidents, the definition of risk assessment plan and training and awareness programs on IT security.[295]

A large part of these elements have been already dealt in broad and unspecific terms in the current national cyber security strategy, outlined in the 2013 National Strategic Framework for cybernetic space security ('*Quadro strategico nazionale per la sicurezza dello spazio cibernetico'*) [296] and the 2017 National Cyber Security and Information Security Plan of 2017 ('*Piano nazionale per la protezione cibernetica e la sicurezza informatica*')[297]. However, a further specification of this strategy will be necessary so that all the elements referred to in Article 7 of the NIS Directive are dealt with in a specific and detailed manner, in accordance with the EU provisions.

---

[292] Decreto Legislativo 18 maggio 2018, n. 65 Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione. (18G00092) (GU Serie Generale n.132 del 09-06-2018) (LD 65/2018).

[293] For the sake of completeness is reported the definition thereof. See Decreto Legislativo 4 marzo 2014, n. 38, Attuazione della direttiva 2011/24/UE concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera, nonche' della direttiva 2012/52/UE, comportante misure destinate ad agevolare il riconoscimento delle ricette mediche emesse in un altro stato membro.) (GU n.67 del 21-3-2014, where 'Health care providers' are defined in art 3(1)(h) as 'any natural or legal person or any other entity legally providing health care in the territory of a Member State of the European Union'.

[294] LD 65/2018, art 6.

[295] LD 65/2018, art 6(2).

[296] Presidenza del Consiglio dei Ministri, 'Quadro Strategico Nazionale per la Sicurezza dello Spazio Cibernetico' 2013.

[297] Presidenza del Consiglio dei Ministri, 'Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica', 2017.

Security Measures

LD 65/2018 **reiterates the generic security obligations provided for by the NIS Directive** in Article 14. Notably, operators of essential services will have to adopt technical and organizational measures adequate and proportionate to the management of risks' and prevention of IT incidents.[298] The decree specifies, however, that when adopting these measures operators will have to take into due consideration the guidelines that will be issued by the EU Cooperation Group (as of Article 11 of the NIS Directive). The competent NIS authorities may also impose the adoption of specific security measures.

Duties of Notification

With regard to the **duty of notification** for operators of essential services, the LD 65/2018 specifies that operators of essential services must forward to the **Italian CSIRT** (and for information to the competent NIS authority in their sector) notifications of cyber incidents with a significant impact on the services provided.[299] The decree does not set a strict time limit for the notifications, but specifies that they must be carried out '**without unjustified delay**'.

The decree also provides that the competent NIS authorities can draft guidelines for the notification of incidents.

Competent authority and point of contact

The designation of the **competent authorities** for the implementation of the NIS legislation and the monitoring of compliance with it follows a decentralised institutional model. Five Ministries (ie, Economic development, Infrastructures and Transport, Economy, Health and Environment) have been designated as competent authorities.[300] Each Ministry is responsible for one or more sectors falling within their areas of competence. For the healthcare sector, the competent authority is the '*Ministero della Sanità'*.

The Department of Safety Information ('*Dipartimento delle Informazioni per la Sicurezza'*, DIS) has been appointed as a **single point of contact** in accordance with Article 8(3) of the Directive. DIS is therefore in charge of performing the liaison with the European Union and to coordinate with the competent authorities from other Member States.

Italian CSIRT

The decree also provides for the establishment at the Presidency of the Council of Ministers of a single Computer Security Incident Response Team, known as Italian CSIRT, which will replace the precedent National Computer Emergency Response Teams (CERTs) – formerly operating at the Ministry of Economic Development) and CERT-PA – operating at the Agency for Digital Italy ('*Agenzia per l'Italia Digitale'*, AgID).

Confidentiality

The Legislative Decree also contains references to confidentiality that are worth to report. Notably, Article 1 of LD 65/2018 foresees that:

- The exchange of confidential information between the European Commission and other competent authorities must occur only to the extent that such exchange is necessary for

[298] LD 65/2018, art 12(1).
[299] LD 65/2018, art 12(5).
[300] LD 65/2018, art 7.

the purpose application of the Legislative Decree. The exchange of information must ensure confidentiality and must protect the security and commercial interest of operators of essential services.[301]

- The Legislative Decree applies without prejudice to the measures in order to safeguard the essential functions of the State, in particular of protection of national security, including measures to protect information, in cases where disclosure is held contrary to essential security and maintenance interests public order, in particular for investigation, assessment and prosecution of crimes.[302]

Penalties

According to Article 21 of the Legislative Decree, competent authorities may apply administrative fines of up to 150,000 euros in case of violation by operators of essential services of the obligations under the decree.

[301] LD 65/2018, art 1(5).
[302] LD 65/2018, art 1(6).

6. Ethics

Main findings of Chapter 6

- Moral principles in medical ethics:
  - The assessment of ethical constraints is being led by fundamental moral principles, which are accompanied by secondary principles;
  - The four main fundamental moral principles are i) the principle of respect for persons and autonomy, ii) the principle of justices, iii) the principle of non-maleficence, iv) the principle of beneficence;
  - The secondary principles are namely i) responsibility, ii) dignity, and iii) accountability.
- Ethical constraints addressed through and going beyond the law:
  - The data protection legislation, mainly the GDPR, addresses several issues, which may arise in the SAFECARE project, such as through consent as a prerequisite for autonomous decision-making, or through the principle of accountability embracing the responsible handling of data, etc.
  - Certain aspects are not covered by legislation but need to be considered for ethical reasons, such as the possibility of re-identification through the combination of anonymous data, which may interfere with the concept of autonomy, etc.

The objective of this section is not only to assure compliance with the legal conditions but to ensure that the project is guided by ethical deliberations and values on which the EU is established.[303] This chapter therefore aims to complete the analysis by taking ethical principles into consideration. The chapter will start with a brief introduction and explain in which ways ethics can have an impact in decision-making, and will then examine the fundamental moral principles in the second subsection in order to provide a better understanding of the ethical guidelines to Consortium Partners. Finally, it will be followed by the investigation of sensitive issues analysed and illustration of an overview including ethical constraints in the specific context of SAFECARE.

6.1. The interplay between law and ethics

The legal requirements on data protection and privacy build a framework, which aims to protect natural persons in relation to data processing[304] and shapes the activities of individuals, institutions and third parties. Besides, ethical guidelines, as a system of moral principles, can influence the decision-making process of human beings and their lives too as they can build a basis for the law or provide guidance for the interpretation of the law as a normative resource. Moreover, ethical principles can provide further guidance that is sometimes additional to what

[303] See European Commission, 'Ethics and data protection' (Guidance for H2020, 14 November 2018) 3 <http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-data-protection_en.pdf>.
[304] GDPR, Recital 1 and 2.

the law requires, and help assessing the risks and benefits of tangible forms of harm. In summary, ethical principles can support stakeholders to safeguard human values in form of individual and public interests such as freedom, health, and security, which is why ethical considerations are of ultimate importance in a system of governance as they shape the actions of people and affect the design of technologies by providing standards, operational guidance and imposing constraints.[305]

6.2. Moral principles in medical ethics

For the assessment of ethical constraints, a mixed approach, combining the concept of *Principlism* and supplementary principles, will be used. Beauchamp and Childress[306] have identified four main moral principles which are being considered for ethical decision-making in a health environment, namely: (1) the principle of respect for persons and autonomy, (2) the principle of justice, (3) the principle of non-maleficence, and (4) the principle of beneficence. These principles will form the basis of the approach in SAFECARE. When applying these principles, we contend three additional principles, namely dignity, responsibility and accountability.

6.2.1. Fundamental moral principles

- The *principle of respect for persons and autonomy* protects one's fundamental right to self-determination considering the respect for a person's autonomous choices which includes at least two prerequisites: the first condition concerns liberty, the freedom to make intentional choices without being controlled by external sources or limitations, and secondly, agency, acknowledging one's right to hold opinions and to take action based upon them. The principle for persons and autonomy is two-folded as it includes a positive and a negative obligation. The positive obligation embraces the respectful treatment in disclosing information in order to enhance autonomous decision-making, while the negative obligation states that autonomous actions should not be subject to controlling constraints by others. [307]

- The *principle of justice* is being associated with three notions: *fairness, desert (in the sense 'what is deserved')*, and *entitlement*, which have in common that all three of them relate to what is due or owed to a person based on morally relevant properties or situations. Moreover, it takes into account further principles such as the principle of equality, non-discrimination and property ownership.[308] Particularly in the context of eHealth, the principle of justice protects the party concerned from being stigmatised based on one's socio-economic status or ethnic origin. Thus, individuals can be protected from these threats by ensuring the proper handling of health data and by limiting the data processing to the necessary minimum. Also, in order to respect the principle of ownership and non-discrimination which coincide with the principle of justice, it is necessary to prevent the improper disclosure of one's own data as it might lead to discrimination and cause personal and/or economic harm to the individual. It can also harm and/or reduce opportunities.

[305] G Verhenneman, A Vedder, 'WITDOM "empoWering prIvacy and securiTy in non-trusteD envirOnMents", D6.1 – Legal and Ethical framework and privacy and security principles' (30 June 2015) 7 <http://www.witdom.eu/deliverables>.
[306] TL Beauchamp, JF Childress, *Principles of Biomedical Ethics* (7th edn, Oxford University Press, 2013).
[307] ibid 104-107.
[308] ibid 250.

- The *principle of non-maleficence* underlies the Hippocratic Oath 'Above all [or first] do not harm', historically sworn physicians. It incorporates the obligation not to cause harm to others but also not to impose risks of harm as far as it lies within one's power. Harm can be defined as any action having an adverse effect on another person's interest. Thus, drawbacks towards someone's privacy or liberty can be considered as harmful actions, whether these values were put at risk with or without malicious or harmful intent.[309]
- Whereas it is sufficient for the principle of non-maleficence to refrain from harming others, the *principle of beneficence* requires to contribute to their well-being and to help. This principle deserves attention as an implicit assumption of beneficence exists in the context of medical care.[310] The aim therefore is to maximise potential benefits and to minimise potential harm.

6.2.2. Secondary principles

- A principle deriving from the four main principles is *responsibility*. The responsibility principle states that a person is obliged to fulfil duties that arise from basic moral principles or from a social or professional role.
- A further secondary principle is *the principle of dignity*. It requires respect for human beings as moral and rational agents, who are free and capable of making their own decisions, and who guide their own conduct by reason.[311] However, issues may occur within the interplay of dignity and autonomy, for instance, if the healthcare professional leaves the purportedly self-managing patient with too much responsibility, which may impact on his or her dignity. It may therefore me required to ask if autonomy is in the best interest of the individual concerned and if it has an impact on his or her dignity.[312]
- The *principle of accountability* entails the transparency about the decisions and actions that are being made. It is important that the person responsible is held accountable for complying with the prescribed legal measures and duties. It ensures that stakeholders are able to follow the policymaking process, and builds trust and legitimacy in the process.

6.3. Analysis of the ethical principles

The objective of SAFECARE is to provide solutions that will improve physical and cyber security in a seamless way, and will promote new technologies and approaches to enhance threat prevention, threat detection, incident response and mitigation of impacts while participating in increasing the compliance between security tools and European regulation about ethics and privacy for health services. Even though privacy and data protection is assisted by ethical considerations, law alone will not be able to prevent all morally undesirable consequences from happening. The following section thus aims to raise Consortium Partner's awareness of the occurrence of potential ethical obstacles arising throughout the project, also considering the

[309] ibid 150, 153-154.
[310] ibid 202.
[311] G Verhenneman, A Vedder 'WITDOM "empoWering prIvacy and securiTy in non-trusteD envirOnMents", D6.2 – Legal requirements on privacy, data protection and security in WITDOM scenarios' (30 November 2016) 57 <http://www.witdom.eu/deliverables>.
[312] C Delmar, 'The interplay between autonomy and dignity: summarizing patients voices' (2012) 975-976 Medicine, Health Care and Philosophy, <https://doi.org/10.1007/s11019-012-9416-6>.

progress achieved and information obtained so far in SAFECARE. The next section will therefore introduce ethical constraints that have been addressed in the legal framework which are considering the protection of informational privacy, and follow up with an investigation of ethical constraints going beyond the legal framework.

6.3.1. Ethical constraints considered in the legal framework

'Informational privacy can be defined as an individual's right to determine whether, what, when, by whom and for what purpose personal information is collected, accessed, used or disclosed'[313]. Several legal instruments at various levels aim to guarantee a high level of protection for an individual's privacy and data, and address certain ethical constraints within their framework; to name a few: the Universal Declaration of Human Rights, the Charter of Fundamental Rights of the European Union, the General Data Protection Regulation.

Taking these into account, an issue arising is the increasing possibility of re-identification methods. Nowadays, anonymous data about individuals are being collected in order to achieve complete datasets. Even when using anonymised data, individuals can become identifiable by combining several anonymous datasets from multiple sources. Current legislation however does not cover the protection of anonymised data or data expressed in an aggregated form, which can interfere with the *concept of autonomy*. Therefore, it is necessary to establish a new normative category of data protection reflecting privacy and ethical considerations in order to avoid misuse of an individual's personal data in aggregated form.[314] A key prerequisite for autonomous actions in the context of healthcare and research is *informed consent* as it demonstrates the notion of control over one's data.[315] Hereto, it is necessary to inform the data subject sufficiently in order to enable a free decision-making process. Moreover, due to the increasing possibility of re-identification of data, it may not only be enough to ensure properly obtained consent but to enhance the responsibility of the data controller on how he/she manages the data in order to prevent re-identification.[316]

A protection in a broad sense in terms of *dignity* can be found when expanding international human rights law which is declaring that people should be secure, free and protected. Dignity is indispensable to personal well-being and to the public good and hence addresses different types of personal needs that can enhance a person's self-empowerment through technology. Therefore, the meaningful use of data and treating it as a positive asset can strengthen one's dignity, drives economic opportunity and improves the quality of an individual's life. Nevertheless, treating data as an economic asset may bear the risk to interfere with an individual's *autonomy* as the person concerned does not have control over how the data is being managed. This may not only require

[313] G Verhenneman, A Vedder, 'WITDOM "empoWering prIvacy and securiTy in non-trusteD envirOnMents", D6.1 – Legal and Ethical framework and privacy and security principles' (30 June 2015) 41 <http://www.witdom.eu/deliverables>.
[314] A Vedder, 'Responsibilities for Information on the Internet' in KE Himma, HT Tavani (eds), *The Handbook of Information and Computer Ethics* (John Wiley & Sons 2009) 339-359.
[315] TL Beauchamp, JF Childress, *Principles of Biomedical Ethics* (7th edn, Oxford University Press, 2013) 110.
[316] Executive Office of the President, 'Big Data: Seizing opportunities preserving values' (Policy Report of the White House, 1 May 2014) <https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf>.

informed consent but also the responsible handling of data and *accountability* of the data collector.[317]

As outlined in the first chapter on data protection, the project will involve the processing of personal health data. The European Commission states in its new 'Ethics and Data Protection' guidelines for H2020 that the processing of special categories of data bears the risk to rise ethical issues more likely. This is the case even if the processing concerns anonymised data as 'he origin or acquisition of the data may still raise significant ethics issues.'[318] Therefore, special categories of data must be subject to more stringent data-protection safeguards.[319] Finally, given the fact of interconnectedness of technology systems due to a number of stakeholders who are developing a technology jointly, it may be difficult to assign responsibility to particular stakeholder. With that in mind, *the principle of responsibility* will be effective in terms of building a high level of trust and responsibility regardless of juridical territories if every party, including third parties, remains conscious about his or her duties and responsibilities when collecting (sensitive health) data.[320] Also, considering the responsible handling with data, this could mean to only communicate those kind of incidental findings that might be relevant for the interested subject, and, for the sake of transparency, to inform the individual about the use of his personal data and its consequences.

Data processing operations using camera systems to monitor behaviour or record sensitive information may also entail higher ethical risks according to the European Commission's guidelines as using technologies for surveillance may be vulnerable to misuse, which is why technological and/or organisational solutions may have to be considered.[321] For instance, it must be ensured that unauthorised access to the monitoring system is being prevented. The *principle of non-discrimination* requires that measures safeguarding discriminatory elements gained through data processing should not be implemented and are not factored into prediction.[322] Besides, *informed consent* is a key consideration when it comes to the justification of monitoring, i.e. in terms of video solutions that include human subjects. This is particularly necessary considering that video surveillance enables to recognise faces and/or monitors behaviour.

Even though consent aims to guarantee the notion of control over one's data and expresses the authorisation about the use of one's personal data, the notion of consent can be challenged in the age of big data. Ethical issues may arise if the efficacy of consent is being questioned as the processing of large data sets might undermine the ability of the data subject to actually control

[317] See G Verhenneman, A Vedder 'WITDOM "empoWering prIvacy and securiTy in non-trusteD envirOnMents", D6.2 – Legal requirements on privacy, data protection and security in WITDOM scenarios' (30 November 2016) 9 <http://www.witdom.eu/deliverables>.
[318] European Commission, 'Ethics and data protection' (Guidance for H2020, 14 November 2018) 5 <http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-data-protection_en.pdf>.
[319] ibid 5.
[320] G Verhenneman, A Vedder, 'WITDOM "empoWering prIvacy and securiTy in non-trusteD envirOnMents", D6.1 – Legal and Ethical framework and privacy and security principles' (30 June 2015) 9 <http://www.witdom.eu/deliverables>.
[321] European Commission, 'Ethics and data protection' (Guidance for H2020, 14 November 2018) 6, 15 <http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-data-protection_en.pdf>.
[322] G Verhenneman, A Vedder 'WITDOM "empoWering prIvacy and securiTy in non-trusteD envirOnMents", D6.2 – Legal requirements on privacy, data protection and security in WITDOM scenarios' (30 November 2016) 13 <http://www.witdom.eu/deliverables>.

his or her personal data.[323] It is therefore of ultimate importance to sufficiently inform the data subject about the specific data processing procedures in order to provide real control and clarity to the individual about his or her consent.

6.3.2. Ethical constraints going beyond the law

Besides increasing the level of protection of human rights, ethical principles can provide further guidance to what the law requires. It can help assessing the risks and benefits of tangible forms of harm, such as to health and life, and prevent drawbacks and benefits that may not be quantifiable.

Therefore, protections have to be established in order to ensure that personal data is not disclosed, handled, or used in any other way that may cause material or immaterial damage. The infringement of privacy as a result of public disclosure of information about an individual may cause economic harm or reduce opportunities, especially to the most vulnerable individuals of society. For instance, the public disclosure of information about a person who has been diagnosed with a certain disease may result in the payment of a higher insurance premium or the refusal of coverage, which ultimately may violate *the principle of justice*. Even though data protection and privacy law aims to address these issues, practical ways should be found to prevent harmful disclosure of information by implementing further protections based on categories beyond personal data and enforcing privacy assurance mechanisms. Also, the safeguarding and proper handling of data on the basis of categories (e.g. individuals with physical disability and mental health) can prevent stigmatisation, and hence protect vulnerable groups from becoming victims of injustices. [324]

The rule that technology should be used in a way that benefits mankind and that prevents harm to human beings, other living creatures, the environment and oneself derives from *the principle of non-maleficence*. It can help to scrutinise whether the information obtained will be used in a way which may cause unwarranted harm or adversely affect an individual's safety. Besides, it may provide guidance for ensuring safety of the data (e.g. authenticity and integrity of data) by establishing trusted access control schemas. [325]

The principle of beneficence rules that one should not harm others, and that possible benefits should be maximised whereas possible harms should be minimised. Taking this dogma into consideration, the following can be concluded for its application: '1) Protect and defend the rights of others. 2) Prevent harm from occurring to others. 3) Remove conditions that will cause harm to others. 4) Help persons with disabilities. 5) Rescue persons in danger.'[326] This means in particular that the collection of data should be finalised to an output which eventually evokes potential benefit for the interested subject.

---

[323] E Vayena, A Blasimme, 'Health Research with Big Data: Time for Systemic Oversight' (2018) 46 The Journal of Law, Medicine & Ethics <https://doi.org/10.1177/1073110518766026>.
[324] G Verhenneman, A Vedder, 'WITDOM "empoWering prIvacy and securiTy in non-trusteD envirOnMents", D6.1 – Legal and Ethical framework and privacy and security principles' (30 June 2015) 43 <http://www.witdom.eu/deliverables>.
[325] ibid 44.
[326] ibid 44.

7. Conclusion

The primary objective of the SAFECARE project is to protect health infrastructure, and eventually to protect the health of the patient. It focuses on the development of technologies mainly collecting and processing non-personal data, inter alia in form of technical or incident data. However, the technologies to be developed under the project also include the processing of personal data, in particular health data. The processing of personal data, regardless of the amount of personal data that is being collected, bear the risk to undermine the protection due to the partially unexpected capabilities of fast evolving technologies. This deliverable therefore aimed at addressing upcoming issues while focusing on the protection of personal data as foreseen by the legal framework protecting personal data, in particular sensitive health data.

This deliverable has outlined the legal framework for the protection of personal data, including data protection, privacy, confidentiality, security, as well as the ethical principles as applicable to the SAFECARE project. The deliverable provided an overview of the current EU framework and legislations concerning the aforementioned matters and highlighted specific variances at a national level (particularly in France, the Netherlands and Italy – where SAFECARE field trials will take place). More specifically, an EU level analysis has been carried out in relation to the Privacy and Data Protection framework (including the GDPR and EU case law) and Critical Infrastructure Protection framework (including the ECI Directive and the NIS Directive). A National level analysis provided an insight to national legislations with regard to the processing of health data, medical confidentiality, and national approaches for the protection of critical infrastructure specifically for the health sector as well as the transposition of the NIS Directive in France, the Netherlands and Italy.

The last section provided an analysis with respect to the ethical use of technologies in the healthcare sector in order to foster within the SAFECARE Consortium a reflection on ethics and law with regard to IT practices, the development of technologies and their possible impacts for the patient, the healthcare environment and society as a whole.

This overview provides an insight into the considerations that will be necessary to take into account throughout the execution of the SAFECARE project. This Deliverable will form the basis of the future Deliverable, D3.10 (Implementation of ethics, privacy and confidentiality), which will be delivered in M27.

8. List of European and national legislations/sources

European legislation

- *European Convention on Human Rights:* Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, ETS 5, 4 November 1950.
- *Charter of Fundamental Rights:* European Union, Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02.
- *Data Protection Convention:* Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 108, 28.01.1981.
- *Convention on Human Rights and Biomedicine:* Convention for the protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine, ETS No. 164, 01.12.1999.
- *General Data Protection Regulation (GDPR):* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119, 4 May 2016.
- *ECI Directive:* Council Directive 2008/11/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection [2008] OJ L345/75.
- *NIS Directive:* Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L194/1.
- *Framework Directive:* Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications network and services [2002] OJ L108.
- Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare, OJ L 88, 4.4.2011.

National legislation

France

- Code de la santé publique
- Code de déontologie médicale
- Code civil (French Civil Code)
- Code général des collectivités territoriales
- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
- Ordonnance n° 2004‑1374 du 20 décembre 2004 Code de la Défense
- Loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité
- Décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique

The Netherlands

- Burgerlijk Wetboek (Civil code)
- Wet op de beroepen in de individuele gezondheidszorg (BIG)
- Wet op de geneeskundige behandelingsovereenkomst (WGBO)
- Wet op de lijkbezorging
- Wet marktordening gezondheidszorg
- Dutch Code of Conduct for doctors
- NEN 7510 Medische informatica - Informatiebeveiliging in de zorg, D.1 Management systeem, D.2. Beheersmaatregelen; NEN 7512 Medische informatica - Informatiebeveiliging in de zorg - Vertrouwensbasis voor gegevensuitwisseling; NEN 7513 Medische informatica - Logging - Vastleggen van acties op elektronische patiëntdossiers. Available on <https://www.nen.nl>

Italy

- Decreto del Presidente della Repubblica 5 aprile 1950, n.221
- Decreto Legislativo 10 agosto 2018, n. 101
- Decreto Legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali)
- Decreto Legislativo 18 maggio 2018, n. 65
- Decreto Legislativo 4 marzo 2014, n. 38
- Codice di deontologia medica (CDM)

9. Main references

9.1. Books

Beauchamp TL, Childress JF, *Principles of Biomedical Ethics* (7th edn, Oxford University Press, 2013)

Bygrave LA, *Data privacy law– An international perspective* (Oxford University Press 2014)

Castro-Edwards J, *EU General Data Protection Regulation – A guide to the new law* (The Law Society 2017)

Ergec R, Velu J, *La Convention Européenne des droits de l'homme* (Bruylant 2014)

Feiler L, Forgó N, Weigl M, *The EU General Data protection Regulation (GDPR) : A commentary* (German Law Publishers 2018)

Gonin L, Bigler O, *La Convention européenne des droits de l'homme (CEDH) : commentaire des articles 1 à 18 CEDH* (Stämpfli & LexisNexis 2018)

Grabenwarter C, *European Convention on Human Rights: Commentary* (Bloomsbury Academic 2013)

Jay R e.a. (eds.) *Guide to the General Data protection regulation – A companion to Data Protection Law and Practice* (4th edn Sweet & Maxwell 2017)

Kindt EJ, *Privacy and data protection issues of biometric applications – a comparative legal analysis* (Springer 2013)

Kranenborg HR, Verhey LFM, *De Algemene Verordening Gegevensbescherming in Europees en Nederlands* perspectief (Wolters Kluwer 2018)

Laude A, Mathieu B, Tabuteau D, *Droit de la santé* (3rd edn PUF 2012)

Leenen HJJ, e.a., *Handboek gezondheidsrecht* (6th edn Boom 2014)

Moquet-Anger M-L, *Droit Hospitalier* (5th edn LGDJ 2018)

Nouwt J, *Zorg voor privacy – Informatietechnologie en informationele privacy in de gezondheidszorg* (SDU 1997)

Rainey B, Wicks E, Ovey C, *The European Convention on Human Rights* – (7th edn OUP 2017)

Schabas WA, *The European Convention on Human Rights – A commentary* (Oxford University Press 2015)

Tamò-Larrieux A, *Designing for Privacy and its Legal Framework – Data protection by design and default for the internet of things* (Springer 2018)

Vasiliki K, *Fundamental Rights in EU Internal Market Legislation* (Hart 2015)

Voigt P, von dem Bussche A, *The EU General Data protection regulation (GDPR) – A practical Guide* (Springer 2017)

Welsch S, *Responsabilité du médecin – Risques et réalités judiciaires* (Litec 2000)

9.2. Articles and book contributions

Delmar C, 'The interplay between autonomy and dignity: summarizing patients voices' (2012) 975-976 Medicine, Health Care and Philosophy

Dunn M, 'Understanding Critical Information Infrastructures' in Dunn M and Mauer V (eds) *International CIIP Handbook 2006 vol II* (Center for Security Studies at ETH Zurich 2006)

Duijst WLJM, Morsink MEB, 'Het medische beroepsgeheim: Heilige huisjes en juridische fictie' (2017) 2 Tijdschrift voor Bijzonder Strafrecht & Handhaving

Gibar R, 'Medical Confidentiality and Communication with the Patient's Family: Legal and Practical Perspectives' (2012) 24 (2) Child and Family Law Quarterly

Kokott J, Sobotta C, 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR' (2013) 3 (4) International Data Privacy Law

Kranenborg H, 'Protection of Personal Data', in Peers S, Hervey T, Kenner J and Ward A (eds.), *The EU Charter of Fundamental Rights: A Commentary* (Hart 2014)

Luiijf E, Burger H, Klaver M, 'Critical Infrastructure Protection in the Netherlands: A quick-scan', in Gattiker UE (ed), *EICAR Best Paper Conference Proceedings,* (EICAR 2003)

Ohm P, 'Broken Promises Of Privacy: Responding To The Surprising Failure Of Anonymization'(2010) 57 (6) UCLA Law Review

Rinaldi SM, Peerenboom JP, and Kelly TK, 'Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies' [2001] 11 IEEE Control Systems Magazine.

Seatzu F, Fanni S, 'The Experience of the European Court of Human Rights with the European Convention on Human Rights and Biomedicine' (2015) 31 Utrecht J. Int'l & Eur. L.

Sokalska ME, 'Medical Confidentiality – Quo Vadis ?' (2004) 11 European Journal of Health Law

Spindler G, Schmechel P, Personal Data and Encryption in the European General Data Protection Regulation, (2016) 7 J. Intell. Prop. Info. Tech. & Elec. Com. L.

Stalla-Bourdillon S, Knight A, 'Anonymous Data v. Personal Data - False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data' (2016) 34 Wis. Int'l L.J.

Taylor MJ, 'Legal bases for disclosing confidential patient information for public health: distinguishing between health protection and health improvement' (2015) 23 (3) Medical Law Review

Vayena E, Blasimme A, 'Health Research with Big Data: Time for systemic oversight' (2018) 46 The Journal of Law, Medicine & Ethics

Vedder A, 'Privacy and confidentiality. Medical Data, New information technologies, and the need for normative principles other than privacy rules', in Freeman M, Lewis A (eds.), *Law and Medicine: Current Legal Issues Volume 3* (Oxford University Press 2000)

Vedder A, 'Responsibilities for Information on the Internet' in Himma KE, Tavani HT (eds), *The Handbook of Information and Computer Ethics* (John Wiley & Sons 2009)

Wachter S, 'The GDPR and the Internet of Things: a three-step transparency model' (2018) 10(2) Law, Innovation and Technology

Zarsky TZ, 'Incompatible: The GDPR in the Age of Big Data' (2017) 47 Seton Hall L. Rev.

9.3. Additional documents

Verhenneman G, Vedder A, 'WITDOM "empoWering prIvacy and securiTy in non-trusteD envirOnMents", D6.1 – Legal and Ethical framework and privacy and security principles' (30 June 2015)

Biasin E, Kamenjasevic E, 'Deliverable 6.1 – Legal and ethical inventory and in-depth analysis in the Made4You project, EU H2020 grant agreement No. 780298